Plan Anual de Sensibilización

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 un 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 en 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. Fortalecer este eslabón es una tarea vital en las organizaciones.

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).

Desafortunadamente el mitigar el riesgo al que está expuesta la organización solo se logra, cuando se toma conciencia de que las personas podrían ser el eslabón más débil de la cadena en temas de seguridad. La tecnología sin lugar a duda ha proporcionado herramientas para incrementar la productividad, pero también ha evolucionado a actividades amenas asociadas con interacción social digital. Esta interacción social es una atractiva fuente de opciones de ataque para los ciber delincuentes.

De aquí deriva la importancia de no solo comunicar, sino buscar una alternativa que garantice maximizar la posibilidad de concientizar sobre la importancia de cumplir a cabalidad con lo estipulado en el SGSI. Para ello tenemos la firme convicción en que se debe buscar un proceso en el que uno de los elementos rompe con el orden que nuestro cerebro establece para hacer previsible la transmisión de mensajes. Tenemos la firme convicción que, para lograr objetivos superiores, debemos salir del convencionalismo y llamar la atención.

2. Introducción

El presente documento describe el plan de sensibilización y concientización en seguridad de la información para la Comisión De Regulación De Energía y Gas -CREG

Este plan tiene como objetivo comunicar, sensibilizar y capacitar a los funcionarios, contratistas y proveedores de la institución sobre el Sistema de Gestión de Seguridad de la Información (SGSI), y se han diseñado diversas actividades a llevar a cabo en el año 2023

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

El contenido de las campañas de sensibilización en seguridad de la información, incluyendo materiales como boletines, presentaciones, videos y otros recursos, serán generados por Five Strategy. Cada uno de estos recursos será cuidadosamente diseñado y estará perfectamente alineado a la imagen corporativa de la Comisión de Regulación de Energía y Gas (CREG), con el fin de garantizar un mensaje coherente y consistente en todas las comunicaciones

No obstante, es importante destacar que la responsabilidad de compartir estos recursos de manera oportuna y efectiva ya sea a través del correo electrónico, la página web de la CREG, la intranet o las redes sociales, será completamente de la propia CREG. Por tanto, se requiere del compromiso y la diligencia de los responsables de la implementación del plan de sensibilización para asegurar que el material llegue a la audiencia adecuada en el momento adecuado, y así lograr el impacto deseado en la organización

3. Objetivo General

Mejorar la cultura de seguridad en la organización y concienciar a los empleados y colaboradores sobre la importancia de proteger la información de la Comisión De Regulación De Energía y Gas -CREG

4. Objetivos Específicos

Fomentar una cultura de seguridad de la información en la CREG, donde los funcionarios y los contratistas tomen en serio la protección de los activos de información de la organización.

Mantener informadas al personal de la organización sobre las amenazas de seguridad de la información y cómo pueden protegerse ellos mismos y la organización de ellas.

Garantizar que tanto los funcionarios como contratistas de la CREG tenga un conocimiento sólido de la política de seguridad de la información y cómo aplicarla en su trabajo diario.

Aumentar la conciencia del personal de la CREG sobre la importancia de proteger la información confidencial y personal de los clientes, proveedores y colaboradores

Fomentar el uso de buenas prácticas de seguridad de la información, como contraseñas seguras, autenticación de dos factores y actualización de software.

Evaluar el éxito de la campaña de sensibilización en seguridad de la información.

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 anual de sensibilización en seguridad de la información 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 financiera y estratégica de la organización y aquellos que trabajan con sistemas y redes de información.

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:

Pilares de la Seguridad de la Información y Responsabilidades: Este tema cubrirá los pilares de la seguridad de la información, es decir, la confidencialidad, integridad y disponibilidad, y cómo se aplican a los datos de la organización. Además, se abordarán las responsabilidades que tienen los funcionarios o colaboradores en la protección de la información de la organización, incluyendo cómo manejar la información confidencial, cómo proteger sus contraseñas y credenciales, y la aplicación de buenas prácticas en este tema.

Incidentes de la Seguridad de la Información: Este tema abordará los diferentes tipos de incidentes de seguridad, cómo reconocerlos y cómo responder ante ellos. También se destacará la importancia de reportar cualquier incidente de seguridad o sospecha de violación de datos de inmediato, y cómo hacerlo de manera efectiva.

Políticas y Procedimientos: Este tema cubrirá las políticas y procedimientos de seguridad de la información de la CREG, y cómo los funcionarios y contratistas pueden cumplir con ellos para garantizar la seguridad de la información.

Riesgos: Este tema cubrirá los diferentes tipos de riesgos, incluyendo amenazas internas y externas, y cómo estos riesgos pueden afectar a la organización. Además, se discutirán las mejores prácticas para identificar y mitigar los riesgos en la seguridad de la información.

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.

Dispositivos móviles y teletrabajo: Este tema abordará cómo los empleados pueden trabajar de manera segura con dispositivos móviles y en entornos de teletrabajo, incluyendo cómo proteger los datos de la organización mientras se trabaja fuera de la oficina

Sistema de Gestión de Seguridad de la Información: el objetivo de este tema será asegurarse de que los funcionarios comprendan los conceptos básicos de un sistema de gestión de seguridad de la información y su relevancia para la organización en su conjunto.

Este tema cubrirá los diferentes aspectos del sistema de gestión de seguridad de la información, los funcionarios aprenderán sobre los requisitos de los estándares de seguridad de la información, como la norma ISO 27001, y cómo estos estándares pueden ayudar a garantizar la seguridad de la información en la organización

Día de la seguridad de la información: En consideración a que el eslabón más débil en la cadena de la seguridad de información somos las personas, para el día de la seguridad de la información proponemos una experiencia vivencial. En ella se realizarán etapas en la que inicialmente se evalué que tan preparadas se encuentran los funcionarios en temas de seguridad de la información y como responden a las continuas técnicas que utilizan los delincuentes informáticos, se propone iniciar la campaña con la ejecución de ejercicios de ingeniería social para reforzar todo lo que se debe tener en cuenta de una manera disruptiva, pero con un lenguaje sencillo y que genere recordación.

7. Estrategias de comunicación

Para una efectiva sensibilización en seguridad de la información se pueden utilizar diversos formatos que permitan llegar al personal de una organización de manera clara y concisa.

Se realizarán las actividades de sensibilización y capacitación teniendo en cuenta las siguientes estrategias de comunicación:

- Banner.
- Intranet
- Teams
- Correo Institucional masivo
- Carteleras digitales
- Capacitación

En el marco del plan de sensibilización en seguridad de la información para la CREG, se han identificado diferentes formatos que serán utilizados para alcanzar los objetivos de la campaña.

Los formatos seleccionados incluyen presentaciones, videos, carteles, juegos, correos electrónicos y sesiones de entrenamiento. Cada uno de estos formatos tiene una función específica y serán utilizados de manera efectiva para comunicar los mensajes clave de seguridad de la información al público objetivo. Además, se considerará la adaptación de los formatos a los diferentes perfiles y necesidades de los empleados, de manera que la información sea transmitida de manera clara y efectiva. Se espera que la combinación de estos formatos ayude a aumentar la conciencia y el conocimiento en seguridad de la información y fomentar una cultura de seguridad en la organización.

Los formatos de sensibilización que se utilizarán durante las campañas de seguridad de la información serán los siguientes:

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.

Videos: Los videos son una excelente forma de hacer que los mensajes de seguridad de la información sean más atractivos y entretenidos. Se pueden crear videos animados, explicativos o de simulación de situaciones de riesgo. Los videos se pueden compartir a través de la intranet, correo electrónico o redes sociales internas

Carteles: Los carteles serán colocados en lugares visibles como pasillos, salas de reuniones, etc, y ayudan a reforzar los mensajes de seguridad de la información. Los carteles pueden incluir imágenes y mensajes impactantes y directos que llamen la atención de los funcionarios.

Juegos: Los juegos pueden ser una forma divertida y efectiva de sensibilizar a los empleados sobre los riesgos de seguridad de la información. Los juegos pueden incluir preguntas de seguridad de la información o simulaciones de situaciones de riesgo

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.

La información compartida y las sesiones de entrenamiento se realizarán de modalidad virtual, permitiendo que tanto los funcionarios y contratistas que se encuentran laborando en trabajo remoto como aquellos que están en modalidad presencial, tengan acceso a la información o puedan asistir a la sesión programada.

Adicionalmente se utilizará el sharepoint como herramienta para recopilar toda la información de los temas de seguridad de la información. Allí se las noticias, eventos, tips, concursos, actividades, resultados de auditorías internas realizadas sobre el SGSI, etc.

8. Plan de acción y actividades

Campaña	Periodo	Tema	Objetivo	Estrategia de comunicación	Formato	Público Objetivo
Campaña Mes de mayo	15-may-23 al 19-may-23	Sistema de Gestión de Seguridad de la Información	Evaluar la campaña de sensibilización de seguridad de la Información.	Correo Institucional	Juego Kahoot	Todos los funcionarios y contratistas.
	15-may-23 al 19-may-23	Sistema de Gestión de Seguridad de la Información	Dar a conocer el oficial de seguridad del CREG	Correo Institucional	Boletín	Todos los funcionarios y contratistas.
	26-may-23	Pilares de SI y Responsabilidades	Fomentar una cultura de seguridad de la información en la CREG	Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.
Campaña Mes de junio	05-jun-23 al 09-jun-23	Incidentes de la Seguridad de la Información	• Fomentar una cultura de SI en la CREG. • Preparar al personal de la organización para identificar y manejar posibles incidentes de SI. • Mantener informadas al personal sobre las amenazas de SI y cómo pueden protegerse.	Banner en la intranet	Imagen Jpeg o png	Todos los funcionarios y contratistas.
	30-jun-23	• Pilares de SI y Responsabilidades. • Incidentes de la Seguridad de la Información		Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.
Campaña Mes de julio	04-jul-23 al 07-jul-23	Políticas y Procedimientos:	• Garantizar que tanto los funcionarios como contratistas de la CREG tenga un	Correo Institucional	Boletín	Todos los funcionarios y contratistas.

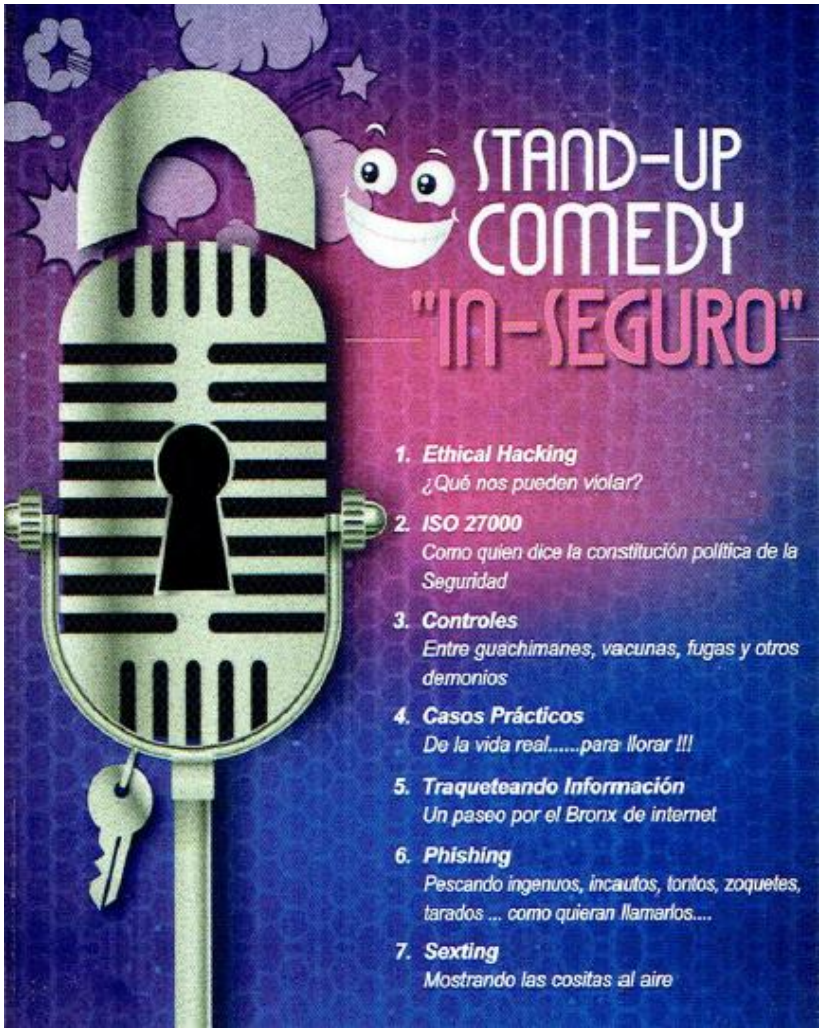
Campaña	Periodo	Tema	Objetivo	Estrategia de comunicación	Formato	Público Objetivo
	28-jul-23		conocimiento sólido de la política de SI y cómo aplicarla en su trabajo diario • Aumentar la conciencia del personal de la CREG sobre la importancia de proteger la información confidencial y personal de los clientes, proveedores y colaboradores.	Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.
Campaña Mes de agosto	08-ago-23 al 11-ago-23	Riesgos	• Mantener informadas al personal sobre las amenazas de SI y cómo pueden protegerse. • Preparar al personal de la organización para identificar y manejar posibles riesgos de SI.	Correo Institucional	Video	Todos los funcionarios y contratistas.
	25-ago-23			Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.
Campaña Mes de septiembre	04-sep-23 al 08-sep-23	Protección de Datos Personales:	• Aumentar la conciencia del personal de la CREG sobre la importancia de proteger la información confidencial y personal de los clientes, proveedores y colaboradores. • Fomentar una cultura de seguridad de la información en la CREG.	Correo Institucional	Presentación	Todos los funcionarios y contratistas.
	29-sep-23			Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.
Campaña Mes de octubre	09-oct-23 al 13-oct-23l	Dispositivos móviles y teletrabajo:	• Garantizar que tanto los funcionarios como contratistas de la CREG tenga un conocimiento sólido de la política de seguridad de la información y cómo aplicarla en su trabajo diario. • Fomentar una cultura de seguridad de la información en la CREG, donde los funcionarios y los contratistas tomen en	Correo Institucional	Video	Todos los funcionarios y contratistas.
	27-oct-23			Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.

Campaña	Periodo	Tema	Objetivo	Estrategia de comunicación	Formato	Público Objetivo
			serio la protección de los activos de información de la organización.			
Campaña Mes de noviembre	07-nov-23 al 10-nov-23	Sistema de Gestión de Seguridad de la Información	Fomentar una cultura de seguridad de la información en la CREG	Correo Institucional	Boletin	Todos los funcionarios y contratistas.
			Evaluar periódicamente el éxito de la campaña de sensibilización en	Correo Institucional	Juego Kahoot	Todos los funcionarios y contratistas.
	24/nov/23		• Garantizar que tanto los funcionarios como contratistas de la CREG tenga un conocimiento sólido de la política de seguridad de la información y cómo aplicarla en su trabajo diario.	Capacitación	Sesión de entrenamiento virtual	Todos los funcionarios y contratistas.
Día de la seguridad de la información	27-Nov-23		• Garantizar que tanto los funcionarios como contratistas de la CREG tenga un conocimiento sólido de la política de seguridad de la información y cómo aplicarla en su trabajo diario. • Aumentar la conciencia del personal de la CREG sobre la importancia de proteger la información confidencial y personal de los clientes, proveedores y colaboradores. • Fomentar el uso de buenas prácticas de seguridad de la información, como contraseñas seguras, autenticación de dos factores y actualización de software. • Preparar al personal de la organización para identificar y manejar posibles incidentes de seguridad de la información y minimizar el impacto de estos.	Capacitación	Sesión de stand up Comedy	Todos los funcionarios y contratistas.

Campaña	Periodo	Tema	Objetivo	Estrategia de comunicación	Formato	Público Objetivo
			• Reconocer el buen trabajo y cumplimiento de las políticas en la seguridad de la información.	Premiación al funcionario seguro	Sesión Stand up Comnedy	Todos los funcionarios y contratistas.
			Presentar de las estadísticas de los comparendos de seguridad y la asistencia a la jornada pedagógica Presentación de los resultados del ejercicio de ingeniería social		Cartelera Sesión Stand up Comnedy	Todos los funcionarios y contratistas. Todos los funcionarios y contratistas

9. Propuesta Día de la Seguridad de la Información

En consideración a que el eslabón más débil en la cadena de la seguridad de información somos las personas, para el día de la seguridad de la información proponemos una experiencia vivencial. En ella se realizarán etapas en la que inicialmente se evalué que tan preparadas se encuentran los funcionarios en temas de seguridad de la información y como responden a las continuas técnicas que utilizan los delincuentes informáticos, se propone iniciar con la ejecución de ejercicios de ingeniería social para reforzar todo lo que se debe tener en cuenta de una manera disruptiva, pero con un lenguaje sencillo y que genere recordación.



In-Seguro es una "Una divertida puesta en escena que hace énfasis en la importancia de entender los conceptos seudotécnicos y ante todo cotidianos del mundo a veces extraño de la seguridad de la información.

¿POR QUE UN STAND-UP COMEDY?

El uso de una estrategia disruptiva como la propuesta, se fundamenta en los estudios de varias empresas a nivel mundial han determinado que la mayoría de los empleados no tienen conciencia sobre las amenazas de seguridad más conocidas, ni en la relevancia de un SGSI. Sólo unos pocos consideran que en sus manos también está la responsabilidad de cuidar la información, mientras que un 12% cree que las medidas de seguridad frenan la innovación.

En la mayoría de los casos es la falta de conciencia y la ignorancia sobre la importancia de un SGSI, la causa de los fallos, y no la malevolencia. «Los empleados esperan que los mecanismos de seguridad implementados por la empresa se ocupen de todo, y tampoco son conscientes del verdadero peligro de las amenazas», concluye en una de sus investigaciones Cisco.

Cisco destaca un dato como sorprendente, y se trata del hecho que el 77% de los trabajadores no son conscientes de los ataques o amenazas más conocidas, a pesar de haber adelantado tareas de concientización tradicionales.

Es por esta razón que Five Strategy propone sensibilizar a los directivos, funcionarios, contratistas y proveedores de la CREG de una forma diferente. Esta forma disruptiva consiste en llevar este mensaje, y es a través de un stand-up comedy, que combina la lúdica y teoría de seguridad de la información.

El éxito de la sensibilización mediante un Stand-Up Comedy se fundamenta en que, mediante una buena sesión de humor, se buscaría la identificación del personal de la CREG con casos representativos asociados a las amenazas informáticas.

Reiteramos que esta divertida puesta en escena de conceptos seudotécnicos tendrá especial énfasis en que sea entendible por todo tipo de personal). El “comediante” es también un experto en seguridad informática con certificaciones y títulos académicos del más alto nivel. Lo cual da una un toque adicional de credibilidad al ejercicio.

10. Recursos y Presupuesto

Para el desarrollo del presente plan de sensibilización en seguridad de la información, 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 equipo de Five Strategy estará conformado por expertos en seguridad de la información y comunicación, quienes serán los encargados de diseñar y elaborar el material necesario para la campaña de sensibilización, así como de coordinar y ejecutar las actividades programadas en el plan. 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.

Además, se contará con los recursos tecnológicos necesarios para la realización de las actividades, incluyendo el uso de plataformas virtuales y herramientas de comunicación que permitan la interacción con los colaboradores de la CREG.

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

El presupuesto asignado para la implementación del Plan de Sensibilización en Seguridad de la Información, 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). El presupuesto contempla la producción de los materiales didácticos y audiovisuales, así como la realización de actividades presenciales, en caso de ser necesario

En caso de requerirse, la CREG pondrá a disposición el auditorio o sitio donde se vayan a realizar las actividades presenciales

11. Monitoreo y Evaluación del Plan

El monitoreo y evaluación del Plan de Sensibilización de Seguridad de la Información 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

12. Mejora continua del plan

Para garantizar la efectividad del plan de sensibilización de seguridad de la información, 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 de sensibilización de seguridad de la información, 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