



FACULTAD DE POSGRADOS

DISEÑO DE UN PROGRAMA DE GESTION DE
SEGURIDAD DE LA INFORMACION PARA UNA
EMPRESA DEL SECTOR INDUSTRIAL

Autor

Diego David Guzmán Calderón

Año

2021



FACULTAD DE POSGRADOS

DISEÑO DE UN PROGRAMA DE GESTION DE SEGURIDAD DE LA
INFORMACION PARA UNA EMPRESA DEL SECTOR INDUSTRIAL

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

Autor

Diego David Guzmán Calderón

Año

2021

AGRADECIMIENTOS

Agradezco a toda mi familia, compañeros, profesores y amigas que me apoyaron en el camino de esta maestría

DEDICATORIA

Para todas las personas que siempre estuvieron a mi lado en cada momento difícil y brindándome su apoyo incondicional-

RESUMEN

El presente trabajo consiste en realizar el diseño de un programa de gestión de seguridad e información SGSI, para una organización que brinda servicios de diseño, construcción y puesta en marcha de sistemas eléctricos de control, monitoreo e información, a empresas del sector industrial, energético y petrolero del país.

Este programa se concentra en establecer un modelo de gobierno y gestión de la seguridad de la información, que sea adecuado a los objetivos, metas, visión, misión y líneas de negocio de la organización. Esto siempre alineado al riesgo al que se encuentra expuesta la organización y su apetito frente a un incidente o evento de seguridad.

El programa de SGSI está diseñado en base a dos marcos de referencia que ayudan a evaluar, gestionar, controlar y mejorar la gestión de la información. Estos marcos de referencia son COBIT 2019 y la NIST. Estos dos son ampliamente conocidos a nivel global por su historia y mejora continua según los cambios repentinos en el mercado a nivel global.

Como puntapié del presente programa, se evalúa el estado de la gestión de la seguridad de la información de la organización, para identificar el nivel de fortaleza de la empresa. Posterior a esto, se evalúa el riesgo de la organización y sus activos físicos y lógicos con respecto a la Integridad, Confidencialidad, Disponibilidad y Privacidad de sus activos de información.

Una vez realizado el análisis de riesgos que puede tomar la organización, se obtiene su activo más crítico sobre el cual, se evalúa las amenazas y vulnerabilidades, para posterior implementar controles que mejoren el SGSI. Con estos controles, el SGSI se retroalimenta por sí mismo, y en base a los marcos de referencia anteriormente comentados, se implementan nuevos controles que día a día permiten a la organización mejorar su gestión de la información.

ABSTRACT

This project consists of designing an ISMS information and security management program for an organization that provides design, construction and commissioning services for electrical control, monitoring and information systems to companies in the industrial sector. energy and oil of the country.

This program focuses on establishing an information security governance and management model that is appropriate to the organization's objectives, goals, vision, mission, and lines of business. This is always aligned with the risk to which the organization is exposed and its appetite in the face of an incident or security event.

The ISMS program is designed based on two reference frameworks that help evaluate, manage, control and improve information management. These frameworks are COBIT 2019 and NIST. These two are widely known globally for their history and continuous improvement based on sudden changes in the global market.

As a kick-off of this program, the state of the organization's information security management is evaluated, to identify the level of strength of the company. After this, the risk of the organization and its physical and logical assets is evaluated with respect to the Integrity, Confidentiality, Availability and Privacy of its information assets.

Once the risk analysis that the organization can take has been carried out, its most critical asset is obtained, on which threats and vulnerabilities are evaluated, to later implement controls that improve the ISMS. With these controls, the ISMS provides feedback on its own, and based on the aforementioned reference frameworks, new controls are implemented that day by day allow the organization to improve its information management.

ÍNDICE

INTRODUCCIÓN	2
DESARROLLO DEL PROYECTO DE TITULACIÓN	4
1. Caso de Negocio.....	4
1.1 Introducción	4
1.2 Presupuesto	5
1.3 Alcance.....	5
2. Modelo Operación y Métricas de los procesos	6
2.1 Modelo Operacional.....	6
2.2 Métricas de los procesos	11
3. Diagnóstico del SGSI	13
4. Apetito al riesgo de la organización	14
5. Clasificación de Información e Inventario de activos	16
6. Evaluación del riesgo del activo crítico	20
7. Planes de acción para el activo crítico	30
8. Políticas de alto nivel.....	33
9. Planes de acción del SGSI	36
CONCLUSIONES Y RECOMENDACIONES.....	39
Conclusiones	39
Recomendaciones	39
REFERENCIAS.....	40

ANEXOS	41
--------------	----

ÍNDICE DE TABLAS

Tabla 1 Presupuesto inicial SGSI.....	5
Tabla 2 Diagnóstico actual SGSI.....	13
Tabla 3 Identificación del riesgo para los tipos de información	18
Tabla 4 Identificación del activo de información y evaluación	19
Tabla 5 Calificación de los componentes del activo de información “Workflow”	20
Tabla 6 Mejoras esperadas en el SGSI.....	38

ÍNDICE DE FIGURAS

Figura 1. Cronograma de los principales ataques a ICS. (Security, 2018).....	2
Figura 2. Los 15 países y territorios principales clasificados por porcentaje de equipos ICS en los que se bloquearon objetos maliciosos. H2 2020 (CERT, 2021)	3
Figura 3. Macro procesos del SGSI	7
Figura 4. Ejemplo del diagnóstico del SGSI.	12
Figura 5. Roles y responsabilidades de la organización en el SGSI.	36

INTRODUCCIÓN

El sector industrial y sus sistemas de control se han visto fuertemente vulnerables a incidentes de seguridad en los últimos años. Desde el año 2009, la ITS Security ha recopilado los principales ciber ataques (Figura 1) registrados en el sector industrial y que han afectado fuertemente a este sector.

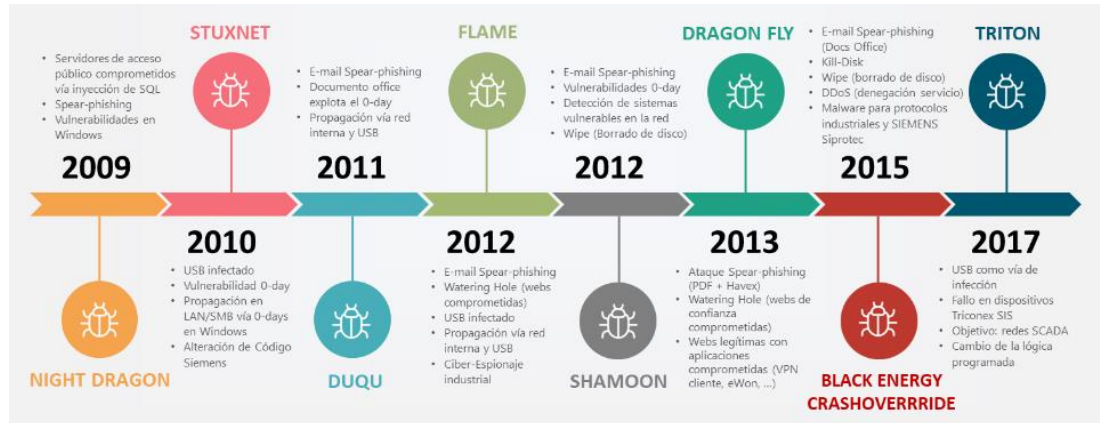


Figura 1. Cronograma de los principales ataques a ICS. (Security, 2018)

A pesar que el sector industrial tiene fuertes controles de su operación, la llegada de la llamada “Industria 4.0” y las tecnologías inteligentes, han abierto una brecha gigante de seguridad, tanto es así que la empresa estadounidense Claroty en uno de sus informes detalla que “Durante el primer semestre de 2021, se publicaron 637 vulnerabilidades de ICS (Sistemas de Control Industrial), que afectaron a los productos vendidos por 76 proveedores. El 70,93% de las vulnerabilidades se clasifican como altas o críticas, aproximadamente a la par con el segundo semestre de 2020” (Fradkin, 2021).

En relación de eventos e incidentes maliciosos de seguridad en el Ecuador, la empresa Kaspersky en su publicación “Threat landscape for industrial automation systems. Statistics for H2 2020”, coloca al país en el top 15 de los países que han recibido el mayor número de eventos de seguridad en equipos ICS, y el porcentaje de eventos que han logrado ser bloqueados.

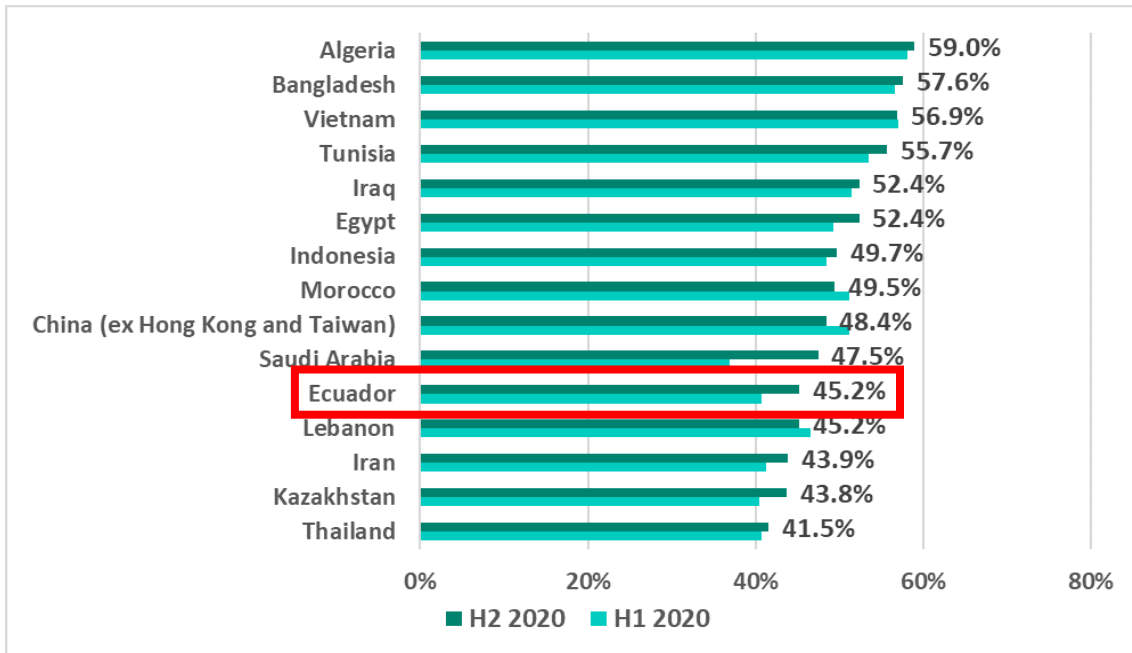


Figura 2. Los 15 países y territorios principales clasificados por porcentaje de equipos ICS en los que se bloquearon objetos maliciosos. H2 2020 (CERT, 2021)

Tomando en cuenta estos antecedentes, es importante gestionar y gobernar la seguridad de la información de manera efectiva, en todos quienes son parte de este sector, es por ello que el presente proyecto, se enfoca diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para un proveedor de este sector, logrando crear valor hacia sus clientes y asegurando sus servicios y operaciones ante un evento o incidente de seguridad de la información.

DESARROLLO DEL PROYECTO DE TITULACIÓN

1. Caso de Negocio

1.1 Introducción

La organización para la que se diseña el presente SGSI, tiene entre sus principales servicios el diseño, construcción y puesta en marcha de sistemas eléctricos de control, monitoreo e información para empresas del sector industrial.

El principal objetivo frente a sus clientes, es prestar el servicio adecuado y oportuno, atendiendo de manera inmediata todos los requerimientos y problemas que puedan surgir en el transcurso de nuestra asesoría y ejecución.

En este contexto, una brecha de seguridad de la información en esta organización, puede afectar organizacionalmente a:

- Posibles pérdidas financieras
- Reducción de productividad
- Daños a la reputación de la organización
- Pérdida de oportunidad y competitividad en mercado
- Penalizaciones económicas por incumplimiento de legislación vigente (RGPD)
- Compromiso con el cliente

Tomando en cuenta las afectaciones detalladas, el SGSI debe estar alineadas a gestionar y brindar mayor valor a estas, por lo que los beneficios del presente programa son:

- Aprendizaje continuo: Buscar, aprender y transmitir nuevos conocimientos y experiencias para usarlas en el perfeccionamiento de los servicios.
- Compromiso: Decidir actuar responsablemente enfocándose en el éxito de las iniciativas y servicios entregados por la organización.
- Excelencia: Conseguir el mejor resultado buscando el mejor camino.

- Integridad: Honradez, sinceridad, justicia en todas las acciones de la organización.
- Vocación de servicios: Atender con actitud positiva, espontánea, proactiva y con esfuerzo, los requerimientos de los clientes.

1.2 Presupuesto

A continuación, se detalla el presupuesto inicial que el SGSI necesita para poder dar sus primeros pasos en la organización.

Tabla 1 Presupuesto inicial SGSI

Factor	Descripción	Costos
Documentación	Todos los documentos para análisis de impactos en el negocio, evaluación y tratamiento de riesgos, gobierno y gestión, check list de certificación de normativas, etc.	\$2,500 dólares
Formación o Capacitación	Dentro de una empresa o una organización, si todos los empleados tuvieran conocimiento y conciencia de los problemas de ciberseguridad reales existentes en la actualidad y su repercusión, es muy probable que no se produjeran la mayor parte de los incidentes en las empresas.	\$600 dólares semestralmente
Ayuda Externa	Un consultor externo nos va a guiar para que nuestro equipo se centre en aquellas actividades y debilidades que debemos subsanar, y a que no nos perdamos en tareas que puedan incluso dar lugar a costes mayores.	\$3,000 dólares
Tecnología	La inversión en tecnología, nos ayudará a alcanzar los objetivos del SGSI y reducirá a su vez costes que se generan cuando el proceso de gestiona de forma tradicional.	\$20,000 dólares
Tiempo	El tiempo que nuestros empleados dediquen a la implementación se va a ver afectado por la madurez del sistema actual.	Aproximadamente 8 meses

1.3 Alcance

El alcance del presente programa de SGSI se divide en 5 fases:

- Fase 1: Diagnostico

- Evaluación del estado actual de la organización en el manejo de seguridad de la información según Cobit 2019 y NIST.
- Fase 2: Clasificación de la información
 - Evaluación de los datos que la organización posee y el nivel de protección que cada uno requiere.
- Fase 3: Inventario de activos de información
 - Identificar claramente cada uno de los activos que la tiene la organización y su correcta organización.
- Fase 4: Evaluación de Riesgos (Análisis de amenazas y vulnerabilidades)
 - Determinar el nivel de exposición y la predisposición a la pérdida de un activo de la organización ante una amenaza.
- Fase 5: Documentación y entrega del diseño SGSI
 - Recopilación de información y presentación de un SGSI ajustado a las prioridades de la organización.

2. Modelo Operación y Métricas de los procesos

2.1 Modelo Operacional

Para poner en puesta en marcha el diseño del programa SGSI, lo primero es analizar los objetivos de la organización para poder alinearlos con un marco de referencia que se adapte a los mismos, para ello iniciamos con:

1. La priorización del alcance: se identifica los objetivos, misión, visión y prioridades en alto nivel de la organización, para evaluar la mejor estrategia de ciberseguridad.
2. Orientación del SGSI: se analiza y determina el objetivo del SGSI según el marco de referencia que mejor se adapte al alcance de la organización.
3. Diagnostico actual: se levanta una evaluación inicial del estado de la organización en temas de ciberseguridad.
4. Evaluación de riesgos: se evalúa el entorno operativo para discernir la probabilidad de un evento de ciberseguridad y el impacto que el evento

podría tener en la organización y los activos que pueden ser críticos para su operación

5. Objetivos de mejora: se plantea los resultados deseados de la implementación del SGS, según los resultados iniciales y la evaluación de riesgo.
6. Plan de acción: una vez concluido los pasos anteriores, se tomarán planes de acciones para dar constante cumplimiento a los objetivos de mejora planteados.

Para apoyar cada uno de los pasos comentados, es importante poder distribuir el SGSI en varias fases. Estas fases tendrán un objetivo específico, que permitirán conocer el estado de la organización y sus planes de acción para mejorarlos.

Para la operación del SGSI se ha determinado trabajar en los siguientes 5 macro procesos:



Figura 3. Macro procesos del SGSI

- **Identificación**

La organización desarrollara la comprensión organizacional para administrar el riesgo de ciberseguridad para sus sistemas, activos, datos y capacidades, en función de la identificación, evaluación, implementación y monitoreo de las siguientes categorías:

- Gestión de activos: todos los datos, el personal, los dispositivos, los sistemas y las instalaciones que tiene la organización
- Entorno empresarial: la misión, los objetivos, las partes interesadas y las actividades de la organización
- Gobernanza: políticas, procedimientos y procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización
- Evaluación de riesgos: riesgo de las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.
- Estrategia de gestión de riesgos: estrategia para responder a las prioridades, las limitaciones, las tolerancias de riesgo y los supuestos de la organización
- Gestión de riesgos de la cadena de suministro: la gestión para responder a las prioridades, las limitaciones, las tolerancias de riesgo y los supuestos de la organización

- **Protección**

La organización implementará las salvaguardas apropiadas para garantizar la entrega de sus servicios, en función de la identificación, evaluación, implementación y monitoreo de las siguientes categorías:

- Gestión de identidad, autenticación y control de acceso: acceso a los activos físicos y lógicos y las instalaciones, limitado a usuarios, procesos y dispositivos autorizados.

- Concientización y capacitación: nivel de toda la organización en cuanto a la concientización de la ciberseguridad de acuerdo con las políticas, procedimientos y acuerdos relacionados
- Seguridad de los datos: información y los registros (datos) que se gestionan.
- Procesos y procedimientos de protección de la información: políticas de seguridad, los procesos y los procedimientos para gestionar la protección de los sistemas y activos de información
- Mantenimiento: nivel de la organización en cuanto al mantenimiento y las reparaciones de los componentes del sistema de información.
- Tecnología de protección: soluciones de seguridad técnica para garantizar la seguridad y la resistencia de los sistemas y activos.

- **Detección**

El SGSI determinará las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad, en función de la identificación, evaluación, implementación y monitoreo de las siguientes categorías:

- Anomalías y Eventos: actividad anómala y se comprende el impacto potencial de los eventos.
- Monitorización continua de seguridad: sistema de información y los activos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.
- Procesos de detección: procesos y procedimientos de detección para garantizar el conocimiento de eventos anómalos

- **Respuesta**

Se analiza el nivel de la organización para tomar medidas con respecto a un evento de ciberseguridad detectado, en función de la identificación, evaluación, implementación y monitoreo de las siguientes categorías:

- Planificación de respuesta: procesos y procedimientos de respuesta que se ejecutan y mantienen para garantizar la respuesta a los incidentes de ciberseguridad detectados
- Comunicaciones: actividades de respuesta coordinadas con las partes interesadas internas y externas
- Análisis: garantizar una respuesta eficaz y respaldar las actividades de recuperación.
- Mitigación: nivel de la organización para realizar las actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.
- Mejoras: nivel para entender, analizar y ejecutar lecciones aprendidas de las actividades de detección / respuesta actuales y anteriores.

- **Recuperación**

Se evalúa el nivel de la organización y sus planes de resiliencia y restauración de las capacidades o servicios que se vieron afectados debido a un evento de ciberseguridad, en función de la identificación, evaluación, implementación y monitoreo de las siguientes categorías:

- Planificación de recuperación: procesos y procedimientos de recuperación que se ejecutan y mantienen para garantizar la restauración de sistemas o activos afectados por incidentes de ciberseguridad.
- Mejoras: mejora de la planificación y los procesos de recuperación incorporando las lecciones aprendidas
- Comunicaciones: actividades de restauración que se coordinan con partes internas y externas

2.2 Métricas de los procesos

Para dar una facilidad de medición al SGSI, se evaluará cada uno de los procesos y sus categorías, mencionadas en el modelo operacional, para aterrizarlas en un sistema de gobierno y gestión (COBIT 2019), que permite nivelar la capacidad de la organización para cumplir con sus objetivos de mejora según cada proceso.

Estos niveles de capacidad responden a la siguiente escala en base a la seguridad de la información:

- Nivel 2
 - El proceso logra su propósito mediante la aplicación de un conjunto básico de actividades o procesos.
- Nivel 3
 - El proceso logra su propósito de una manera mucho más organizada utilizando activos organizacionales.
- Nivel 4
 - El proceso logra su propósito, está bien definido y su desempeño se mide (cuantitativamente).
- Nivel 5
 - El proceso logra su propósito, está bien definido, su desempeño se mide para mejorar el desempeño y se persigue la mejora continua. (ISACA, 2020)

Gracias a que el marco de referencia (NIST) usado para el presente SGSI, permite adaptarse fácilmente a otros marcos de referencia, se cotejan actividades de seguridad de la información y sus niveles de capacidad (COBIT 2019), con cada proceso y las categorías comentadas en el modelo operacional. Esto permite la parametrización y métrica de cada proceso, evaluando el nivel de implementación que tiene la organización y posterior porcentaje de cumplimiento de su capacidad, como se puede observar a continuación:

Categoría	Subcategoría	Referencias Informativas COBIT 2019 IS	Actividades específicas de seguridad de la información	Nivel de capacidad	Porcentaje de implementación	Cumplimiento de capacidad
Gestión de activos (ID.AM): los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	ID.AM-1: Se inventarian los dispositivos y sistemas físicos dentro de la organización.	BAI09.01 Identificar y registrar activos corrientes	Visualice y documente los activos de I&T de la empresa para incluir el flujo de datos.	2	60%	58%
			Identificar los requisitos de seguridad de la información para los activos corrientes.		55%	
			Abordar la seguridad de la información para activos, datos y formularios de I&T, etc.	3	65%	53%
		Verifique que un inventario de activos completo y preciso informa la implementación de los procesos de seguridad (administración de parches, administración de vulnerabilidades, etc.).	40%			
		BAI09.02 Gestionar activos críticos	Defina los niveles de criticidad e identifique la criticidad de los activos en un registro de activos.	2	40%	40%
			Hacer cumplir los requisitos de seguridad de la información en los activos.	3	45%	50%
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.	55%					
Asegúrese de que la clasificación de seguridad de los datos esté incorporada en el inventario de activos.	4	35%	35%			

Figura 4. Ejemplo del diagnóstico del SGSI.

Se detalla cada uno de los campos presentados en el gráfico:

- Categoría: procesos de evaluación correspondiente a cada macro proceso del marco de referencia NIST.
- Subcategoría: detalla los diferentes sub procesos internos para cada categoría
- Referencia informativa COBIT 2019: dominio del marco de referencia COBIT que aplicada a cada subcategoría de la NIST
- Actividades de seguridad de la información: actividades con las que se evalúa cada dominio.
- Nivel de capacidad: nivel de correspondencia para cada actividad.
- Porcentaje de implementación: evalúa el estado de implementación para cada actividad.
- Cumplimiento de la capacidad: calcula la capacidad de la organización para completar el nivel de capacidad según las actividades correspondientes.

De esta manera, se puede evidenciar de manera rápida, que planes de acción debe tomar la organización para mejorar su capacidad de respuesta en seguridad de la información, además de plantear los objetivos de cumplimiento a futuro por cada proceso del SGSI.

Los planes de acción se plantearán según el nivel de capacidad en el que se encuentra la organización y su mejora continua a lo largo del SGSI.

3. Diagnóstico del SGSI

Tal como se ha indicado en el presente documento, el diagnóstico del estado actual, se lo realiza en base a los marcos de referencia Cobit 2019 y NIST, en donde se obtiene el siguiente resultado inicial.

Tabla 2 Diagnóstico actual SGSI

IDENTIFICACION	
Actual Total	12%
Observación	Actualmente solo existe con una básica identificación e inventario de activos, que se archivan en un software diseñado especialmente para la organización. Adicional esta identificación e inventario no se encuentra actualizado con la realidad actual de la organización. No cuenta con ningún plan o estrategia de identificación de riesgo de los activos, cadena de suministro, gobernanza de activos que pueden afectar en su entorno organizacional
PROTECCION	
Actual Total	12%
Observación	Existe una protección básica para el control de accesos y asignación de credenciales para cada uno de sus activos. No se tiene una evaluación del riesgo que puede ocasionar una falla de seguridad en los datos ni estrategia para responder a ellas. No se concientiza ni capacita a toda la organización sobre buenas prácticas de seguridad de la información, solo quien administra los accesos conoce sobre la importancia de proteger la información. No existe procesos o procedimientos que se centren en la protección de los datos de la organización. No existen registros ni controles en los mantenimientos de los activos, más que un registro de las actividades que se registran.
DETECCION	
Actual Total	6%
Observación	No existen gestión ni controles para detectar anomalías o incidentes de seguridad, más que una básica gestión de la red y su conectividad.
RESPUESTA	
Objetivo	15%
Observación	No existen procedimientos ni estrategias para responder ante incidentes de seguridad
RECUPERACIÓN	
Objetivo	15%
Observación	No existen procedimientos ni estrategias para recuperar a la organización ante incidentes de seguridad

Como se puede evidenciar, actualmente la empresa es altamente vulnerable a un problema de seguridad de la información, por lo que se vuelve más importante aún iniciar cuanto antes el diseño del programa SGSI.

4. Apetito al riesgo de la organización

Para iniciar con la clasificación de la información de la organización y la evaluación de sus activos, es necesario antes conocer el riesgo que está dispuesto a correr la organización frente a un incidente de seguridad y que este afecte a sus servicios frente a sus clientes.

A continuación, se detalla los principales pilares y objetivos de la organización frente a sus clientes y su modulador de apetito al riesgo.

- Servicio técnico de baja calidad y deficiente.
 - Modulador del apetito: Aversión
 - Criterio: El compromiso de la organización es prestar un servicio técnicamente excelente que será aplicado de manera consistente.
- Respuesta tardía a requerimientos y problemas de los clientes.
 - Modulador del apetito: Aversión
 - Criterio: El plan organizacional de la empresa se centra en atender de manera inmediata todos los requerimientos y problemas que puedan surgir en el transcurso de la asesoría y ejecución.
- Baja reputación empresarial.
 - Modulador del apetito: Aversión
 - Criterio: La visión de la empresa es ser reconocida por todos los clientes como una empresa que entrega soluciones tecnológicas óptimas de manera eficiente.
- Talento humano deficiente
 - Modulador del apetito: Neutral
 - Criterio: La misión de la organización es desarrollar talento humano para proveer soluciones tecnológicas e innovadoras con el fin de mejorar la calidad, eficiencia y productividad del sector empresarial.

Determinado el modulador de apetito para cada pilar y objetivo de la organización, se procede a evaluar los niveles de riesgo a los cuales la organización está dispuesta a llegar.

- Servicio técnico de baja calidad y deficiente.
 - Riesgo insignificante: No aplica para la organización.
 - Riesgo menor: No aplica para la organización.
 - Riesgo moderado: No aplica para la organización.
 - Riesgo mayor: Servicio técnico con capacidad técnica básica y comparable con el mercado.
 - Riesgo catastrófico: Servicio técnico sin capacidad técnica consistente.
- Respuesta tardía a requerimientos y problemas de los clientes.
 - Riesgo insignificante: No aplica para la organización.
 - Riesgo menor: No aplica para la organización.
 - Riesgo moderado: Se brindó respuesta al cliente en menos de 1 hora.
 - Riesgo mayor: Se brindó respuesta al cliente entre 1 hora a 2 horas
 - Riesgo catastrófico: Se brindó respuesta al cliente en más de 2 horas.
- Baja reputación empresarial.
 - Riesgo insignificante: No aplica para la organización.
 - Riesgo menor: No aplica para la organización.
 - Riesgo moderado: No aplica para la organización.
 - Riesgo mayor: Ser una organización con soluciones básicas y sin ofertas de valor para los clientes.
 - Riesgo catastrófico: Ser una organización con soluciones sobre dimensionadas y de alta complejidad.
- Talento humano deficiente
 - Riesgo insignificante: No aplica para la organización.
 - Riesgo menor: No aplica para la organización.
 - Riesgo moderado: No aplica para la organización.
 - Riesgo mayor: Talento humano con capacidad productiva, pero sin compromiso organizacional.
 - Riesgo catastrófico: Talento humano sin productividad, eficiencia, calidad y sin compromiso con la organización.

5. Clasificación de Información e Inventario de activos

Una vez determinado el riesgo al que es capaz de afrontar la organización, es momento de clasificar su información para lo cual la principal información que maneja la organización es la siguiente.

- Clientes
 - Datos principales: Engloba la información básica del cliente o empresa cliente como: Nombres, RUC, C.I., teléfonos, correos, personas de contacto, redes sociales, apoderados legales, nóminas de socios y accionistas etc.
 - Información Financiera: Se detalla la información del estado del buró de crédito, pago de impuestos, índices financieros del cliente o empresa cliente, facturación.
 - Información Bancaria: Se detalla las cuentas de banco, estados de cuentas, tarjetas de crédito, pólizas del cliente o empresa cliente.
 - Servicios: Se define como los servicios o productos que la organización presta al cliente o empresa cliente.
 - Core del negocio: Se define como el mercado en el que se mueve el cliente o empresa cliente.
 - Infraestructura tecnológica: Componentes de hardware y software habituales: instalaciones, centros de datos, servidores, sistemas de escritorio de hardware de red y soluciones de software del cliente o empresa cliente.
 - Ubicación: Ubicación geográfica de la organización, tanto casa matriz como sus sucursales del cliente o empresa cliente.
 - Protocolos de seguridad y salud: Se define como normas, parámetros o reglas que define el cliente para ingresar u operar en las instalaciones del cliente o empresa cliente.
- Empleados
 - Información Personal: Engloba la información básica de los empleados como: Nombres, C.I., teléfonos, correos, personas de

contacto, redes sociales, familiares, etc. de los empleados de la organización.

- Información Bancaria: Se detalla las cuentas de banco, estados de cuentas, tarjetas de crédito de los empleados de la organización.
- Información de Salud: El estado de completo bienestar físico, mental y social de los empleados de la organización.
- Formación académica: Engloba el nivel académico, cursos, certificaciones, idiomas extranjeros, entidades educativas de los empleados de la organización.
- Experiencia laboral: Información del recorrido laboral, certificados de trabajo, aportaciones al IESS de los empleados de la organización.
- Organización
 - Proyectos: Información de los proyectos que la organización tiene como responsabilidad de entregar a sus clientes.
 - Equipo tecnológico: Información de los equipos tecnológicos (PC's, servidores, celulares, etc) de cada uno de los empleados de la organización.
 - Partners: Información de los convenios entre la organización y marcas de equipos que se ofrecen como parte del portafolio de productos y servicios.
 - Estrategia Empresarial y de Negocio: Información de la planeación para mejorar y optimizar los resultados, conjunto de actividades que permitirán que la empresa alcance una ventaja competitiva.
 - Portafolio de productos y servicios: Información de los productos, servicios, capacitaciones, cursos marcas, etc. Que se ofrece a cada uno de los clientes.

Una vez definido el tipo de información que manipula la organización, se procede a evaluarla con respecto a 4 pilares fundamentales: privacidad, confidencialidad, disponibilidad e integridad. Estos pilares van muy de la mano al apetito al riesgo evaluado en el apartado anterior, como resultado se obtiene.

Tabla 3 Identificación del riesgo para los tipos de información

Entidad	Nombre del tipo de información	Impacto Privacidad	Impacto Disponibilidad	Impacto Integridad	Impacto Confidencialidad
Cliente	Datos principales	Insignificante	Insignificante	Insignificante	Insignificante
Cliente	Información Financiera	Catastrófico	Mayor	Mayor	Catastrófico
Cliente	Información Bancaria	Catastrófico	Mayor	Mayor	Catastrófico
Cliente	Servicios	Catastrófico	Catastrófico	Catastrófico	Catastrófico
Cliente	Core del negocio	Mayor	Mayor	Mayor	Catastrófico
Cliente	Infraestructura tecnológica	Catastrófico	Catastrófico	Catastrófico	Catastrófico
Cliente	Ubicación	Insignificante	Insignificante	Insignificante	Insignificante
Cliente	Protocolos de seguridad y salud	Menor	Moderado	Catastrófico	Moderado
Empleados	Información Personal	Menor	Menor	Menor	Menor
Empleados	Información Bancaria	Catastrófico	Mayor	Mayor	Catastrófico
Empleados	Información de Salud	Catastrófico	Menor	Mayor	Catastrófico
Empleados	Formación académica	Insignificante	Insignificante	Mayor	Insignificante
Empleados	Experiencia laboral	Menor	Menor	Mayor	Menor
Organización	Proyectos	Catastrófico	Mayor	Catastrófico	Catastrófico
Organización	Equipo tecnológico	Catastrófico	Catastrófico	Catastrófico	Mayor
Organización	Partners	Catastrófico	Menor	Moderado	Moderado
Organización	Estrategia Empresarial y de Negocio	Catastrófico	Moderado	Mayor	Catastrófico
Organización	Portafolio de productos y servicios	Mayor	Moderado	Mayor	Mayor

Identificados los tipos de información y el impacto que puede causar cada uno de ellos en la organización, corresponde calificar al tipo de información e identificar el activo en el que se encuentra el mismo.

Tabla 4 Identificación del activo de información y evaluación

Entidad	Nombre del tipo de información	Calificación del tipo de información	Activo de Información
Cliente	Datos principales	BAJO	OneDrive_1
Cliente	Información Financiera	ALTO	OneDrive_1
Cliente	Información Bancaria	ALTO	OneDrive_1
Cliente	Servicios	CRÍTICO	Workflow
Cliente	Core del negocio	ALTO	Workflow
Cliente	Infraestructura tecnológica	CRÍTICO	Workflow
Cliente	Ubicación	BAJO	OneDrive_1
Cliente	Protocolos de seguridad y salud	ALTO	OneDrive_2
Empleados	Información Personal	MEDIO	OneDrive_3
Empleados	Información Bancaria	ALTO	OneDrive_4
Empleados	Información de Salud	ALTO	OneDrive_3
Empleados	Formación académica	BAJO	CarpetaFisica_1
Empleados	Experiencia laboral	MEDIO	CarpetaFisica_1
Organización	Proyectos	CRÍTICO	Workflow
Organización	Equipo tecnológico	CRÍTICO	Workflow
Organización	Partners	MEDIO	OneDrive_5
Organización	Estrategia Empresarial y de Negocio	ALTO	OneDrive_4
Organización	Portafolio de productos y servicios	ALTO	OneDrive_4

Se observa claramente que el activo de información más crítico es el denominado "Workflow", por lo cual, será el activo sobre el que se realiza el análisis de amenazas y vulnerabilidad y posteriores controles.

6. Evaluación del riesgo del activo crítico

Identificado el activo más crítico para la organización, definimos su rol en la organización y los componentes que son parte de este activo.

El activo "Workflow" maneja la información de los procesos de trabajo que se desarrollan interna y externamente en la organización y se compone de:

- Servidor: Activo que almacena, distribuye y suministra información que se genera en el workflow.
- Web-launched Designer: Herramienta que los desarrolladores modifican, configuran y administran la información que contiene el workflow.
- Web-launched Clients: Herramienta que los usuarios utilizan para acceder a la información que contiene el workflow.
- Base de datos: Es el activo donde se almacena la información, misma que está organizada de manera que se pueda acceder, administrar y actualizar fácilmente desde el workflow.
- Web Services: Interfaz mediante la que el workflow puede interactuar con otros sistemas o activos de información.
- ERP Systems: Sistema de manejo de información empresarial, de clientes, logística, entre otros.

Es importante calificar estos componentes del activo crítico principal, para evaluar respecto al apetito al riesgo e impacto a la organización que puede causar una falla de seguridad en estos, el resultado es el siguiente:

Tabla 5 Calificación de los componentes del activo de información "Workflow"

Activo de Información	Componentes	Calificación
Workflow	Servidor	Crítico
	Web-launched Designer	Bajo
	Web-launched Clients	Bajo
	Base de datos	Crítico
	Web Services	Medio
	ERP Systems	Alto

Se evidencia que, de los componentes, el activo más crítico es la Base de datos, por lo cual sobre esta se trabaja el análisis de amenazas y vulnerabilidad.

Para este análisis el programa se apoya en Margerit V3, que se define como “Metodología de análisis y gestión de riesgos, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.” (Ministerio de Asuntos Económicos y Transformación Digital, 2012).

Adicional, las posibles vulnerabilidades para cada posible amenaza se evalúan con respecto a las determinadas en la ISO 27001 (ISO/IEC, 2013).

El resultado de la evaluación de riesgo para la base de datos del denominado “Workflow” es el siguiente:

- Amenaza Tipo: Errores y fallos no intencionados. Sus posibles amenazas son:
 - Errores de los usuarios. Sus posibles vulnerabilidades son:
 - Interfaz de usuario compleja.
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Fechas incorrectas.
 - Entrenamiento insuficiente del software.
 - Uso incorrecto de software.
 - Falta de conciencia acerca de la seguridad.
 - Errores del administrador. Sus posibles vulnerabilidades son:
 - Interfaz de usuario compleja.
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Entrenamiento insuficiente del software.
 - Uso incorrecto de software.
 - Falta de conciencia acerca de la seguridad.
 - Errores de monitorización (log). Sus posibles vulnerabilidades son:
 - Ausencia de pistas de auditoría.

- Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información.
- Ausencia de registros en las bitácoras (logs) de administrador y operario.
- Errores de configuración. Sus posibles vulnerabilidades son:
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Entrenamiento insuficiente en seguridad.
 - Uso incorrecto de software.
 - Falta de conciencia acerca de la seguridad.
- Difusión de software dañino. Sus posibles vulnerabilidades son:
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Transferencia de contraseñas en claro.
 - Ausencia de mecanismos de monitoreo.
- Escapes de información. Sus posibles vulnerabilidades son:
 - Habilitación de servicios innecesarios.
 - Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados.
 - Ausencia de mecanismos de monitoreo.
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Empleados desmotivados.
- Alteración accidental de la información. Sus posibles vulnerabilidades son:
 - Interfaz de usuario compleja.
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Entrenamiento insuficiente del software.
 - Uso incorrecto de software.

- Falta de conciencia acerca de la seguridad.
- Destrucción de información. Sus posibles vulnerabilidades son:
 - Interfaz de usuario compleja.
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Entrenamiento insuficiente del software.
 - Uso incorrecto de software.
 - Falta de conciencia acerca de la seguridad.
- Fugas de información. Sus posibles vulnerabilidades son:
 - Interfaz de usuario compleja.
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Entrenamiento insuficiente del software.
 - Uso incorrecto de software.
 - Falta de conciencia acerca de la seguridad.
- Vulnerabilidades de los programas (software). Sus posibles vulnerabilidades son:
 - Interfaz de usuario compleja.
 - Ausencia de copias de respaldo.
 - Ausencia de documentación.
 - Configuración incorrecta de parámetros.
 - Entrenamiento insuficiente del software.
 - Uso incorrecto de software.
 - Falta de conciencia acerca de la seguridad.
- Errores de mantenimiento / actualización de programas (software).
Sus posibles vulnerabilidades son:
 - Ausencia de documentación.
 - Entrenamiento insuficiente del software.
 - Ausencia de procedimiento de control de cambios.
 - ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.

- Especificaciones incompletas o no claras para los desarrolladores.
 - Falta de redundancia, copia única.
- Caída del sistema por agotamiento de recursos. Sus posibles vulnerabilidades son:
 - Ausencia de esquemas de reemplazo periódico.
 - Ausencia de mecanismos de monitoreo.
 - Ausencia de planes de continuidad.
 - Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
- Amenaza Tipo: Ataques intencionados. Sus posibles amenazas son:
 - Manipulación de los registros de actividad (log). Sus posibles vulnerabilidades son:
 - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.
 - Ausencia de revisiones regulares por parte de la gerencia.
 - Conexiones de red pública sin protección.
 - Falla en la producción de informes de gestión.
 - Ausencia de procedimiento formal para el control de la documentación del SGSI.
 - Ausencia de procedimiento formal para la supervisión del registro del SGSI.
 - En términos de tiempo utilización de datos errados en los programas de aplicación.
 - Software ampliamente distribuido.
 - Carencia o mala implementación de la auditoría interna.
 - Ausencia de pistas de auditoría.
 - Ausencia de procedimiento formal para el registro y retiro de usuarios.
 - Ausencia de procedimientos de identificación y valoración de riesgos.

- Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
- Manipulación de la configuración. Sus posibles vulnerabilidades son:
 - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.
 - Ausencia de revisiones regulares por parte de la gerencia
 - Conexiones de red pública sin protección.
 - Falla en la producción de informes de gestión.
 - Ausencia de procedimiento formal para el control de la documentación del SGSI.
 - Ausencia de procedimiento formal para la supervisión del registro del SGSI.
 - En términos de tiempo utilización de datos errados en los programas de aplicación.
 - Software ampliamente distribuido.
 - Carencia o mala implementación de la auditoría interna.
 - Ausencia de pistas de auditoría.
 - Ausencia de procedimiento formal para el registro y retiro de usuarios.
 - Ausencia de procedimientos de identificación y valoración de riesgos.
 - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
- Suplantación de la identidad del usuario. Sus posibles vulnerabilidades son:
 - Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario.
 - Tablas de contraseñas sin protección.
 - Gestión deficiente de las contraseñas.
- Abuso de privilegios de acceso. Sus posibles vulnerabilidades son:
 - Asignación errada de los derechos de acceso.

- Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.
- Ausencia de auditorías (supervisiones) regulares.
- Ausencia de pistas de auditoría.
- Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información.
- Ausencia de procedimiento formal para el registro y retiro de usuarios.
- Ausencia de procedimientos de identificación y valoración de riesgos.
- Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
- Ausencia de reportes de fallas en los registros de administradores y operadores.
- Ausencia o insuficiencia de pruebas de software.
- Defectos bien conocidos en el software.
- Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario.
- Gestión deficiente de las contraseñas.
- Tablas de contraseñas sin protección.
- Difusión de software dañino. Sus posibles vulnerabilidades son:
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Falta de herramientas de seguridad de red.
- Alteración de secuencia. Sus posibles vulnerabilidades son:
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Falta de herramientas de seguridad de red.
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.

- Arquitectura insegura de la red.
- Transferencia de contraseñas en claro.
- Acceso no autorizado. Sus posibles vulnerabilidades son:
 - Asignación errada de los derechos de acceso.
 - Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.
 - Ausencia de auditorías (supervisiones) regulares.
 - Ausencia de pistas de auditoría.
 - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información.
 - Ausencia de procedimiento formal para el registro y retiro de usuarios.
 - Ausencia de procedimientos de identificación y valoración de riesgos.
 - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
 - Ausencia de reportes de fallas en los registros de administradores y operadores.
 - Ausencia o insuficiencia de pruebas de software.
 - Defectos bien conocidos en el software.
 - Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario.
 - Gestión deficiente de las contraseñas.
 - Tablas de contraseñas sin protección.
- Interceptación de información (escucha). Sus posibles vulnerabilidades son:
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Falta de herramientas de seguridad de red.
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.

- Arquitectura insegura de la red.
- Transferencia de contraseñas en claro.
- Modificación deliberada de la información. Sus posibles vulnerabilidades son:
 - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.
 - Ausencia de revisiones regulares por parte de la gerencia
 - Conexiones de red pública sin protección.
 - Falla en la producción de informes de gestión.
 - Ausencia de procedimiento formal para el control de la documentación del SGSI.
 - Ausencia de procedimiento formal para la supervisión del registro del SGSI.
 - En términos de tiempo utilización de datos errados en los programas de aplicación.
 - Software ampliamente distribuido.
 - Carencia o mala implementación de la auditoría interna.
 - Ausencia de pistas de auditoría.
 - Ausencia de procedimiento formal para el registro y retiro de usuarios.
 - Ausencia de procedimientos de identificación y valoración de riesgos.
 - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
- Destrucción de información. Sus posibles vulnerabilidades son:
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Falta de herramientas de seguridad de red.
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.

- Transferencia de contraseñas en claro.
- Divulgación de información. Sus posibles vulnerabilidades son:
 - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad.
 - Ausencia de revisiones regulares por parte de la gerencia
 - Conexiones de red pública sin protección.
 - Falla en la producción de informes de gestión.
 - Ausencia de procedimiento formal para el control de la documentación del SGSI.
 - Ausencia de procedimiento formal para la supervisión del registro del SGSI.
 - En términos de tiempo utilización de datos errados en los programas de aplicación.
 - Software ampliamente distribuido.
 - Carencia o mala implementación de la auditoría interna.
 - Ausencia de pistas de auditoría.
 - Ausencia de procedimiento formal para el registro y retiro de usuarios.
 - Ausencia de procedimientos de identificación y valoración de riesgos.
 - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
- Denegación de servicio. Sus posibles vulnerabilidades son:
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Falta de herramientas de seguridad de red.
 - Líneas de comunicación sin protección.
 - Tráfico sensible sin protección.
 - Arquitectura insegura de la red.
 - Transferencia de contraseñas en claro.
- Ataque destructivo. Sus posibles vulnerabilidades son:

- Líneas de comunicación sin protección.
- Tráfico sensible sin protección.
- Arquitectura insegura de la red.
- Falta de herramientas de seguridad de red.
- Líneas de comunicación sin protección.
- Tráfico sensible sin protección.
- Arquitectura insegura de la red.
- Transferencia de contraseñas en claro.

7. Planes de acción para el activo crítico

Los planes de acción para cada uno de los activos de la organización, siempre serán evaluados sobre los 5 macro procesos comentados en la metodología, y para ello, “CIS Controls”, será de gran ayuda.

CIS Controls es una organización sin fines de lucro impulsada por la comunidad, responsable de CIS Controls® y CIS Benchmarks™, las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI. (Center for Internet Security, 2021).

En la versión 8 de CIS Controls, se detalla varias herramientas y controles que se pueden aplicar a diferentes tipos de activos de información. Para este caso, las herramientas y controles se enfocan en el activo crítico por sus diferentes macro procesos (Stocchetti, CIS Controls Version 8).

- Identificar (ID)
 - Establecer y mantener un inventario de software.
 - Asegúrese de que el software autorizado sea compatible actualmente.
 - Establecer y mantener un proceso de gestión de datos.
 - Establecer y mantener un inventario de sistemas de autenticación y autorización.
 - Realice análisis automatizados de vulnerabilidades de los activos internos de la empresa.

- Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente.
- Realice pruebas periódicas de penetración externa.
- Proteger (PR)
 - Bibliotecas autorizadas de lista de permitidos.
 - Scripts autorizados de lista de permitidos.
 - Configurar listas de control de acceso a datos.
 - Hacer cumplir la retención de datos.
 - Elimine los datos de forma segura.
 - Cifrar datos confidenciales en reposo.
 - Procesamiento y almacenamiento de datos de segmentos según la sensibilidad.
 - Implementar una solución de prevención de pérdida de datos.
 - Establecer y mantener un proceso de configuración seguro.
 - Configurar el bloqueo automático de sesiones en activos empresariales.
 - Gestione de forma segura los activos y el software de la empresa.
 - Administrar cuentas predeterminadas en activos y software empresariales.
 - Utilice contraseñas únicas.
 - Restringir los privilegios de administrador a cuentas de administrador dedicadas.
 - Centralizar la gestión de cuentas.
 - Establecer un proceso de concesión de acceso.
 - Establecer un proceso de revocación de acceso.
 - Centralizar el control de acceso.
 - Definir y mantener el control de acceso basado en roles.
 - Establecer y mantener un proceso de gestión de vulnerabilidades.
 - Realice una gestión automatizada de parches de aplicaciones.
 - Establecer y mantener un proceso de gestión de registros de auditoría.
 - Garantizar un almacenamiento adecuado del registro de auditoría.

- Estandarizar la sincronización horaria.
- Conservar registros de auditoría.
- Proteja los datos de recuperación.
- Asegúrese de que la infraestructura de red esté actualizada.
- Establecer y mantener una arquitectura de red segura.
- Gestione de forma segura la infraestructura de red.
- Centralice la autenticación, autorización y auditoría de la red (AAA).
- Uso de protocolos de comunicación y administración de red segura.
- Realizar el filtrado de la capa de aplicación.
- Establecer y mantener un proceso para aceptar y abordar las vulnerabilidades del software.
- Realice un análisis de la causa raíz de las vulnerabilidades de seguridad
- Utilice componentes de software de terceros actualizados y confiables.
- Establecer y mantener un sistema y proceso de clasificación de gravedad para las vulnerabilidades de las aplicaciones.
- Sistemas separados de producción y no producción.
- Capacitar a los desarrolladores en conceptos de seguridad de aplicaciones y codificación segura.
- Aplicar principios de diseño seguro en arquitecturas de aplicaciones.
- Aproveche los módulos o servicios examinados para los componentes de seguridad de las aplicaciones.
- Implementar verificaciones de seguridad a nivel de código.
- Realizar pruebas de penetración de aplicaciones.
- Realización de modelos de amenazas.
- Remediar los resultados de las pruebas de penetración.
- Validar medidas de seguridad.
- Detectar (DE)
 - Utilice herramientas de inventario de software automatizadas.

- Registro de acceso a datos confidenciales.
- Recopilar registros de auditoría.
- Recopile registros de auditoría detallados.
- Centralizar registros de auditoría.
- Realizar revisiones de registros de auditoría.
- Centralice las alertas de eventos de seguridad.
- Implemente una solución de detección de intrusiones en la red.
- Recopilar registros de flujo de tráfico de red.
- Ajustar los umbrales de alerta de eventos de seguridad.
- Supervisar proveedores de servicios.
- Responder (RS)
 - Deshabilitar cuentas inactivas.
 - Establecer y mantener un proceso de remediación.
 - Remediar las vulnerabilidades detectadas.
- Recuperar (RC)
 - Establecer y mantener un proceso de recuperación de datos.
 - Realice copias de seguridad automatizadas.
 - Establecer y mantener una instancia aislada de datos de recuperación.
 - Prueba de recuperación de datos.

8. Políticas de alto nivel

Al ser una organización nueva en la gestión de seguridad, se establecen políticas de alto nivel en los puntos más débiles para fortalecer los controles y el programa de SGSI. Estas políticas y sus procesos son los siguientes:

- Almacenamiento de Información: Usar de manera controlada y correcta los sistemas, servidores y servicios de almacenamiento que provee la organización a sus empleados para un óptimo tratamiento de la información, evitando la fuga, duplicidad, pérdida o alteración de la misma.
 - Inventario de los servidores de almacenamiento.
 - Criterios de almacenamiento.

- Clasificación de la información.
 - Control de acceso.
 - Copias de seguridad.
 - Auditoría.
 - Cifrado de la información.
- Protección contra virus: Brindar la protección adecuada a todos los activos de información de la organización para evitar infecciones por códigos maliciosos o virus
 - Contratación de las herramientas de antivirus y antimalware.
 - Configuración de las herramientas de antivirus y antimalware.
 - Actualización de las herramientas de antivirus y antimalware.
 - Procedimiento de respuesta ante la infección.
 - Buenas prácticas de seguridad.
- Aplicaciones permitidas en activos de la organización: Controlar el uso de aplicaciones y software licenciado para el buen uso de la información.
 - Instalación, configuración, mantenimiento y borrado de las aplicaciones.
 - Sanciones por uso de aplicaciones no autorizadas.
 - Repositorio de aplicaciones permitidas.
 - Autorización y licenciamiento de las aplicaciones.
- Auditoría de sistemas: Control, monitoreo y gestión de información y evidencia del cumplimiento de seguridad de los activos de información de la organización.
 - Inventario de activos críticos.
 - Mejora continua.
 - Auditorías externas.
 - Análisis de resultados y plan de remediación.
- Clasificación de la Información: Clasificar los activos de información según su nivel de riesgo:
 - Inventario de la información.
 - Criterios de clasificación de la información.
 - Evaluación del riesgo de la Información.

- Tratamiento de la Información.
- Formación y Concienciación: Mantener a todos los empleados de la organización en continuo aprendizaje sobre la importancia de la seguridad de la información.
 - Difusión de la política de seguridad.
 - Programas de formación.
 - Evaluación de aprendizaje.
 - Cultura de seguridad de la información.
- Continuidad del negocio: Mantener un plan de continuidad de negocio actualizado y que permita a la organización reaccionar de manera oportuna ante un incidente.
 - Alcance del plan de continuidad de negocio.
 - Planteamiento del BIA.
 - Análisis del plan de continuidad.
 - Estrategias del plan de continuidad.
 - Respuesta ante los incidentes.
 - Prueba y evaluación del plan de continuidad de negocio.
 - Comunicación interna y externa de un incidente.
- Gestión y control de accesos: Gestionar y controlar de manera adecuada como los empleados de la organización pueden acceder a la información, herramientas, aplicaciones o software.
 - Perfilamiento de usuarios.
 - Gestión de cuentas de usuario con permisos.
 - Mecanismos de autenticación.
 - Registro de eventos.
 - Revisión de permisos.
- Copias de Seguridad: Establecer los procesos necesarios para mantener la información disponible, protegida y asegurada.
 - Definir información crítica.
 - Periodicidad de las copias de seguridad.
 - Caducidad de copias de seguridad.
 - Procedimientos de copia y restauración.

- Cifrado de las copias de información.
- Controles de cambio: Definir los procesos y métodos para realizar cambios en los activos de información de la organización
 - Plan de cambio
 - Evaluación del riesgo de cambio
 - Ejecución del cambio

Para gestionar y controlar cada uno de los procesos y sus políticas, se determinan roles dentro de la organización, los que serán encargados de dar cumplimiento a cada uno de ellos.

En base a la estructura actual de la organización, se definen los siguientes roles.

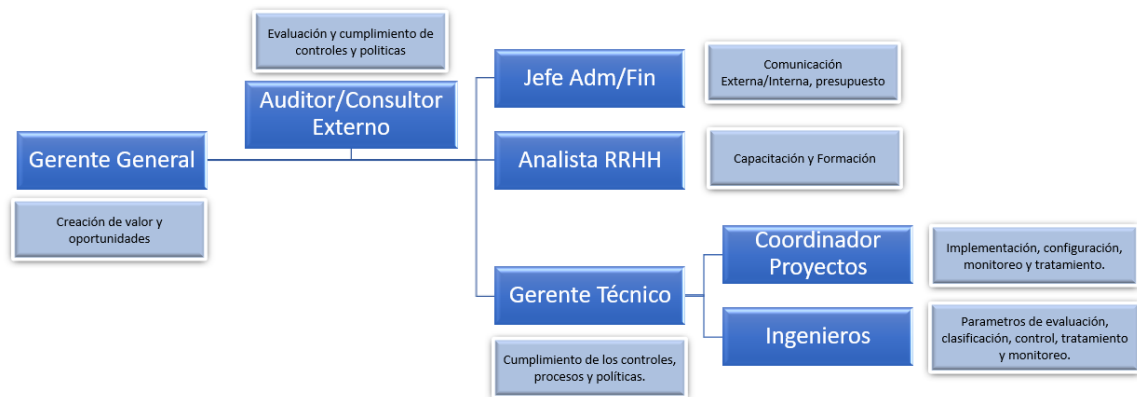


Figura 5. Roles y responsabilidades de la organización en el SGSI.

9. Planes de acción del SGSI

Con el diagnóstico inicial de la organización y el análisis realizado a lo largo del presente diseño del SGSI, se plantea implementar los primeros planes de acción para que la organización pueda empezar a gestionar el programa y retroalimentarlo constantemente cada que se cumplan los hitos de los planes de acción.

Los planes de acción iniciales según los macro procesos del programa SGSI son:

- Identificar (ID)

- Establecer, actualizar y mantener un inventario detallado de activos empresariales.
- Evaluar e identificar los activos críticos de la organización.
- Comprender y priorizar la importancia de la seguridad de la información para la línea de negocio de la organización.
- Diseñar un sistema de gobernanza de gestión de seguridad de la información.
- Diseñar una estrategia de gestión de riesgos de la organización.
- Proteger (PR)
 - Gestionar, evaluar y controlar el acceso a activos físicos y lógicos de la organización.
 - Diseñar planes de capacitación y concientización de seguridad de la información en toda la organización.
 - Gestionar y registrar los procesos de mantenimiento de los activos de la organización.
 - Implementar procesos y procedimientos de protección de la información en los activos más críticos de la organización.
 - Evaluar las mejores herramientas de seguridad que protejan a la organización para reducir el riesgo de fallas de seguridad .
- Detectar (DE)
 - Analizar y comprender los eventos de seguridad que pueden afectar a la organización.
 - Diseñar un proceso de monitoreo continuo de seguridad en los activos de la organización.
- Responder (RS)
 - Diseñar y planificar procesos de respuesta ante un incidente de seguridad.
 - Definir las acciones y roles de comunicación en caso de un evento de seguridad.
- Recuperar (RC)
 - Diseñar un plan de recuperación y restauración de los activos de la organización ante un incidente de seguridad.

Implementando los controles mencionados, el programa busca en una primera intervención, mejorar la gestión de seguridad en la organización de la siguiente forma.

Tabla 6 Mejoras esperadas en el SGSI

Macro-Procesos	Evaluación
Identificar (ID)	Inicio 12%
	↓ Cargando ↓
	Mejoras 30%
Proteger (PR)	Inicio 12%
	↓ Cargando ↓
	Mejoras 30%
Detectar (DE)	Inicio 6%
	↓ Cargando ↓
	Mejoras 15%
Responder (RS)	Inicio 0%
	↓ Cargando ↓
	Mejoras 15%
Recuperar (RC)	Inicio 0%
	↓ Cargando ↓
	Mejoras 15%

Cumplido el primer objetivo de mejora en la organización, el programa SGSI se retroalimentará para promover nuevas mejoras en la organización incluyendo nuevos planes de acciones, herramientas, procesos y procedimientos que ayudaran a controlar y gestionar los eventos e incidentes de seguridad.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Actualmente la organización es altamente vulnerable a incidentes de seguridad, la respuesta y recuperación ante esto, es completamente nula, lo que puede ocasionar una seria afectación a su operatividad y el cumplimiento de los servicios con sus clientes.

La facilidad de combinar varios marcos de referencia para diseñar un programa SGSI, como en el presente caso (Cobit 2019 - NIST), ayuda a realizar un evaluación más profunda y aterrizada a la necesidad de una organización, no basta solo con cumplir normativas o certificaciones, se trata de proteger la organización y sus beneficios.

El programa diseñado, sea ajusta a las necesidades de la organización, orientado sus mejoras a ser un apoyo en el cumplimiento de la visión y misión de la organización, tomando en cuenta que el sector a que provee servicios la organización es apetecible para quienes se encargan de la ciber delincuencia.

Recomendaciones

Es necesario ponerle énfasis a la implementación del presente programa SGSI, iniciar pronto con los planes de acción y hacer entender a la organización la importancia de proteger los datos e información, todo esto con el fin de evitar remordimientos futuros del por qué no se implementó a tiempo.

Reforzar urgente uno de los puntos más importantes dentro de una organización, como es el control e identificación de los activos, ya que al no conocer el total de los activos de la empresa y tener registro y control sobre ellos, no se tendrá el control sobre un incidente o evento de seguridad en esos activos y quizás la organización puede estar vulnerada hace tiempo atrás por estos activos.

Mantener la retroalimentación continua del programa SGSI para proteger y probar la fortaleza de la organización en la defensa contra incidentes de seguridad, recordar que el implementar una herramienta o proceso no hace a

ninguna organización invisible frente a los ataques, los ciber ataques están en constante crecimiento y toda organización debe adaptarse a los cambios con ellos.

REFERENCIAS

Center for Internet Security, I. (. (2021). *Center for Internet Security*. Obtenido de Center for Internet Security: <https://www.cisecurity.org/about-us/>

CERT, K. I. (2021). *Threat landscape for industrial automation systems*. AO KASPERSKY LAB.

ISACA. (2020). *COBIT Focus Area: Information Security sing COBIT 2019*. Schaumburg: ISACA.

ISO/IEC. (2013). *INTERNATIONAL STANDARD ISO/IEC 27001*. Switzerland: ISO/IEC.

Ministerio de Asuntos Económicos y Transformación Digital, E. (2012). *Portal de Administración Electrónica*. Obtenido de Portal de Administración Electrónica:
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#

Security, I. (2018). *Sistemas de Control Industrial (ICS), Principal objetivo de los ciberataques*. ITS Security.

Stocchetti, V. (s.f.). *CIS Controls Version 8*. Obtenido de Center for Internet Security, Inc: <http://www.cisecurity.org/controls/>

ANEXOS

Caso de Negocio

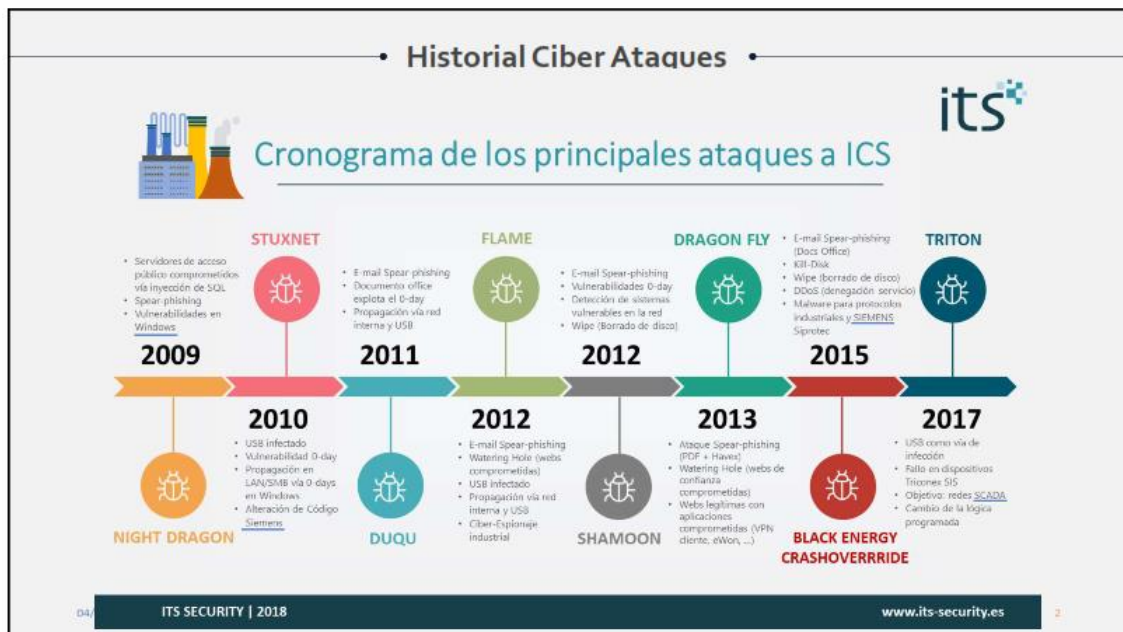
Caso de Negocio

Diseño del Programa del Sistema de Gestión de Seguridad de Información (SGSI)

"Solo hay dos tipos de empresas: las que han sido pirateadas y las que serán"

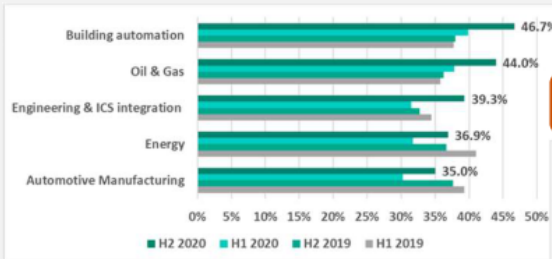
Robert Mueller

Realizado por
Diego David Guzmán Calderón

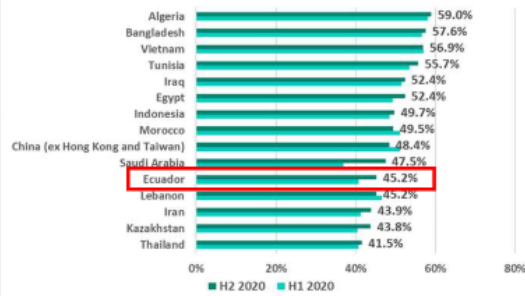


Actualidad

Porcentaje de equipos ICS donde se bloquearon objetos maliciosos en industrias seleccionadas



Top 15 de países y territorios por porcentaje de computadoras ICS en donde fueron bloqueados objetos maliciosos



04/09/2021 **Revisión anual**
Fuente: Threat landscape for industrial automation systems (statistics for H2 2020) - © 2021 AO KASPERSKY LAB

3

Resumen de la organización

Empresa que presta el servicio adecuado y oportuno, atendiendo de manera inmediata todos los requerimientos y problemas que puedan surgir en el transcurso de nuestra asesoría y ejecución. Desde la provisión de software y equipos hasta el desarrollo de soluciones tecnológicas integrales, fáciles de mantener y de pronto retorno en la inversión.

Misión

Desarrollar talento humano para proveer soluciones tecnológicas e innovadoras con el fin de mejorar la calidad, eficiencia y productividad del sector empresarial.

Visión

Ser reconocida por todos nuestros clientes como una empresa que entrega soluciones tecnológicas óptimas de manera eficiente.

Valores

- Aprendizaje
- Compromiso
- Excelencia
- Integridad
- Vocación de Servicio

Servicios

- Provisión de equipos de sistemas de control
- Diseño, construcción y puesta en marcha de sistemas eléctricos de control, monitoreo e información
- Entrenamiento técnico

Áreas de Servicio

- Petróleo y Gas
- Alimentos
- Manufactura
- Automotriz
- Telecomunicaciones

04/09/2021 **Revisión anual**

4

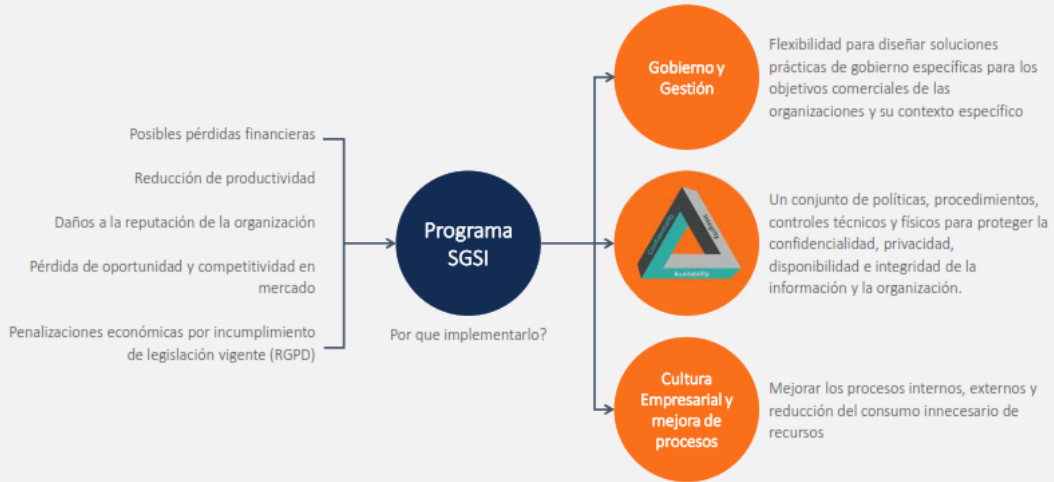
Afectación Organizacional



Alineación SGSI con la organización




Visión General SGSI



Presupuesto

Factor	Descripción	Costos
Documentación	Todos los documentos para análisis de impactos en el negocio, evaluación y tratamiento de riesgos, gobierno y gestión, check list de certificación de normativas, etc.	\$2,500 dólares
Formación o Capacitación	Dentro de una empresa o una organización, si todos los empleados tuvieran conocimiento y conciencia de los problemas de ciberseguridad reales existentes en la actualidad y su repercusión, es muy probable que no se produjeran la mayor parte de los incidentes en las empresas.	\$600 dólares semestralmente
Ayuda Externa	Un consultor externo nos va a guiar para que nuestro equipo se centre en aquellas actividades y debilidades que debemos subsanar, y a que no nos perdamos en tareas que puedan incluso dar lugar a costes mayores.	\$3,000 dólares
Tecnología	La inversión en tecnología, nos ayudará a alcanzar los objetivos del SGSI y reducirá a su vez costes que se generan cuando el proceso de gestión de forma tradicional.	\$20,000 dólares
Tiempo	El tiempo que nuestros empleados dediquen a la implementación se va a ver afectado por la madurez del sistema actual	Aproximadamente 8 meses


























"Si gastas más en café
que en seguridad de TI,
serás pirateado".
Además, mereces ser
pirateado."

Richard Clarke

Diagnóstico inicial

Categoría	Subcategoría	Referencias Informativas COBIT 2019 IS	Nivel de capacidad	Porcentaje de implementación	Cumplimiento de capacidad	Implementación actual	Codificación del programa SGSI	
Gestión de activos (ID.AM): los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	ID.AM-1: Se inventarian los dispositivos y sistemas físicos dentro de la organización.	BAI09.01 Identificar y registrar activos corrientes	2	80%		56%	ORG-ID.AM1	
				80%				
			3	60%				
		40%						
		BAI09.02 Gestionar activos críticos	2	50%				
				70%				
	3		50%					
			40%					
	ID.AM-2: Se inventarian las plataformas y aplicaciones de software dentro de la organización.	BAI09.01 Identificar y registrar activos corrientes	2	80%		63%		ORG-ID.AM2
				80%				
			3	70%				
		50%						
		BAI09.02 Gestionar activos críticos	2	80%				
				50%				
3	50%							
	50%							
BAI09.05 Gestionar licencias	3	50%						
	4	70%						
Gestión de activos (ID.AM): los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	ID.AM-3: Se mapean la comunicación organizacional y los flujos de datos	DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	90%		48%	ORG-ID.AM3	
				90%				
				80%				
			3	80%				
				50%				
				40%				
	4	60%						
		10%						
	ID.AM-4: Se catalogan los sistemas de información externos	APO02.02 Evaluar las capacidades actuales, el desempeño y la madurez digital de la empresa.	2	60%		53%		ORG-ID.AM4
				60%				
		APO10.04 Gestionar el riesgo del proveedor.	4	50%				
			3	50%				
	DSS01.02 Gestionar servicios de I&T subcontratados.	4	50%					
			50%					
ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor	APO03.03 Seleccionar oportunidades y soluciones.	3	60%		43%	ORG-ID.AM5		
			60%					
	APO03.04 Definir la implementación de la arquitectura.	3	50%					
			0%					
APO12.01 Recopilar datos.	3	0%						
		0%						
BAI04.02 Evaluar el impacto empresarial.	4	0%						
		0%						

comercial.			0%			
	BAI09.02 Gestionar activos criticos	2	80%	80%	23%	ORG-ID.AM6
		3	70%	60%		
			50%			
4	50%	50%				
ID.AM-6: Se establecen los roles y responsabilidades de ciberseguridad para toda la fuerza laboral y terceros interesados (por ejemplo, proveedores, clientes, socios)	APO01.02 Comunicar los objetivos de gestión, la dirección y las decisiones tomadas.	2	10%	10%		
		3	10%	5%		
	APO07.06 Gestionar personal contratado.	2	50%	50%		
			50%			
	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	2	0%	0%		
			0%			
			0%			
			0%			
			0%			
			0%			
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	3	40%	40%			
	4	30%	30%			

ID.BE-1: Se identifica y comunica el papel de la organización en la cadena de suministro.	APO08.01 Comprender las expectativas comerciales.	2	10%	10%	4%	ORG-ID.BE1		
		3	0%	0%				
	APO08.04 Coordinar y comunicar.	4	0%	0%				
	APO08.05 Proporcionar información para la mejora continua de los servicios.	5	10%	10%				
	APO10.03 Gestionar relaciones y contratos con proveedores.	2	50%	17%				
			0%					
			0%					
			0%					
			50%					
0%								
4	0%	0%						
5	0%	0%						
APO10.04 Gestionar el riesgo del proveedor.	4	0%	0%					
APO10.05 Supervisar el desempeño y el cumplimiento de los proveedores.	4	0%	0%					
ID.BE-2: Se identifica y comunica el lugar de la organización en la	APO02.06 Comunicar la estrategia y dirección de I&T.	2	40%	40%				
		3	0%	0%				
		2	0%	0%				

Entorno empresarial (ID.BE): se comprenden y priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar las funciones, responsabilidades y decisiones de gestión de riesgos de la seguridad cibernética.	logos de la organización en la infraestructura crítica y su sector industrial	APO03.01 Desarrollar la visión de la arquitectura empresarial.	3	0%	0%	8%	ORG-ID.BE2				
				0%	0%						
			4	0%	0%						
				0%	0%						
	ID.BE-3: Se establecen y comunican las prioridades para la misión, los objetivos y las actividades de la organización.		APO02.01 Comprender el contexto y la dirección de la empresa.	2	0%			0%	0%	ORG-ID.BE3	
								0%			0%
			APO02.06 Comunicar la estrategia y dirección de I&T.	2	0%			0%			
								0%			0%
					3			0%			0%
								0%			0%
APO03.01 Desarrollar la visión de la arquitectura empresarial.			2	0%	0%						
					0%	0%					
				3	0%	0%					
					0%	0%					

ID.BE-4: Se establecen las dependencias y funciones críticas para la prestación de servicios críticos		APO10.01 Identificar y evaluar las relaciones y los contratos con los proveedores.	3	0%	0%	20%	ORG-ID.BE4				
					0%			0%			
		BAI04.02 Evaluar el impacto empresarial.	4	0%	0%						
					0%			0%			
		BAI09.02 Gestionar activos críticos	2	50%	50%						
			3	50%	40%						
				30%	10%						
			4	10%	10%						
		ID.BE-5: Se establecen requisitos de resiliencia para respaldar la prestación de servicios críticos para todos los estados operativos (por		BAI03.02 Diseñar componentes de solución detallados.	2			0%	0%	0%	ORG-ID.BE5
				D504.02 Mantener la resiliencia empresarial.	2			0%	0%		

ID.GV-1: Se establece y se comunica la política de ciberseguridad			APO01.03 Implementar procesos de gestión (para apoyar el logro de los objetivos de gobernanza y gestión).	2	20%	20%	4%	ORG-ID.GV1		
						0%			0%	
					4	0%			0%	
			APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).			2			0%	0%
									0%	
									0%	
									0%	
									0%	
									0%	
									0%	
			0%							

organizacional	EDM01.01 Evaluar el sistema de gobierno.	2	0%	0%
			0%	
			0%	
		3	0%	0%
			0%	
			0%	
	EDM01.02 Dirigir el sistema de gobierno.	2	50%	17%
			0%	
			0%	
		3	0%	0%
			0%	
			0%	
4		0%	0%	
		0%		
		0%		
APO01.02 Comunicar los objetivos de gestión, la dirección y las decisiones tomadas.	2	0%	0%	
		0%		
	3	0%		

Gobernanza (ID.GV)- Las políticas, procedimientos y procesos para administrar y	ID.GV-2: Los roles y responsabilidades de ciberseguridad están coordinados y alineados con roles internos y socios externos	APO10.03 Gestionar relaciones y contratos con proveedores.	0%	0%		
			0%			
			0%			
			0%			
			0%			
			0%			
		APO13.02 Definir y administrar un plan de tratamiento de riesgos de privacidad y seguridad de la información.	3	0%	0%	
				0%		
				0%		
			4	0%		0%
				0%		
				0%		
	APO10.03 Gestionar relaciones y contratos con proveedores.	4	0%	0%		
			0%			
		5	0%	0%		
			0%			
		APO13.02 Definir y administrar un plan de tratamiento de riesgos de privacidad y seguridad de la información.	3	0%	0%	
				0%		
0%						
4	0%		0%			
	0%					
	0%					
			12%	ORG-ID.GV2		

monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se entienden e informan la gestión del riesgo de ciberseguridad.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	2	50%	50%	42%		
		10%				
	3	60%				
		40%				
		50%				
		50%				
	4	30%	30%			
30%						
ID.GV-3: Se comprenden y gestionan los requisitos legales y reglamentarios relacionados con la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles.	2	0%	0%	0%		ORG-ID.GV3
		0%				
	3	0%	0%			
		0%				
MEA03.01 Identificar los requisitos de cumplimiento externos.	2	0%	0%			
		0%				
	3	0%	0%			
		0%				
MEA03.04 Obtener garantía de cumplimiento externo.	2	0%	0%			
ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad	2	0%	0%	0%		ORG-ID.GV4
		0%				
		0%				
		0%				
	3	0%	0%			
		0%				
		0%				
		0%				
ADM12.02 Analizar riesgos						

		<p>AP012.04 Analizar riesgo.</p> <table border="1"> <tr><td></td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td>4</td><td>0%</td></tr> <tr><td>5</td><td>0%</td></tr> </table>		0%		0%	4	0%	5	0%				
	0%													
	0%													
4	0%													
5	0%													
		<p>AP012.05 Definir una cartera de acciones de gestión de riesgos.</p> <table border="1"> <tr><td>2</td><td>0%</td></tr> <tr><td>3</td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> </table>	2	0%	3	0%		0%						
2	0%													
3	0%													
	0%													
		<p>DSS04.02 Mantener la resiliencia empresarial.</p> <table border="1"> <tr><td>2</td><td>0%</td></tr> </table>	2	0%										
2	0%													
		<p>AP012.01 Recopilar datos.</p> <table border="1"> <tr><td>3</td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td>3</td><td>0%</td></tr> </table>	3	0%		0%		0%	3	0%				
3	0%													
	0%													
	0%													
3	0%													
		<p>AP012.02 Analizar riesgo.</p> <table border="1"> <tr><td></td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td>4</td><td>0%</td></tr> <tr><td>5</td><td>0%</td></tr> </table>		0%		0%		0%	4	0%	5	0%		
	0%													
	0%													
	0%													
4	0%													
5	0%													
		<p>AP012.03 Mantener un perfil de riesgo.</p> <table border="1"> <tr><td>3</td><td>0%</td></tr> </table>	3	0%										
3	0%													
	<p>ID.RA-1: las vulnerabilidades de los activos se identifican y documentan</p>	<p>AP012.04 Riesgo articulado.</p> <table border="1"> <tr><td>3</td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td></td><td>0%</td></tr> <tr><td>4</td><td>0%</td></tr> </table>	3	0%		0%		0%		0%	4	0%	<p>9%</p>	<p>ORG-ID.RA1</p>
3	0%													
	0%													
	0%													
	0%													
4	0%													

	DSS05.01 Proteger contra software malintencionado.	3	0%	0%		
	DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	80%	80%	17%	
			80%			
			80%			
			80%			
		3	50%			
		0%				
		0%				
		4	0%			
		0%				
		0%				
ID.RA-2: la inteligencia sobre amenazas cibernéticas se recibe de fuentes y foros de intercambio de información	BAI08.01 Identificar y clasificar fuentes de información para el gobierno y la gestión de I&T.	2	0%	0%	0%	ORG-ID.RA2
		3	0%	0%		
		4	0%	0%		
	APO12.01 Recopilar datos.	3	0%	0%		

Evaluación de riesgos (ID.RA): la organización comprende el riesgo de ciberseguridad 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-3: Las amenazas, tanto internas como externas, se identifican y documentan	APO12.02 Analizar riesgo.	3	0%	0%	0%	ORG-ID.RA3	
				0%				
				0%				
				0%				
				0%				
				0%				
			4	0%	0%			
			5	0%	0%			
			APO12.03 Mantener un perfil de riesgo.	3	0%			0%
				3	0%			0%

	APO12.04 Riesgo articulado.		0%			
			0%			
		4	0%	0%		
ID.RA-4: Se identifican los posibles impactos y probabilidades comerciales	D5504.02 Mantener la resiliencia empresarial.	2	0%	0%	0%	ORG-ID.RA4
ID.RA-5: Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo.	APO12.02 Analizar riesgo.	3	0%	0%	0%	ORG-ID.RA5
			0%			
			0%			
			0%			
			0%			
		4	0%	0%		
		5	0%	0%		
ID.RA-6: Se identifican y priorizan las respuestas al riesgo	APO12.05 Definir una cartera de acciones de gestión de riesgos.	2	0%	0%	0%	ORG-ID.RA6
		3	0%	0%		
	3		0%	0%		
		0%				
		0%				
		0%				
		0%				
4	0%	0%				
			0%			

			3	0%	0%		
		APO12.04 Riesgo articulado.		0%			
				0%			
			4	0%	0%		
		APO12.05 Definir una cartera de acciones de gestión de riesgos.	2	0%	0%		
			3	0%	0%		
	ID.RM-1: Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización.			0%		0%	ORG-ID.RM1
				0%			
			3	0%	0%		
		APO13.02 Definir y administrar un plan de tratamiento de riesgos de privacidad y seguridad de la información.		0%			
				0%			
				0%			
				0%			
			4	0%	0%		
		BAI02.03 Gestionar el riesgo de requisitos.	4	0%	0%		
		BAI04.02 Evaluar el impacto empresarial.	4	0%	0%		
				0%			
	ID.RM-2: La tolerancia al riesgo organizacional está determinada y claramente expresada	APO12.06 Responder al riesgo.	4	0%	0%	0%	ORG-ID.RM2
				0%			
				0%			
			3	0%	0%		
				0%			
	ID.RM-3: La determinación de la tolerancia al riesgo de la organización se basa en su papel en la infraestructura crítica y el análisis de	APO12.02 Analizar riesgo.		0%		0%	ORG-ID.RM3

Estrategia de gestión de riesgos (ID.RM): las prioridades, las limitaciones, las tolerancias de riesgo y los supuestos de la organización se establecen y utilizan para respaldar las decisiones de riesgo operativo.

	riesgo específico del sector.			0%		
			4	0%	0%	
			5	0%	0%	
		APO10.01 Identificar y evaluar las relaciones y los contratos con los proveedores.	3	0%	0%	
				0%		
		APO10.04 Gestionar el riesgo del proveedor.	4	0%	0%	
		APO12.04 Riesgo articulado.	3	0%	0%	
				0%		
				0%		
				0%		
			4	0%	0%	
	ID.SC-1: Los procesos de gestión de riesgos de la cadena de suministro cibernético son identificados, establecidos, evaluados, gestionados y acordados por las partes interesadas de la organización.		2	0%	0%	
		APO12.05 Definir una cartera de acciones de gestión de riesgos.	3	0%	0%	
				0%		
		APO13.02 Definir y administrar un plan de tratamiento de riesgos de privacidad y seguridad de la información.	3	0%	0%	
				0%		
				0%		
				0%		
				0%		
			4	0%	0%	
		BAI01.03 Gestionar la participación de las partes interesadas.	3	0%	0%	
	0%					
	0%					
					0%	ORG-ID.SC1

		4	0%	0%		
	BAI02.03 Gestionar el riesgo de requisitos.	4	0%	0%		
	BAI04.02 Evaluar el impacto empresarial.	4	0%	0%		
			0%			
			0%			
	APO10.01 Identificar y evaluar las relaciones y los contratos con los proveedores.	3	0%	0%		
		2	0%	0%		
			0%			
			0%			
	APO10.02 Seleccionar proveedores.	3	0%	0%		
			0%			
			0%			
			0%			
	APO10.04 Gestionar el riesgo del proveedor.	4	0%	0%		
	APO10.05 Supervisar el desempeño y el cumplimiento de los proveedores.	4	0%	0%		
	APO12.01 Recopilar datos.	3	0%	0%		
	APO12.02 Analizar riesgo.	3	0%	0%		
			0%			
			0%			
			0%			
			0%			

ID.SC-2: Los proveedores y socios externos de sistemas de información, componentes y servicios se

<p>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 ciberseguridad de una organización y el Plan de gestión de riesgos de la cadena de suministro cibernético.</p>	<p>APO10.02 Seleccionar proveedores.</p>		0%		<p>0%</p>	<p>ORG-ID.SC3</p>
			0%			
			0%			
		3	0%	0%		
			0%			
	<p>APO10.03 Gestionar relaciones y contratos con proveedores.</p>		0%			
			0%			
			0%			
		2	0%	0%		
			0%			

			0%			
			0%			
		4	0%	0%		
		5	0%	0%		
			0%			
	<p>APO10.04 Gestionar el riesgo del proveedor.</p>	4	0%	0%		
			0%			
	<p>APO10.05 Supervisar el desempeño y el cumplimiento de los proveedores.</p>	4	0%	0%		
			0%			
	<p>APO10.01 Identificar y evaluar las relaciones y los contratos con los proveedores.</p>	<p>APO10.01 Identificar y evaluar las relaciones y los contratos con los proveedores.</p>	3	0%		
			0%			
<p>APO10.03 Gestionar relaciones y contratos con proveedores.</p>			0%			
			0%			
		2	0%	0%		
		0%				

ID.SC-4: Los proveedores y socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que están cumpliendo con sus obligaciones contractuales.			0%		0%	ORG-ID.SC4
		4	0%	0%		
		5	0%	0%		
	APO10.04 Gestionar el riesgo del proveedor.	4	0%	0%		
	APO10.05 Supervisar el desempeño y el cumplimiento de los proveedores.	4	0%	0%		
	MEA01.01 Establecer un enfoque de seguimiento.	2	0%	0%		
			0%			
			0%			
			0%			
			0%			
			0%			
	MEA01.02 Establecer objetivos de rendimiento y cumplimiento.	2	0%	0%		
			0%			
	MEA01.03 Recopilar y procesar datos de rendimiento y conformidad.	2	0%	0%		
0%						
MEA01.04 Analizar e informar sobre el rendimiento.	3	0%	0%			
MEA01.05 ORGurar la implementación de acciones correctivas.	2	0%	0%			
ID.SC-5: La planificación y las pruebas de respuesta y recuperación se llevan a cabo con proveedores y proveedores externos.	DSS04.04 Ejercitar, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta a desastres (DRP).	0%	0%			
		0%				
		0%				
		0%				
		0%				
	3	0%	0%			
	4	0%	0%			
	5	0%	0%			
				0%	ORG-ID.SCS	

Categoría	Subcategoría	Referencias Informativas COBIT 2019 IS	Nivel de capacidad	Porcentaje de implementación	Cumplimiento de	Implementación	Codificación del programa SGSI
Gestión de identidad, autenticación y control de acceso (PR.AC): el acceso a los activos físicos y lógicos y las instalaciones asociadas está limitado a usuarios, procesos y dispositivos autorizados, y se gestiona de forma coherente con el riesgo evaluado de acceso no autorizado a actividades y transacciones autorizadas.	PR.AC-1: Las identidades y credenciales se emiten, administran, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados.	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	2	50%	50%	50%	ORG_PR.AC1
			3	50%	50%		
				50%			
				50%			
				50%			
				50%			
		4	50%	50%			
		DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	3	50%	50%		
	4	50%	50%				
	PR.AC-2: El acceso físico a los activos se gestiona y protege	DSS01.04 Gestionar el medio ambiente.	3	50%	50%	38%	ORG_PR.AC2
		DSS05.05 Gestionar el acceso físico a los activos de I&T.	2	30%	20%		
				0%			
				0%			
				50%			
			3	50%	43%		
80%	0%						
PR.AC-3: Se gestiona el acceso remoto	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	2	0%	0%	16%	ORG_PR.AC3	
			0%				
			0%				
			0%				
			0%				
			0%				
	DSS01.04 Gestionar el medio ambiente.	3	0%	0%			
	DSS05.03 Gestionar la seguridad de los terminales.	2	80%	52%			
			50%				
			50%				
50%							
PR.AC-4: Se gestionan permisos y autorizaciones de acceso, incorporando los principios de privilegio mínimo y separación de funciones	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	2	50%	36%	ORG_PR.AC4		
			40%				
			10%				
		3	40%			38%	
			35%				
			35%				
	40%						
	4	30%	30%				
		30%					
	PR.AC-5: La integridad de la red está protegida (p. Ej., Segregación de la red, segmentación de la red)	DSS01.05 Gestionar instalaciones.	3	50%	50%	51%	ORG_PR.AC5
DSS05.02 Gestionar la seguridad de la red y la conectividad.		2	50%	54%			
			55%				
			55%				
			50%				
		3	50%	50%			
			50%				
			50%				
4	50%	50%					
	50%						
2	50%	50%					

deberes y responsabilidades relacionados con la ciberseguridad de acuerdo con las políticas, procedimientos y acuerdos relacionados.	PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades			0%		0%	ORG_PR.AT3	
		APO07.06 Gestionar personal contratado.	2	0%	0%			
		APO10.04 Gestionar el riesgo del proveedor.	4	0%	0%			
		APO10.05 Supervisar el desempeño y el cumplimiento de los proveedores.	4	0%	0%			
	PR.AT-4: Los altos ejecutivos comprenden sus roles y responsabilidades	EDM01.01 Evaluar el sistema de gobierno.			0%		0%	ORG_PR.AT4
				2	0%	0%		
				3	0%	0%		
				3	0%	0%		
		APO01.02 Comunicar los objetivos de gestión, la dirección y las decisiones tomadas.	2	0%	0%			
			3	0%	0%			
		APO07.03 Mantener las habilidades y competencias del personal.	2	0%	0%			
			3	0%	0%			
	PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades	APO07.03 Mantener las habilidades y competencias del personal.	2	0%	0%	0%	ORG_PR.AT5	
				3	0%			0%
				3	0%			0%
			3	0%	0%			
	APO01.06 Optimizar la ubicación de la función de TI.	2	0%	0%				
		3	0%	0%				
	BAI02.01 Definir y mantener los requisitos técnicos y funcionales del negocio.	2	0%	0%				
			3	0%			0%	
			3	0%			0%	
			3	0%			0%	
PR.DS-1: Los datos en reposo están protegidos	BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio.	2	0%	0%	8%	ORG_PR.DS1		
		3	0%	0%				
	DS504.07 Gestionar arreglos de respaldo.	2	0%	0%				
	DS505.03 Gestionar la seguridad de los terminales.	2	50%	49%				
			50%					
			50%					
			50%					
			50%					
			50%					
	DS506.06 Activos de información seguros	3	30%	30%				
PR.DS-2: Los datos en tránsito están protegidos	APO01.06 Optimizar la ubicación de la función de TI.	2	0%	0%	27%	ORG_PR.DS2		
		3	0%	0%				
	DS505.02 Gestionar la seguridad de la red y la conectividad.	2	50%	50%				
			50%					
			50%					
			50%					
	DS506.06 Activos de información seguros	3	50%	50%				
			50%					
PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	BAI09.03 Gestionar el ciclo de vida de los activos.	2	0%	0%	0%	ORG_PR.DS3		
		3	0%	0%				
		4	0%	0%				
PR.DS-4: Capacidad adecuada para	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	2	0%	0%				
			0%					
			0%					
			0%					
			0%					
			0%					

<p>Seguridad de los datos (PR.DS): la información y los registros (datos) se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.</p>	<p>garantizar que se mantenga la disponibilidad</p>	<p>BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.</p>	<p>2</p>	<p>0%</p>	<p>0%</p>	<p>0%</p>	<p>ORG_PR_DS4</p>		
			3	0%	0%				
			4	0%	0%				
				0%					
	<p>PR.DS-5: Se implementan protecciones contra fugas de datos</p>	<p>DSS05.04 Gestionar la identidad del usuario y el acceso lógico.</p>	<p>DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.</p>	<p>2</p>	<p>0%</p>			<p>0%</p>	
					3			0%	0%
					<p>3</p>			50%	50%
								50%	50%
								50%	50%
								50%	50%
								50%	50%
					<p>4</p>			40%	25%
								10%	
					<p>2</p>			0%	0%
0%						0%			
0%						0%			
3					0%	0%			
<p>2</p>					0%	0%			
	0%								
	0%								
	0%								
	0%								
<p>3</p>	0%	0%							
	0%								
	0%								
	0%								
<p>PR.DS-6: Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>2</p>	<p>0%</p>	<p>0%</p>				
				3	0%	0%			
				<p>2</p>	0%	0%			
					0%				
					0%				
					0%				
					0%				
				<p>3</p>	0%	0%			
					0%				
					0%				
					0%				
					0%				
				<p>PR.DS-6: Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>2</p>	<p>0%</p>	<p>0%</p>
								3	0%
<p>2</p>	0%	0%							
	0%								
	0%								
	0%								
	0%								
<p>3</p>	0%	0%							
	0%								
	0%								
	0%								
	0%								
<p>PR.DS-6: Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>2</p>					<p>0%</p>	<p>0%</p>
								3	0%
				<p>2</p>	0%	0%			
					0%				
					0%				
					0%				
					0%				
				<p>3</p>	0%	0%			
					0%				
					0%				
					0%				
					0%				
				<p>PR.DS-6: Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>2</p>	<p>0%</p>	<p>0%</p>
								3	0%
<p>2</p>	0%	0%							
	0%								
	0%								
	0%								
	0%								
<p>3</p>	0%	0%							
	0%								
	0%								
	0%								
	0%								
<p>PR.DS-6: Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>DSS06.02 Controlar el procesamiento de la información.</p>	<p>2</p>					<p>0%</p>	<p>0%</p>
								3	0%
				<p>2</p>	0%	0%			
					0%				
					0%				
					0%				
					0%				
				<p>3</p>	0%	0%			
					0%				
					0%				
					0%				
					0%				

	PR.DS-7: El (los) entorno (s) de desarrollo y prueba están separados del entorno de producción	BAI07.04 Establezca un entorno de prueba.	3	0% 0% 0% 0%	0%	0%	ORG_PR_DS7				
	PR.DS-8: Los mecanismos de verificación de integridad se utilizan para verificar la integridad del	BAI03.05 Construir soluciones.	3	0% 0%	0%	0%	ORG_PR_DS8				
	PR.IP-1: Se crea y mantiene una configuración básica de tecnología de la información / sistemas de control industrial incorporando principios de seguridad (por ejemplo, concepto de funcionalidad mínima)	BAI10.01 Establecer y mantener un modelo de configuración.	3	0%	0%	13%	ORG_PR_IP1				
BAI10.02 Establecer y mantener un repositorio de configuración y una línea de BORG.		3	30% 50%	43%							
		4	50%	54%							
BAI10.03 Mantener y controlar elementos de configuración.		2	0% 0%	0%							
		3	0%	0%							
BAI10.05 Verificar y revisar la integridad del repositorio de configuración.	4	0% 0% 0%	0%								
		5	0%	0%							
PR.IP-2: Se implementa un ciclo de vida de desarrollo de sistemas para administrar sistemas	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	2	0% 0% 0% 0% 0%	0%	0%	ORG_PR_IP2					
			BAI03.01 Diseñar soluciones de alto nivel.	2			0%	0%			
			BAI03.02 Diseñar componentes de solución detallados.	2			0%	0%			
			BAI03.03 Desarrollar componentes de solución.	3			0%	0%			
PR.IP-3: Se han implementado procesos de control de cambios de configuración	BAI01.06 Monitorear, controlar e informar sobre los resultados del programa.	4	0% 0% 0% 0% 0%	0%	0%	ORG_PR_IP3					
			BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio.	2			0% 0%	0%			
				3			0% 0%	0%			
			PR.IP-4: Se realizan, mantienen y prueban copias de seguridad de la información	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).			2	0% 0% 0% 0% 0%	0%	0%	ORG_PR_IP4
								DSS01.01 Realizar procedimientos operativos.	3		
	2	0%			0%						
DSS04.07 Gestionar arreglos de respaldo.	2	0%		0%							

Procesos y procedimientos de protección de la información (PR.IP): las políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de gestión y la coordinación entre las entidades organizativas), los procesos y los procedimientos se mantienen y utilizan para gestionar la protección de los sistemas y activos de información. .

PR.IP-5: Se cumplen las políticas y regulaciones con respecto al entorno operativo físico para los activos de la organización.	DSS01.04 Gestionar el medio ambiente.	3	0%	0%	0%	ORG_PR.IP5			
	DSS05.05 Gestionar el acceso físico a los activos de I&T.	2	0%	0%					
			0%						
			0%						
		3	0%	0%					
			0%						
			0%						
	PR.IP-6: Los datos se destruyen de acuerdo con la política	BAI09.03 Gestionar el ciclo de vida de los activos.	2	0%			0%	0%	ORG_PR.IP6
			3	0%			0%		
			4	0%			0%		
DSS05.06 Gestionar documentos confidenciales y dispositivos de salida.			2	0%	0%				
		3	0%	0%					
			0%						
PR.IP-7: Se mejoran los procesos de protección	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_PR.IP7			
DSS04.05 Revisar, mantener y mejorar los planes de continuidad.	3	0%	0%						
PR.IP-8: Se comparte la eficacia de las tecnologías de protección	BAI08.04 Evaluar y actualizar o retirar información.	3	0%	0%	0%	ORG_PR.IP8			
			0%						
			0%						
DSS03.04 Resolver y cerrar problemas.	4	0%	0%						
	PR.IP-9: Planes de respuesta (respuesta ante incidentes y continuidad del negocio) y planes	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_PR.IP9		
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.	2	0%	0%						
PR.IP-10: Se prueban los planes de respuesta y recuperación	DSS04.04 Ejercitar, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta a desastres (DRP).	2	0%	0%	0%	ORG_PR.IP10			
			0%						
			0%						
		3	0%	0%					
		4	0%	0%					

PR.IP-11: La ciberseguridad está incluida en las prácticas de recursos humanos (p. Ej., Desaprovisionamiento, selección de personal)	APO07.01 Adquirir y mantener personal adecuado y apropiado.	2	0%	0%	0%	ORG_PR.IP11
	APO07.02 Identificar al personal clave de TI.	2	0%	0%		
	APO07.03 Mantener las habilidades y competencias del personal.	2	0%	0%		
			0%			
	3	0%	0%			
		0%				
	APO07.04 Evaluar y reconocer / recompensar el desempeño laboral de los empleados.	3	0%	0%		
	APO07.05 Planificar y realizar un seguimiento del uso de TI y recursos humanos empresariales.	2	0%	0%		
			0%			
		3	0%	0%		
0%						
PR.IP-12: Se desarrolla e implementa un plan de gestión de vulnerabilidades.	BAI03.10 Mantener soluciones.	4	0%	0%	13%	ORG_PR.IP12
	DSS05.01 Proteger contra software malintencionado.	3	0%	0%		
			0%			
	DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	50%	50%		
			50%			
			50%			
		3	0%	13%		
			40%			
	4	0%	0%			
	BAI03.10 Mantener soluciones.	4	0%	0%		
0%						
0%						

<p>Mantenimiento (PR.MA): El mantenimiento y las reparaciones de los componentes del sistema de información y control industrial se realizan de acuerdo con las políticas y procedimientos.</p>	<p>PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y registran, con herramientas aprobadas y controladas.</p>	BAI09.02 Gestionar activos críticos	3	0%	0%	0%	ORG_PR.MA1			
			4	0%	0%					
		BAI09.03 Gestionar el ciclo de vida de los activos.	2	0%	0%					
			3	0%	0%					
			4	0%	0%					
		DSS01.05 Gestionar instalaciones.	3	0%	0%					
	<p>PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, registra y realiza de manera que se evite el acceso no autorizado.</p>	<p>DSS05.04 Gestionar la identidad del usuario y el acceso lógico.</p>	2	50%	50%	42%	ORG_PR.MA2			
			3	50%	50%					
				50%						
				50%						
50%										
50%										
4			30%	25%						
			20%							
<p>PR.PT-1: Los registros de auditoría / registro se determinan, documentan, implementan y revisan de acuerdo con la política.</p>			APO11.04 Realizar seguimiento, control y revisiones de la calidad	3	0%			0%	16%	ORG_PR.PT1
			BAI03.05 Construir soluciones.	3	0%			0%		
	<p>DSS05.04 Gestionar la identidad del usuario y el acceso lógico.</p>	2	50%	50%						
		3	50%	50%						
			50%							
			50%							
			50%							
	4	30%	25%							
		20%								
	<p>PR.PT-2: Los medios extraíbles están protegidos y su uso restringido de acuerdo con la política.</p>	<p>DSS05.02 Gestionar la seguridad de la red y la conectividad.</p>	<p>DSS05.07 Gestionar vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.</p>	4	30%	25%	16%	ORG_PR.PT2		
2				20%	0%					
				0%						
				0%						
				0%						
				0%						
3				0%	0%					
				0%						
<p>MEA02.01 Supervisar los controles internos.</p>				3	0%	0%				
				2	0%	0%				
	0%									
<p>APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).</p>	<p>DSS05.02 Gestionar la seguridad de la red y la conectividad.</p>	<p>PR.PT-2: Los medios extraíbles están protegidos y su uso restringido de acuerdo con la política.</p>	2	0%	0%	16%	ORG_PR.PT2			
			2	80%	80%					
				80%						
				80%						
				80%						
				50%						
			3	0%	17%					
				0%						
			4	0%	0%					
				0%						
2	0%	0%								
	0%									

Tecnología de protección (PR.PT): las soluciones de seguridad técnica se administran para garantizar la seguridad y la resistencia de los sistemas y activos, de acuerdo con las políticas, los procedimientos y los acuerdos relacionados.		DSS05.06 Gestionar documentos confidenciales y dispositivos de salida.	3	0%	0%	13%	ORG_PR.PT3	
	PR.PT-3: El principio de funcionalidad mínima se incorpora configurando sistemas para proporcionar solo capacidades esenciales	DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	80%	80%			0%
				80%				
				80%				
			3	30%	10%			
				0%				
				0%				
			4	0%	0%			
				0%				
			DSS05.06 Gestionar documentos confidenciales y dispositivos de salida.	2	0%			0%
					0%			
				3	0%			0%
					0%			
0%								
0%								
DSS05.05 Gestionar el acceso físico a los activos de I&T.	2	0%	0%					
		0%						
		0%						
	3	0%	0%					
		0%						
		0%						
PR.PT-4: Las redes de comunicaciones y control están protegidas	DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	80%	80%	0%			
			80%					
			80%					
		3	30%	10%				
			0%					
			0%					
		4	0%	0%				
			0%					
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, intercambio en caliente) para lograr los requisitos de resiliencia en situaciones normales y adversas.	APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	2	0%	0%	0%	ORG_PR.PT5
			BAI04.01 Evaluar la disponibilidad, el rendimiento y la capacidad actuales y crear una línea de bORG.	3	0%	0%		
					0%			
					0%			
BAI04.02 Evaluar el impacto empresarial.	4			0%	0%			
				0%				
				0%				
BAI04.03 Plan para requisitos de servicio nuevos o modificados.	4		0%	0%				
	2		0%	0%				
BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.	3		0%	0%				
	4		0%	0%				
DSS01.05 Gestionar instalaciones.	3		0%	0%				

Categoría	Subcategoría	Referencias Informativas COBIT 2019 IS	Nivel de capacidad	Porcentaje de	Cumplimiento de	Implementación	Codificación del programa SGSI
Anomalías y eventos (DE.AE): Se detecta actividad anómala y se comprende el impacto potencial de los eventos.	DE.AE-1: Se establece y gestiona una línea de bORG de operaciones de red y flujos de datos esperados para usuarios y sistemas.	DSS03.01 Identificar y clasificar problemas.	2	10%	10%	10%	ORG_DE.AE1
	DE.AE-2: Los eventos detectados se analizan para comprender los objetivos y métodos de los ataques.	DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.	2	0%	0%	0%	ORG_DE.AE2
			0%				
			0%				
			0%				
	3	0%	0%				
	DE.AE-3: Los datos de eventos se recopilan y correlacionan desde múltiples fuentes y sensores	BAI08.02 Organizar y contextualizar la información en conocimiento.	3	10%	10%	10%	ORG_DE.AE3
	DE.AE-4: Se determina el impacto de los eventos	APO12.06 Responder al riesgo.	3	10%	10%	10%	ORG_DE.AE4
		DSS03.01 Identificar y clasificar problemas.	2	10%	10%		
	DE.AE-5: Se establecen umbrales de alerta de incidentes	APO12.06 Responder al riesgo.	3	10%	10%	10%	ORG_DE.AE5
DSS03.01 Identificar y clasificar problemas.		2	10%	10%			
Monitoreo continuo de seguridad (DE.CM): el sistema de información y los activos se monitorean para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	DE.CM-1: La red se monitorea para detectar posibles eventos de ciberseguridad	DSS01.03 Monitorear la infraestructura de I&T.	4	10%	10%	2%	ORG_DE.CM1
		DSS03.05 Realice una gestión proactiva de problemas.	3	0%	0%		
			0%				
			0%				
	4	0%	0%				
	DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de ciberseguridad	DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.	2	0%	0%	0%	ORG_DE.CM2
			0%				
			0%				
			0%				
	3	0%	0%				
DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de ciberseguridad	DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.	2	0%	0%	0%	ORG_DE.CM3	
		0%					
		0%					
		0%					
3	0%	0%					
DE.CM-4: Se detectó código malicioso	DSS05.01 Proteger contra software malintencionado.	3	0%	0%	0%	ORG_DE.CM4	
		0%					
DE.CM-5: Se detecta código móvil no	DSS05.01 Proteger contra software	3	0%	0%	0%	ORG_DE.CM5	

autorizado	malintencionado.	3	0%	0%	0%	ORG_DE.CM3
DE.CM-6: Se monitorea la actividad del proveedor de servicios externos para detectar posibles eventos de ciberseguridad	APO07.06 Gestionar personal contratado.	2	20%	20%	10%	ORG_DE.CM6
	APO10.05 Supervisar el desempeño y el cumplimiento de los proveedores.	4	0%	0%		
DE.CM-7: Se realiza el monitoreo de personal, conexiones, dispositivos y software no autorizados	DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	20%	35%	19%	ORG_DE.CM7
			40%			
		3	30%			
			0%	10%		
	4	0%	0%			
		DSS05.05 Gestionar el acceso fisico a los activos de I&T.	2	30%		
	0%					
	3		0%	30%		
30%						
DE.CM-8: Se realizan análisis de vulnerabilidades	BAI03.10 Mantener soluciones.	4	20%	20%	10%	ORG_DE.CM8
DSS05.01 Proteger contra software malintencionado.	3	0%	0%			

DE.DP-1: Las funciones y responsabilidades de detección están bien definidas para garantizar la rendición de cuentas	APO01.02 Comunicar los objetivos de gestión, la dirección y las decisiones tomadas.	2	0%	0%	4%	ORG_DE.DP1
	DSS05.01 Proteger contra software malintencionado.	3	0%	0%		
		3	0%	0%		
	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	3	10%	10%		
4		10%	10%			
DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables	DSS06.01 Alinear las actividades de control integradas en los procesos comerciales con los objetivos empresariales.	2	30%	30%	12%	ORG_DE.DP2
		3	40%	0%		
	MEA03.03 Confirmar cumplimiento externo.	3	0%	0%		
			0%			
		4	0%	0%		
	5	0%	0%			
	MEA03.04 Obtener garantía de cumplimiento externo.	2	0%	0%		
				0%		

Procesos de detección (DE.DP): Los procesos y procedimientos de detección se mantienen y prueban para garantizar el conocimiento de eventos anómalos.	DE.DP-3: Se prueban los procesos de detección	APO13.02 Definir y administrar un plan de tratamiento de riesgos de privacidad y seguridad de la información.	3	0%	3%	12%	ORG_DE.DP3	
				0%				
				20%				
				0%				
				0%				
			4	0%	0%			
		DSS05.02 Gestionar la seguridad de la red y la conectividad.	2	50%	50%			50%
				50%	50%			50%
				50%	50%			50%
				20%	7%			
0%	0%							
	3	0%	0%					
	4	0%	0%					
DE.DP-4: Se comunica la información de detección de eventos	APO08.04 Coordinar y comunicar.	3	0%	0%	0%	ORG_DE.DP4		
		4	0%	0%				
		APO12.06 Responder al riesgo.	3	0%			0%	
DE.DP-5: Los procesos de detección se mejoran continuamente	DSS02.05 Resolver y recuperarse de incidentes.	2	0%	0%	0%	ORG_DE.DP5		
		APO12.06 Responder al riesgo.	3	0%			0%	
	DSS04.05 Revisar, mantener y mejorar los planes de continuidad.	3	0%	0%				

Categoría	Subcategoría	Referencias Informativas COBIT 2019 IS	Nivel de capacidad	Porcentaje de implementación	Cumplimiento de	Implementación actual	Codificación del programa SGSI
Planificación de respuesta (RS.RP): Los procesos y procedimientos de respuesta se ejecutan y mantienen para garantizar la respuesta a los incidentes de ciberseguridad detectados.	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RS.RP1
Comunicaciones (RS.CO): las actividades de respuesta se coordinan con las partes interesadas internas y externas (p. Ej., Apoyo externo de los 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	EDM03.02 Gestión de riesgo directo.	2	0%	0%	0%	ORG_RS.CO1
				0%			
				0%			
				0%			
				0%			
		3	0%	0%			
	RS.CO-2: Los incidentes se notifican de acuerdo con los criterios establecidos	APO01.02 Comunicar los objetivos de gestión, la dirección y las decisiones tomadas.	2	0%	0%	0%	
			3	0%	0%		
			3	0%	0%		
	RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	APO12.03 Mantener un perfil de riesgo.	3	0%	0%		
RS.CO-2: Los incidentes se notifican de acuerdo con los criterios establecidos	DSS01.03 Monitorear la infraestructura de I&T.	4	0%	0%	0%	ORG_RS.CO2	
RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	DSS03.04 Resolver y cerrar problemas.	4	0%	0%	0%	ORG_RS.CO3	
RS.CO-4: La coordinación con las partes interesadas se produce de forma coherente con los planes de respuesta.	DSS03.04 Resolver y cerrar problemas.	4	0%	0%	0%	ORG_RS.CO4	
RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una conciencia más amplia de la situación de la ciberseguridad.	BAI08.04 Evaluar y actualizar o retirar información.	3	0%	0%	0%	0%	ORG_RS.CO5
			0%				
			0%				

				0%			
Análisis (RS.AN): el análisis se realiza para garantizar una respuesta eficaz y resaltar las actividades de	RS.AN-1: Se investigan las notificaciones de los sistemas de detección	DSS02.04 Investigar, diagnosticar y asignar incidencias.	3	0%	0%	0%	ORG_RS.AN1
		DSS02.07 Realice un seguimiento del estado y genere informes.	3	0%	0%		
			4	0%	0%		
	RS.AN-2: Se entiende el impacto del incidente	DSS02.02 Registrar, clasificar y priorizar solicitudes e incidencias.	2	0%	0%	0%	ORG_RS.AN2
			3	0%	0%		
	RS.AN-3: Se realizan análisis forenses	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RS.AN3
		DSS03.02 Investigar y diagnosticar problemas.	3	0%	0%		
		DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.	2	0%	0%		
			2	0%	0%		
			3	0%	0%		
	RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta	DSS02.02 Registrar, clasificar y priorizar solicitudes e incidencias.	2	0%	0%	0%	ORG_RS.AN4
	Respuesta (RS.RE): se establecen los procedimientos de recuperación.	RS.AN-5: Los procesos se establecen para recibir, analizar y responder a las vulnerabilidades reveladas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	EDM03.02 Gestión de riesgo directo.	3	0%	0%	0%
2				0%	0%		
				3	0%	0%	
DSS05.07 Gestione vulnerabilidades y supervise la infraestructura para detectar eventos relacionados con la seguridad.			2	0%	0%		
			2	0%	0%		
			3	0%	0%		
Mitigación (RS.MI): las actividades se realizan para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	RS.MI-1: Los incidentes están contenidos	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RS.MI1
	RS.MI-2: Se mitigan los incidentes	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RS.MI2
	RS.MI-3: Las vulnerabilidades identificadas recientemente se mitigan o documentan como riesgos aceptados	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RS.MI3
Mejoras (RS.IM): las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección / respuesta actuales y anteriores.	RS.IM-1: Se actualizan las estrategias de respuesta	DSS04.08 Realizar una revisión posterior a la reanudación	4	0%	0%	0%	ORG_RS.IM1
			5	0%	0%		

Categoría	Subcategoría	Referencias Informativas COBIT 2019 IS	Nivel de capacidad	Porcentaje de implementación	Cumplimiento de capacidad	Implementación actual	Codificación del programa SGI		
Planificación de recuperación (RC.RP): Los procesos y procedimientos de recuperación se ejecutan y mantienen para garantizar la restauración de sistemas o activos afectados por incidentes de ciberseguridad.	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RC.RP1		
		DSS02.05 Resolver y recuperarse de incidentes.	2	0%	0%				
		DSS03.04 Resolver y cerrar problemas.	4	0%	0%				
Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran incorporando las lecciones aprendidas en las actividades futuras.	RC.IM-1: Los planes de recuperación incorporan lecciones aprendidas	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RC.IM1		
		BAI05.07 Mantener cambios.	3	0%	0%				
		DSS04.08 Realizar una revisión posterior a la reanudación	4	0%	0%				
			5	0%	0%				
	RC.IM-2: Se actualizan las estrategias de recuperación	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RC.IM2		
		BAI07.08 Realizar una revisión posterior a la implementación.	3	0%	0%				
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 atacantes, víctimas, otros CSIRT y proveedores).	RC.CO-1: Se gestionan las relaciones públicas	EDM03.02 Gestión de riesgo directo.	2	0%	0%	0%	ORG_RC.CO1		
				0%					
				0%					
				0%					
	RC.CO-2: La reputación se repara después de un incidente	MEA03.02 Optimizar la respuesta a los requisitos externos.	3	0%	0%	0%	ORG_RC.CO2		
				0%					
				0%					
				4				0%	0%
				5				0%	0%
	RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como a los equipos ejecutivos y de gestión.	APO12.06 Responder al riesgo.	3	0%	0%	0%	ORG_RC.CO3		

Inventario de Activos y Evaluación de Riesgos

Activo de Información	Componentes	Descripción	Calificación
Workflow	Servidor	Activo que almacena, distribuye y suministra información que se generará en el workflow	CRÍTICO
	Web-launched Designer	Herramienta que los desarrolladores modifican, configuran y administran la información que contiene el workflow	BAJO
	Web-launched Clients	Herramienta que los usuarios utilizan para acceder a la información que contiene el workflow	BAJO
	Base de datos	Es el activo donde se almacena la información, misma que está organizada de manera que se pueda acceder, administrar y actualizar fácilmente desde el workflow	CRÍTICO
	Web Services	Interfaz mediante la que el workflow puede interactuar con otros sistemas o activos de información	MEDIO
	ERP Systems	Sistema de manejo de información empresarial, de clientes, logística, entre otros	ALTO
OneDrive_1	Office 365	Programas que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint	BAJO
	Share Point Microsoft	Plataforma de colaboración donde se almacena información de la organización	BAJO
	One Drive Microsoft	Servicio de alojamiento de archivos e información de la organización en la nube	BAJO
OneDrive_3	Office 366	Programas que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint	BAJO
	Share Point Microsoft	Plataforma de colaboración donde se almacena información de la organización	BAJO
	One Drive Microsoft	Servicio de alojamiento de archivos e información de la organización en la nube	BAJO
OneDrive_2	Office 367	Programas que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint	BAJO
	Share Point Microsoft	Plataforma de colaboración donde se almacena información de la organización	BAJO
	One Drive Microsoft	Servicio de alojamiento de archivos e información de la organización en la nube	BAJO
OneDrive_5	Office 368	Programas que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint	BAJO
	Share Point Microsoft	Plataforma de colaboración donde se almacena información de la organización	BAJO
	One Drive Microsoft	Servicio de alojamiento de archivos e información de la organización en la nube	BAJO
OneDrive_4	Office 370	Programas que nos permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint	BAJO
	Share Point Microsoft	Plataforma de colaboración donde se almacena información de la organización	BAJO
	One Drive Microsoft	Servicio de alojamiento de archivos e información de la organización en la nube	BAJO
CarpetaFisica_1	Hojas de Vida	Información del historial de estudio y trabajo de los empleados	BAJO
	Seguros Medicos	Información médica de los empleados de la organización	BAJO
	Informacion Personal	Información de vivienda, estado civil, familia, etc de los empleados de la organización	BAJO

EVALUACION DEL RIESGO - BASE DE DATOS - WORKFLOW		
	Posibles Amenazas	Posibles Vulnerabilidades
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	<ul style="list-style-type: none"> - Interfaz de usuario compleja - Ausencia de documentación - Configuración incorrecta de parámetros - Fechas incorrectas - Entrenamiento insuficiente del software - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.2] Errores del administrador	<ul style="list-style-type: none"> - Interfaz de usuario compleja - Ausencia de documentación - Configuración incorrecta de parámetros - Entrenamiento insuficiente del software - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.3] Errores de monitorización (log)	<ul style="list-style-type: none"> - Ausencia de pistas de auditoría - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información - Ausencia de registros en las bitácoras (logs) de administrador y operario.
	[E.4] Errores de configuración	<ul style="list-style-type: none"> - Ausencia de documentación - Configuración incorrecta de parámetros - Entrenamiento insuficiente en seguridad - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.8] Difusión de software dañino	<ul style="list-style-type: none"> - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - Transferencia de contraseñas en claro - Ausencia de mecanismos de monitoreo
	[E.14] Escapes de información	<ul style="list-style-type: none"> - Habilitación de servicios innecesarios - Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados - Ausencia de mecanismos de monitoreo - Líneas de comunicación sin protección - Tráfico sensible sin protección - Empleados desmotivados.
	[E.15] Alteración accidental de la información	<ul style="list-style-type: none"> - Interfaz de usuario compleja - Ausencia de documentación - Configuración incorrecta de parámetros - Entrenamiento insuficiente del software - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.18] Destrucción de información	<ul style="list-style-type: none"> - Interfaz de usuario compleja - Ausencia de documentación - Configuración incorrecta de parámetros - Entrenamiento insuficiente del software - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.19] Fugas de información	<ul style="list-style-type: none"> - Interfaz de usuario compleja - Ausencia de documentación - Configuración incorrecta de parámetros - Entrenamiento insuficiente del software - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.20] Vulnerabilidades de los programas (software)	<ul style="list-style-type: none"> - Interfaz de usuario compleja - Ausencia de copias de respaldo - Ausencia de documentación - Configuración incorrecta de parámetros - Entrenamiento insuficiente del software - Uso incorrecto de software - Falta de conciencia acerca de la seguridad
	[E.21] Errores de mantenimiento / actualización de programas (software)	<ul style="list-style-type: none"> - Ausencia de documentación - Entrenamiento insuficiente del software - Ausencia de procedimiento de control de cambios - Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos. - Especificaciones incompletas o no claras para los desarrolladores - Falta de redundancia, copia única.
	[E.24] Caída del sistema por agotamiento de recursos	<ul style="list-style-type: none"> - Ausencia de esquemas de reemplazo periódico. - Ausencia de mecanismos de monitoreo - Ausencia de planes de continuidad - Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
	[A.3] Manipulación de los registros de actividad (log)	<ul style="list-style-type: none"> - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad - Ausencia de revisiones regulares por parte de la gerencia - Conexiones de red pública sin protección - Falla en la producción de informes de gestión - Ausencia de procedimiento formal para el control de la documentación del SGSI - Ausencia de procedimiento formal para la supervisión del registro del SGSI - En términos de tiempo utilización de datos errados en los programas de aplicación - Software ampliamente distribuido - Carencia o mala implementación de la auditoría interna. - Ausencia de pistas de auditoría - Ausencia de procedimiento formal para el registro y retiro de usuarios - Ausencia de procedimientos de identificación y valoración de riesgos - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
	[A.4] Manipulación de la configuración	<ul style="list-style-type: none"> - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad - Ausencia de revisiones regulares por parte de la gerencia - Conexiones de red pública sin protección - Falla en la producción de informes de gestión - Ausencia de procedimiento formal para el control de la documentación del SGSI - Ausencia de procedimiento formal para la supervisión del registro del SGSI - En términos de tiempo utilización de datos errados en los programas de aplicación - Software ampliamente distribuido - Carencia o mala implementación de la auditoría interna. - Ausencia de pistas de auditoría - Ausencia de procedimiento formal para el registro y retiro de usuarios - Ausencia de procedimientos de identificación y valoración de riesgos - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso.
	[A.5] Suplantación de la identidad del usuario	<ul style="list-style-type: none"> - Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario - Tablas de contraseñas sin protección - Gestión deficiente de las contraseñas

[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso	<ul style="list-style-type: none"> - Asignación errada de los derechos de acceso - Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo - Ausencia de auditorías (supervisiones) regulares - Ausencia de pistas de auditoría - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información - Ausencia de procedimiento formal para el registro y retiro de usuarios - Ausencia de procedimientos de identificación y valoración de riesgos - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso - Ausencia de reportes de fallas en los registros de administradores y operadores - Ausencia o insuficiencia de pruebas de software - Defectos bien conocidos en el software - Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario - Gestión deficiente de las contraseñas - <u>Tablas de contraseñas sin protección</u>
	[A.8] Difusión de software dañino	<ul style="list-style-type: none"> - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - Falta de herramientas de seguridad de red - <u>Líneas de comunicación sin protección</u>
	[A.10] Alteración de secuencia	<ul style="list-style-type: none"> - Tráfico sensible sin protección - Arquitectura insegura de la red - Falta de herramientas de seguridad de red - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - <u>Transferencia de contraseñas en claro</u>
	[A.11] Acceso no autorizado	<ul style="list-style-type: none"> - Asignación errada de los derechos de acceso - Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo - Ausencia de auditorías (supervisiones) regulares - Ausencia de pistas de auditoría - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información - Ausencia de procedimiento formal para el registro y retiro de usuarios - Ausencia de procedimientos de identificación y valoración de riesgos - Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso - Ausencia de reportes de fallas en los registros de administradores y operadores - Ausencia o insuficiencia de pruebas de software - Defectos bien conocidos en el software - Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario - Gestión deficiente de las contraseñas - <u>Tablas de contraseñas sin protección</u>
	[A.14] Interceptación de información (escucha)	<ul style="list-style-type: none"> - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - Falta de herramientas de seguridad de red - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - <u>Transferencia de contraseñas en claro</u>
	[A.15] Modificación deliberada de la información	<ul style="list-style-type: none"> - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad - Ausencia de revisiones regulares por parte de la gerencia - Conexiones de red pública sin protección - Falta en la producción de informes de gestión - Ausencia de procedimiento formal para el control de la documentación del SGSI - Ausencia de procedimiento formal para la supervisión del registro del SGSI - En términos de tiempo utilización de datos errados en los programas de aplicación - Software ampliamente distribuido - Carencia o mala implementación de la auditoría interna. - Ausencia de pistas de auditoría - Ausencia de procedimiento formal para el registro y retiro de usuarios - Ausencia de procedimientos de identificación y valoración de riesgos - <u>Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso</u>
	[A.18] Destrucción de información	<ul style="list-style-type: none"> - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - Falta de herramientas de seguridad de red - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - <u>Transferencia de contraseñas en claro</u>
	[A.19] Divulgación de información	<ul style="list-style-type: none"> - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad - Ausencia de revisiones regulares por parte de la gerencia - Conexiones de red pública sin protección - Falta en la producción de informes de gestión - Ausencia de procedimiento formal para el control de la documentación del SGSI - Ausencia de procedimiento formal para la supervisión del registro del SGSI - En términos de tiempo utilización de datos errados en los programas de aplicación - Software ampliamente distribuido - Carencia o mala implementación de la auditoría interna. - Ausencia de pistas de auditoría - Ausencia de procedimiento formal para el registro y retiro de usuarios - Ausencia de procedimientos de identificación y valoración de riesgos - <u>Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso</u>
	[A.24] Denegación de servicio	<ul style="list-style-type: none"> - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - Falta de herramientas de seguridad de red - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - <u>Transferencia de contraseñas en claro</u>
	[A.26] Ataque destructivo	<ul style="list-style-type: none"> - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - Falta de herramientas de seguridad de red - Líneas de comunicación sin protección - Tráfico sensible sin protección - Arquitectura insegura de la red - <u>Transferencia de contraseñas en claro</u>

CONTROLES Y PLANES DE ACCION - BASE DE DATOS - WORKFLOW		
Proceso	Controles	Descripción
Identificar (ID)	Establecer y mantener un inventario de software	Establezca y mantenga un inventario detallado de todo el software con licencia instalado en los activos de la empresa. El inventario de software debe documentar el título, el editor, la fecha de instalación / uso inicial y el propósito comercial de cada entrada; cuando corresponda, incluya el localizador único de recursos (URL), la lista de versiones de aplicaciones, la lista de versiones (es), el mecanismo de implementación y la fecha de retirada. Revise y actualice el inventario de software cada dos años o con mayor frecuencia.
	Asegúrese de que el software autorizado sea compatible actualmente	Asegúrese de que solo el software compatible actualmente esté designado como autorizado en el inventario de software para activos empresariales. Si el software no es compatible, pero es necesario para el cumplimiento de la misión de la empresa, documente una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software no compatible sin una documentación de excepción, designe como no autorizado. Revise la lista de software para verificar la compatibilidad del software al menos una vez al mes o con más frecuencia.
	Establecer y mantener un proceso de gestión de datos	Establezca y mantenga un proceso de gestión de datos. En el proceso, aborde la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, los flujos de retención de datos y los requisitos de eliminación, según los estándares de sensibilidad y retención de la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.
	Establecer y mantener un inventario de sistemas de autenticación y autorización	Establezca y mantenga un inventario de los sistemas de autenticación y autorización de la empresa, incluidos los aliados en el sitio o en un proveedor de servicios remoto. Revise y actualice el inventario, como mínimo, anualmente o con mayor frecuencia.
	Realice análisis automatizados de vulnerabilidades de los activos internos de la empresa	Realice escaneos automatizados de vulnerabilidades de los activos internos de la empresa de forma trimestral o con mayor frecuencia. Realice análisis automatizados y no automatizados, utilizando una herramienta de análisis de vulnerabilidades compatible con SCAP.
	Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente	Realice escaneos automatizados de vulnerabilidades de activos empresariales expuestos externamente utilizando una herramienta de escaneo de vulnerabilidades compatible con SCAP. Realice exploraciones manuales o con mayor frecuencia.
	Realice pruebas periódicas de penetración externa	Realice pruebas de penetración externas periódicas basadas en los requisitos del programa, no menos de una vez al año. Las pruebas de penetración externas deben incluir reconocimiento empresarial y ambiental para detectar información explotable. Las pruebas de penetración requieren habilidades y experiencia especializadas y deben realizarse a través de una parte calificada. La prueba puede ser caja transparente o caja opaca.
	Bibliotecas autorizadas de lista de permisos	Utilice controles técnicos para asegurarse de que solo las bibliotecas de software autorizadas, como archivos específicos .dll, .ocx, .so, etc., puedan cargarse en un proceso del sistema. Bloquee la carga de bibliotecas no autorizadas en un proceso del sistema. Vuelva a evaluar dos veces al año o con más frecuencia.
	Scripts autorizados de lista de permisos	Utilice controles técnicos, como firmas digitales y control de versiones, para asegurarse de que solo se permita la ejecución de scripts autorizados, como archivos específicos .ps1, .py, etc. Bloquee la ejecución de scripts no autorizados. Vuelva a evaluar dos veces al año o con más frecuencia.
	Configurar listas de control de acceso a datos	Configure listas de control de acceso a datos según la necesidad de conocimiento del usuario. Aplique listas de control de acceso a datos, también conocidas como permisos de acceso, a sistemas de archivos, bases de datos y aplicaciones locales y remotas.
Hacer cumplir la retención de datos	Conserve los datos de acuerdo con el proceso de gestión de datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.	
Eliminar los datos de forma segura	Deseste los datos de forma segura como se describe en el proceso de gestión de datos de la empresa. Asegúrese de que el proceso y el método de eliminación sean adecuados con la confidencialidad de los datos.	
Cifrar datos confidenciales en reposo	Cifre los datos confidenciales en reposo en servidores, aplicaciones y bases de datos que contienen datos confidenciales. El cifrado de la capa de almacenamiento, también conocido como cifrado del lado del servidor, cumple con el requisito mínimo de esta protección. Los métodos de cifrado adicionales pueden incluir el cifrado de la capa de aplicación, también conocido como cifrado del lado del cliente, donde el acceso a los dispositivos de almacenamiento de datos no permite el acceso a los datos de texto en formato.	
Procesamiento y almacenamiento de datos de segmentos según la sensibilidad	Segmente el procesamiento y almacenamiento de datos en función de la sensibilidad de los datos. No procese datos confidenciales en activos empresariales destinados a datos de menor confidencialidad.	
Implementar una solución de prevención de pérdida de datos	Implemente una herramienta automatizada, como una herramienta de prevención de pérdida de datos (DLP) basada en host para identificar todos los datos confidenciales almacenados, procesados o transmitidos a través de los activos de la empresa, incluidos los que se encuentran en el sitio o en un proveedor de servicios remoto, y actualizar los datos confidenciales de la empresa. Inventario.	
Establecer y mantener un proceso de configuración seguro	Establezca y mantenga un proceso de configuración seguro para los activos de la empresa (dispositivos de usuario final, incluidos servidores y dispositivos portátiles y móviles, no informáticos (IoT) y software (sistemas operativos y aplicaciones). Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	
Configurar el bloqueo automático de sesiones en activos empresariales	Configure el bloqueo automático de sesiones en los activos de la empresa después de un periodo definido de inactividad. Para los sistemas operativos de propósito general, el periodo no debe exceder los 15 minutos. Para dispositivos móviles de usuario final, el periodo no debe exceder los 2 minutos.	
Gestione de forma segura los activos y el software de la empresa	Administre de forma segura los activos y el software de la empresa. Las implementaciones de ejemplo incluyen la gestión de la configuración a través de una infraestructura controlada por versiones como código y el acceso a interfaces administrativas a través de protocolos de red seguros, como Secure Shell (SSH) y Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de administración inseguros, como Telnet (red de texto) o HTTP, a menos que sean operativamente esenciales.	
Administrar cuentas predeterminadas en activos y software empresariales	Administre cuentas predeterminadas en activos y software de la empresa, como root, administrador y otras cuentas de proveedores predeterminadas. Las implementaciones de ejemplo incluyen deshabilitar cuentas predeterminadas y inutilizarlas.	
Utilice contraseñas únicas	Utilice contraseñas únicas para todos los activos de la empresa. La implementación de las mejores prácticas incluye, como mínimo, una contraseña de 8 caracteres para las cuentas que usan MFA y una contraseña de 14 caracteres para las cuentas que no usan MFA.	
Restringir los privilegios de administrador a cuentas de administrador dedicadas	Restrinja los privilegios de administrador a las cuentas de administrador dedicadas en los activos de la empresa. Lleve a cabo actividades informáticas generales, como navegación por internet, como electrónico y uso de la suite de productividad, desde la cuenta principal no privilegiada del usuario.	
Centralizar la gestión de cuentas	Centralice la gestión de cuentas a través de un directorio o servicio de identidades.	
Establecer un proceso de concesión de acceso	Establezca y siga un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa ante una nueva contratación, concesión de derechos o cambio de rol de un usuario.	
Establecer un proceso de revocación de acceso	Establezca y siga un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación o revocación de derechos o cambio de rol de un usuario. Es posible que sea necesario deshabilitar cuentas, en lugar de eliminar cuentas, para conservar las pistas de auditoría.	
Centralizar el control de acceso	Centralice el control de acceso para todos los activos de la empresa a través de un servicio de directorio o proveedor de SSO, donde sea compatible.	
Definir y mantener el control de acceso basado en roles	Definir y mantener el control de acceso basado en roles, a través de la determinación y documentación de los derechos de acceso necesarios para que cada rol dentro de la empresa lleve a cabo con éxito sus tareas asignadas. Realice revisiones de control de acceso de los activos de la empresa para validar que todos los privilegios estén autorizados, de forma periódica, como mínimo una vez al año, o con mayor frecuencia.	
Proteger (PR)	Establecer y mantener un proceso de gestión de vulnerabilidades	Establezca y mantenga un proceso de gestión de vulnerabilidades documentado para los activos de la empresa. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.
	Realice una gestión automatizada de parches de aplicaciones	Realice actualizaciones de aplicaciones en los activos de la empresa a través de la gestión automatizada de parches de forma mensual o con mayor frecuencia.
	Establecer y mantener un proceso de gestión de registros de auditoría	Establezca y mantenga un proceso de gestión de registros de auditoría que defina los requisitos de registro de la empresa. Como mínimo, aborde la recolección, revisión y retención de registros de auditoría para activos empresariales. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.
	Garantizar un almacenamiento adecuado del registro de auditoría de la empresa	Asegúrese de que los destinos de registro mantengan un almacenamiento adecuado para cumplir con el proceso de gestión de registros de auditoría de la empresa.
	Estandarizar la sincronización horaria	Estandarice la sincronización horaria. Configure al menos dos fuentes de tiempo sincronizadas en los activos de la empresa, donde sea compatible.
	Conservar registros de auditoría	Conserve los registros de auditoría de los activos de la empresa durante un mínimo de 90 días.
	Proteja los datos de recuperación	Proteja los datos de recuperación con controles equivalentes a los datos originales. Cifrado de referencia o separación de datos, según los requisitos.
	Asegúrese de que la infraestructura de red esté actualizada	Asegúrese de que la infraestructura de red se mantenga actualizada. Las implementaciones de ejemplo incluyen la ejecución de la última versión estable de software y / o el uso de ofertas de red como servicio (RaaS) admitidas actualmente. Revise las versiones de software mensualmente, o con más frecuencia, para verificar la compatibilidad del software.
	Establecer y mantener una arquitectura de red segura	Establezca y mantenga una arquitectura de red segura. Una arquitectura de red segura debe abordar la segmentación, los privilegios mínimos y la disponibilidad, como mínimo.
	Gestione de forma segura la infraestructura de red	Gestione de forma segura la infraestructura de red. Las implementaciones de ejemplo incluyen infraestructura de versión controlada como código y el uso de protocolos de red seguros, como SSH y HTTPS.
Centralice la autenticación, autorización y auditoría de la red (AAA)	Centralizar la red AAA.	
Uso de protocolos de comunicación y administración de red seguros	Utilice protocolos de comunicación y administración de red seguros (por ejemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise o superior).	
Realizar el filtrado de la capa de aplicación	Realice el filtrado de la capa de aplicación. Las implementaciones de ejemplo incluyen un proxy de filtrado, un firewall de la capa de aplicación o una puerta de enlace.	
Establecer y mantener un proceso para aceptar y abordar las vulnerabilidades del software	Establezca y mantenga un proceso para aceptar y abordar los informes de vulnerabilidades de software. Incluya la provisión de un medio para que las entidades externas informen. El proceso debe incluir elementos tales como: una política de manejo de vulnerabilidades que identifique el proceso de informes, la parte responsable de manejar los informes de vulnerabilidades y un proceso para la admisión, asignación, remediación y pruebas de remediación. Como parte del proceso, utilice un sistema de seguimiento de vulnerabilidades que incluya calificaciones de gravedad y métricas para medir el tiempo de identificación, análisis y corrección de vulnerabilidades. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	
Realice un análisis de la causa raíz de las vulnerabilidades de seguridad	Realice un análisis de la causa raíz de las vulnerabilidades de seguridad. Al revisar las vulnerabilidades, el análisis de la causa raíz es el área de evaluar los problemas subyacentes que crean vulnerabilidades en el código, y permite a los equipos de desarrollo ir más allá de simplemente corregir las vulnerabilidades individuales a medida que surgen.	
Utilice componentes de software de terceros actualizados y confiables	Utilice componentes de software de terceros actualizados y confiables. Cuando sea posible, elija bibliotecas y marcos establecidos y probados que brinden la seguridad adecuada. Adquiera estos componentes de fuentes confiables o evalúe el software en busca de vulnerabilidades antes de usarlo.	
Establecer y mantener un sistema y proceso de clasificación de gravedad para las vulnerabilidades de las aplicaciones	Establezca y mantenga un sistema de clasificación de gravedad y un proceso para las vulnerabilidades de las aplicaciones que facilite la priorización del orden en que se corrigen las vulnerabilidades descubiertas. Este proceso incluye establecer un nivel mínimo de aceptabilidad de seguridad para la liberación de códigos o aplicaciones. Las clasificaciones de gravedad brindan una forma sistemática de clasificar las vulnerabilidades que mejora la gestión de riesgos y ayuda a garantizar que los errores más graves se solucionen primero. Revise y actualice el sistema y el proceso anualmente.	
Sistemas separados de producción y no producción	Mantenga entornos separados para sistemas de producción y no producción.	
Capacitar a los desarrolladores en conceptos de seguridad de aplicaciones y codificación segura	Asegúrese de que todo el personal de desarrollo de software reciba capacitación en la escritura de código seguro para su entorno de desarrollo y responsabilidades específicas. La capacitación puede incluir principios generales de seguridad y prácticas estándar de seguridad de aplicaciones. Realice capacitación al menos una vez al año y diseñe de manera que promueva la seguridad dentro del equipo de desarrollo y cree una cultura de seguridad entre los desarrolladores.	
Aplicar principios de diseño seguro en arquitecturas de aplicaciones	Aplique principios de diseño seguro en arquitecturas de aplicaciones. Los principios de diseño seguro incluyen el concepto de privilegio mínimo y la aplicación de la mediación para validar cada operación que realiza el usuario, promoviendo el concepto de "nunca confiar en la entrada del usuario". Los ejemplos incluyen asegurarse de que se realice y documente la verificación explícita de errores para todas las entradas, incluido el tamaño, el tipo de datos y los rangos o formatos aceptables. El diseño seguro también significa minimizar la superficie de ataque de la infraestructura de aplicaciones, como apagar puertos y servicios desprotegidos, eliminar programas y archivos innecesarios y cambiar el nombre o eliminar cuentas predeterminadas.	

Aproveche los módulos o servicios examinados para los componentes de seguridad de las aplicaciones	Aproveche los módulos o servicios examinados para los componentes de seguridad de las aplicaciones, como la administración de identidades, el cifrado y la auditoría y el registro. El uso de características de la plataforma en funciones de seguridad críticas reducirá la carga de trabajo de los desarrolladores y minimizará la probabilidad de errores de diseño o implementación. Los sistemas operativos modernos proporcionan mecanismos efectivos para la identificación, autenticación y autorización y ponen esos mecanismos a disposición de las aplicaciones. Utilice solo algoritmos de cifrado estandarizados, actualmente aceptados y ampliamente revisados. Los sistemas operativos también proporcionan mecanismos para crear y mantener registros de auditoría seguros.
Implementar verificaciones de seguridad a nivel de código	Aplicar herramientas de análisis estáticas y dinámicas dentro del ciclo de vida de la aplicación para verificar que se sigan las prácticas de codificación segura.
Realizar pruebas de penetración de aplicaciones	Realice pruebas de penetración de aplicaciones. Para aplicaciones críticas, las pruebas de penetración automatizadas son más adecuadas para encontrar vulnerabilidades de lógica empresarial que el escaneo de código y las pruebas de seguridad automatizadas. Las pruebas de penetración se basan en la habilidad del evaluador para manipular manualmente una aplicación como un usuario autenticado y no autenticado.
Realización de modelos de amenazas	Realice modelos de amenazas. El modelado de amenazas es el proceso de identificar y abordar las fallas de diseño de seguridad de las aplicaciones dentro de un diseño, antes de que se cree el código. Se lleva a cabo a través de personas especialmente capacitadas que evalúan el diseño de la aplicación y miden los riesgos de seguridad para cada punto de entrada y nivel de acceso. El objetivo es mapear la aplicación, la arquitectura y la infraestructura de una manera estructurada para comprender sus debilidades.
Remediar los resultados de las pruebas de penetración	Responda los hallazgos de las pruebas de penetración según la política de la empresa para el alcance y la priorización de la remediación.
Validar medidas de seguridad	Valide las medidas de seguridad después de cada prueba de penetración. Si lo considera necesario, modifique los conjuntos de reglas y las capacidades para detectar las técnicas utilizadas durante las pruebas.
Utilice herramientas de inventario de software automatizadas	Utilice herramientas de inventario de software, cuando sea posible, en toda la empresa para automatizar el descubrimiento y la documentación del software instalado.
Registro de acceso a datos confidenciales	Registre el acceso a datos confidenciales, incluida la modificación y eliminación.
Recopilar registros de auditoría	Recopile registros de auditoría. Asegúrese de que el registro, según el proceso de gestión de registros de auditoría de la empresa, se haya habilitado en todos los activos de la empresa.
Recopile registros de auditoría detallados	Configure el registro de auditoría detallado para los activos empresariales que contienen datos confidenciales. Incluya el origen del evento, la fecha, el nombre de usuario, la marca de tiempo, las direcciones de origen, las direcciones de destino y otros elementos útiles que podrían ayudar en una investigación forense.
Centralizar registros de auditoría	Centralice, en la medida de lo posible, la recopilación y retención de registros de auditoría en todos los activos de la empresa.
Realizar revisiones de registros de auditoría	Realice revisiones de los registros de auditoría para detectar anomalías o eventos anómalos que podrían indicar una amenaza potencial. Realice revisiones de forma semanal o con mayor frecuencia.
Centralice las alertas de eventos de seguridad	Centralice las alertas de eventos de seguridad en los activos de la empresa para la correlación y el análisis de registros. La implementación de las mejores prácticas requiere el uso de un SIEM, que incluye alertas de correlación de eventos derivadas por el proveedor. Una plataforma de análisis de registros configurada con alertas de correlación relevantes para la seguridad también satisface esta protección.
Implemente una solución de detección de intrusiones en la red	Implemente una solución de detección de intrusiones en la red en los activos de la empresa, cuando corresponda. Las implementaciones de ejemplo incluyen el uso de un sistema de detección de intrusiones en la red (NIDS) o un servicio equivalente de proveedor de servicios en la nube (CSP).
Recopilar registros de flujo de tráfico de red	Recopile registros de flujo de tráfico de red y/o tráfico de red para revisar y alertar sobre los dispositivos de red.
Ajustar los umbrales de alerta de eventos de seguridad	Ajuste los umbrales de alerta de eventos de seguridad mensualmente o con mayor frecuencia.
Supervisar proveedores de servicios	Supervise a los proveedores de servicios de acuerdo con la política de gestión de proveedores de servicios de la empresa. El monitoreo puede incluir una reevaluación periódica del cumplimiento del proveedor de servicios, el monitoreo de las notas de la versión del proveedor de servicios y el monitoreo de la web oscura.
Deshabilitar cuentas inactivas	Elimine o deshabilite las cuentas inactivas después de un período de 45 días de inactividad, cuando sea posible.
Establecer y mantener un proceso de remediación	Establezca y mantenga una estrategia de remediación basada en riesgos documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.
Remediar las vulnerabilidades detectadas	Repare las vulnerabilidades detectadas en el software a través de procesos y herramientas de forma mensual o más frecuente, según el proceso de corrección.
Establecer y mantener un proceso de recuperación de datos	Establezca y mantenga un proceso de recuperación de datos. En el proceso, aborde el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos de respaldo. Revise y actualice la documentación anualmente, o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.
Realice copias de seguridad automatizadas	Realice copias de seguridad automatizadas de los activos empresariales incluidos en el alcance. Ejecute copias de seguridad semanalmente, o con mayor frecuencia, según la confidencialidad de los datos.
Establecer y mantener una instancia aislada de datos de recuperación	Establezca y mantenga una instancia aislada de datos de recuperación. Las implementaciones de ejemplo incluyen versiones que controlan los depósitos de respaldo a través de sistemas o servicios fuera del línea, en la nube o fuera del sitio.
Prueba de recuperación de datos	Pruebe la recuperación de copias de seguridad trimestralmente, o con mayor frecuencia, para obtener una muestra de los activos empresariales incluidos en el alcance.

Clasificación de Información y Activos Críticos

Parámetros para Tipología de Impacto	Modulador del apetito	Criterio
Servicio técnico de baja calidad y deficiente	Aversión	El compromiso de la organización es prestar un servicio técnicamente excelente que será aplicado de manera consistente.
Respuesta tardía a requerimientos y problemas de los clientes	Aversión	El plan organizacional de la empresa se centra en atender de manera inmediata todos los requerimientos y problemas que puedan surgir en el transcurso de la asesoría y ejecución.
Baja reputación empresarial	Aversión	La visión de la empresa es ser reconocida por todos los clientes como una empresa que entrega soluciones tecnológicas óptimas de manera eficiente.
Talento humano deficiente	Neutral	La misión de la organización es desarrollar talento humano para proveer soluciones tecnológicas e innovadoras con el fin de mejorar la calidad, eficiencia y productividad del sector empresarial.

Parámetros para Tipología de Impacto	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
Servicio técnico de baja calidad y deficiente	N/A	N/A	N/A	Servicio técnico con capacidad técnica básica y comparable con el mercado	Servicio técnico sin capacidad técnica consistente
Respuesta tardía a requerimientos y problemas de los clientes	N/A	N/A	Se brindó respuesta al cliente en menos de 1 hora	Se brindó respuesta al cliente entre 1 hora a 2 horas	Se brindó respuesta al cliente en más de 2 horas
Baja reputación empresarial	N/A	N/A	N/A	Ser una organización con soluciones básicas y sin ofertas de valor para los clientes	Ser una organización con soluciones sobre dimensionadas y de alta complejidad
Talento humano deficiente	N/A	N/A	N/A	Talento humano con capacidad productiva pero sin compromiso organizacional	Talento humano sin productividad, eficiencia, calidad y sin compromiso con la organización

Entidad	Nombre del tipo de información	Definición del tipo de información	Impacto Privacidad	Impacto Disponibilidad	Impacto Integridad	Impacto Confidencialidad	Calificación del tipo de información	Activo de Información
Cliente	Datos principales	Engloba la información básica del cliente o empresa cliente como: Nombres, RUC, C.I., teléfonos, correos, personas de contacto, redes sociales, apoderados legales, nominas de socios y accionistas etc.	INSIGNIFICANTE	INSIGNIFICANTE	INSIGNIFICANTE	INSIGNIFICANTE	BAJO	OneDrive_1
Cliente	Información Financiera	Se detalla la información del estado del buró de crédito, pago de impuestos, índices financieros del cliente o empresa cliente, facturación.	CATASTRÓFICO	MAYOR	MAYOR	CATASTRÓFICO	ALTO	OneDrive_1
Cliente	Información Bancaria	Se detalla las cuentas de banco, estados de cuentas, tarjetas de crédito, pólizas del cliente o empresa cliente.	CATASTRÓFICO	MAYOR	MAYOR	CATASTRÓFICO	ALTO	OneDrive_1
Cliente	Servicios	Se define como los servicios o productos que la organización presta al cliente o empresa cliente.	CATASTRÓFICO	CATASTRÓFICO	CATASTRÓFICO	CATASTRÓFICO	CRITICO	Workflow
Cliente	Core del negocio	Se define como el mercado en el que se mueve el cliente o empresa cliente.	MAYOR	MAYOR	MAYOR	CATASTRÓFICO	ALTO	Workflow
Cliente	Infraestructura tecnológica	Componentes de hardware y software habituales: instalaciones, centros de datos, servidores, sistemas de escritorio de hardware de red y soluciones de software del cliente o empresa cliente.	CATASTRÓFICO	CATASTRÓFICO	CATASTRÓFICO	CATASTRÓFICO	CRITICO	Workflow
Cliente	Ubicabilidad	Ubicación geográfica de la organización, tanto casa matriz como sus sucursales del cliente o empresa cliente.	INSIGNIFICANTE	INSIGNIFICANTE	INSIGNIFICANTE	INSIGNIFICANTE	BAJO	OneDrive_1
Cliente	Protocolos de seguridad y salud	Se define como normas, parametros o reglas que define el cliente para ingresar u operar en las instalaciones del cliente o empresa cliente.	MENOR	MODERADO	CATASTRÓFICO	MODERADO	ALTO	OneDrive_2

Empleados	Información Personal	Engloba la información básica de los empleados como: Nombres, C.I., teléfonos, correos, personas de contacto, redes sociales, familiares, etc de los empleados de la organización.	MENOR	MENOR	MENOR	MENOR	MEDIO	OneDrive_3
Empleados	Información Bancaria	Se detalla las cuentas de banco, estados de cuentas, tarjetas de crédito de los empleados de la organización.	CATASTRÓFICO	MAYOR	MAYOR	CATASTRÓFICO	ALTO	OneDrive_4
Empleados	Información de Salud	El estado de completo bienestar físico, mental y social de los empleados de la organización.	CATASTRÓFICO	MENOR	MAYOR	CATASTRÓFICO	ALTO	OneDrive_3
Empleados	Formación académica	Engloba el nivel académico, cursos, certificaciones, idiomas extranjeros, entidades educativas de los empleados de la organización.	INSIGNIFICANTE	INSIGNIFICANTE	MAYOR	INSIGNIFICANTE	BAJO	CarpetaFisica_1
Empleados	Experiencia laboral	Información del recorrido laboral, certificados de trabajo, aportaciones al IESS de los empleados de la organización.	MENOR	MENOR	MAYOR	MENOR	MEDIO	CarpetaFisica_1
Organización	Proyectos	Información de los proyectos que la organización tiene como responsabilidad de entregar a sus clientes	CATASTRÓFICO	MAYOR	CATASTRÓFICO	CATASTRÓFICO	CRITICO	Workflow
Organización	Equipo tecnologico	Información de los equipos tecnológicos (PC's, servidores, celulares, etc) de cada uno de los empleados de la organización.	CATASTRÓFICO	CATASTRÓFICO	CATASTRÓFICO	MAYOR	CRITICO	Workflow
Organización	Partners	Información de los convenios entre la organización y marcas de equipos que se ofrecen como parte del portafolio de productos y servicios	CATASTRÓFICO	MENOR	MODERADO	MODERADO	MEDIO	OneDrive_5

Organización	Estrategia Empresarial y de Negocio	Información de la planeación para mejorar y optimizar los resultados, conjunto de actividades que permitirán que la empresa alcance una ventaja competitiva	CATASTRÓFICO	MODERADO	MAYOR	CATASTRÓFICO	ALTO	OneDrive_4
Organización	Portafolio de productos y servicios	Información de los productos, servicios, capacitaciones, cursos marcas, etc. Que se ofrece a cada uno de los clientes	MAYOR	MODERADO	MAYOR	MAYOR	ALTO	OneDrive_4

-----IMPORTANTE-----

Se identifica que el activo de información mas crítico es el Workflow, ya que contiene información con impacto "Catastrófico" para los riesgos de la empresa.

Para seguir con el detalle de este activo crítico presione el siguiente enlace.

[ACTIVO CRÍTICO](#)