POLÍTICA DE CONFIDENCIALIDAD

La presente Política de Confidencialidad tiene como objetivo establecer los principios y lineamientos para garantizar la protección, confidencialidad, integridad y uso adecuado de la información generada, administrada o compartida por DEYFOR E.I.R.L., tanto dentro de la organización como con terceros en el desarrollo de sus operaciones.

Toda la información generada en DEYFOR constituye un activo estratégico de la organización y propiedad intelectual de la empresa, por lo que su acceso, uso, almacenamiento y divulgación deberán realizarse conforme a las disposiciones establecidas en esta política y en los estándares internos de gestión de información.

1. **ALCANCE**

La presente política aplica a:

- Todos los colaboradores de DEYFOR
- Directivos y personal administrativo
- Proveedores y contratistas
- Clientes y aliados estratégicos
- Cualquier tercero que tenga acceso a información de la empresa

Asimismo, aplica a toda la información gestionada en:

- Sistemas de información y ERP
- Sistemas documentales y repositorios digitales
- Comunicaciones electrónicas
- Documentos físicos o digitales
- Bases de datos
- Información contractual, financiera, operativa o estratégica

2. **PRINCIPIO DE ACCESO A LA INFORMACIÓN**

- El acceso a la información dentro de DEYFOR se rige por el principio de “necesidad de conocer”, por el cual los colaboradores solo podrán acceder a la información estrictamente necesaria para el cumplimiento de sus funciones y responsabilidades dentro de la organización.
- Los permisos de acceso serán asignados conforme al nivel de responsabilidad del colaborador y la clasificación de la información.

POLÍTICA DE CONFIDENCIALIDAD

3. CLASIFICACIÓN DE LA INFORMACIÓN

- En DEYFOR la información se clasifica según su nivel de confidencialidad y el acceso a la misma se asigna de acuerdo con el nivel de responsabilidad del colaborador, conforme al principio de **necesidad de conocer**.

Nivel de Información	Descripción	Ejemplos	Nivel de Usuario con Acceso	Reglas para compartir
N0 – Pública	Información que puede difundirse sin riesgo para la organización	página web, material institucional, comunicaciones públicas	Todos los usuarios	Difusión libre
N1 – Interna	Información de uso interno para el desarrollo de actividades organizacionales	manuales, procedimientos, formatos	Usuarios N1 o superiores	Solo uso interno
N2 – Interna Controlada	Información operativa que debe compartirse únicamente con equipos autorizados	reportes de proyectos, indicadores internos, inventarios	Usuarios N2 o superiores	Requiere autorización del responsable del proceso
N3 – Restringida	Información sensible que puede afectar intereses organizacionales si se divulga	contratos, presupuestos, licitaciones, valorizaciones	Usuarios N3 o superiores	Requiere autorización del **Jefe del Macroproceso Administrador**
N4 – Crítica / Confidencial	Información altamente sensible cuyo acceso debe ser estrictamente controlado	datos personales, planillas, credenciales, respaldos, información de ciberseguridad	Usuarios N4	Prohibido compartir salvo autorización expresa de **SEA**

POLÍTICA DE CONFIDENCIALIDAD

El detalle de permisos de creación, lectura, modificación, eliminación y autorización se encuentra definido en el **Estándar de Clasificación y Control de Información de DEYFOR**

4. **NOTIFICACIÓN Y GESTIÓN DE INCIDENTES**

Cualquier incidente relacionado con la seguridad o confidencialidad de la información deberá ser reportado inmediatamente para su evaluación y gestión.

Se consideran incidentes, entre otros:

- Pérdida o extravío de información.
- Accesos no autorizados.
- Filtración de datos.
- Uso indebido de información.
- Fallas de seguridad en sistemas o repositorios.

Los incidentes deberán reportarse a través de los siguientes canales institucionales:

- Correo electrónico institucional del área responsable o del área SEA.
- Jefatura directa o responsable del macroproceso
- Área de Tecnologías de la Información (TI)
- Sistema interno de gestión de acciones o registro de incidentes, cuando corresponda

Una vez reportado el incidente, la organización realizará la evaluación, investigación y adopción de las medidas correctivas o preventivas necesarias para proteger la información.

5. **CUMPLIMIENTO LEGAL**

- DEYFOR se compromete a cumplir con la legislación peruana aplicable en materia de protección de datos e información, incluyendo:
- Ley N° 29733 – Ley de Protección de Datos Personales
- Reglamento aprobado mediante DS 003-2013-JUS
- Normativa laboral aplicable al tratamiento de datos de trabajadores
- Obligaciones contractuales de confidencialidad con clientes y proveedores

En el tratamiento de información y datos personales, DEYFOR garantiza el respeto de los principios de legalidad, consentimiento, finalidad, proporcionalidad, seguridad y confidencialidad, asegurando que los datos sean tratados únicamente conforme a la normativa vigente, recolectados con fines legítimos y específicos, limitados a la información necesaria para el cumplimiento de dichos fines, protegidos mediante medidas de seguridad adecuadas y resguardados contra accesos, usos o divulgaciones no autorizadas.

6. **RESPONSABILIDAD, INCUMPLIMIENTO Y CONSECUENCIAS**

- Todos los colaboradores de DEYFOR son responsables de proteger la información a la que tengan acceso en el ejercicio de sus funciones, debiendo clasificarla adecuadamente, utilizarla únicamente para fines autorizados y evitar cualquier divulgación no autorizada.
- Asimismo, deberán reportar inmediatamente cualquier incidente o riesgo que pueda comprometer la confidencialidad, integridad o disponibilidad de la información.
- El incumplimiento de esta política o la divulgación no autorizada de información podrá dar lugar a sanciones disciplinarias conforme al Reglamento Interno de Trabajo, la terminación de relaciones contractuales con terceros y la adopción de acciones legales cuando corresponda.
- Toda filtración o uso indebido de información clasificada como **N2, N3 o N4** será considerada un **incidente grave de seguridad de la información** y será investigada por la organización para determinar responsabilidades y aplicar las medidas correctivas correspondientes.

Cajamarca, 30 de Enero de 2026

Guillermo Huamán Mantilla
GERENTE GENERAL