ADAPTACIÓN AL RGPD Y AL ENS

www.inycom.es
info@inycom.es
+34 902 995 820

Consultoría e implantación de medidas para el cumplimiento normativo

LA SOLUCIÓN

La implantación de medidas de seguridad de la información es fundamental para las Administraciones y para todos los entes de titularidad pública, especialmente por la gran cantidad de datos de carácter personal que deben tratar.

Además de ser imprescindible para fomentar la confianza de los ciudadanos en las administraciones, las obligaciones impuestas por el Esquema Nacional de Seguridad (ENS) y por el Reglamento General de Protección de Datos Europeo (RGPD) hacen que el aseguramiento del cumplimiento normativo se convierta en una prioridad para estas entidades.

Esta obligación hace necesario implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) que proporcione seguridad en las siguientes dimensiones:

- **Confidencialidad,** asegurando que la información es solo accesible para aquellas personas autorizadas.
- **Integridad,** garantizando la exactitud de la información y que ésta sea completa, así como los métodos de su procesamiento.
- **Disponibilidad,** asegurando que los usuarios autorizados tienen acceso a la información y que el servicio público se mantiene disponible para el ciudadano.
- **Autenticidad,** asegurando que dicha información es auténtica
- **Trazabilidad,** haciendo posible comprobar a posteriori quién ha accedido a, o modificado, cierta información.

OBJETIVOS

- Adaptar los procesos de la organización que utilizan medios electrónicos al ENS para el cumplimiento de la normativa.
- Adaptar los procesos de la organización que implican el tratamiento de datos personales al RGPD, con el fin de asegurar su cumplimiento.
- Fomentar la confianza en el uso de los medios electrónicos que permita a los ciudadanos ejercer sus derechos y a las Administraciones Públicas cumplir sus deberes a través de estos medios.
- Establecer la política de seguridad de la entidad pública en la utilización de medios electrónicos en el ámbito del marco normativo actual, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en cuanto a seguridad de las tecnologías de la información para una homogeneización de las medidas en esta materia.

¿A QUIÉN VA DIRIGIDO?

La adaptación al RGPD y el ENS es exigible a todas las Administraciones y entidades públicas.

Nuestro foco se dirige a:

- Entidades locales de tamaño medio.
- Empresas y entidades de titularidad pública.
- Consejerías de Comunidad Autónoma.

Dado que esta solución afecta tanto al plano técnico (para la implantación de la tecnología necesaria) como al plano jurídico (para considerar las consecuencias legales de los incidentes y asegurar el cumplimiento normativo), el mensaje puede ir dirigido tanto a Responsables de Sistemas como a Responsables de Servicios Jurídicos, que pueden ser susceptibles de asumir la figura de DPO o CISO.

El RGPD no exime de ninguna responsabilidad en caso de no existir la figura del DPO, por lo que en estos casos debe dirigirse a las figuras de máxima responsabilidad (Directores Generales, alcaldes o gerentes).

ADAPTACIÓN AL RGPD Y AL ENS

www.inycom.es
info@inycom.es
+34 902 995 820

SOLUCIÓN PLANTEADA

FASE I:
Desarrollo de los Planes de Adecuación

- Análisis de la situación del cliente respecto al cumplimiento del ENS
- Análisis de la documentación a entregar al CCN.
- Consultoría previa de los procesos.
- Análisis de riesgos.
- Diagnóstico de cumplimiento.
- Consultoría ISO 27000

FASE II:
Implantación de medidas

- Implantación y mantenimiento de SGSI (medidas ciber / legal / organizativas)
- Implantación ISO 27000.
- Servicios de DPO
- Seguridad gestionada y alertas.

FASE III:
Mantenimiento y mejora.

- Revisión y auditoría de las implantaciones.
- Evaluaciones de impacto
- Concienciación y formación en ciberseguridad.
- Formación a los responsables en aspectos y consecuencias legales.
- Análisis de la situación mediante la herramienta de Análisis de Riesgos PILAR y la herramienta de adecuación al ENS INES.

BENEFICIOS APORTADOS

- Asegurar el cumplimiento y adaptación a la normativa legal.
- Generar confianza en el ciudadano.
- Ahorro de costes económicos en resolución de incidentes de seguridad mediante la inversión en medidas preventivas.
- Ahorro de costes reputacionales mediante la reducción de incidentes.
- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- Facilitar un tratamiento continuado de la seguridad.
- Promover comportamientos centrados en la seguridad para situaciones del mundo real y reforzar las prácticas recomendadas de ciberseguridad en el trabajo.
- Trasladar los problemas y el lenguaje de la ciberseguridad a la lógica de los negocios (en nuestro caso, prioridades de la gerencia y atención al ciudadano).

TECNOLOGÍAS

- Firewalls y equipamiento de seguridad perimetral.
- Soluciones de detección de hacking, ciberamenazas y comportamientos sospechosos.
- Herramientas Data Loss Prevention.
- Soluciones MDM.
- Soluciones de seguridad Endpoint.
- vSOC
- Herramientas anti ransomware.
- Análisis de malware
- Soluciones de concienciación y formación.
- Cibersafety Games.
- Norma ISO 27000
- Guías y recomendaciones CCN-STIC-800 (ENS)

paloalto NETWORKS · SOPHOS · Microsoft · Symantec. · vmware · KASPERSKY · Bitdefender · DARKTRACE · hp z

Rev. 001 Enero 2018

GANADOR PREMIO A LA EXCELENCIA EMPRESARIAL EN ARAGÓN 2006 GRANDES EMPRESAS · CMMI DEV/2 Exp. 2016-06-20 / Appraisal #20592 · ITIL