Procedimiento de Gestión de Incidentes

Este procedimiento se establece conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador, su reglamento (Decreto Ejecutivo 904), y en cumplimiento con las normas ISO/IEC 27001, 27002, 27005 y 27701. Tiene como objetivo gestionar eficazmente los incidentes de seguridad que involucren datos personales.

1. Identificación de Incidentes

Proceso diseñado para identificar y reportar cualquier brecha de seguridad que ponga en riesgo los datos personales. Incluye las siguientes actividades:

- Detección de eventos inusuales en los sistemas de información.
- Clasificación del incidente según su impacto en los datos personales.
- Comunicación inmediata al responsable de seguridad de la información.

2. Notificación y Respuesta

Procedimiento formalizado para notificar de forma inmediata a los titulares de los datos afectados y a la Autoridad de Protección de Datos Personales, cuando sea necesario. Incluye los siguientes pasos:

- La naturaleza y tipo de vulneración;
- Identificar los titulares o interesados afectados;
- El detalle inicial de los sistemas vulnerados;
- La causa presunta de la vulneración:
- El volumen y tipos de datos expuestos o comprometidos;
- Las medidas adoptadas y previstas para responder y remediar la vulneración con la finalidad de mitigar las
- consecuencias presuntas;
- La evaluación del riesgo que la vulneración implica para los derechos y libertades de los titulares; y,
- Otros aspectos determinados por la Autoridad de Protección de Datos Personales.

3. Registro de Incidentes

Se mantiene un registro centralizado y actualizado de todos los incidentes de seguridad reportados, que incluye:

- Fecha y hora del incidente.
- Descripción del incidente y sistemas afectados.
- Datos personales comprometidos, si los hubiere.
- Acciones correctivas y preventivas adoptadas.
- Resultado de la investigación y cierre del incidente.

Este documento debe revisarse y actualizarse periódicamente, y estar disponible para auditorías internas y externas conforme a la normativa aplicable.