POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Introducción

La información constituye un activo esencial para las organizaciones, ya que resulta imprescindible para la prestación de sus servicios. Las tecnologías de la información y la comunicación (TIC) permiten su tratamiento eficiente, pero también introducen nuevos riesgos.
Por ello, es necesario establecer medidas adecuadas para proteger la información y los servicios asociados, reduciendo los riesgos a niveles aceptables.
Este documento establece la Política de Seguridad de la Información de la **Associació de Ciberseguretat de Catalunya (ASCICAT)**, con el objetivo de que todo el personal y colaboradores conozcan y apliquen las medidas de seguridad definidas.

1. Misión y objetivos

ASCICAT adopta un modelo de gestión de la seguridad alineado con el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, reconociendo la información y los sistemas como activos estratégicos.
Los objetivos principales son:

- Contribuir al cumplimiento de la misión de la organización
- Garantizar el cumplimiento normativo
- Asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
- Garantizar la continuidad de los servicios
- Proteger los activos frente a amenazas

ASCICAT mantiene un compromiso continuo con la gestión de riesgos (ENS - MAGERIT) y la mejora continua.

2. Alcance

Esta política aplica a todos los activos de información y a todas las personas con acceso a los sistemas.

3. Marco normativo

- La política se basa en:
- Real Decreto 311/2022 (ENS)
- Reglamento (UE) 2016/679 (RGPD)
- Ley Orgánica 3/2018
- Ley 34/2002 (LSSI-CE)

4. Organización de la Seguridad

- Responsable de la información
- Responsable del servicio
- Responsable de seguridad
- Responsable del sistema

5. Gestión de riesgos

Se realizan análisis periódicos para identificar amenazas y aplicar medidas adecuadas.

6. Principios de Seguridad

- Seguridad por defecto
- Mínimo privilegio
- Protección de la información
- Registro de actividad
- Control de interconexiones

7. Control de accessos

Acceso limitado a usuarios autorizados.

8. Gestión de incidentes

Procedimientos para detección y resolución de incidentes.

9. Continuidad del Servicio

Medidas de backup y recuperación.

10. Relación con terceros

Los terceros deben cumplir las medidas de seguridad.

11. Mejora continua

ASCICAT mejora continuamente su modelo de seguridad.

Clasificación

Documento de uso público.