Política de control de acceso

Forestal Collicura Limitada

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.

Tabla de contenido

1. *Introducción*

Dentro de la realidad actual de las organizaciones, controlar quién accede a la información de la empresa es un primer paso para protegerla. Es esencial que podamos decidir quién tiene permisos para acceder a nuestra información, cómo, cuándo y con qué finalidad. La presente política define los principales componentes para un correcto control de acceso a la información contenida en las diferentes plataformas, y una correcta gestión para las cuentas de usuarios y contraseñas.

2. *Objetivo*

El propósito de esta política es delimitar el acceso y uso aceptable de todo el equipamiento computacional, servicios y sistemas de información, así como a la red interna de **FORESTAL COLLICURA LIMITADA**. Estas reglas están orientadas a proteger a los colaboradores y a **FORESTAL COLLICURA LIMITADA** sobre el uso inapropiado de la información, los servicios de red y equipos informáticos.

3. *Alcance*

Esta política es aplicable a todos los sistemas de información y plataformas tecnológicas de propiedad de **FORESTAL COLLICURA LIMITADA** actual y futura. Además, aplica para todo el personal con contrato parcial, tiempo completo, a honorarios, y estudiante en práctica y también al personal externo que preste o prestare servicios, remunerados o no a **FORESTAL COLLICURA LIMITADA**.

4. *Definiciones*

Control de acceso: Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

Autenticación: Proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

Sistema de información: Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

Derechos privilegiados: Conjunto de permisos o atributos dados a un usuario, quien de acuerdo con sus funciones y/o tareas encomendadas, puede acceder a un determinado recurso.

5. *Política*

5.1 Control de acceso a los sistemas de información

Todo el personal bajo el alcance de esta política debe tener acceso solo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de **FORESTAL COLLICURA LIMITADA**, siguiendo el principio de "Todo está prohibido a no ser que se permita expresamente". La asignación de privilegios y acceso a los activos de información (correo electrónico, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos, y deben basarse en los siguientes principios:

- "La necesidad de conocer": sólo se da acceso a aquella información necesaria para realizar las tareas (diferentes tareas/roles recogen diferentes 'necesidades de conocer' y por tanto diferentes perfiles de acceso).

- "La necesidad de usar": sólo se da acceso a los recursos necesarios para el tratamiento de la información (equipos, aplicaciones, procedimientos, instalaciones de TI) para la realización de la tarea/trabajo/rol.

5.2 Acceso a las redes y a los servicios de red

El acceso a los sistemas y a la red interna de **FORESTAL COLLICURA LIMITADA** es otorgado sólo a usuarios identificados y autenticados. Para todo sistema de información, el usuario debe señalar quién es (identificación) y luego deberá comprobar que es quién dice ser (autenticación). La identificación se realizará con una cuenta de usuario asignada a cada funcionario y la autenticación se realizará con una contraseña secreta. Para servicios externos o correos electrónicos será necesario y vital la doble autentificación.

Los usuarios deben tener acceso a la red y a los servicios de red para los que han sido autorizados específicamente, lo cual debe quedar establecido en la asignación de privilegios correspondiente.

5.3 Gestión de acceso de usuario

5.3.1 Registro y baja de usuario

Para el proceso de gestión de identificadores de usuarios:

- El identificador de usuario debe ser único y le hace responsable al usuario de sus acciones. El uso de identificadores compartidos o genéricos solo se permite cuando fuera necesario por razones de negocio o de operación y su uso debe ser aprobado y quedar documentado.
- La inhabilitación o eliminación de las cuentas de usuario se debe realizar inmediatamente después que el usuario deja **FORESTAL COLLICURA LIMITADA**, para lo cual el área de soporte debe contar con un procedimiento respectivo.

5.3.2 Provisión de acceso de usuario

Para el proceso de asignación o revocación de los derechos de acceso de usuario:

- Obtener la autorización del propietario del sistema de información o del servicio para el uso de éste.
- Verificar que el nivel de acceso concedido es apropiado de acuerdo con las políticas de acceso
- Asegurarse que los derechos de acceso no se activen antes de concluir el proceso de autorización
- Mantener un registro central de derechos de acceso a sistemas y servicios concedidos a los usuarios.
- Adaptar los derechos de acceso de usuarios que han cambiado de rol o de tareas y la eliminación o bloqueo inmediato de los derechos de acceso de los usuarios que han dejado **FORESTAL COLLICURA LIMITADA**.
- Revisar periódicamente los derechos de acceso concedidos con los propietarios de los sistemas de información o de los servicios

5.3.3 Gestión de privilegios de acceso

La asignación de derechos de acceso privilegiados debe estar controlada a través de un proceso formal de autorización de acuerdo con la política de control de acceso aplicable (véase 5.1). Los siguientes puntos deben ser considerados:

- Deben identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso, por ejemplo, sistema operativo, el sistema de gestión de base de datos y cada aplicación, junto con los usuarios a los que hay que asignarlos.
- Los derechos de acceso privilegiados deben asignarse a los usuarios en base a la 'necesidad de uso' y caso a caso de acuerdo con la política de control de acceso (véase 5.1), es decir, basados en los requisitos mínimos para el desempeño de sus funciones.
- Debe mantenerse un proceso de autorización y registro de todos los privilegios asignados. Los derechos de acceso privilegiados no deben ser concedidos hasta que se complete el proceso de autorización.
- Los derechos de acceso privilegiados deben asignarse a un identificador (ID) de usuario diferente al usado en las actividades normales de **FORESTAL COLLICURA LIMITADA**. Las actividades normales de **FORESTAL COLLICURA LIMITADA** no pueden ser ejecutadas desde un identificador (ID) privilegiado.
- Deben revisarse periódicamente las competencias de los usuarios con derechos de acceso privilegiados verificando que se correspondan con sus tareas.
- Para el identificador (ID) de usuario administrador genérico, debe mantenerse la confidencialidad de la información secreta de autenticación cuando estas cuentas sean compartidas (por ejemplo, cambiando las contraseñas con frecuencia y tan pronto como sea posible cuando un usuario privilegiado deje **FORESTAL COLLICURA LIMITADA** o cambie de trabajo).

5.3.4 Gestión de la información secreta de autenticación de los usuarios

El proceso debe incluir los siguientes requisitos:

- La primera clave de autenticación para cualquier sistema debe ser temporal la cual debe cambiarse obligatoriamente en el primer uso.

- La información de autenticación secreta debe proporcionarse a los usuarios de manera segura; evitando el uso de terceras partes o de correos electrónicos no protegidos (sin cifrar).
- La contraseña por defecto de cualquier aplicativo, debe cambiarse inmediatamente después de la instalación del sistema o del software.

5.3.5 Revisión de los derechos de acceso de usuario

La revisión de los derechos de acceso debe considerar lo siguiente:

- Los derechos de acceso de usuario deben revisarse a intervalos regulares y tras cualquier cambio, como un ascenso, o finalización del empleo.
- Los derechos de acceso de usuario deben revisarse y reasignarse cuando éste cambie de rol dentro de **FORESTAL COLLICURA LIMITADA**.
- La asignación de privilegios debe verificarse a intervalos regulares para asegurar que no se han obtenido privilegios no autorizados.

5.4 Responsabilidades del usuario

Los usuarios deben tener en consideración los siguientes puntos:

- Mantener confidencial la información de autenticación, asegurando que no se divulgue a cualquier otra parte, incluyendo personas con autoridad.
- Evitar guardar (por ejemplo, en papel, en un archivo de software o en un dispositivo portátil) la información secreta de autenticación, a no ser que ésta pueda ser almacenada de forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, en repositorios seguros para contraseñas).

- Cambiar la información secreta de autenticación siempre que haya indicios de su posible compromiso.
- Comunicar a su Jefatura directa y al departamento de Informática y/o Ciberseguridad cualquier situación anómala en relación con sus accesos.

5.4.1 Política de contraseñas para cuentas de dominio y sistemas críticos

- Para las cuentas de dominio y sistemas críticos debe existir un historial de contraseñas con un mínimo de 5 contraseñas anteriores recordadas.
- Debe existir una antigüedad mínima de la contraseña que debe establecerse entre 3 y 7 días. Con el fin de evitar que un usuario intente cambiar la contraseña muchas veces con el propósito de eludir el historial de contraseñas guardadas y utilizar una contraseña anterior.
- La contraseña debe tener una antigüedad máxima de 90 días, fecha en la que debe ser cambiada por una nueva.
- La contraseña debe tener una longitud mínima de 12 caracteres, y debe contar con tres de los cuatro caracteres disponibles: letras minúsculas, letras mayúsculas, números y símbolos.
- Se debe notificar al usuario cuando la contraseña está por expirar para que la modifique antes de que caduque. (Esto debe hacerse por sistema)
- Todos los sistemas deben tener un mecanismo de recuperación de su contraseña, validado y securitizado de acuerdo con las normas.

5.5 Procedimientos seguros de inicio de sesión

El procedimiento de inicio de sesión debe considerar obligatoriamente:

- Proteger contra los intentos de fuerza bruta de inicio de sesión
- Generar un evento de seguridad cuando se detecte un intento potencial o con éxito de violación de los controles de inicio de sesión.
- No transmitir por la red contraseñas sin cifrar.
- Terminar las sesiones inactivas tras un periodo de inactividad.

5.6 Acceso a Data Center, Sala Servicios de Telecomunicaciones y lugares declarados como Reservados

Los Data Center, Salas de Servicios de telecomunicaciones, Rack y otros lugares declarados como Reservados por **FORESTAL COLLICURA LIMITADA,** deben tener un acceso restringido sólo para personal autorizado, y debe existir un procedimiento particular para cada uno de estos en donde se detalle el proceso de autorización, acceso y normas generales dentro de las dependencias. Este proceso, debe tener algún tipo de control de acceso electrónico que permita identificar los ingresos por lo menos 60 días hacia atrás. Si no se pudiera un control como el detallado anteriormente, el sitio deberá tener una chapa de seguridad con control de llaves sólo de los encargados.

6. Responsabilidades y cumplimiento

Encargado/Jefe de Informática y/o ciberseguridad: En su calidad de tal, responde ante la autoridad máxima de **FORESTAL COLLICURA LIMITADA** la existencia y cumplimiento de las medidas que mantengan un nivel de seguridad de la información acorde con el rol de **FORESTAL COLLICURA LIMITADA** y los recursos disponibles.

Usuario: Persona que utiliza un sistema informático y recibe un servicio, tales como: correo electrónico o red de conectividad proporcionado o administrado por **FORESTAL COLLICURA LIMITADA.**

Propietario de sistema: Responsable del sistema por razones de negocio y encargado de autorizar el acceso a los usuarios.}

7. Documentación de referencia

El presente documento constituye una política específica destinada al control de acceso que sigue los lineamientos del "Código de prácticas para los controles de seguridad de la información ISO/IEC 27002". Todos los procedimientos relacionados con los controles de acceso se deben alinear con esta política.