




**Política de Capacitación y Concientización
en Seguridad de la Información**

Forestal Collicura Limitada

Versión 1.0	Política de Capacitación y Concientización en Seguridad de la Información	
-------------	---	---

Información del Documento

Versión	Fecha de Creación		Descripción
1.0	28-07-2023		Creación y primera versión del documento.

(*) La última versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los efectos.



Versión 1.0	Política de Capacitación y Concientización en Seguridad de la Información	
-------------	---	---

Tabla de contenido

1. Introducción	4
2. Objetivo	4
3. Alcance	4
4. Política	4
4.1 Plan de concientización	4
5. Responsabilidades	5
6. Documentación de referencia	5

Versión 1.0	Política de Capacitación y Concientización en Seguridad de la Información	
-------------	---	---

1. Introducción

Esta política presenta los principales requisitos que debe contar el plan de concientización de seguridad de la información en **FORESTAL COLLICURA LIMITADA** y la importancia de este control a la hora de proteger nuestros activos de información.

2. Objetivo

Hacer conciencia a todos los empleados de **FORESTAL COLLICURA LIMITADA** sobre sus responsabilidades en materia de seguridad de la información.

3. Alcance

Esta política se aplica a todo el personal con contrato parcial, tiempo completo, a honorarios, y estudiante en práctica de **FORESTAL COLLICURA LIMITADA**.


4. Política

4.1 Plan de concientización

FORESTAL COLLICURA LIMITADA debe contar con un programa de concientización en seguridad de la información, con una planificación anual que considere las políticas y procedimientos internos de **FORESTAL COLLICURA LIMITADA** y los principales riesgos de ciberseguridad a los que se está expuesto.

El programa de concientización debe considerar los siguientes aspectos mínimos:

- Incluir diferentes actividades tales como campañas (por ejemplo, un “día de la seguridad de la información”) y la elaboración de folletos y boletines.
- Las actividades incluidas en el plan se deben programar con una determinada regularidad, de manera que las actividades se repitan y den cobertura a los nuevos empleados y contratistas.

Versión 1.0	Política de Capacitación y Concientización en Seguridad de la Información	
-------------	---	---


- El programa de concientización debe actualizarse regularmente para que se mantenga en línea con las políticas y procedimientos de **FORESTAL COLLICURA LIMITADA**, y debe considerar las lecciones aprendidas sobre los incidentes de seguridad de la información que se reporten de acuerdo al CIRT de Gobierno u otras entidades concedoras de estos temas.
- La formación en seguridad de la información puede utilizar diferentes medios, incluyendo formación presencial, a distancia, basada en la web, autoaprendizaje y otros medios.
- Incluir los procedimientos básicos de seguridad de la información tales como la notificación de incidentes de ciberseguridad y los controles básicos como la seguridad de las contraseñas, los controles de software malicioso y escritorio limpio.
- El programa de concientización no sólo debe centrarse en el "qué" y "cómo", sino también en el "por qué". Es importante que los colaboradores entiendan el propósito de la seguridad de la información y el impacto potencial, positivo y negativo, sobre la empresa que tiene su propio comportamiento.
- Realizar mediciones del grado de comprensión y adherencia a las políticas y procedimientos de seguridad de la información en las diferentes actividades del programa.

5. Responsabilidades

Usuarios: Responsables de cumplir con las políticas de seguridad de la información, cumplir con las diferentes actividades del programa de concientización y adherirse a las sugerencias y buenas prácticas de ciberseguridad.

Gerencia: Debe suministrar los recursos necesarios para que los programas de capacitación en Ciberseguridad sean competentes, actualizados y además evaluados para todos los colaboradores.

Área de Informática y/o Ciberseguridad: Responsable de construir y mantener el programa de concientización en seguridad de la información, y velar por el cumplimiento de esta política.

Versión 1.0	Política de Capacitación y Concientización en Seguridad de la Información	
-------------	---	---

6. Documentación de referencia

“Código de prácticas para los controles de seguridad de la información ISO/IEC 27002:2013”