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 Seguridad para Todos los Proyectos de la Organización.

Análisis de proyectos

Todos los proyectos nuevos se deben analizar y evaluar mediante una solicitud previa a su ejecución donde se evalúen sus riesgos e impactos, además de los riesgos relacionados a la seguridad de la información.

Procedimiento de Gestión de Cambios

Se deben aplicar controles estrictos durante la implementación de cambios y durante la ejecución del proyecto, siguiendo el procedimiento correspondiente. Éste debe garantizar que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Activos y Administración

Toda la información utilizada para almacenar, procesar o transmitir datos de clientes o de DigiPro, deberá ser propiedad de Digipro y debe ser administrada por personal interno. Además, debe sujetarse a las diferentes políticas de la organización y de la certificación ISO 27001.

Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas deben ser revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad mediante el proceso de gestión de cambios.

Restricción del Cambio de Paquetes de Software

La modificación de paquetes de software suministrados por proveedores, con previa autorización del responsable del Área Informática debe:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
b) Determinar la conveniencia de que la modificación sea efectuada por la organización, por el proveedor o por un tercero.
c) Evaluar el impacto que se produce si la organización se hace cargo del mantenimiento.
d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente en caso de aplicarlo a nuevas versiones.

Canales Ocultos y Código Malicioso

Se deben redactar normas y procedimientos que incluyan:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.
b) Controlar el acceso y las modificaciones al código instalado.
c) Utilizar herramientas para la protección contra la infección del software con código malicioso.

Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecen normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos.
b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
d) Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

2 Cumplimiento.

- ISO/IEC 27001:2022 / Apéndice A / A.5 Controles Organizacionales / A. 5.8 Seguridad de la información en la gestión de proyectos
- ISO/IEC 27001:2022 / Apéndice A / A.8 Controles Tecnológicos / A. 8.32 Gestión del cambio
- ISO/IEC 27001:2022 / Apéndice A / A.8 Controles Tecnológicos / A. 8.30 Desarrollo subcontratado