RGPD y Seguridad de la Información

Alvaro Moreton Poch

Project Manager en Rooter

XIX Jornada de actualización bancaria

18/11/2021

Principios del tratamiento

- **Licitud, lealtad y transparencia**
  - Licitud: Tratamiento conforme a bases legales
  - Lealtad: Rige la relación entre el interesado y el responsable del tratamiento
  - Transparencia: Deber de informar
- **Limitación de la finalidad**: Tratamiento para una finalidad determinada y de acuerdo a la información que se ha dado al interesado
- **Minimización de datos:** El tratamiento debe limitarse a lo estrictamente necesario para el cumplimiento de los fines determinados
- **Principio de exactitud:** Supresión o rectificación de forma rápida aquellos datos personales que sean inexactos
- **Principio de limitación del plazo de conservación:** Los datos no deberán conservarse más tiempo del necesario para cumplir con los fines del tratamiento
- **Principio de integridad y confidencialidad :** Aplicación de medidas de seguridad

Medidas de seguridad

- **Procedimientos, sistemas de control y otras medidas** que se adoptan en las empresas y organizaciones para garantizar la seguridad de los datos personales
- Su objetivo es **aumentar la seguridad** evitando, fundamentalmente, el tratamiento ilícito de datos personales, así como la pérdida, destrucción o daño accidental de los mismos

Medidas organizativas

- Las medidas organizativas son todas aquellas medidas que están encaminadas a construir una **cultura de conciencia y sensibilización** así como a la creación de **políticas organizacionales y protocolos de actuación en relación con la seguridad**
- Algunos ejemplos:
  - Políticas de seguridad de la información (por ejemplo de acceso, de continuidad etc..)
  - Conciencia y capacitación
  - Evaluación de riesgos
  - Auditorias
  - Informes periódicos

Medidas técnicas

- Las **medidas técnicas** se pueden definir como las medidas y controles que **se aplican a los sistemas informáticos (dispositivos, redes y hardware) y** también las medidas físicas de seguridad (sobre las instalaciones y los documentos) que se implementan con el fin **de garantizar la integridad de los datos almacenados**
- Algunos ejemplos:
  - Seguridad del edificio
  - Seguridad cibernética (protección del correo, protección web, parches, gestión de contraseñas, copias de seguridad)
  - Tratamiento/ eliminación de documentos y dispositivos
  - BYOD/ Acceso remoto
  - Network Access Control
  - Anonimizarían/ pseudonimizacion / cifrado

¿Como se aplican según el RGPD?

- El RGPD determina que el sistema de protección de datos se debe basar en una **responsabilidad proactiva** por parte de la organización
- La aplicación de medidas de seguridad debe realizarse en función de los **riesgos detectados**
- Se deberán aplicar unas u otras medidas en función de **distintos criterios** (sensibilidad de los datos, complejidad del sistema de información, practicas comerciales etc..)
- El RGPD establece que las organizaciones deben seguir ciertos procesos para probar y **evaluar con regularidad** la efectividad de las medidas que haya adoptado
- El RGPD establece que, en caso de que ocurra una **violación de seguridad**, el responsable del tratamiento deberá **informar a la autoridad de control**, a más tardar, **72 horas** después haber tenido conocimiento de ésta
- Asimismo, si existiera la posibilidad de que la violación de seguridad supusiera un riesgo para los derecho y libertades de las personas físicas, el responsable deberá **comunicarla a los interesados** a la mayor brevedad posible

ISO 27001

- **Estándar** internacional para los **Sistemas Gestión de la Seguridad de la Información** permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos
- Busca preservar la **integridad, confidencialidad, disponibilidad y resiliencia**
- Los principales puntos de la norma son:
  - Contexto de la organización
  - Liderazgo
  - Planificación, soporte y operación
  - Evaluación de desempeño (auditorias)
  - Mejora

Muchas gracias

Correo electrónico: alvaro.moreton@rooter.es