

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Versión 01

1. Introducción

En el **CENTRO DE ARBITRAJE DEL COLEGIO DE ABOGADOS DE LIMA** nos comprometemos a proteger los activos de información en control del centro frente a la pérdida de confidencialidad, integridad y disponibilidad. Conscientes de la importancia de esto, hemos desarrollado un Sistema de Gestión de Seguridad de la información basado en la norma ISO 27001:2022.

2. Referencias normativas

- ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información

3. Objetivo

Garantizar que la información obtenida y procesada durante la provisión de nuestros servicios se maneje con los más altos estándares de seguridad, en cumplimiento con las exigencias de nuestros clientes y las normativas aplicables. A través de esta política, buscamos proteger la confidencialidad, integridad y disponibilidad de la información, asegurando un adecuado control y protección durante todo el ciclo de vida de esta.

4. Aplicabilidad

Esta política aplica a todos los trabajadores, árbitros y peritos que interactúan con información generada o recibida durante la ejecución de los servicios de la empresa. Se extiende a todos los sistemas de información, procesos, y activos que manejan información confidencial de clientes y la propias del centro.

5. Compromisos

Por ello nos comprometemos a cumplir con las siguientes promesas:

- **Clasificación de la información:** Toda la información se clasificará en los siguientes niveles, en función de su sensibilidad y del impacto que podría causar su divulgación, alteración o pérdida.
 - **Información Pública:** Información que puede ser compartida libremente sin necesidad de restricciones. Ejemplo: publicaciones de marketing aprobadas, contenido de la web pública, catálogo de servicios, documentación técnica del servicio.
 - **Información Interna:** Información que no es de acceso público, pero cuya divulgación no tendría un impacto significativo. Ejemplo: políticas internas, procedimientos operativos no confidenciales, presupuestos, estrategias comerciales y planes de negocio, información de árbitros autorizados, registro de Información sobre reclamos, incidentes.
 - **Información Confidencial:** Información sensible que requiere protección contra accesos no autorizados. Incluye historial y Datos personales de los clientes, expedientes del proceso arbitral, laudos, etc.

- **Cumplimiento Legal:** Respetar y cumplir con las leyes, regulaciones y normativas aplicables a nuestras actividades, tanto nacionales como con ISO/IEC 27001:2022
- **Responsabilidades:** Todo el personal de la empresa y partes externas pertinentes deben cumplir con esta política y con los procedimientos establecidos para garantizar la confidencialidad, integridad y disponibilidad de la información. El incumplimiento de esta política será sujeto a sanciones, de acuerdo con el marco legal vigente y las políticas internas.
- **Mejora Continua:** La empresa revisará y mejorará continuamente sus políticas y controles de seguridad de la información, alineándose con las mejores prácticas del sector y los cambios regulatorios, así como con las expectativas de los clientes.

6. Mecanismos de comunicación

Para garantizar que la Política de Seguridad de la Información del CENTRO DE ARBITRAJE DEL COLEGIO DE ABOGADOS DE LIMA sea comprendida, aplicada y mantenida en todos los niveles de la organización, se han establecido los siguientes mecanismos de comunicación:

a) Difusión Interna:

- Publicación en áreas visibles dentro de las instalaciones donde el personal interno del CEAR CAL desarrolle sus funciones.
- Explicación de la política en reuniones periódicas y capacitaciones dirigidas a todo el personal.
- Inducción a nuevos colaboradores para asegurar su conocimiento desde el inicio de sus funciones.

b) Comunicación Externa:

- Publicación en la página web de la empresa y redes sociales corporativas.
- Inclusión en documentos informativos dirigidos a clientes y partes interesadas.

c) Evaluación de la Comprensión y Aplicación:

- Encuestas periódicas para medir el nivel de entendimiento de la política por parte del personal.
- Auditorías internas para verificar su implementación y cumplimiento.
- Revisión anual de la política y sus mecanismos de comunicación para asegurar su efectividad y actualización.

7. Objetivos

Para garantizar la eficacia de nuestro Sistema de Gestión de Seguridad de la Información (SGSI), establecemos los siguientes objetivos:

- Implementar controles de acceso (lógicos y físicos) que aseguren la confidencialidad de la información sensible (expedientes, documentos de arbitraje, datos personales) haciendo que solo sea accesible al personal autorizado.

- Establecer mecanismos de respaldo y verificación de integridad de datos que permitan detectar y corregir corrupciones o alteraciones, con pruebas de restauración exitosas al menos semestrales.
- Capacitar y sensibilizar continuamente al personal interno, árbitros y colaboradores externos sobre la seguridad de la información, los riesgos asociados y los controles implementados.
- Programar y ejecutar auditorías internas para asegurar la alineación del sistema de gestión de seguridad de la información con los requisitos de ISO 27001:2022

Esta política será revisada anualmente o cuando sea necesario, para garantizar su vigencia y efectividad ante los cambios internos, las necesidades de los clientes, o las modificaciones en la normativa aplicable.

Lima, 23 de abril del 2025