POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo principal de la presente Política de alto nivel es definir los principios y las reglas básicas para el debido flujo de la información documentada en su creación, almacenamiento, disponibilidad y control de cambios, integrado a la gestión de la seguridad de la información. El fin último es lograr se garantice la seguridad de la información y minimicen los riesgos de naturaleza no financiera derivados de un impacto provocado por una gestión ineficaz de la misma.

Adaptación y desarrollo: Cada uno de los proyectos que conforman la empresa, deberá usar la Política definida en el presente documento como requisito mínimo y adaptarla a sus condiciones y manera de trabajar, mediante diferentes tipos de documentación, para conseguir definir los requisitos de seguridad a nivel operativo.

Clasificación de la información: El modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad se encuentra detallado en el *ES-SMC-001 Gestión de la Información Documentada,* poniendo a disposición plantillas de formatos generales que se reevaluarán y actualizarán periódicamente para adecuar su eficacia, cumpliendo el principio de mejora continua.

En función de la sensibilidad de la información, la empresa DEYFOR cataloga la información en cinco niveles: Uso público, Difusión limitada, Información confidencial, Información reservada, Información secreta.

Con el fin de alinear e integrar, Deyfor establece **principios básicos**, que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- **Alcance estratégico:** Las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal, contando con el compromiso y apoyo de todos los niveles ejecutivos de los macroprocesos, proyectos o servicios.
- **Seguridad integral:** La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- **Gestión de riesgos y proporcionalidad:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información, donde el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos.
- **Datos de carácter personal:** Asegurar la privacidad con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos.
- **Mejora continua:** La gestión de activos y las medidas de seguridad se deben optimizar con periodicidad mínima anual y/o de acuerdo con la necesidad contextual.

A su vez presentamos las siguientes responsabilidades con la organización:

- **Jefe(a) de MP:** Tener identificados e inventariados los activos de información necesarios para la prestación de sus procesos de negocio y asegurar su cumplimiento junto a sus lineamientos.
- **Especialistas/Supervisión:** Impulsar la divulgación y la concienciación de la Seguridad de la Informaciónentre los colaboradores de la empresa DEYFOR, considerando los riesgos de seguridad de la información en la toma de decisiones.
- **Asistentes/Documentalista:** Designados por el jefe de MP y/o SMC, quién es el encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida. El responsable deberá mantener un registro formal de los usuarios con acceso autorizado a dicho activo, asegurando que el activo esté inventariado, correctamente clasificado y adecuadamente protegido. Se deberán actualizar de manera periódica las configuraciones de los activos para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

Son de obligatorio cumplimiento según la aplicabilidad del documento los siguientes lineamientos:

- LN-SMC-001 Lineamiento de firmas por tipo de documento
- LN-SMC-002 Lineamiento de estructura de portadas
- LN-SMC-003 Lineamiento para encabezado y pie de página
- LN-SMC-004 Lineamiento de codificación documental
- LN-SMC-005 Lineamiento de codificación documental PRQ, FQ, PETS
- LN-SMC-006 Lineamiento para el cuerpo de documentos
- LN-SMC-007 Lineamiento para la codificación de informes
- ES-TI-08 Estándar de la Seguridad de la Información
- CA-TI-08 Política de arquitectura de la información
- No se permite compartir o difundir archivos del tipo base de datos sin previa autorización de gerencia.

U otras disposiciones que el Sistema de Mejora Continua difunda formalmente en medios de comunicación oficiales de la empresa, siendo uno de ellos que.

Puesto que la Seguridad de la Información incumbe a todo el personal de la empresa DEYFOR, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.

Guillermo Huamán Mantilla
GERENTE GENERAL

Cajamarca, 06 de enero de 2023