Política y Plan de Respuesta a Incidentes de Seguridad de la Información y Datos Personales

Soluciones Integrales en Software LTDA
RUT: 76.490.675-6

01.12.2025

www.climaoLa.com

+56 23 210 5000 Alameda 1302, Of. 70, Santiago, Chile. info@climaola.com

Política y Plan de Respuesta a Incidentes de Seguridad de la Información y Datos Personales

1. Objetivo.

Establecer el marco normativo, metodológico y operativo para **prevenir, detectar, gestionar y responder** de manera oportuna y controlada ante incidentes o vulnerabilidades que afecten la seguridad de la información y/o los datos personales utilizados en la prestación de los servicios de Evaluación de Clima Organizacional.

El objetivo principal es minimizar el impacto, proteger los derechos de las personas evaluadas y asegurar la continuidad y confiabilidad del servicio.

2. Alcance

Este plan aplica a:

- Datos personales y datos sensibles tratados en proyectos de Clima Organizacional.
- Sistemas, plataformas, bases de datos, archivos y respaldos asociados.
- Todo el personal interno, colaboradores externos y proveedores que participen en el tratamiento de información.

3. Marco de Referencia

Este documento se basa en buenas prácticas de gestión de seguridad de la información y considera principios alineados con:

- Legislación de protección de datos personales aplicable.
- Principios de confidencialidad, integridad y disponibilidad de la información.
- Modelos de referencia como ISO 9000, a nivel conceptual.

4. Definición de Incidente de Seguridad

Se considera incidente de seguridad cualquier evento real o potencial que comprometa o pueda comprometer:

- La **confidencialidad** de los datos (acceso, divulgación o uso no autorizado).
- La **integridad** de la información (alteración, pérdida o corrupción de datos).
- La **disponibilidad** de los sistemas o datos necesarios para el servicio.

Ejemplos:

- Acceso no autorizado a bases de datos.
- Filtración o exposición de información personal.
- Pérdida, robo o eliminación accidental de datos.
- Fallas de seguridad en plataformas tecnológicas.

5. Roles y Responsabilidades

5.1 Dirección de la Consultora

- Aprobar el presente plan.
- Tomar decisiones estratégicas frente a incidentes de alto impacto.

5.2 Responsable de Seguridad / Líder del Incidente

- Coordinar la ejecución del plan de respuesta.
- Evaluar el impacto y definir acciones inmediatas.
- Mantener comunicación con la Dirección.

5.3 Equipo de Proyecto / Consultores
- Reportar inmediatamente cualquier incidente o sospecha.
- Colaborar en acciones de contención y análisis.

5.4 Soporte Tecnológico / Proveedores
- Apoyar técnicamente la investigación y remediación.
- Implementar medidas correctivas en sistemas y plataformas.

6. Metodología de Respuesta a Incidentes

Fase 1: Detección y Notificación
- Identificación del incidente por monitoreo, reporte interno o aviso externo.
- Notificación inmediata al Responsable de Seguridad.
- Registro inicial del incidente (fecha, origen, sistemas afectados).

Fase 2: Evaluación y Clasificación
- Análisis preliminar del alcance y tipo de datos comprometidos.
- Clasificación del incidente según impacto (bajo, medio, alto).
- Determinación de riesgos para las personas evaluadas y para el cliente.

Fase 3: Contención Inmediata
- Aislamiento de sistemas afectados.
- Suspensión temporal de accesos comprometidos.
- Aplicación de medidas para evitar mayor exposición.

Fase 4: Investigación y Análisis de Causa Raíz
- Revisión técnica y operativa del incidente.
- Identificación de vulnerabilidades explotadas.
- Documentación detallada de hallazgos.

Fase 5: Remediación y Recuperación
- Corrección de vulnerabilidades detectadas.
- Restauración segura de sistemas y datos desde respaldos.
- Validación de integridad y funcionamiento normal.

Fase 6: Comunicación
- Comunicación interna a las áreas involucradas.
- Información oportuna al cliente, cuando corresponda.
- Notificación a autoridades o terceros, si la normativa lo exige.

Fase 7: Cierre y Aprendizaje
- Cierre formal del incidente.
- Registro de lecciones aprendidas.
- Definición de acciones preventivas.

7. Gestión de Comunicaciones

Toda comunicación relacionada con un incidente debe:
- Ser clara, oportuna y veraz.
- Evitar especulaciones o información no validada.
- Ser coordinada por la Dirección o Responsable de Seguridad.

8. Registro y Evidencia
- Todos los incidentes son documentados en un registro interno.
- Se conserva evidencia técnica y documental según plazos definidos.
- Los registros son confidenciales y de acceso restringido.

9. Pruebas y Capacitación
- El plan es revisado y probado periódicamente.
- El personal recibe capacitación básica en detección y reporte de incidentes.

10. Revisión y Mejora Continua

Este plan se revisa al menos una vez al año o ante:

- Cambios relevantes en tecnologías o procesos.
- Incidentes significativos ocurridos.
- Actualizaciones normativas aplicables.

11. Vigencia

El presente Plan de Respuesta a Incidentes entra en vigencia desde su aprobación por la Dirección de la Consultora y es de cumplimiento obligatorio para todas las personas involucradas en el tratamiento de datos personales.