integra
INFORMACIÓN Y COMUNICACIÓN

ALFA

eDUC@MOS

GrupoDC Solutions

www.planalfa.es

www.integratics.com

Reglamento General de Protección de Datos
Evaluación de Impacto (EIPD)

Fecha: 13 de febrero, 2018

Reglamento General de Protección de Datos
Introducción

- **Entró en vigor en mayo de 2016**
- **Aplicable a partir de mayo de 2018**
- **Norma directamente aplicable, no requiere normas de trasposición**
- **La ley que sustituye a la actual Ley Orgánica de LOPD.**
  - La AGPD podrá incluir precisiones.
  - Las empresas que ya cumplen con la actual LOPD tienen una buena base de cumplimiento, pero es necesario adaptarse
- **Elementos de carácter general que las diferencia:**
  - **Principio de Responsabilidad Activa** (necesidad de aplicación de medidas de seguridad y organizativas): Qué datos tratan, con qué finalidad, que operaciones de tratamiento realizan
  - **Enfoque de riesgo**: debe tenerse en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento así como el riesgo para los derechos y libertades de los afectados

Principios básicos de la RGPD

EIPD y el Análisis del riesgo

- **El responsable del tratamiento:**

  Será responsable del cumplimiento de la normativa y debe ser capaz de demostrarlo (Art. 5 RGPD). Actitud consciente, diligente y proactiva.

- **Obligatorio si:**
  - ¿Se tratan datos sensibles?
  - ¿Se incluyen datos de una gran cantidad de personas?
  - ¿Se elaboran perfiles de comportamiento?
  - ¿Se tratan datos de menores?
  - ¿Se van a utilizar para una finalidad distinta?
  - ¿Hay técnicas de análisis tipo Big Data?
  - ¿Se cruzan datos aportados por los interesados con otros de otras fuentes?
  - ¿Se utilizan tecnología invasivas para la privacidad tipo geolocalización, video-vigilancia o aplicaciones de Internet de las cosas?

Evaluación de Impacto de Protección de Datos

Contenido mínimo

❖ La EIPD deberá incluir como mínimo:

- **Una descripción sistemática de las operaciones de tratamiento** previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

- **Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento** con respecto a su finalidad;

- **Una evaluación de los riesgos para los derechos y libertades de los interesados**

- **Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos** que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Determinación y atenuación del riesgo

Análisis y tratamiento

- **Gestión del riesgo:**
  En un proceso estructurado cuya finalidad es conocer y reducir la incertidumbre relativa a las amenazas que afectan a los activos (bienes y servicios) de una organización.

- **Análisis de riesgo**:
  Realizar mediciones cuantitativas y cualitativas sobre el nivel de afectación de una determinada amenaza sobre un determinado activo:
  - Inventario de activos
  - Determinación de las amenazas
  - Las probabilidades de que ocurran
  - Impacto

- **Tratamiento de los riesgos**:
  Técnicas y estrategias cuyo objetivo es la disminución del riesgo inicial, aplicando salvaguardas (medidas de carácter técnico u organizativo) para conseguir:
  - Evitar o eliminar el riesgo
  - Reducirlo o mitigarlo
  - Transferirlo, compartirlo o asignarlo a terceros
  - Aceptarlo

Principios de la Gestión del Riesgo

Objetivo

- **Proteger el valor**, es decir, contribuir a la consecución de los objetivos y la mejora del desempeño
- Ser una **parte integral de todos los procesos** de la organización
- Formar **parte de la toma de decisiones**
- **Tratar explícitamente la incertidumbre**
- **Ser sistemática, estructurada y oportuna**
- Basarse en la **mejor información** disponible
- Facilitar la **mejora continua**
- **Adaptarse**, alineándose con el contexto interno y externo y con los perfiles del riesgo
- Integrar **factores humanos** y culturales.
- **Ser trasparente y participativa**
- **Dinámica, iterativa** y responde a los cambios

Gestión de riesgos de la seguridad de la información

Fundamentos

Desde el punto de vista de la RGPD, los activos a identificar son aquellos directamente relacionados con los sistemas de información, o sea, aquellos elementos de hardware y de software que intervienen en el procesamiento, almacenamiento, comunicación, transformación, consulta, modificación o producción de información de carácter personal.

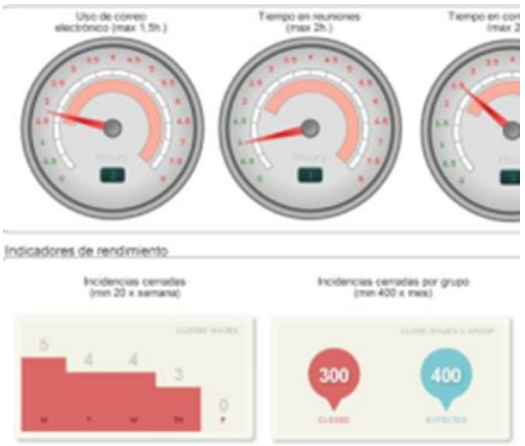
- **Objetivos**
  - Confidencialidad
  - Integridad
  - Disponibilidad

- **Amenazas**
  - De Origen Natural (Incendios, inundaciones, rayos…)
  - Fallos en los sistemas Informáticos y de comunicaciones
  - Error humano

- **Vulnerabilidades**
  - Equipamiento informático susceptible a variaciones de temperatura o humedad
  - Sistemas operativos que por su estructura, configuración o mantenimiento son más vulnerables a algunos ataques
  - Localizaciones que son más propensas a desastres naturales como por ejemplo inundaciones o que están en lugares con variaciones de suministro eléctrico
  - Aplicaciones informáticas, que por su diseño, son más inseguras que otras
  - Personal sin la formación adecuada, ausente o sin supervisión

Gestión de riesgos de la seguridad de la información

Auditoría de Seguridad Global



- **El objetivo**

  Realizar un mapa de riesgos que permite detectar y corregir problemas de seguridad en distintos ámbitos que permitirá poner en marcha los sistemas necesarios para garantizar la calidad, la seguridad y el rendimiento del Sistema Informático

- **Auditoría de Seguridad Global**
  - Evaluación de las Infraestructuras.
  - Evaluación del uso: Análisis del tráfico de red: protocolos, aplicaciones, cuotas, control de contenidos, balanceo de enlaces, horarios de uso, comunicaciones entre redes, P2P, ataques, vulnerabilidades, etc.
  - Análisis de implantación de medidas de seguridad en relación a la RGPD

Gestión de riesgos de la seguridad de la información

Evaluación de Infraestructuras y análisis de tráfico de red

- **Servidores:**
  - Auditoria de rendimiento, dimensionamiento del Hardware, análisis de servicios, recursos disponibles y escalabilidad.
  - Dispositivos de Almacenamiento propios y comunes.
  - Sistema operativo y estado de parches y actualizaciones de seguridad.

- **Infraestructuras de red:**
  - Electrónica de red, rendimiento y escalabilidad.
  - Estado del cableado, tipología de red, normalización del cableado.
  - Routers, accesos a WAN, firewalls, proxis y PLC, rendimientos y escalabilidad.

- **Impresoras y otros recursos de red:**
  - Ubicación.
  - Políticas de compartición.
  - Personal que tiene acceso, tipo de datos almacenados o impresos.

Gestión de riesgos de la seguridad de la información

Evaluación de Infraestructuras y análisis de tráfico de red

- **Sistemas de protección:**
  - Sistemas de Alimentación ininterrumpida.
  - Sistemas de protección contra subidas de tensión de eléctrica.
  - Sistemas antiincendios (Extintores, cajas ignífugas…).

- **Control de accesos a Internet:**
  - Firewalls, reglas, tablas de enrutamiento y registro de accesos remotos.
  - Proxys, reglas de filtrado por protocolos, puertos, IPs y usuarios, tratamiento de los logs, bloqueo de aplicaciones no autorizadas.
  - Antivirus, AntiSpam y otras amenazas, estado de las suscripciones, automatización de actualizaciones, monitorización de contenidos por categorías
  - Filtrado de contenidos web.
  - Uso de aplicaciones y protocolos más corrientes
  - Ataques y denegación de servicio
  - Cuotas de uso por usuario
  - Balanceo de enlaces y optimización
  - Establecimiento de redes, subredes y Vlan’s

Gestión de riesgos de la seguridad de la información

Resultado de la auditoría: Análisis de riesgos

- **Afinar el nivel de amenaza** que el uso de las infraestructuras generan cuando no se conoce en profundidad el uso que de ella, hacen los usuarios de la red, rendimiento, dimensionamiento y escalabilidad

- **Conocer si es correcta o no, la configuración de elementos críticos del sistema** como recursos compartidos, políticas de contraseñas, configuración de copias de seguridad, perfiles, roles, etc.

- **Comprobar el nivel de eficacia real de los sistemas de protección** como firewalls, antivirus, y AntiSpyWare y herramientas de control de contenidos

- **Supervisión del cableado, tipología de red, e infraestructuras**, como puntos de acceso, routers, etc.

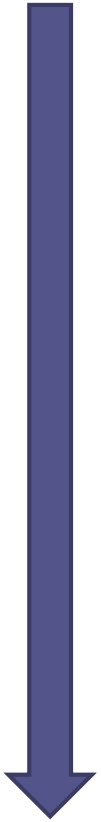
- **Existencia de uso de aplicativos no autorizados**, intrusiones, ataques y vulnerabilidades

Gestión de riesgos de la seguridad de la información

Aplicando Salvaguardas y determinando el Riesgo Residual

Por el tipo de protección las salvaguardas se clasifican en:

- Preventivas (disminuyen la probabilidad)
  - Prevención
  - Disuasión
  - Eliminación
- Acotan la degradación (disminuyen el impacto)
  - Minimización del impacto
  - Corrección
  - Recuperación
- Consolidación (Mantenimiento)
  - Monitorización
  - Detección
  - Concienciación
  - Administración



ACTIVO

AMENAZA

VULNERABILIDAD

IMPACTO

RIESGO

SALVAGUARDAS

RIESGO RESIDUAL

Gestión de riesgos de la seguridad de la información

Redacción, publicación e integración del informe de Auditoría

- **Identificación clara del proyecto**, la persona o personas responsables de la EIPD y sus datos de contacto, la fecha de realización del informe y número de versión del mismo.
- **Resumen del informe con los resultados esenciales** escrito con claridad y concisión.
- Introducción y **descripción general del proceso de evaluación** para aquellos lectores que no estén familiarizados con esta técnica.
- **Resultado del análisis de necesidad de la evaluación** y su justificación.
- **Descripción general del proyecto** con el nivel de detalle necesario (se pueden incluir como anexos los documentos relevantes del proyecto que se juzguen oportunos).
- **Descripción detallada de los flujos de datos personales**.
- **Análisis de cumplimiento normativo**
- **Riesgos identificados.**
- **Detalle de posibles deficiencias detectadas y propuestas de solución** para eliminar, evitar, mitigar, transferir o aceptar los riesgos para la privacidad incluidas las de carácter organizativo.

Integra Información y Comunicación S.L.

Twitter: @GDCS_

Web: www.grupodcsolutions.com

Blog: https://www.grupodcsolutions.com/blog

- Más información:
  - 917454270
  - proxi@planalfa.es
  - www.planalfa.es