RESUMEN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

nubelco

1. Política de Seguridad de la Información

La organización mantiene una política de seguridad de la información orientada a proteger sus sistemas, servicios y activos de información frente a amenazas accidentales o intencionadas. Su objetivo es garantizar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de la información, así como la continuidad de los servicios prestados.

Esta política se aplica a todo el personal, colaboradores, proveedores y terceros que, por su actividad, accedan, gestionen o traten información o servicios de la organización. Su alcance incluye los sistemas que dan soporte a los servicios tecnológicos y a las aplicaciones propias, así como a las infraestructuras, redes, plataformas, entornos y servicios auxiliares necesarios para su operación.

2. Principios de seguridad

La seguridad se basa en un enfoque preventivo y continuo. La organización aplica medidas organizativas, técnicas y procedimentales adecuadas al nivel de riesgo y a la criticidad de cada sistema, con el fin de reducir la probabilidad e impacto de incidentes de seguridad.

Entre los principios fundamentales destacan:

- La **prevención**, mediante controles y buenas prácticas que minimicen riesgos.
- La **detección y vigilancia continua**, con capacidades de monitorización y registro para identificar anomalías, vulnerabilidades o degradaciones del servicio.
- La **respuesta**, con procedimientos para gestionar incidentes de forma ordenada, escalable y trazable.
- La **recuperación**, garantizando respaldo, restauración, continuidad y retorno seguro a la normalidad.
- La **proporcionalidad**, adaptando las medidas de seguridad al análisis de riesgos y a la categoría del sistema.

La seguridad se integra en todo el ciclo de vida de los sistemas, desde su diseño y adquisición hasta su explotación, mantenimiento y retirada. Además, la organización mantiene una mejora continua de su sistema de seguridad para adaptarse a la evolución de las amenazas y a los cambios del entorno.

3. Organización y responsabilidades

La política establece una estructura clara de responsabilidades para asegurar una gestión ordenada de la seguridad. Existen roles definidos para la dirección de la seguridad, la gestión del servicio, la gestión de la información y la administración del sistema, junto con funciones técnicas delegadas cuando sea necesario.

La organización dispone de un comité de seguridad encargado de aprobar la política, impulsar la estrategia de seguridad, supervisar riesgos e incidentes, y apoyar la asignación de recursos necesarios. Asimismo, los conflictos sobre requisitos, medidas o riesgos residuales se resuelven mediante los mecanismos de coordinación internos establecidos.

4. Gestión de riesgos, cambios e incidentes

Todos los sistemas incluidos en el alcance cuentan con análisis de riesgos actualizados, revisados periódicamente y cuando se producen cambios relevantes o incidentes de seguridad.

La organización mantiene inventarios actualizados de activos y controla que cualquier cambio en sistemas, configuraciones o accesos sea autorizado, evaluado y registrado.

Además, dispone de un procedimiento de gestión de incidentes que cubre su detección, análisis, respuesta y cierre, así como la revisión periódica de las medidas de continuidad y recuperación.

5. Protección de datos y relación con terceros

La política integra las obligaciones de protección de datos personales y exige que la seguridad de la información y la privacidad se coordinen de forma continua. Esto incluye control de accesos, trazabilidad, gestión de brechas, contratación con encargados del tratamiento y conservación de evidencias.

Las relaciones con proveedores y terceros se formalizan mediante cláusulas y controles que aseguren confidencialidad, seguridad, gestión de accesos, notificación de incidentes, continuidad, derecho de auditoría cuando proceda y devolución o destrucción de la información al finalizar la relación. Además, se evalúan los riesgos asociados a terceros cuando la criticidad del servicio o la sensibilidad de la información lo requieren.

6. Obligaciones del personal

Todo el personal debe conocer y cumplir la política y la normativa de desarrollo. También debe usar correctamente los activos de información y comunicar sin demora cualquier incidente, debilidad o incumplimiento detectado.

La organización promueve la concienciación en seguridad mediante formación periódica y acciones específicas para nuevas incorporaciones o puestos con responsabilidades técnicas, administrativas o de seguridad.

7. Cumplimiento y revisión

El incumplimiento de la política puede dar lugar a medidas disciplinarias, contractuales, organizativas o legales según corresponda. La política se revisa al menos una vez al año y siempre que existan cambios relevantes en el alcance, la tecnología, la normativa, los incidentes o los procesos de auditoría y renovación.

La documentación asociada al sistema de gestión de seguridad se mantiene controlada, versionada y disponible para quienes deban conocerla por razón de sus funciones.