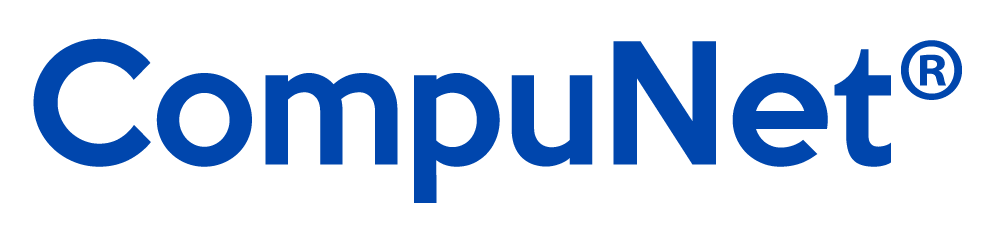
****

Plan de Entrenamiento y Concientización de Usuarios en Seguridad de la Información y Ciberseguridad

2023

|  |  |  |  |
| --- | --- | --- | --- |
| HISTORIA DEL DOCUMENTO | | | |
| Nombre del Documento: | Plan de Capacitación y concientización de usuarios en Seguridad de la Información y Ciberseguridad | | |
| Creado por: | NOMBRE APPATERNO APMATERNO – NOMBRE DEL CARGO | | |
| Responsable del Documento: | NOMBRE Y CARGO DEL RESPONSABLE | | |
| Aprobado por: | CARGO DEL APROBADOR | Fecha de Aprobación: | xx-xx-2023 |

**Control de cambios**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Tipo de cambio** | **Responsable** |
| 1 | xx/xx/2023 | Redacción inicial | NOM AP1 AP2 |
|  |  |  |  |

La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a URL\_INTRANET.

Este documento es de propiedad exclusiva de la EMPRESA y su empleo debe ceñirse a lo dispuesto en su normativa interna. Su uso y distribución sólo está autorizado al interior de EMPRESA y por parte del personal debidamente habilitado.

Tabla de Contenido

[1 Objetivo General. 5](#_Toc27407067)

[2 Alcance General. 5](#_Toc27407068)

[3 Ámbito. 6](#_Toc27407069)

[4 Marco Normativo. 6](#_Toc27407070)

[5 Introducción 7](#_Toc27407071)

[6 Objetivos Generales 7](#_Toc27407072)

[7 Objetivos Específicos 8](#_Toc27407073)

[8 Política de Cumplimiento y No Cumplimiento de Objetivos 8](#_Toc27407074)

[8.1 No Cumplimiento 9](#_Toc27407075)

[8.2 Cumplimiento 9](#_Toc27407076)

[9 Estrategia 10](#_Toc27407077)

[10 Actividades por realizar 11](#_Toc27407078)

[10.1 Inducción de Seguridad y Ciberseguridad para nuevos colaboradores 11](#_Toc27407079)

[10.2 Inducción de Seguridad y Ciberseguridad para colaboradores actuales 11](#_Toc27407088)

[10.3 Comunicados de Seguridad y Ciberseguridad 12](#_Toc27407097)

[10.4 Prueba de Ingeniería Social 12](#_Toc27407106)

[10.5 Campaña Protector de Pantallas 12](#_Toc27407115)

# Objetivo General.

El presente documento describe un programa de entrenamiento y concientización para todos los usuarios de EMPRESA enmarcado en mejorar el conocimiento de los usuarios para con los riesgos de seguridad de la información y ciberseguridad con el propósito de implantar una cultura basada en riesgos.

# Alcance General.

El objetivo principal de este documento es describir las actividades asociadas al programa de entrenamiento y concientización de usuarios en seguridad de la información y ciberseguridad de la EMPRESA.

# Ámbito.

El siguiente programa cubre el control A.7.2.2 “Concientización, educación y formación en seguridad de la información” del dominio 7 “Seguridad ligada a los recursos humanos” de la norma NCh–ISO 27001:2013 para asegurar que los empleados y contratistas entiendan sus responsabilidades, u que sea aptos para los roles para los cuales están siendo considerados.

# Marco Normativo.

* Norma Chilena ISO 27001:2013
* Norma Chilena ISO 27002:2013
* Política General de Seguridad de la información de la EMPRESA vigente.
* Política de Concientización, Educación y Entrenamiento de usuarios en seguridad de la información y ciberseguridad.

# Introducción

El presente plan define los objetivos e iniciativas para generar una cultura de riesgo en seguridad y ciberseguridad mediante un adecuado entrenamiento y concientización a todos los colaboradores y funcionarios de la EMPRESA abordando los aspectos fundamentales de la Seguridad de la Información, Continuidad de Negocios, Gestión de Incidentes y Ciberseguridad.

# Objetivos Generales

* Contribuir al desarrollo de las competencias individuales de los funcionarios de la EMPRESA en relación con materias de Seguridad de la Información y Ciberseguridad.
* Generar un clima más satisfactorio entre nuestros funcionarios y aumentar su motivación y receptividad, convirtiéndose en agentes activos dentro de la organización en la gestión de Seguridad de la Información y Ciberseguridad (cultura basada en riesgo).
* Desarrollar la comprensión de los aspectos fundamentales de los ámbitos asociados a la gestión de Seguridad y Ciberseguridad.
* Acercar a los colaboradores a los objetivos que la organización/institución busca alcanzar a través del sistema de gestión de seguridad y ciberseguridad.

# Objetivos Específicos

**Seguridad de la Información y Ciberseguridad:**

* Concientizar a las personas sobre aspectos de seguridad y ciberseguridad relevantes para la organización/institución, haciendo hincapié en el manejo y protección de la información sensible y el impacto sobre la organización/institución.
* Difundir principales tópicos tratados en las políticas, normas y estándares de seguridad de la EMPRESA, asegurando que los colaboradores y funcionarios no solo las lean, sino que las entiendan y apliquen.

# Política de Cumplimiento y No Cumplimiento de Objetivos

El cumplimiento del presente programa es mandatorio para todos los colaboradores debido a la alineación estratégica que representa el proceso de concientización y entrenamiento para con el riesgo, la seguridad y ciberseguridad de nuestra organización/institución. En este escenario, de cumplimiento, se presentan dos estados posibles para todo colaborador:

# 8.1 No Cumplimiento

Comprende las acciones, o no acciones:

* Falla en completar los entrenamientos asignados por área, rol, departamento, función u otros.
* Fallas reiteradas en los ejercicios de Ingeniería Social.

# 8.2 Cumplimiento

Comprende las acciones, o no acciones:

* Termino exitoso y completo de los entrenamientos asignados.
* Éxito en la identificación de ejercicios de Ingeniería Social.

# Estrategia

Durante el presente año se contempla la realización de actividades tendientes al entrenamiento y concientización respecto de la responsabilidad e importancia de la participación de todo el personal en la gestión diaria de la Gestión Seguridad de la Información y Ciberseguridad a través de temas como: Continuidad del Negocio, Seguridad de la Información, y Ciberseguridad.

Para ello se contempla la realización de las siguientes actividades:

1. Inducción de Seguridad y Ciberseguridad para nuevos colaboradores
2. Inducción de Seguridad y Ciberseguridad para colaboradores actuales
3. Charlas sobre casos de fraude, cracking o consejos sobre cómo protegerse frente a ciberamenazas.
4. Comunicados de Seguridad de la Información y Ciberseguridad.
5. Prueba de Ingeniería Social

# Actividades por realizar

# Inducción de Seguridad y Ciberseguridad para nuevos colaboradores

**Objetivo:** Sensibilizar y concientizar los temas de Seguridad y Ciberseguridad desde el inicio del ciclo de vida de un colaborador.

|  |  |
| --- | --- |
| Periodicidad | Descripción |
| En demanda | Realizar charla de concientización en material de seguridad de la información durante los primeros cinco días de incorporación de un nuevo colaborador. |
| Fecha de Inicio | A definir. |
| Entregable | Registro de asistencia de colaborador |

# Inducción de Seguridad y Ciberseguridad para colaboradores actuales

**Objetivo**: Sensibilizar y concientizar los temas de Seguridad y Ciberseguridad a los colaboradores actual con énfasis en las particularidades de su participación en los distintos procesos y la información a la cual estos tienen acceso directa e indirectamente.

|  |  |
| --- | --- |
| Periodicidad | Descripción |
| Semestral | Realizar bi-anual una charla de concientización en material de seguridad, ciberseguridad. |
| Fecha de Inicio | Semestre 1 – Semestre 2 |
| Entregable | Registro de asistencia de colaboradores |

# Comunicados de Seguridad y Ciberseguridad

**Objetivo:** Sensibilizar en temas de Seguridad y Ciberseguridad a los colaboradores, en cualquiera de los ámbitos que se gestionan en la EMPRESA.

|  |  |
| --- | --- |
| Periodicidad | Descripción |
| Mensual | Realizar mensualmente un comunicado a los colaboradores. |
| Fecha de Inicio | Mensual |
| Entregable | Registro de envío-lectura |

# 10.4 Prueba de Ingeniería Social

**Objetivo:** Realizar una prueba de Ingeniería Social, de forma de validar el comportamiento del usuario frente a un ataque dirigido simulado.

|  |  |
| --- | --- |
| Periodicidad | Descripción |
| Anual | Realizar anualmente un ejercicio de concientización de usuarios a través de correos Phishing. |
| Fecha de Inicio | < a definir> |
| Entregable | Registro de ejecución de campaña y cantidad de usuarios que participaron en esta. |

# 10.5 Campaña Protector de Pantallas

**Objetivo:** Ejecutar Camapañas de material gráfico en protectores de pantalla, fondos de pantalla u otro medio..

|  |  |
| --- | --- |
| Periodicidad | Descripción |
| Semestral | Realizar semestralmente un ejercicio cambio de protector de pantallas, trípticos, poster o similar en áreas visibles. |
| Fecha de Inicio | Semestre 1 – Semestre 2 |
| Entregable | Registro de ejecución de campaña. |

# 10.6 Campaña Entrenamiento RIESGOS

**Objetivo:** Realizar un entrenamiento respecto de los riesgos y su impacto al negocio. Entrenamiento diferido en dos partes con público objetivo: JEFATURAS – LIDERES DE AREA

|  |  |
| --- | --- |
| Periodicidad | Descripción |
| A definir | Realizar anualmente. |
| Fecha de Inicio | <DEFINIR> |
| Entregable | Registro de ejecución asistencia. |

# Indicador de cumplimiento del proceso

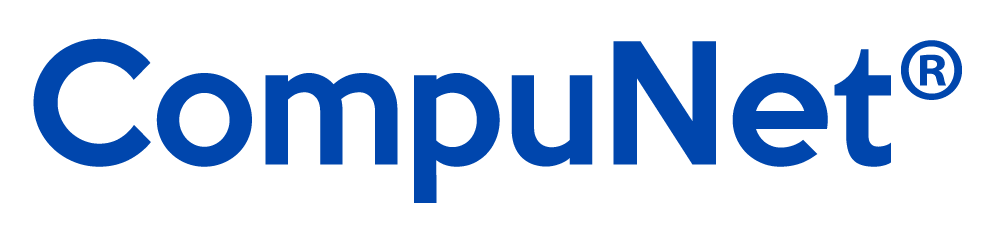
El indicador de cumplimiento está dado por la siguiente formula:

|  |  |  |
| --- | --- | --- |
| Indicador = | N° de campañas en programa | \* 100 |
| N° Total de campañas ejecutadas en el periodo |

El compromiso es de al menos un 90% de las campañas dispuestas en el programa de concientización, educación y entrenamiento de usuarios en seguridad de la información.

# Anexos

A.7.2.2\_Indicadores – Documento el cual registra el nivel de cumplimiento respecto al presente programa.

****