DigiPro, S.A. de C.V.

Hoja de revisión.

Este documento fue creado conforme a los requerimientos institucionales, revisado por el área de Control y Cumplimiento y aprobado por la Dirección de Tecnologías de Información.

Estamos de acuerdo con su contenido e implementación, en caso de haber cualquier modificación o adición a este documento, es responsabilidad del área emisora indicar la modificación o adición, previa aprobación de las áreas involucradas para evitar errores, incrementar el control interno y/o mejorar la productividad de los departamentos involucrados.

Control de Cambios		
Versión	**Cambios realizados**	**Fecha**
01	Documento de nueva creación	13/01/2025

Tabla de contenidos

1 Política de Control de Acceso 4

1.1 Generales 4

1.2 Acceso a Red 4

1.3 Acceso a Sistemas o Aplicaciones 4

1.4 Gestión de Contraseñas o Información Secreta de Autentificación 5

1.5 Responsabilidad De Uso De Contraseñas o Información Secreta De Autentificación 5

2 Cumplimiento 6

1 Política de Control de Acceso

1.1 Generales

- Todo acceso está restringido a menos que este expresamente permitido.
- Todos los accesos creados a los diferentes sistemas de DigiPro (Cuentas de usuario, Roles, Privilegios, etc.) deberán ser creados bajo el principio de privilegios mínimos para poder cumplir con las tareas que requiere el usuario o rol.
- Identificar y registrar el acceso a los servicios de red y sistemas operativos o aplicaciones.
- Utilizar mecanismos de autenticación para el acceso a redes de la organización como validación por dominio, usuario y/o contraseña.
- Se retirarán todos los accesos de personal que deje de laborar en la organización máximo 24 horas hábiles posteriores a la baja.
- Ante un cambio de funciones o de área de un empleado, se deberá considerar un máximo de 21 días para realizar una revisión de acceso y derecho y eliminar los accesos innecesarios para realizar sus nuevas funciones.
- Revisar los accesos cada 6 meses, después de cambios mayores o cuando se produzca un incidente de seguridad.
- Retirar los accesos cuando se considere que la seguridad de la información está comprometida.
- Permitir la verificación del cumplimiento de estas políticas por el área de Seguridad Informática y/o Infraestructura de la empresa que realiza la verificación.

1.2 Acceso a Red

- Utilizar el protocolo de seguridad WPA2 o superior en redes inalámbricas.
- Restringir el acceso o descarga de archivos en sitios peer to peer.
- Restringir el acceso a redes internas a personal externo.

1.3 Acceso a Sistemas o Aplicaciones

- Restringir los privilegios de administrador a usuarios finales a excepción de los usuarios del área de Desarrollo.
- No se permite la creación de usuarios genéricos para el acceso privilegiado (administradores) a servidores o aplicaciones críticas.
- Asegurar el uso de procedimientos de inicio seguros de sesión:
  - Asegurar que no se proporcione el acceso hasta que todos los datos de entrada se hayan ingresado y validado.

- Evitar proporcionar mensajes de ayuda durante el proceso de autenticación.
- Limitar el número de intentos fallidos.
- Evitar la visualización de contraseñas digitadas dentro de los sistemas.

1.4 Gestión de Contraseñas o Información Secreta de Autentificación

- Utilizar mecanismos seguros para la creación de contraseñas:
  - La longitud de contraseñas debe ser de al menos 14 caracteres.
  - Utilizar mecanismos alfanuméricos.
  - Forzar el cambio de contraseñas en el primer inicio de sesión cuando el sistema o área de T.I. haya creado la misma.
  - Evitar palabras que sean fáciles de adivinar como: 12345, fecha de nacimiento, soporte1, nombres propios, etc.
- Evitar el envío de contraseñas en texto plano.
- Forzar el cambio de contraseñas al menos una vez cada 30 días.
- Registrar las actividades del personal que proporciona acceso privilegiado mediante herramienta JobControl.
- Limitar el uso de redes, aplicaciones o sistemas a un número mínimo necesario de usuarios de confianza.

1.5 Responsabilidad De Uso De Contraseñas o Información Secreta De Autentificación

- No habilitar la función de “Recordar contraseñas”.
- Está prohibido compartir la cuenta de usuario y/o las contraseñas de usuario/aplicaciones.
- No guardar las contraseñas en lugares fácilmente identificables.
- Mantener secreta la información de autenticación.
- Cambiar la información secreta de autenticación siempre que exista un indicio mínimo de riesgo.

2 Cumplimiento

- ISO/IEC 27001:2022 / Apéndice A / A.8 Controles Tecnológicos / A.8.5 Autenticación segura
- ISO/IEC 27001:2022 / Apéndice A / A.8 Controles Tecnológicos / A.8.3 Restricción de acceso a la información
- ISO/IEC 27001:2022 / Apéndice A / A.8 Controles Tecnológicos / A.8.2 Derechos de acceso privilegiado
- ISO/IEC 27001:2022 / Apéndice A / A.5 Controles Organizacionales / A.5.15 Control de acceso
- ISO/IEC 27001:2022 / Apéndice A / A.5 Controles Organizacionales / A.5.17 Información de autenticación