

## Introducción

Todo esfuerzo de gran interés para las Organizaciones debe ser avalado por la Dirección General. Además, de esto, el hecho de difundir las labores que se ejecutan de cara a un proyecto de gran importancia es crucial para lograr una completa integración de las personas que forman parte directa e indirecta del proyecto, a través del fortalecimiento del manejo del cambio que reduzca la resistencia. Por esta razón, el presente plantea la campaña de difusión que se hará del Sistema de Gestión Seguridad de la Información y proporciona recomendaciones específicas para su implementación, además de medir el grado de efectividad de la campaña implementada, de cara a mejorarla de manera constante, volviendo más asertivos los esfuerzos de difusión Corporativa.

## Antecedentes

La Compañía ha manifestado un interés profundo en la implementación de un Sistema de Gestión de Seguridad de la Información y así mismo en la implementación de una cultura de seguridad de la información. Si bien ya se cuenta con actividades de prevención enfocadas a la Administración de Incidentes, es necesario implementar las mejores prácticas de seguridad de la información y sobre todo difundir la información para que todas las personas se encuentren enteradas de su responsabilidad y sus funciones en materia de seguridad.

## Objetivos

Los objetivos del presente documento son:

1. Asegurar que La Compañía introduzca los términos y los conceptos más comunes de Seguridad de la Información dentro de su cultura Organizacional.
2. Implementar, reforzar y mantener un programa de difusión relacionado a todas las actividades del Programa de Administración de la Seguridad de la Información.
3. Permitir a la Organización conocer la información necesaria, de la manera más adecuada y ordenada, para comprender el alcance, objetivos y acciones específicas que serán demandadas para el buen funcionamiento del Sistema de Gestión de Seguridad de la Información.
4. Asegurar que los empleados y terceros que tiene relación directa con el SGSI y su operación comprendan la contribución que hacen de cara al logro de los objetivos de recuperación planteados.
5. Garantizar que la campaña sea efectiva a través de la medición del proceso de difusión.

## Alcance

El alcance del presente documento es aplicable a todas las personas que laboran en La Compañía, con la siguiente división de acceso a la información:

**En el nivel 1** llamado Staff se encuentra el personal que le dedica de un 80% a un 100% de su tiempo para las actividades de Seguridad de la Información; está directamente involucrado y es directamente responsable de la implementación del Sistema de Gestión de Seguridad de la Información. En este grupo se incluye por ejemplo al Oficial de Seguridad.

**En el nivel 2** se incluyen los cargos de las personas que dedican un 50% de su tiempo en las actividades de Seguridad de la Información, en este grupo se encuentran el personal que opera los procesos y/o servicios críticos a todos los niveles. En este grupo se incluye por ejemplo a los responsables de la implementación de los controles de seguridad.

**En el nivel 3** se encuentra todo el personal restante, que, si bien no es responsable directo de tareas o actividades de seguridad, debe tener conocimiento de los conceptos de seguridad de la información, la política de Seguridad de la Información y la implementación de los controles de seguridad. Para este nivel no es necesario incluir ninguna competencia en la descripción de cargo de cada puesto.

## Metodología

Para conocer la Metodología que sustenta la elaboración del Plan de Concientización y mecanismos de evaluación consulte el documento de **“Metodología para medir la efectividad de la concientización”**

Se busca la Implantación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la cultura de la Organización para:

- a) Elevar, realzar y mantener el compromiso con el SGSI a través de la educación continua y un programa de información del SGSI para todos los empleados y establecer un proceso para evaluar la eficacia de consecución del compromiso con respecto al SGSI; y
- b) Comunicar a todos los empleados la importancia de:
  - El cumplimiento de los objetivos
  - El cumplimiento de la política de seguridad de la información; y
  - La mejora continua
- c) Procurar que todos los empleados sean conscientes de cómo contribuyen a la consecución de los objetivos de seguridad de la información de la organización. Cabe mencionar que todos los temas propuestos para el desarrollo del presente documento y plan de concientización están basados íntegramente en la norma ISO 27001.

## Metodología de elaboración del Plan de Concientización y mecanismos de evaluación

La metodología utilizada para la creación del presente ejecuta las siguientes actividades:

1. Reunión de revisión de medios tecnológicos y de mercadotecnia disponibles en La Compañía para la publicación de mensajes relacionados con el proyecto.
2. Selección consensada (por los responsables del proyecto) de medios a utilizar para la difusión.
3. Desarrollo de sugerencias de temas de difusión, mensajes clave y periodicidad.
4. Desarrollo de sugerencias de mecanismos de evaluación.

## Contenido del Plan de Concientización

### Listado de temas para difusión.

1. Inicio o avance de proyecto de implementación de la norma ISO 27001
2. Definiciones y nomenclatura estándar
3. Beneficios de la Seguridad de la Información
4. Alcance y objetivos del proyecto
5. Programa de Seguridad de la Información (AR, BIA)

### Desarrollo de temas

En las siguientes tablas se muestra por Tema, los mensajes, el personal al que debe ser difundido de acuerdo con su nivel de participación y la frecuencia sugerida.

En la columna de mensajes se mostrará la idea principal a ser difundida, la cual se puede encontrar como instrucciones; las cuáles indican que información poner y a quien solicitarla, mensaje literal; el cual está colocado entre comillas, y como espíritu de mensaje; el cual se presenta en formato de texto sin comillas y es la idea para desarrollar.

La columna de mensajes hace referencia al nivel de difusión presentado en el apartado de alcance. La frecuencia sugerida indica la periodicidad de difusión del mensaje, pudiendo ser publicados varios mensajes al mismo tiempo, ya sea del mismo o diferente tema.

### Inicio o avance de proyecto de implementación de la norma ISO 27001

Mensaje	Nivel de Difusión	Frecuencia
Se dará inicio con un proyecto el cual reforzará las acciones de seguridad de la información en nuestra Organización.	Nivel 3	Única vez, al inicio del proyecto
Notificar a los responsables y líderes del proyecto, así como la constitución del Comité de Seguridad de la Información.	Nivel 2	Al inicio de proyecto o si existen cambios en los responsables.
Resultados de avance del proyecto (será proporcionado por el Responsable de proyecto)	Nivel 2 y 3	Mensual
Dar a conocer la política de Seguridad de la Información del SGSI	Nivel 2 y 3 y Clientes	Al inicio del proyecto, publicación constante y notificaciones en caso de cambios

### Definiciones y nomenclatura estándar

Mensaje	Nivel de Difusión	Frecuencia
Dar a conocer los términos estándares y propios de La Compañía y del SGSI	Nivel 2 y 3	Al inicio del programa

### Beneficios de la Seguridad de la Información

Mensaje	Nivel de Difusión	Frecuencia
“Comprender los riesgos a lo que los procesos de La Compañía se encuentran sometidos en temas de seguridad de la información”	Nivel 2 y 3	Mensual
“Identificar el impacto potencial de la falta de controles de seguridad”	Nivel 2 y 3	Mensual
“Fomentar la mejora operativa entre responsables de negocio y sus proveedores (internos y externos)”	Nivel 2 y 3	Mensual
“Desarrollar las competencias adecuadas en materia de seguridad de la información”	Nivel 2 y 3	Mensual
“Aumentar la confianza de la Alta Dirección de cara a las capacidades de Seguridad de la Información”	Nivel 2 y 3	Mensual
“Potencial ventaja competitiva a través de la demostración del cumplimiento de las mejores prácticas en Seguridad de la Información”.	Nivel 2 y 3	Mensual
Posibilidad de comercialización de servicios a mercados muy especializados que requieren del cumplimiento de normas específicas de seguridad, confiabilidad y continuidad.	Nivel 2 y 3 y clientes.	Mensual

### Alcance y objetivos del proyecto

Mensaje	Nivel de Difusión	Frecuencia
“El presente proyecto está enfocado en la protección de la información de la Compañía cuidando la Confidencialidad, Integridad y Disponibilidad”	Nivel 2 y 3	Semestral
“Objetivo 1. Comprender los principales riesgos a los que están sometidos los procesos críticos de La Compañía”	Nivel 2 y 3	Semestral
“Objetivo 2. Implementar los controles de seguridad”	Nivel 2 y 3	Semestral
“Objetivo 3. Establecimiento de un SGSI”	Nivel 2 y 3	Semestral

### Programa de Seguridad de la Información

Mensaje	Nivel de Difusión	Frecuencia
Resultados de avance del Análisis de Riesgo (será proporcionado por el Responsable del programa)	Nivel 2 y 3	Anual o cada que existan cambios en el AR
Resultados de avance del BIA de cada área (proporcionados por el responsable del programa)	Nivel 2 y 3	Anual o cada que existan cambios en el BIA

### Comparación de estado final vs. Inicial

#### Sugerencias de mecanismos de evaluación.

#### Conclusiones, recomendaciones y factores críticos de éxito.

Los programas de Difusión tienden a funcionar muy bien cuando se les da seguimiento en las Organizaciones. Sin embargo, si el proceso no se mide frecuentemente, es posible que no se alcancen los niveles óptimos de efectividad del programa.

Por otro lado, el buen uso de los programas de difusión facilita el manejo del cambio, minimizando la resistencia y volviendo a todas las personas de una Organización una parte importante para la implementación como agentes de cambio.

En este caso, las recomendaciones y factores críticos de éxito para que el presente programa siga siendo efectivo y cumpla sus objetivos son:

1. Utilizarlo lo más apegado a la sugerencia de frecuencia de uso.
2. Analizar detalladamente los resultados de evaluación de la efectividad del programa y tomar decisiones de mejora continua basadas en los resultados.
3. Que durante la ejecución del proyecto se provea de la información necesaria para dar mensajes oportunos, por ejemplo, en el tema de pruebas.
4. Que, al terminar la implementación del proyecto, este programa se mantenga y mejore como parte de la cultura Organizacional.