Medidas de Seguridad

Enfoque basado en riesgos

Todas las organizaciones estamos obligadas a proteger la información que tratamos, garantizando que en el desempeño de nuestras funciones se velará por la protección de la privacidad, evitando toda acción que pueda impactar negativamente en los derechos y libertades de las personas.

1 ¿Qué deben garantizar las medidas de seguridad en el tratamiento de los datos de carácter personal?

Confidencialidad

Deben **garantizar** que sólo accederán a los datos las personas que tengan la correspondiente autorización.

Integridad

Deben **proteger** la veracidad y exactitud de los datos.

Disponibilidad

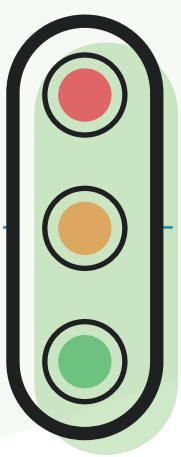
Deben **asegurar** que los datos permanecerán disponibles.

Resiliencia

Deben **comprometer** la capacidad de recuperación y establecimiento del estado inicial de los datos en caso de verse afectados por un incidente.

2 ¿Qué medidas deben aplicar las organizaciones?

Antes del RGPD



Los responsables de los tratamientos o los ficheros y los encargados del tratamiento tenían reguladas las medidas que debían aplicar en función del nivel de los datos:

Básico

IDENTIFICATIVOS

- Nombre
- Apellidos,
- Direcciones de contacto (físicas o electrónicas)
- Teléfono (fijo o móvil)
- Otros

Medio

INFRACCIONES/PERFILES

- Comisión infracciones penales o administrativas
- Ficheros de Solvencia
- Ficheros de AA.Tributarias
- Seguridad Social y Mutuas
- Ficheros de EEFF (Serv.Financieros)
- Elaboración de perfiles (ej. selección de personal)

Alto

ESPECIALMENTE PROTEGIDOS

- Ideología
- Afiliación sindical
- Religión
- Creencias
- Origen racial
- Salud
- Vida sexual
- Violencia de género
- Fines policiales (obtenidos sin consentimiento)

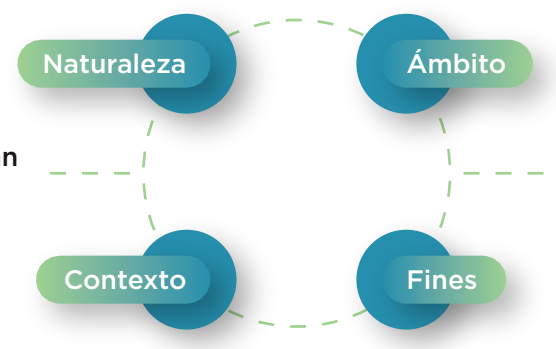
Después del RGPD

Enfoque basado en riesgos

1º Identificar riesgos

Las medidas de seguridad deben adoptarse en función del riesgo que supone el tratamiento de los datos para los derechos y libertades de las personas, como pueden ser consecuencias negativas de exclusión social, laboral, etc.

Para analizar los riesgos se tendrán en cuenta aspectos como:



del tratamiento

2º Aplicar medidas técnicas y organizativas para garantizar el nivel de seguridad adecuado en función de los riesgos detectados

Toda organización deberá aplicar por tanto las medidas técnicas y organizativas adecuadas para la actividad del tratamiento desarrollada y sus objetivos, algunas de ellas por ejemplo, pueden ser: aplicar la minimización y la seudonimización de los datos, técnicas de cifrado, regular el control de acceso a los datos, etc.

El análisis de riesgos en el RGPD forma parte del principio de **Accountability:** cumplir con la normativa y poder demostrar ese cumplimiento en todo momento.

3 ¿Qué son las Evaluaciones de Impacto sobre la Protección de Datos o “PIAS”?

Cuando el tratamiento de los datos suponga un alto riesgo para los derechos y libertades de las personas deberá realizarse una Evaluación especial de Impacto en la protección de datos personales.

¿En qué casos?

- En la elaboración de perfiles tras el análisis de los datos, por ejemplo, para el envío de información comercial.
- En el caso de tratamiento de datos a gran escala de categorías especiales (las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical).
- Observación sistemática a gran escala de una zona de acceso público.

CONCLUSIONES

La aplicación de medidas previstas por el RGPD debe adaptarse a las características de las organizaciones y el riesgo que los tratamientos de los datos de carácter personal puedan suponer para los derechos y libertades de las personas.

Cumplir con los principios de protección de la privacidad y aplicar las medidas que nuestra organización haya implementado garantizará el correcto tratamiento de los datos y la protección de la privacidad.