Plan de Seguridad y Privacidad de la Información

COMISIÓN DE REGULACIÓN DE ENERGÍA Y GAS - CREG

MAYO 2023

info@fivestrategy.com
http://www.fivestrategy.com
+57 (1) - 7053184

Tabla de contenido

1. Generalidades

La necesidad de garantizar el mejor nivel posible de seguridad de los ecosistemas tecnológicos y de comunicaciones de las organizaciones crece día a día, debido principalmente al incremento de la cantidad y la criticidad de la información que diariamente se procesa, la cual es en un amplio porcentaje sensible y confidencial. Otro factor crítico es la creciente cantidad (de manera exponencial) y sofisticación de las amenazas informáticas. Pero uno de los aspectos más críticos es la concientización de los usuarios con respecto a la criticidad de las amenazas.

En consideración de lo anterior, muchas organizaciones han hecho esfuerzos importantes para mejorar los niveles de seguridad, optimizando sus accesos a Internet y previniendo ataques generados desde el exterior o aun por usuarios internos, que por diferentes motivos pueden causar grandes pérdidas, no solo económicas sino también en otros aspectos relevantes para la operación. Sin embargo, el fenómeno de la hiperconectividad, ha hecho que las personas sean ahora uno de los blancos predilectos de los ciberdelincuentes, debido a que podrían ser el eslabón más débil de la cadena relacionada con el resguardo de la información, no sólo de los datos propios sino también los de las empresas en donde trabajan.

A nivel de diversos cuadros directivos se tiende a pensar que el tema de seguridad de la información es responsabilidad exclusiva de los departamentos TIC y del CIO. Para solucionar sus problemas de seguridad las entidades inicialmente se centraron en tener una infraestructura tecnológica (hardware y software) de protección. Las empresas evolucionaron hacia la necesidad de tener un Sistema de Gestión de Seguridad de la Información (SGSI).

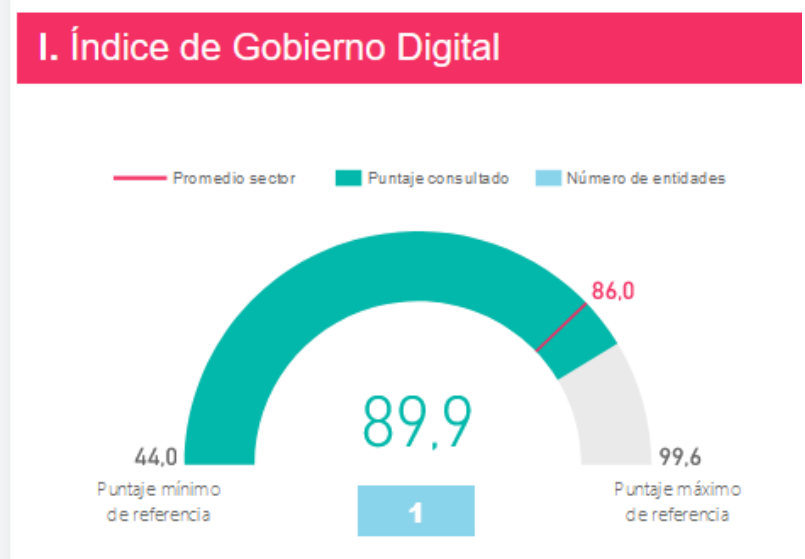
El presente plan involucra dos variables clave la seguridad de la información relacionada con la confidencialidad, integridad y disponibilidad, y dentro de esta triada se contemplan los elementos relacionados con la privacidad de la información, que parte de la identificación y clasificación de esta a fin de garantizar su protección a través del SGSI (ISMS[1]).

[1] information security management systems (ISMS)

2. Introducción

El presente documento describe el Plan de Seguridad y Privacidad de la Información para la Comisión de Regulación de Energía y Gas -CREG, es importante aquí recalcar que el plan es un desarrollo de buenas prácticas que deberían incluirse en el desarrollo del Sistema de Gestión de Seguridad de la Información SGSI de la CREG, apoyado en este momento por Five Strategy, sin embargo, es clave que sea la CREG la que aplique y desarrolle los componentes descritos en este plan de la mano de la firma consultora y de continuidad después de terminar la contratación especifica, mejorando el SGSI.

De acuerdo con las mediciones de MinTic en relación con el Gobierno Digital, que involucra componentes de seguridad de la información[2], los resultados para la entidad[3] en 2021 (última medición), son:



En donde se identifica una brecha a cerrar frente al puntaje de referencia, que es recomendable cerrar en este año.

[2] Este habilitador busca desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.
[3] https://gobiernodigital.mintic.gov.co/portal/Mediciones/

Otra medición que se realiza es el ITA (Índice de Transparencia y Acceso a la Información[4]) de la Procuraduría General de la República[5], el cual incluye elementos de seguridad y protección.

¿Qué hay de nuevo en seguridad informática? Los ataques cibernéticos son costosos, disruptivos y una amenaza creciente para las empresas, los gobiernos y la sociedad por igual.

Para abordar los desafíos globales de ciberseguridad y mejorar la confianza digital, se acaba de publicar una versión nueva y mejorada de ISO/IEC 27001. El estándar más conocido del mundo sobre gestión de la seguridad de la información que ayuda a las organizaciones a proteger sus activos de información, vital en el mundo cada vez más digital de hoy.

El cibercrimen se está volviendo cada vez más severo y sofisticado a medida que los piratas informáticos desarrollan técnicas de cibercrimen más avanzadas. El informe Global Cybersecurity Outlook del Foro Económico Mundial indica que los ataques cibernéticos aumentaron un 125% a nivel mundial en 2021. En este panorama que cambia rápidamente, los líderes deben adoptar un enfoque estratégico de los riesgos cibernéticos.

Para abordar estos desafíos de ciberseguridad, las organizaciones deben mejorar su resiliencia e implementar esfuerzos de mitigación de amenazas cibernéticas. Así es como ISO/IEC 27001:2022[6] relacionada con la Seguridad y Privacidad de la Información beneficiará a la CREG:

- Protejer la información en todas sus formas, incluidos los datos en papel, en la nube y digitales
- Aumentar la resiliencia a los ciberataques

[4] https://www.procuraduria.gov.co/Pages/ita.aspx / https://apps.procuraduria.gov.co/ita/publico/consultaMatrizDetallada/#

[5] Con la expedición de la Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”, se regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

[6] Esta tercera edición anula y sustituye a la segunda edición (ISO/IEC 27001:2013), que ha sido revisada técnicamente. También incorpora las correcciones técnicas ISO/IEC 27001:2013/Cor 1:2014 e ISO/IEC 27001:2013/Cor 2:2015.

- Proporcionar un marco administrado centralmente que protege toda la información en un solo lugar
- Garantizar la protección en toda la organización, incluso contra los riesgos basados en la tecnología y otras amenazas
- Responda a las amenazas de seguridad en evolución
- Reducir costes y gastos en tecnología de defensa ineficaz
- Proteger la integridad, confidencialidad y disponibilidad de los datos

Las organizaciones que adoptan la resiliencia cibernética a través de una vulnerabilidad segura emergen rápidamente como líderes en su industria y establecen el estándar para su ecosistema. El enfoque holístico de ISO/IEC 27001 significa que toda la organización está cubierta, no solo TI. Las personas, la tecnología y los procesos se benefician.

Cuando se utiliza ISO/IEC 27001, demuestra a las partes interesadas y a los clientes que está comprometido con la gestión segura de la información. Es una excelente manera de promover su organización, celebrar sus logros y demostrar que se puede confiar en la CREG.

Este Plan de Seguridad y Privacidad de la Información específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de la organización. Este documento también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización.

La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de seguridad de la información de una organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y la estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la **confidencialidad, integridad** y **disponibilidad** de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.

Es importante que el sistema de gestión de seguridad de la información forme parte de los procesos de la organización y la estructura general de gestión y que la seguridad de la información se tenga en cuenta en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se escale de acuerdo con las necesidades de la organización.

Es importante destacar que, para el desarrollo e implementación del plan, es necesario el compromiso de todos los responsables relacionados en el documento.

3. Objetivo General

Mejorar la Seguridad y Privacidad de la Información de la Comisión de Regulación de Energía y Gas -CREG a través del sistema de gestión de la seguridad y privacidad de la información.

4. Objetivos Específicos

- Establecer el sistema de gestión de la seguridad y privacidad de la información
- Implementar el sistema de gestión de la seguridad y privacidad de la información.
- Monitorear y revisar el sistema de gestión de la seguridad y privacidad de la información
- Mantener y mejorar el sistema de gestión de la seguridad y privacidad de la información
- Desarrollar la implementación de controles para el tratamiento del riesgo.
- Preparar al personal de la organización para identificar y manejar posibles incidentes de seguridad de la información y minimizar el impacto de estos

5. Audiencia Objetiva

Este plan está dirigido a todos los miembros de la Comisión de Regulación de Energía y Gas -CREG, incluyendo funcionarios, contratistas y colaboradores, independientemente de su posición o nivel de responsabilidad. En especial está dirigido a aquellos que manejan información confidencial y personal, a aquellos que tienen acceso a información crítica y aquellos que trabajan con tecnología.

6. Temáticas del plan

Con el propósito de instruir y sensibilizar al personal de la CREG acerca de los diversos aspectos que contempla el sistema de gestión de seguridad de la información, se tratarán, entre otros, los siguientes temas:

- **Gobernanza de la seguridad de la información (Roles, Políticas y Procedimientos):** Este tema cubrirá los roles, políticas y procedimientos de seguridad y protección de la información de la CREG.
- **Incidentes de la Seguridad de la Información:** Este tema abordará los procedimientos de respuesta a los diferentes tipos de incidentes de seguridad.
- **Riesgos:** Este tema cubrirá los diferentes tipos de riesgos, incluyendo amenazas internas y externas, y cómo estos riesgos pueden afectar a la organización.
- **Protección de Datos Personales:** Este tema cubrirá los diferentes tipos de datos personales, sensible, privada, semiprivada y pública y cómo esta información debe ser manejada y protegida. También se cubrirá las leyes y regulaciones relacionadas con la protección de datos personales, incluyendo las sanciones por violar estas regulaciones. Además, se destacará la importancia de la privacidad y la confidencialidad en la gestión de datos personales, y cómo esto afecta a la confianza y la reputación de la organización.
- **Sistema de Gestión de Seguridad de la Información:** el objetivo de este tema será asegurar la implementación del SGSI en la CREG con los elementos establecer, implementar, monitorear y revisar, y mantener y mejorar el SGSI.

7. Estrategias de comunicación

Para una efectiva comunicación en seguridad de la información se basará en el plan de sensibilización.

A través de:

- ***Presentaciones:*** Se podrán utilizar presentaciones en PowerPoint o similares para exponer los temas de seguridad de la información de manera detallada y estructurada. Estas presentaciones pueden ser impartidas por los encargados de la campaña de sensibilización, publicados en la intranet o herramientas tecnológicas.
- ***Correos electrónicos:*** Los correos electrónicos pueden ser una herramienta efectiva para compartir información y recordatorios importantes sobre seguridad de la información. Estos correos electrónicos pueden incluir consejos y prácticas de seguridad, así como noticias y actualizaciones relacionadas con la seguridad de la información.
- ***Sesiones de entrenamiento***: Las sesiones de entrenamiento pueden ser una forma más profunda y detallada de sensibilizar a los empleados sobre temas específicos de seguridad de la información. Estas sesiones pueden ser impartidas por expertos en seguridad de la información y se pueden programar en momentos específicos durante la campaña de sensibilización.

Adicionalmente se utilizará el Sharepoint como herramienta para recopilar toda la información de los temas de seguridad de la información.

8. Plan de acción y actividades

ACTIVIDAD	DURACION	COMIENZO	FIN
PLAN DE SEGURIDAD Y PRIVACIDAD CREG 2023			
Planeación el SGSI	**56 días**	**15-may-23**	**31-jul-23**
Actualizar las políticas del SGSI	10 días	15-may-23	2-jun-23
Elaborar, modificar, actualizar la documentación del SGSI	30 días	15-may-23	23-jun-23
Entregar la documentación del SGSI actualizada	1 día	26-jun-23	26-jun-23
Gestionar la aprobación de documentos SGSI	9 días	27-jun-23	07-jul-23
Comunicación de políticas, estándares, normas, procedimientos y guías de SI	17 días	07-jul-23	31-jul-23
Actualizar la matriz de cumplimiento de requisitos legales de SI	10 días	15-may-23	2-jun-23

ACTIVIDAD	DURACION	COMIENZO	FIN
Evidenciar el cumplimiento de requisitos legales de SI	10 días	15-may-23	2-jun-23
Activos de información	**50 días**	**15-may-23**	**21-jul-23**
Revisar y realizar modificaciones al instrumento matriz de activos de información del SGSI	10 días	15-may-23	26-may-23
Programación de reuniones para diligenciamiento de matriz de activos y de matriz de riesgos	5 días	29-may-23	02-jun-23
Reuniones o entrevistas para el diligenciamiento de la matriz de activos de información	15 días	05-jun-23	23-jun-23
Consolidar la matriz de activos de información del SGSI	10 días	26-jun-23	07-jul-23
Gestionar la publicación de los activos de información	10 días	10-jul-23	21-jul-23
Actualizar el índice de información pública, clasificada y reservada	10 días	10-jul-23	21-jul-23
Entrega de la matriz de activos de información	1 día	21-jul-23	21-jul-23
Gestión de Riesgos	**63 días**	**15-may-23**	**09-ago-23**
Revisar y realizar modificaciones al instrumento matriz de riesgos del SGSI	10 días	15-may-23	26-may-23
Reuniones o entrevistas para el diligenciamiento de la matriz de riesgos de la SI	15 días	05-jun-23	23-jun-23
Consolidar la matriz de riesgos del SGSI	10 días	26-jun-23	07-jul-23
Actualizar el plan de tratamiento de riesgos del SGSI	10 días	10-jul-23	21-jul-23
Entrega de la matriz de riesgos y el plan de tratamiento	5 días	03-ago-23	09-ago-23
Gestión de incidentes de seguridad de la información	**15 días**	**15-may-23**	**02-jun-23**
Actualizar el procedimiento de Gestión de incidentes en la CREG	4 días	15-may-23	26-may-23
Enviar el procedimiento de gestión de incidentes al comité de calidad	1 día	19-may-23	26-may-23
Gestionar la aprobación del procedimiento de gestión de incidentes	10 días	22-may-23	02-jun-23
Establecer y socializar el procedimiento de atención de los incidentes de seguridad escalados	10 días	19-may-23	01-jun-23
Sensibilización y capacitación para fortalecer la cultura de seguridad de la información	**141 días**	**15-may-23**	**27-nov-23**
Campaña de mayo- Pilares de la SI y Responsabilidades	13 días	15-may-23	31-may-23
Campaña de junio -Incidentes de SI	22 días	01-jun-23	30-jun-23
Campaña de julio - Políticas y procedimientos	20 días	04-jul-23	31-jul-23
Campaña de agosto- Riesgos de la SI	23 días	01-ago-23	31-ago-23
Campaña de septiembre -Protección de datos personales	21 días	01-sep-23	29-sep-23

ACTIVIDAD	DURACION	COMIENZO	FIN
Campaña de octubre - Ingeniería Social	22 días	02-oct-23	31-oct-23
Campaña de noviembre - Buenas practicas	19 días	01-nov-23	27-nov-23
Planeación del día de la seguridad de la información	3 días	01-nov-23	03-nov-23
Revisión, ajustes y aprobación del día de la seguridad de la información	3 días	07-nov-23	09-nov-23
Día de la seguridad de la información	1 día	27-nov-23	27-nov-23
Revisión de controles del SGSI	**33 días**	**10-jul-23**	**23-ago-23**
Planeación del GAP de cumplimiento de controles	10 días	10-jul-23	21-jul-23
Ejecución del GAP de cumplimiento de controles	3 días	24-jul-23	26-jul-23
Elaboración y entrega del GAP de cumplimiento de controles	5 días	27-jul-23	02-ago-23
Gestionar el plan de acción para evidenciar madurez en la implementación de los controles	15 días	27-jul-23	16-ago-23
Coordinar acciones para evaluar y probar los controles de seguridad	20 días	27-jul-23	23-ago-23
Validación en los proyectos el cumplimiento de los requerimientos del SGSI	5 días	14-ago-23	18-ago-23
Gestión de indicadores y mejora del SGSI	**122 días**	**15-may-23**	**31-oct-23**
Evaluar y definir los indicadores de desempeño y como se van a alimentar	10 días	15-may-23	26-may-23
Realización y entrega del informe de desempeño de junio	5 días	26-jun-23	30-jun-23
Realización y entrega del informe de desempeño de julio	5 días	25-jul-23	31-jul-23
Realización y entrega del informe de desempeño de agosto	5 días	25-ago-23	31-ago-23
Realización y entrega del informe de desempeño de septiembre	5 días	25-sep-23	29-sep-23
Realización y entrega del informe de desempeño de octubre	5 días	25-oct-23	31-oct-23
Evaluar las no conformidades, el estado de acciones correctivas	10 días	26-sep-23	09-oct-23
Identificar las lecciones aprendidas, registrarlas	10 días	26-sep-23	09-oct-23
Actualizar la matriz de mejora	5 días	10-oct-23	16-oct-23
Diligenciar los instrumentos de reporte de avance del SGSI y MPSI	5 días	10-oct-23	16-oct-23
Plan de continuidad del negocio	**31 días**	**10-ago-23**	**21-sep-23**
Documentar el análisis del impacto en la operación	10 días	10-ago-23	23-ago-23
Valorar los riesgos de interrupción de la operación	10 días	10-ago-23	23-ago-23
Definir la estrategia de continuidad de la operación	10 días	24-ago-23	06-sep-23
Elaborar el plan de continuidad de la operación	10 días	07-sep-23	20-sep-23

info@fivestrategy.com
http://www.fivestrategy.com
+57 (1) - 7053184

ACTIVIDAD	DURACION	COMIENZO	FIN
Entregar el plan de continuidad	1 día	21-sep-23	21-sep-23
Auditoría al SGSI	**96 días**	**15-may-23**	**25-sep-23**
Ejecución de la auditoría al proveedor de gestión documental	21 días	01-jun-23	29-jun-23
Envío del plan de auditoría a todos los interesados	1 día	01-jun-23	01-jun-23
Entrega de la documentación para auditoria	1 día	02-jun-23	02-jun-23
Estudio de la documentación	5 días	05-jun-23	09-jun-23
Reunión de inicio de la auditoría	1 día	13-jun-23	13-jun-23
ejecución del plan de auditoria	3 días	14-jun-23	16-jun-23
Elaboración de informes	4 días	20-jun-23	23-jun-23
Socialización de resultados	1 día	27-jun-23	27-jun-23
Entrega de informe de auditoría	1 día	29-jun-23	29-jun-23
Ejecución de la auditoría a los procesos de la CREG seleccionados	18 días	04-jul-23	27-jul-23
Envío del plan de auditoría a todos los interesad	1 día	04-jul-23	04-jul-23
Entrega de la documentación para auditoria	1 día	05-jul-23	05-jul-23
Estudio de la documentación	5 días	06-jul-23	12-jul-23
Reunión de inicio de la auditoría	1 día	13-jul-23	13-jul-23
ejecución del plan de auditoria	4 días	14-jul-23	19-jul-23
Elaboración de informes	3 días	21-jul-23	25-jul-23
Socialización de resultados	1 día	26-jul-23	26-jul-23
Entrega de informe de auditoría	1 día	27-jul-23	27-jul-23
Ejecución de la auditoría al proveedor de tecnología	17 días	01-sep-23	25-sep-23
Envío del plan de auditoría a todos los interesad	1 día	01-sep-23	01-sep-23
Entrega de la documentación para auditoria	1 día	04-sep-23	04-sep-23
Estudio de la documentación	4 días	05-sep-23	08-sep-23
Reunión de inicio de la auditoría	1 día	11-sep-23	11-sep-23
ejecución del plan de auditoria	4 días	12-sep-23	15-sep-23
Elaboración de informes	4 días	18-sep-23	21-sep-23
Socialización de resultados	1 día	22-sep-23	22-sep-23
Entrega de informe de auditoría	1 día	25-sep-23	25-sep-23
Protección de Datos Personales	**75 días**	**05-jun-23**	**15-sep-23**
Definir el programa de protección de datos personales	10 días	05-jun-23	16-jun-23
Establecer los controles para el programa de protección de datos personales	10 días	05-jun-23	16-jun-23
Identificar las bases de datos personales de la organización	5 días	10-jul-23	14-jul-23

ACTIVIDAD	DURACION	COMIENZO	FIN
Registrar y actualizar las bases de datos personales de la CREG ante RNBD	10 días	17-jul-23	28-jul-23
Revisar los contenidos de los contratos de transmisiones internacionales	10 días	01-ago-23	14-ago-23
Analizar las responsabilidades de los cargos de la CREG para el diseño del programa de entrenamiento	10 días	14-ago-23	25-ago-23
Diseño del programa de entrenamiento de protección de datos personales para cada cargo	10 días	15-may-23	26-may-23
Diseño de programa general de entrenamiento de datos personales	10 días	15-may-23	26-may-23
Realizar y entregar el plan de auditoría interna de protección de datos personales	15 días	29-may-23	16-jun-23
Ejercicios de Ingeniería Social	**53 días**	**15-may-23**	**26-jul-23**
Ejecución del 1er ejercicio de ingeniería social	15 días	15-may-23	02-jun-23
Ejecución de 2o ejercicio de ingeniería social	15 días	05-jun-23	23-jun-23
Ejecución de 3er ejercicio de ingeniería social	15 días	26-jun-23	14-jul-23
Elaboración de informes de ingeniería social	3 días	17-jul-23	19-jul-23
Presentación de Resultados de ejercicios de ingeniería social	1 día	20-jul-23	20-jul-23
4.12. Vulnerabilidades	**33 días**	**25-abr-23**	**08-jun-23**
Ejecución del Ethical Hacking Externo	9 días	02-may-23	12-may-23
Ejecución del Ethical Hacking Interno	6 días	12-may-23	19-may-23
Elaboración del plan de Remediación	5 días	22-may-23	26-may-23
Elaboración de Informes Técnico y Ejecutivo	4 días	26-may-23	31-may-23
Presentación de Resultados del Ethical Hacking y entrega de informes	1 día	01-jun-23	01-jun-23
Comité de Seguridad de la Información	**136 días**	**25-may-23**	**30-nov-23**
Comité No 1 - 2023	1 día	31-may-23	31-may-23
Comité No 2 - 2023	1 día	29-jun-23	29-jun-23
Comité No 3 - 2023	1 día	27-jul-23	27-jul-23
Comité No 4 - 2023	1 día	31-ago-23	31-ago-23
Comité No 5 - 2023	1 día	28-sep-23	28-sep-23
Comité No 6 - 2023	1 día	26-oct-23	26-oct-23
Comité No 7 - 2023	1 día	30-nov-23	30-nov-23

9. Recursos y Presupuesto

Para el desarrollo del presente plan, se contará con el equipo de profesionales asignado por Five Strategy, empresa contratada por la CREG para la gestión y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI). Además, la CREG podrá disponer del personal requerido para cada una de las actividades a realizar de acuerdo con las funciones de los respectivos cargos y procesos.

El personal de la CREG asignado al proyecto tendrá la responsabilidad de apoyar en la difusión y promoción de las actividades programadas, así como de colaborar en la logística de los eventos que se realicen.

Es importante destacar que los recursos humanos y tecnológicos mencionados estarán disponibles durante el periodo de tiempo establecido para la realización del plan y estarán sujetos a la disponibilidad y aprobación de la CREG

El presupuesto asignado para la gestión y mantenimiento del del Sistema de Gestión de Seguridad de la Información (SGSI) se encuentra incluido en el contrato de prestación de servicios No 1023-067 ente la Comisión de Regulación de Energía y Gas - CREG y Five Strategy Consulting Group SAS, que tiene como objeto la gestión y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

10. Monitoreo y Evaluación del Plan

El monitoreo y evaluación del Plan será realizado por Five Strategy, quien se encargará de hacer seguimiento al cumplimiento del cronograma establecido y diseñará un indicador que permita medir el avance en la ejecución del plan.

La CREG será informada del avance en las reuniones de seguimiento que se realizarán de manera mensual, donde se presentarán los resultados obtenidos, se analizará el cumplimiento de los objetivos y se identificarán las oportunidades de mejora

11. Indicadores de Desempeño

En el ámbito actual de la seguridad de la información, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se ha vuelto esencial para proteger los activos de información y garantizar la continuidad del negocio. Sin embargo, contar con un SGSI no es suficiente por sí mismo. Para evaluar su eficacia y realizar mejoras continuas, es fundamental contar con indicadores de gestión adecuados.

los indicadores de gestión en un SGSI tienen como objetivo proporcionar una guía práctica para identificar, medir y evaluar los aspectos clave del desempeño de un SGSI. Estos indicadores permiten monitorear y medir el cumplimiento de los objetivos establecidos, así como el grado de efectividad de las medidas de seguridad implementadas.

Los indicadores de desempeño en un Sistema de Seguridad de la Información se alimentan mediante la recopilación y análisis de datos provenientes de sistemas de monitoreo, auditorías, reportes de incidentes y evaluaciones de cumplimiento normativo. Estos indicadores proporcionan una visión objetiva del estado de la seguridad de la información y permiten identificar áreas de mejora y tomar acciones correctivas.

En un Sistema de Seguridad de la Información, existen varios indicadores de desempeño relevantes que permiten evaluar y monitorear la efectividad de las medidas de seguridad implementadas. Los indicadores de desempeño que se implementarán en al CREG para el segundo semestre de 2023 son:

Nombre del Indicador:	***Tiempo de respuesta ante incidentes***
Tipo de Indicador:	Gestión de incidentes
Definición:	El tiempo de respuesta ante incidentes es el intervalo de tiempo transcurrido desde el momento de detección de un incidente de seguridad de la información hasta el inicio de la respuesta y las acciones correspondientes para contener y mitigar el incidente.

Objetivo	Medir la eficacia y eficiencia del equipo de respuesta ante incidentes de seguridad en su capacidad para detectar y responder a los incidentes de manera oportuna
Fórmula	Tiempo de respuesta = Hora de detección del incidente - Hora de inicio de la respuesta
Resultado Aceptable	Menos de una hora para incidentes críticos y un tiempo de respuesta de menos de cuatro horas para incidentes de menor gravedad
Monitoreo	Permanente
Responsable de la Medición	Mesa de Ayuda

Nombre del Indicador:	***Actualización de parches de seguridad***
Tipo de Indicador:	Rendimiento operativo
Definición:	Indicador que mide la frecuencia y la efectividad con la que se aplican los parches de seguridad en los sistemas y aplicaciones de una organización. Este indicador evalúa la capacidad de la organización para mantener sus sistemas actualizados y protegidos contra vulnerabilidades conocidas.
Objetivo	Medir la frecuencia y la puntualidad con la cual se realizan las actualizaciones de parches de seguridad en los sistemas y aplicaciones de la organización.
Fórmula	Porcentaje de sistemas y aplicaciones actualizados = (Número de sistemas y aplicaciones actualizados / Total de sistemas y aplicaciones) * 100
Monitoreo	Trimestral
Resultado Aceptable	95% o superior.
Responsable de la Medición	Proveedor tecnológico

Nombre del Indicador:	***Incidentes resueltos***
Tipo de Indicador:	Gestión de incidentes
Definición:	Métrica utilizada para evaluar la eficacia del sistema de gestión de seguridad de la información de una organización en la resolución de incidentes. Este indicador mide la proporción de incidentes de seguridad que han sido adecuadamente investigados, mitigados y solucionados en relación con el total de incidentes reportados durante un período de tiempo determinado.
Objetivo	Proporcionar una medida cuantitativa del nivel de respuesta y capacidad de resolución de incidentes de seguridad en la organización. Un alto porcentaje de incidentes resueltos indica una respuesta rápida y efectiva ante las amenazas y vulnerabilidades identificadas, lo que a su vez contribuye a minimizar el impacto y riesgo asociado a los incidentes de seguridad.
Fórmula	Porcentaje de incidentes resueltos = (Número de incidentes resueltos / Total de incidentes reportados) x 100
Resultado Aceptable	95% o superior
Monitoreo	Mensual
Responsable de la Medición	Mesa de ayuda

Nombre del Indicador:	***Vulnerabilidades corregidas***
Tipo de Indicador:	Rendimiento operativo
Definición:	Métrica utilizada en un Sistema de Gestión de Seguridad de la Información (SGSI) para evaluar la efectividad de las acciones de corrección de vulnerabilidades en los sistemas y aplicaciones de una organización. Este indicador proporciona una medida cuantitativa del progreso en la corrección de vulnerabilidades, permitiendo evaluar la efectividad de las acciones implementadas para mitigar los riesgos de seguridad. Un mayor porcentaje de vulnerabilidades corregidas indica una mejor gestión de la seguridad de la información y una menor exposición a posibles brechas de seguridad.
Objetivo	Medir el porcentaje de vulnerabilidades identificadas y corregidas en relación con el total de vulnerabilidades detectadas. Proporciona una visión general del grado de mitigación de las vulnerabilidades y la eficiencia en la gestión de la seguridad de la información.
Fórmula	Porcentaje de vulnerabilidades corregidas = (Vulnerabilidades corregidas / Vulnerabilidades totales) * 100 Donde: Vulnerabilidades corregidas: Cantidad de vulnerabilidades identificadas y solucionadas en el periodo establecido. Vulnerabilidades totales: Cantidad total de vulnerabilidades detectadas durante el mismo periodo.
Monitoreo	Mensual
Resultado Aceptable	100% para vulnerabilidades críticas y altas.
Responsable de la Medición	Proveedor tecnológico

Nombre del Indicador:	***Resultados de las evaluaciones de conocimiento***
Tipo de Indicador:	Concientización y capacitación
Definición:	Métrica para medir el nivel de conocimiento y comprensión de los funcionarios y contratistas en cuanto a las políticas, procedimientos y buenas prácticas de seguridad de la información en la organización. A través de evaluaciones periódicas, se evalúa el grado de familiaridad de los empleados con los principios y prácticas de seguridad de la información. Un resultado positivo indica que los empleados han asimilado adecuadamente las políticas y prácticas de seguridad, lo que contribuye a reducir el riesgo de incidentes de seguridad y promover una cultura de seguridad en la organización. Además, los resultados de las evaluaciones pueden servir como base para identificar áreas de mejora en la formación y concienciación en seguridad de la información.
Objetivo	Medir el grado de conocimiento y comprensión que tienen los empleados sobre las políticas y prácticas de seguridad de la información en la organización.
Fórmula	(Resultado total de respuestas correctas / Total de preguntas evaluadas) x 100
Monitoreo	Semestral
Resultado Aceptable	El resultado mínimo aceptable puede definirse como un porcentaje específico de respuestas correctas, como el 80% o superior
Responsable de la Medición	Oficial de seguridad de la información

Nombre del Indicador:	***Porcentaje de empleados que han completado la formación en seguridad***
Tipo de Indicador:	Concientización y capacitación
Definición:	Métrica utilizada para medir la participación y el grado de cumplimiento de los funcionarios y contratistas en la formación relacionada con la seguridad de la información. La formación puede incluir talleres, seminarios, sesiones de capacitación u otras actividades diseñadas para mejorar la conciencia y las habilidades de los empleados en cuanto a la seguridad de la información.
Objetivo	Medir el nivel de participación de los funcionarios y contratistas en la formación en seguridad, lo que a su vez puede indicar el nivel general de conciencia y conocimiento de la seguridad de la información en la organización. Un alto porcentaje de funcionarios y contratistas que han completado la formación puede ser indicativo de un compromiso sólido con la seguridad de la información y una mayor preparación para hacer frente a posibles riesgos y amenazas.
Fórmula	Porcentaje de funcionarios y contratistas que han completado la formación en seguridad = (Número de funcionarios y contratistas que han completado la formación / Total de funcionarios y contratistas) x 100
Monitoreo	Mensual
Resultado Aceptable	75% o superior
Responsable de la Medición	Oficial de seguridad de la información

Nombre del Indicador:	***Porcentaje de empleados que han completado la formación en seguridad***
Tipo de Indicador:	Concientización y capacitación
Definición:	Métrica utilizada para medir la participación y el grado de cumplimiento de los funcionarios y contratistas en la formación relacionada con la seguridad de la información. La formación puede incluir talleres, seminarios, sesiones de capacitación u otras actividades diseñadas para mejorar la conciencia y las habilidades de los empleados en cuanto a la seguridad de la información.
Objetivo	Medir el nivel de participación de los funcionarios y contratistas en la formación en seguridad, lo que a su vez puede indicar el nivel general de conciencia y conocimiento de la seguridad de la información en la organización. Un alto porcentaje de funcionarios y contratistas que han completado la formación puede ser indicativo de un compromiso sólido con la seguridad de la información y una mayor preparación para hacer frente a posibles riesgos y amenazas.
Fórmula	Porcentaje de funcionarios y contratistas que han completado la formación en seguridad = (Número de funcionarios y contratistas que han completado la formación / Total de funcionarios y contratistas) x 100
Monitoreo	Mensual
Resultado Aceptable	75% o superior
Responsable de la Medición	Oficial de seguridad de la información

Durante el mes de junio de 2023, se realizará la evaluación y cálculo inicial de los resultados de los indicadores de gestión establecidos dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI).

Durante el comité de seguridad de la información se evaluará si los valores alcanzados se encuentran dentro de los parámetros definidos como aceptables y se identificarán aquellos indicadores que no cumplen con los objetivos establecidos. A partir de esta evaluación, se tomarán acciones de mejora con el objetivo de optimizar el desempeño del SGSI.

El proceso de evaluación y mejora continua de los indicadores de gestión en el SGSI es esencial para mantener un nivel óptimo de seguridad de la información y garantizar la protección de los activos de la organización. Al tomar acciones concretas y definir valores aceptables, se fortalecerá el sistema de seguridad, se mitigarán riesgos y se fomentará una cultura de seguridad en toda la organización.

12. Mejora continua del plan

Para garantizar la efectividad del plan, se debe realizar una revisión y mejora constante del mismo. La CREG y Five Strategy se comprometen a realizar una evaluación periódica del plan con el fin de identificar posibles debilidades y oportunidades de mejora que permitan fortalecer la implementación del SGSI.

Durante la evaluación se analizarán los resultados obtenidos en cada una de las actividades realizadas y se tomarán en cuenta las sugerencias y observaciones recibidas por parte del personal de la entidad. Además, se tendrán en cuenta los avances tecnológicos, la normativa vigente y las nuevas amenazas o vulnerabilidades que puedan surgir, así como los indicadores y métricas del SGSI.

Con base en los resultados de la evaluación, se propondrán ajustes y mejoras pertinentes al plan, con el fin de asegurar su actualización y su alineación con las necesidades y objetivos de la entidad. Estos ajustes y mejoras se documentarán y se incorporarán al plan, para garantizar que la implementación del SGSI se mantenga actualizada y eficaz en todo momento.