CURSO DE INTELIGENCIA ARTIFICIAL MÁLAGA, 30 mayo a 20 julio 2021

GOBERNANZA, CIBERSEGURIDAD Y PRIVACIDAD DE DATOS 04/06/2021- 16:00 a 18:00

JUAN GARCÍA GALERA

Índice

01

Introducción:
Los datos y la seguridad

Introducción

Sector Salud

Las bombas de insulina de Medtronic anteriores a 2013 podrían sufrir ciberataques

- Una vulnerabilidad encontrada el pasado jueves puede provocar que los usuarios reciban dosis alteradas de esta hormona.
- Medtronic avisa de que al menos 4.000 personas están usando dispositivos antiguos.

SALUD · Los sistemas llevan cuatro días inutilizados

Torrejón, primer hospital español 'secuestrado' por un virus informático

El Hospital de Torrejón, en Madrid, lleva desde el pasado viernes con sus sistemas informáticos bloqueados por lo que parece ser un virus de tipo 'ransomware'.

Pre-2013 Medtronic insulin pumps could be vulnerable to hacking

Medtronic warns that at least 4,000 people are using the older devices.

By Joe Carlson Star Tribune | JUNE 27, 2019 — 8:28PM

PROVIDED PHOTO

Introducción

Sector Transporte

Oleada de ciberataques en el transporte marítimo de mercancías: las 4 mayores compañías del mundo han sido víctimas de ataques con 'ransomware' en menos de 4 años

Adrián Francisco Varela 30 sep. 2020 10:07h. - Actualizado: 30 sep. 2020 10:07h.

Hackeada la aerolínea Air New Zealand

Detalles

Publicado: 12 Agosto 2019

- phishing
- hacking

- **Alrededor de 112.000 personas se han visto afectadas.**
- **La aerolínea neozelandesa Air New Zealand ha sufrido un ataque de phishing que ha expuesto los datos personales del 3,5 % de los miembros de su programa Airpoints.**

Fears Airpoints members' personal information leaked in data breach

Bonnie Flaws · 18:59, Aug 09 2019

SUPPLIED

A phishing scam affecting two staff accounts at Air New Zealand has resulted in customers' data being breached.

Introducción

Administración Pública

El Mundo

Un ciberataque tumba los servicios de varios ayuntamientos de España

El virus escogido se llama Zeppelin, que es otro diferente del detectado en las plataformas del SEPE o en Phone House. Este ransomware se ...

Hace 3 semanas

Xataka

El Ayuntamiento de Castellón sufre un ciberataque y se queda sin acceso al sistema informático, web municipal...

El Ayuntamiento de Castellón (Castelló de la Plana) ha informado que tanto su web municipal, como la sede electrónica, el portal tributario, así ...

31 mar 2021

El Español

150.000 personas cobrarán tarde el paro y las prestaciones tras el ciberataque al SEPE

Teletrabajo. Con todo, a pesar de la recuperación parcial, los efectos de ciberataque todavía permanecen. Ninguno de los empleados del SEPE ...

1 abr 2021

Introducción

Redes Sociales

Cinco Días

11 millones de datos de usuarios españoles de Facebook filtrados en la red: ¿estás tú?

11 millones de datos de usuarios españoles de Facebook filtrados en la red: ¿estás tú? Se trata de una de las mayores filtraciones de la historia ...

Hace 1 mes

Hipertextual

Si tenías una cuenta de Facebook en 2019, tienes un 50% de posibilidades de que tus datos se hayan filtrado

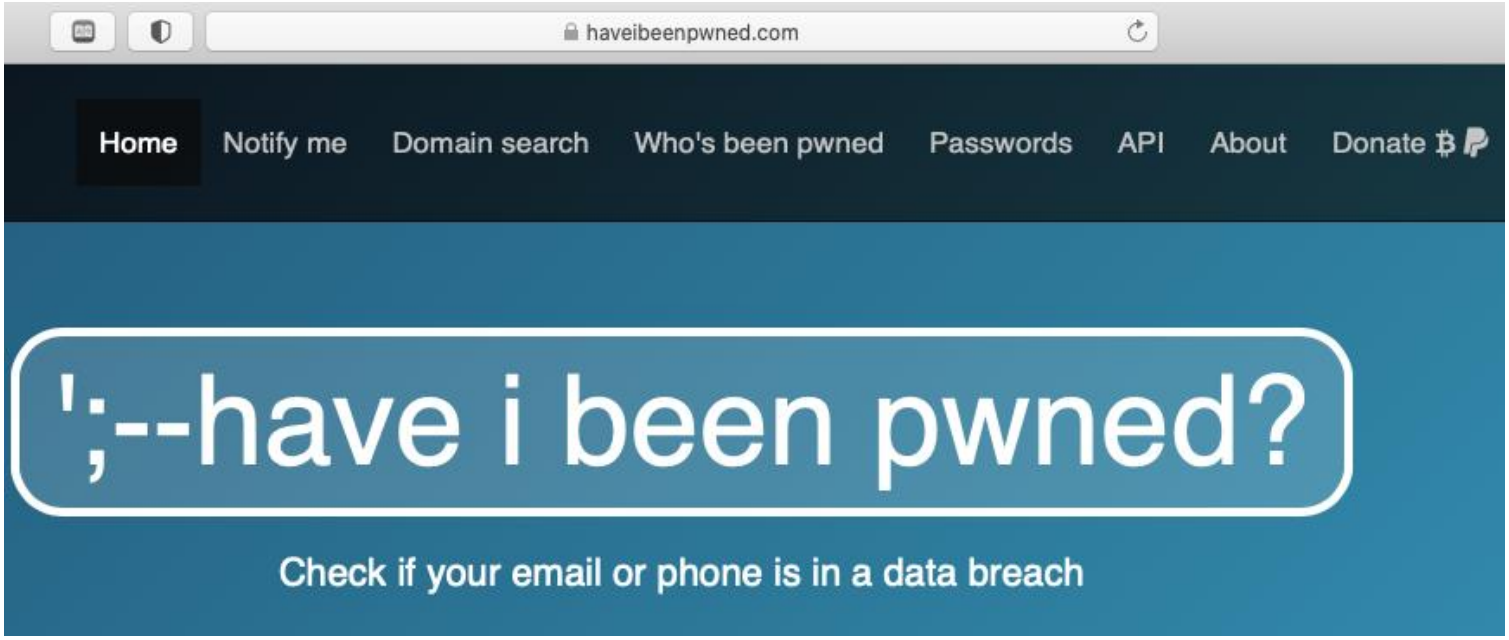
Hacemos un repaso a las fugas y brechas de datos que ha sufrido Facebook a lo largo de su historia. Solo en 2019 la mitad de sus cuentas ...

Hace 1 mes

Una vieja brecha de Facebook ha dejado 533 millones de números de teléfono al descubierto, con casi 11 millones de números españoles

Introducción

¿Probamos?



Introducción

Cualquier sector puede ser víctima

El Periódico

Un ciberataque paraliza la mayor red de oleoductos de Estados Unidos

Un ciberataque amenaza con secar la distribución de combustible en parte de los Estados Unidos. Este viernes, la principal red de oleoductos ...

Hace 3 semanas

Expansión

Glovo sufre un ciberataque a la base de datos de sus clientes y repartidores

Glovo sufre un ciberataque a la base de datos de sus clientes y repartidores. EFE. 4 MAY. 2021 - 21:08.

Hace 4 semanas

Introducción

Cualquier sector puede ser víctima

Introducción

Global Risk Report 2021

WORLD ECONOMIC FORUM

02

Gobernanza de datos desde la ciberseguridad

Gobernanza de datos (desde la seguridad)

¿Qué es el Gobierno de Datos?

Data governance es un "*sistema de decisiones y responsabilidades para procesos relacionados con la información, ejecutados de acuerdo con unos modelos acordados, que describen quién puede tomar qué acciones, con qué datos y cuándo, en qué situaciones, y utilizando qué métodos*"

Gobernanza de datos (desde la seguridad)

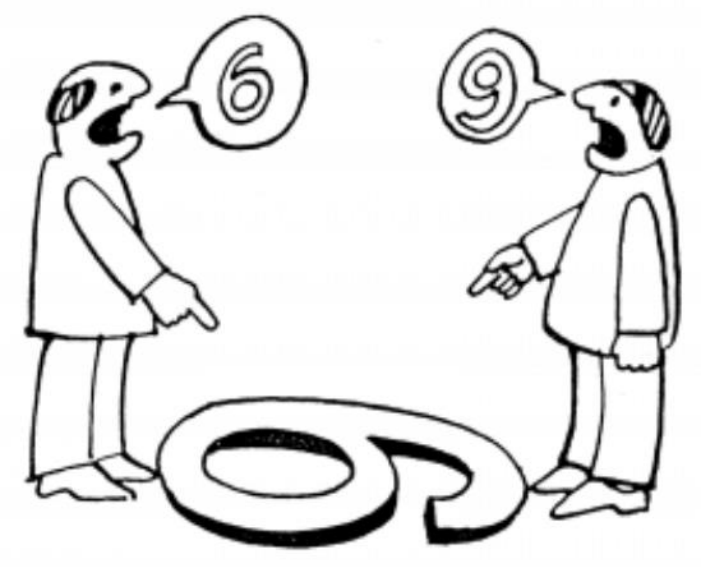
¿Qué es el Gobierno de Datos?

El **gobierno de datos** está formado por políticas, procesos y una estructura organizativa para dar soporte a la gestión de datos empresariales. La estructura de un programa de gobierno de datos permite comprender, proteger y confiar en los datos de una organización a las partes interesadas, especialmente a medida que las empresas crecen y acumulan más activos y orígenes de datos.

Gobernanza de datos (desde la seguridad)

¿Qué es el Gobierno de Datos?

_**Data governance** es el "*ejercicio de toma decisiones y autoridad para asuntos relacionados con los datos*".



Introducción

Roles principales

- CEO – Chief Executive Officer (Director Ejecutivo)
- CIO – Chief Information Officer (Director de Sistemas de Información)
- CTO – Chief Technology Officer (Director de Tecnología)
- CFO – Chief Finantial Officer (Director Financiero)
- CSO – Chief Security Officer (Director de Seguridad)
- CISO – Chief Information Security Officer (Director de Seguridad de Información)
- CDO – Chief Data Officer (Director de Datos)
- DPO – Data Protection Officer (Delegado de Protección de Datos - DPD)

Gobernanza de datos (desde la seguridad)

Roles principales

Bloques de responsabilidad

Gobernanza de datos (desde la seguridad)

Responsable de la Información (ENS)

_Determina los requisitos (de seguridad) de la información tratada, (pone valor a la información en términos de seguridad).

_Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información.

_En el caso del ENS, como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable.

La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto de la legalidad.

Gobernanza de datos (desde la seguridad)

Responsable del Servicio (ENS)

_Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.

_Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información.

_En el caso del ENS, como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.

_El rol de Responsable de la Información y Responsable del Servicio puede recaer en la misma persona o Comité.

Gobernanza de datos (desde la seguridad)

Responsable de la Seguridad de la Información (ENS) / CISO

_Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.

_Deberá ser una persona física, jerárquicamente independiente del Responsable del Sistema.

_Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

_Seguridad como función diferenciada (no puede recaer en el Responsable del Sistema)

Gobernanza de datos (desde la seguridad)

Responsable del Sistema de Información (ENS) / Responsable de Explotación

_Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.

_Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.

Gobernanza de datos (desde la seguridad)

Responsable del Tratamiento (RGPD / LOPD-GDD)

_La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Gobernanza de datos (desde la seguridad)

Encargado del Tratamiento (RGPD / LOPD-GDD)

_La persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del Responsable del Tratamiento.

Gobernanza de datos (desde la seguridad)

DPD – Delegado de Protección de Datos (RGPD / LOPD-GDD)

_La persona física o jurídica, que se encarga de:

-Informar y asesorar a los responsables y encargados del tratamiento de datos personales (y a sus empleados) de las obligaciones que tienen, derivadas tanto de la legislación europea como de la española.

-Supervisar el cumplimiento de dicha legislación y de la política de protección de datos de una Administración Pública, empresa o entidad privada: asignación de responsabilidades, concienciación y formación del personal, auditorías, etc.

-Ofrecer el asesoramiento que se le solicite para hacer la evaluación de impacto de un tratamiento de datos personales, cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, y supervisar luego su aplicación.

-Cooperar con las “autoridades de control” (Agencias de Protección de Datos)

-Actuar como “punto de contacto” de las autoridades de control.

Gobernanza de datos (desde la seguridad)

DPD – Delegado de Protección de Datos (RGPD / LOPD-GDD)

_El art.37.1 del RGPD requiere la designación de un DPD en 3 casos específicos:
-Cuando el tratamiento lo lleven a cabo autoridades u organismos público -> tanto autoridades nacionales como regionales o locales, así como en organismos regidos por el derecho público (por ej. transporte público, suministro de energía, infraestructuras, etc). Su nombramiento obedece a la necesidad de protección adicional que puede requerir una persona que, habitualmente, no tendrá un control sobre si sus datos se tratan y que manera, o bien tienen un escaso poder de decisión.

-Cuando los responsables o encargados tengan entre sus *actividades principales* las operaciones de tratamiento que requieran una *observación habitual y sistemática* de interesados *a gran escala* -> por ejemplo, operadores de una red de telecomunicaciones, aplicaciones móviles con seguimiento de ubicación, publicidad comportamental, dispositivos de medición y seguimiento de estado físico y salud, domótica, coches inteligentes conectados, etc.

-Cuando los Responsables o encargados tengan entre sus *actividades principales* el tratamiento a gran escala de datos sensibles -> categorías especiales de datos personales o datos relativos a condenas e infracciones penales, pues, aunque el artículo indica "y" , no existe ningún motivo normativo que obligue a aplicar ambos criterios simultáneamente.

Gobernanza de datos (desde la seguridad)

Roles principales

Bloques de responsabilidad

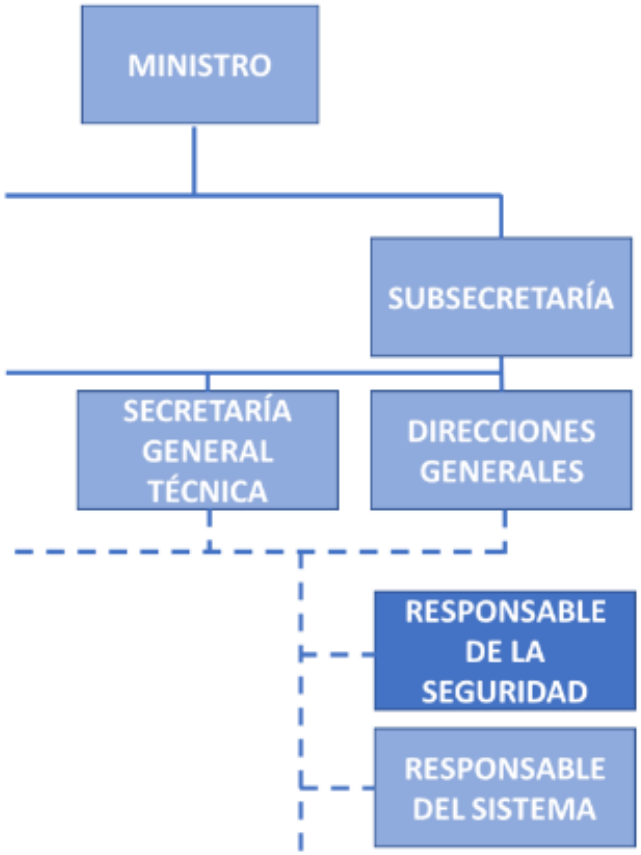
Gobernanza de datos (desde la seguridad)

Roles principales

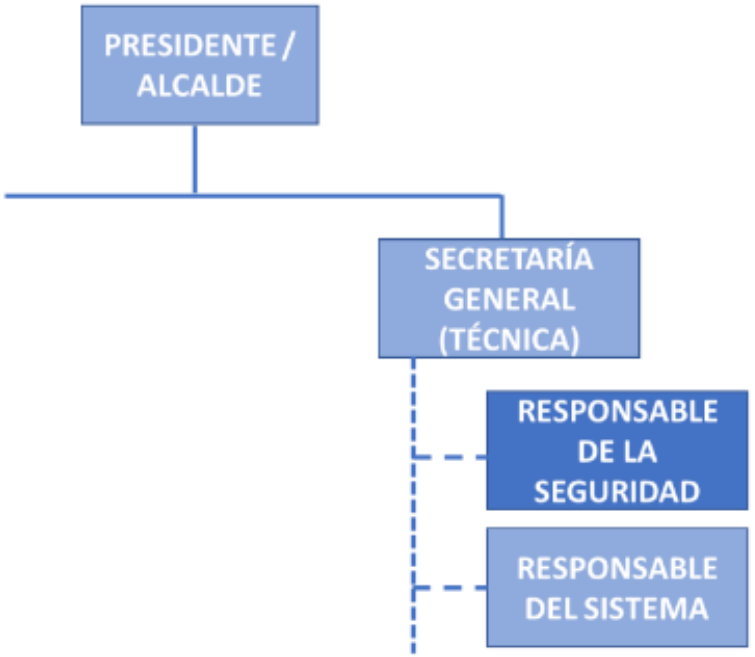
Niveles de la estructura de seguridad

Gobernanza de datos (desde la seguridad)

Organigrama Sector Público



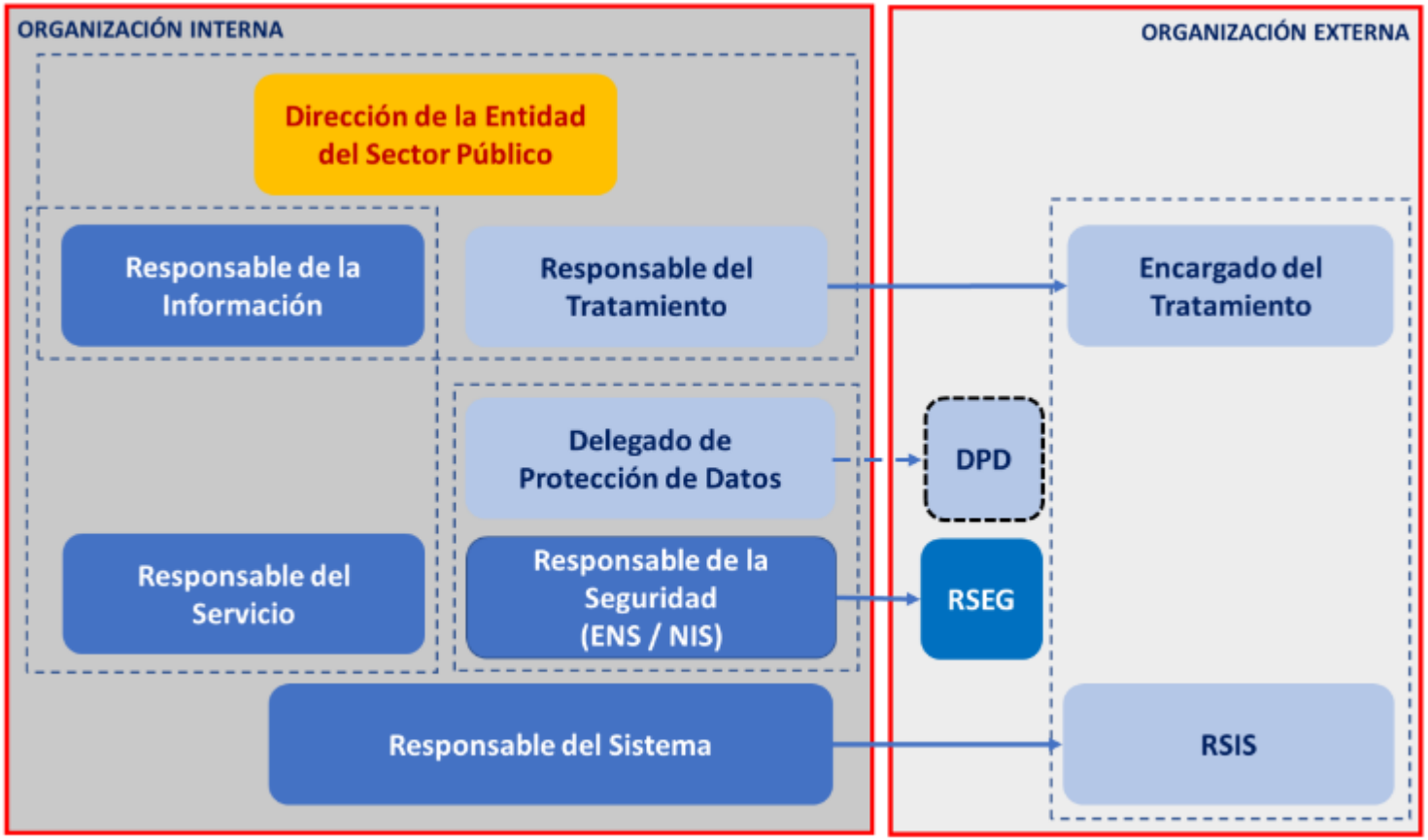
AGE, Departamento Ministerial (tipo)



Entidad Local (tipo)

Gobernanza de datos (desde la seguridad)

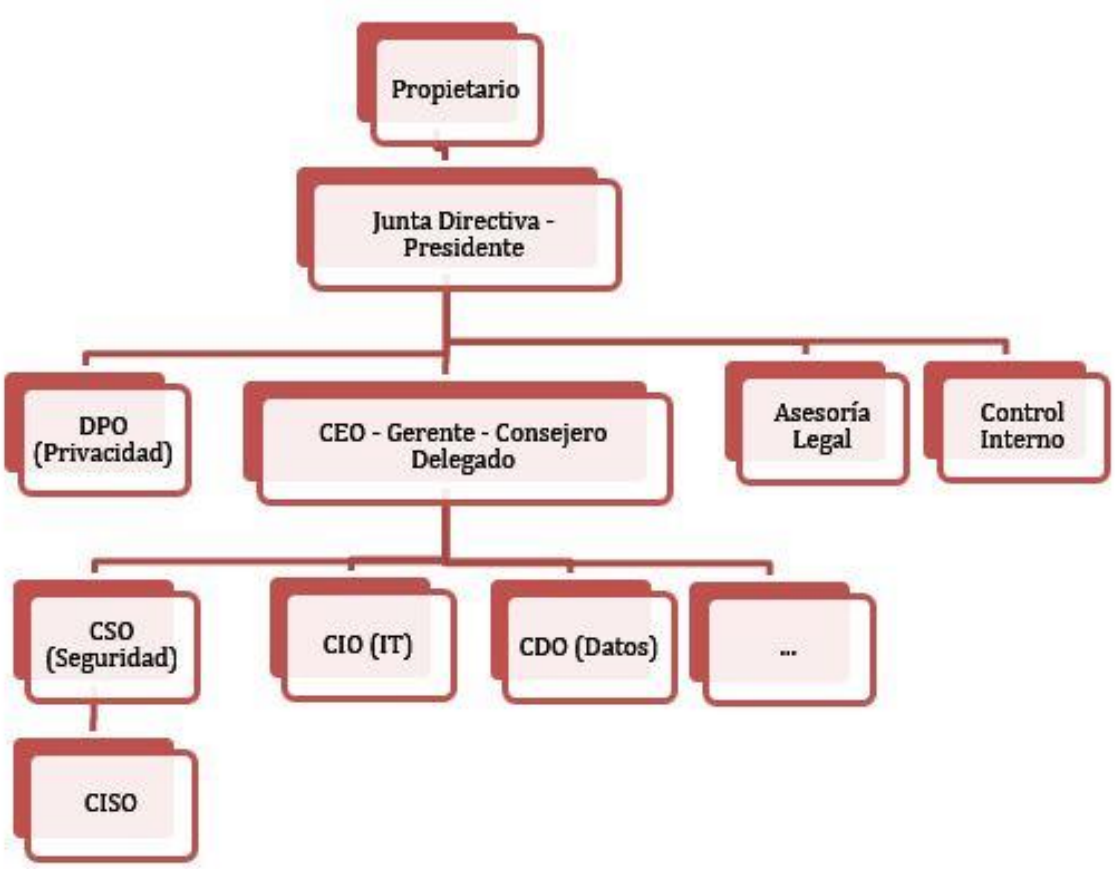
Organigrama Sector Público



Esquema conceptual de la Seguridad de la Información y la Protección de Datos

Gobernanza de datos (desde la seguridad)

Organigrama Sector Privado



Gobernanza de datos (desde la seguridad)

CDO – Chief Data Officer

_**El *chief data officer* (CDO) es el responsable de los datos de una empresa al más alto nivel,** tanto desde un punto de vista tecnológico como de negocio, incluyendo seguridad.

_Ayuda a gestionar el dato como activo corporativo.

_Entre sus funciones se incluyen la estrategia para la explotación del dato y gobierno del dato; es decir, definir políticas de seguridad en la gestión y almacenamiento de los datos, políticas de privacidad, así como mantenerse al día con las novedades en temas de regulación que marca el país o, en este caso, la Unión Europea.

_

Gobernanza de datos (desde la seguridad)

CDO – Chief Data Officer

_el perfil del CDO debe ser híbrido: tecnológico, de negocio y con conocimientos regulatorios, un perfil que sea **muy versátil a nivel empresarial**. Es por ello que suele ser una figura que se elige entre los perfiles que ya trabajan dentro de la empresa, dada la profundidad de conocimiento del negocio que debe tener.

_debe actuar como el puente entre negocio y tecnología. Es habitual que el CDO tenga un equipo técnico y un equipo funcional conocedor del negocio.

_debe contar con un equipo experto en analítica avanzada y un centro de excelencia analítico para extraer el conocimiento de los datos y ponerlo a disposición de toda la compañía.

_

Gobernanza de datos (desde la seguridad)

CDO – Chief Data Officer

_Responsable del gobierno de los datos de la empresa, el CDO debe actuar como puente entre negocio y tecnología. Decide qué datos se usan, cuándo se usan y para qué, valida las tecnologías que se utilizan, tiene que asegurar y consensuar la trazabilidad del dato para tener constancia de toda transformación que sufren y todos los usuarios que hacen uso de ellos, así como la aplicación de negocio que tiene el uso de los datos.

_**Este perfil va ganando peso dentro del organigrama de las empresas y en algunos casos ya forman parte del consejo de administración**, pero sin duda su capacidad de traductor entre las áreas de negocio y tecnología lo sitúan en una posición global con línea directa de *reporting* al CEO.

_

Gobernanza de datos (desde la seguridad)

Marco jurídico en ciberseguridad (Nivel Europeo)

- EU Cybersecurity Strategy Dic 2020.
- Reglamento UE 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.
- Directiva 2019/713 de 17 de abril de 2019 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.
- Directiva UE 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información (Directiva NIS).
- Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Reglamento UE 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior .

Gobernanza de datos (desde la seguridad)

Marco jurídico en ciberseguridad (Nivel Nacional)

- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (Trasposición Directiva NIS).
- Real Decreto ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).

Gobernanza de datos (desde la seguridad)

El tamaño de la empresa y su infraestructura (interna / externa)

Gobernanza de datos (desde la seguridad)

El tamaño de la empresa y su infraestructura (interna / externa)

CCM™
Cloud Controls Matrix

Gobernanza de datos (desde la seguridad)

Relación entre seguridad y datos personales

_**El Reglamento General de Protección de Datos (RGPD)** pone el foco en cómo se deben tratar los datos de terceros, buscando que sea cada sujeto el que tenga que autorizar de forma explícita el propósito del procesamiento a la hora de ceder sus datos.

_La transparencia en la gestión de la información va a ser, por tanto, imprescindible en las compañías, independientemente de su tamaño, que deben también analizar cuáles son los riesgos que se derivan de la utilización de información de terceros, más aún en aquellas organizaciones que manejan datos personales a gran escala.

_La seguridad del tratamiento es un aspecto básico recomendando en el artículo 32 de la normativa, que señala ya cuáles deben ser las medidas, técnicas y organizativas, apropiadas para garantizar un óptimo nivel de seguridad. Éstas deben incluir:

- Seudonimización y cifrado de datos personales.
- Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente.
- Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

_.

Gobernanza de datos (desde la seguridad)

Relación entre seguridad y datos personales

_el artículo 5 del RGPD indica cuáles son los principios relativos al tratamiento de datos personales y que convienen tener muy en cuenta a la hora de afrontar cualquier proyecto de Big Data y de **análisis de datos**, que tienen sus fases más críticas tanto en recolección de datos, como la validación y verificación de los mismos.

_Los principios son:

- Licitud, lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Plazo de conservación.
- Integridad y confidencialidad.

La normativa pone fin al denominado consentimiento tácito, requiriendo por parte del usuario una manifestación inequívoca sobre el mismo

Gobernanza de datos (desde la seguridad)

Relación entre seguridad y datos personales

- Principios de seguridad de la información (el valor de los datos)
- Licitud del tratamiento
- Seguridad de los datos
- Brechas de seguridad

Gobernanza de datos (desde la seguridad)

Relación entre seguridad y datos personales

Principios de seguridad de la información

5.1.f) RGPD los datos personales serán tratados de tal manera **que se garantice una seguridad adecuada** de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas **(«integridad y confidencialidad»).**

Gobernanza de datos (desde la seguridad)

Relación entre seguridad y datos personales

Licitud del tratamiento

_ Art 6 1 f) y considerando 42: seguridad en las redes

_ El RGPD contempla como una de las causas justificativas del tratamiento de datos el interés legítimo perseguido por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

_ Dentro de los intereses legítimos del responsable del tratamiento estaría el estrictamente necesario y proporcionado para **garantizar la seguridad de la red y de la información y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes** por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (equipos de respuesta a incidentes de seguridad informática (proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad En este supuesto se incluiría el impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas

_ Disposición adicional novena LOPD-GDD : Tratamiento de datos personales en relación con la notificación de incidentes de seguridad

_ La normativa nacional contempla que cuando se deban **notificar incidentes de seguridad** las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (equipos de respuesta a incidentes de seguridad informática (proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, **pueden tratar los datos personales contenidos en tales notificaciones**, si bien exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Gobernanza de datos (desde la seguridad)

Relación entre seguridad y datos personales

Seguridad de los datos

_ Seguridad de los datos Art 32 y Considerando 83 RGPD

_ A fin de mantener la seguridad y evitar que el tratamiento infrinja el RGPD, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado Estas medidas **deben garantizar un nivel de seguridad adecuado** incluida la **confidencialidad** teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

_ Evaluación de los riesgos. Artículos 25, 32, 35 y 36 RGPD. Artículo 28 LOGP-GDD.

_ El RGPD recoge que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del propio Reglamento A fin de poder demostrar la conformidad con el RGPD, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

_ Entre los criterios a tener en cuenta para aplicar estos principios se encuentra el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, pero también los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

Gobernanza de datos (desde la seguridad)

Tratamientos de datos personales con fuerte componente innovador que hace uso de nuevas tecnologías

- https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-emprende

Facilita EMPRENDE

aepd agencia española protección datos

RGPD HERRAMIENTA PARA TRATAMIENTOS DE EMPRENDEDORES EMPRENDE

Esta nueva herramienta persigue servir de apoyo a emprendedores y startups cuyos tratamientos se caracterizan por un fuerte componente innovador que hace uso de nuevas tecnologías.

Al igual que FACILITA – RGPD, FACILITA – EMPRENDE es una herramienta fácil de utilizar y gratuita basada en una serie de cuestionarios guiados que permiten caracterizar los tipos de tratamiento realizados por la empresa. Al finalizar su ejecución se generan un conjunto de documentos adaptados que sirven de guía y apoyo para cumplir con las obligaciones impuestas por la normativa en materia de protección de datos. En concreto, obtendrá:

- **una política de información en dos niveles compuesta por las cláusulas de informativas a proporcionar en el momento de la recogida de datos y una política de privacidad.**
- **el Registro de Actividades de Tratamiento (RAT) precumplimentado.**
- **el modelo de hoja de registro de incidentes para cumplir con el artículo 33.5 relativo a la documentación de las brechas de seguridad que afecten o puedan afectar a datos personales.**
- **un conjunto de cláusulas contractuales a incluir en los contratos que suscriba con los encargados de tratamientos de datos y proveedores.**
- **si su empresa cuenta con una página web que utiliza cookies y tecnologías similares, una política de cookies**
- **un conjunto de directrices y recomendaciones, para ayudarle en el proceso de adecuación, en relación con la gestión de brechas de seguridad, la atención al ejercicio de los derechos, recomendaciones sobre videovigilancia, indicaciones específicas con relación a la gestión de los riesgos de sus tratamientos, así como a las estrategias de privacidad y medidas de seguridad que deberá implementar.**
- **Una relación de recomendaciones para prevenir el acoso digital.**

Sin embargo, a diferencia de FACILITA – RGPD y como consecuencia de los tipos de tratamientos que suelen ir asociados a los modelos de negocio desarrollados por el tipo de empresas a las que va dirigida FACILITA - EMPRENDE, puede ser que la empresa no se encuentre en un escenario de bajo riesgo, por ejemplo, si el responsable del tratamiento ofrece una aplicación móvil a sus usuarios a través de la que recoge datos de geolocalización para ofrecer determinados servicios en función de la ubicación del interesado. En esos casos, será necesario que personalice y complemente los entregables obtenidos con otros recursos y materiales ofrecidos por la Agencia y por las salidas de otro tipo de herramientas como GESTIONA – EIPD.

En cualquier caso, tenga en cuenta que esta herramienta constituye sólo una ayuda y que, por tanto, **la obtención de los documentos resultantes no implica, de por sí, el cumplimiento automático de las obligaciones impuestas por la normativa**. Es obligación del responsable, y en su caso del encargado, revisar cuidadosamente la documentación generada para adaptarla y actualizarla a la situación concreta y específica de los tratamientos que se lleven a cabo en su entidad en cada momento.

03

Gestión de ciberincidentes y brechas de seguridad

Gestión de ciberincidentes y brechas de seguridad

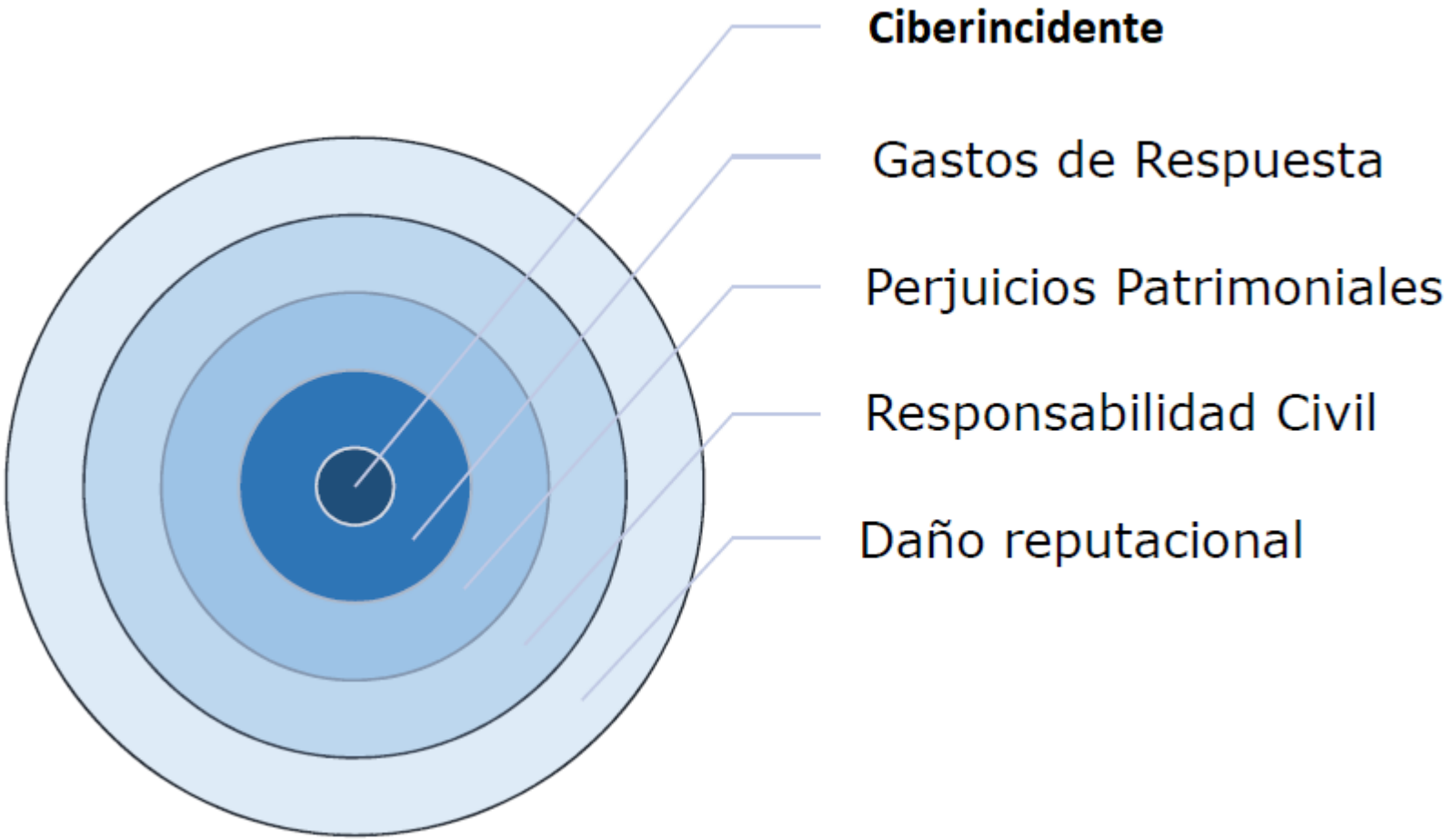
Ciberincidente vs brecha de seguridad

- **Brecha de seguridad**: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de **datos personales** transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
- **Incidente de seguridad** (según ENS): ” como aquel “suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información”
- **Incidente** (Directiva NIS): “todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información”

Todas las brechas (de datos personales) son incidentes pero no al revés

Gestión de ciberincidentes y brechas de seguridad

Consecuencias



Gestión de ciberincidentes y brechas de seguridad

Ciberataques

- Siete de cada diez ciberataques están **dirigidos a PYMES**
- El **coste medio** que supone un ciberataque para una PYME es de **75.000 euros**
- El **60% de las PYMES acaba desapareciendo** seis meses después
- Las denuncias por estafas en Internet, **han crecido en los últimos doce meses un 46,8%**
- Durante las primeras semanas de pandemia se produjo un **aumento del 30.000% en phishing** (*Fuente: Kaspersky*).
- En marzo de 2020 hubo + 1 millón de intentos de ciberataques con la **palabra "covid" como gancho.**
- Con el teletrabajo y el aumento del uso de redes y dispositivos **domésticos,** se han multiplicado los ataques.

Gestión de ciberincidentes y brechas de seguridad

Violaciones o brechas de seguridad

_**Notificación a las autoridades de control** (sin dilación indebida, máx.72horas, si sobrepasamos plazo debemos justificarlo).

_**Notificación a los interesados** (cuando sea probable alto riesgo para derechos y libertades). No es necesario cuando datos anonimizados, existan medidas que garanticen que no existe alto riesgo o suponga un esfuerzo desproporcionado.

_**Documentación vinculada a las brechas de seguridad** (¿En qué registro? ¿Qué información? ¿durante cuánto tiempo?).

_**Procedimientos internos** y **Delegado de Protección de Datos** (obligaciones específicas en materia de seguridad).

Gestión de ciberincidentes y brechas de seguridad

_**Notificación a los interesados** (cuando sea probable alto riesgo para derechos y libertades). No es necesario cuando datos anonimizados, existan medidas que garanticen que no existe alto riesgo o suponga un esfuerzo desproporcionado.

_https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd

Comunica-Brecha RGPD

Comunica-Brecha RGPD es un recurso de utilidad para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de informar a las personas físicas afectadas por una **brecha de seguridad de los datos personales**, tal y como establece el artículo 34 del Reglamento General de Protección de Datos.

Se trata de una herramienta sencilla y gratuita. Una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la Agencia Española de Protección de Datos en ningún caso puede conocer la información que haya sido aportada.

Tenga en cuenta que **Comunica-Brecha RGPD** es una ayuda a la toma de decisiones, pero esta última corresponde ineludiblemente al responsable de tratamiento y en ningún caso su utilización representa el pronunciamiento de esta Agencia sobre la aplicación del art. 34 del RGPD para una brecha de seguridad concreta.

Enlace a la herramienta.

04

Gestión de riesgos y planes de seguridad

Gestión de riesgos y planes de seguridad

Definición

_Ciberriesgo

cualquier riesgo cuyas pérdidas tengan una relación cibernética que provengan de una ataque malicioso (por ejemplo “malware”) o de un evento accidental (por ejemplo, pérdida de datos) que afecte a activos tangibles o intangibles” (Lloyd’sMarketBulletin, -Y5258-2019).

_.

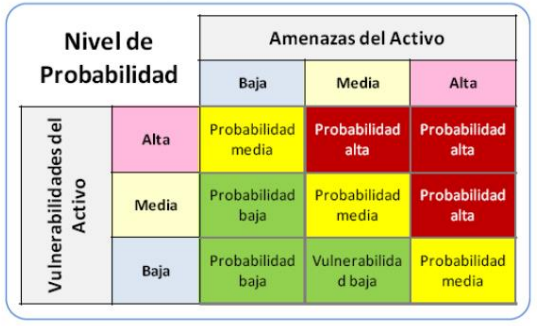
Gestión de riesgos y planes de seguridad

Activos, Amenazas y Vulnerabilidades

Gestión de riesgos y planes de seguridad

Activos, Amenazas y Vulnerabilidades (EJEMPLO)

Activo	Amenaza	Vulnerabilidad	Probabilidad de Amenaza	Impacto
Servidor E-commerce	Error humano (accidental)	Instalar actualizaciones SW sin probarlas	Media	Alto
Servidor E-commerce	Infección Ramsomware	No disponer de anti-malware	Muy alta	Alto
Servidor E-commerce	Fallo eléctrico	Sin redundancia (SAI)	Baja	Alto
Servidor E-commerce	Robo servidor HW	Sin control de acceso físico	Alta	Alto
Servidor E-commerce	Terremoto	CPD en zona no sísmica	Baja	Alto



Gestión de riesgos y planes de seguridad

Activos

¿Qué protegemos?

Activos más críticos para que una organización logre el éxito de los objetivos de negocio o estratégicos

Gestión de riesgos y planes de seguridad

Activos

- Información
- Procesos
- Aplicaciones
- Sistema operativo
- *Hardware*
- Comunicaciones
- Soporte de información
- Instalaciones
- Personal

La información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad.

Gestión de riesgos y planes de seguridad

Activos (valor de la información y servicios)

Gestión de riesgos y planes de seguridad

Confidencialidad

http://www.bbc.com/mundo/noticias/2015/02/150209_television_privacidad_samsung_conversaciones_fp

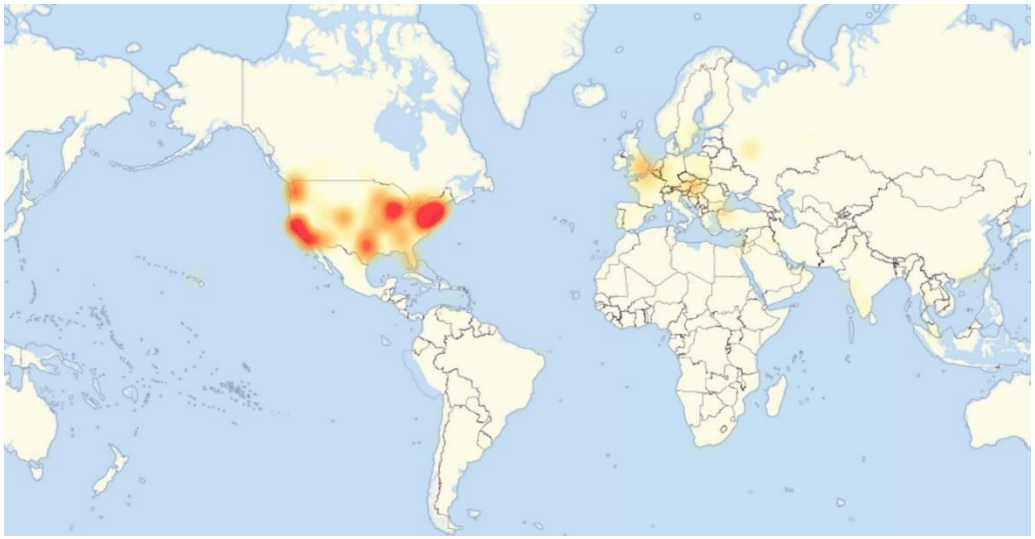
Gestión de riesgos y planes de seguridad

Integridad

http://news.softpedia.com/news/EU-Presidency-Website-Defaced-131187.shtml

Gestión de riesgos y planes de seguridad

Disponibilidad

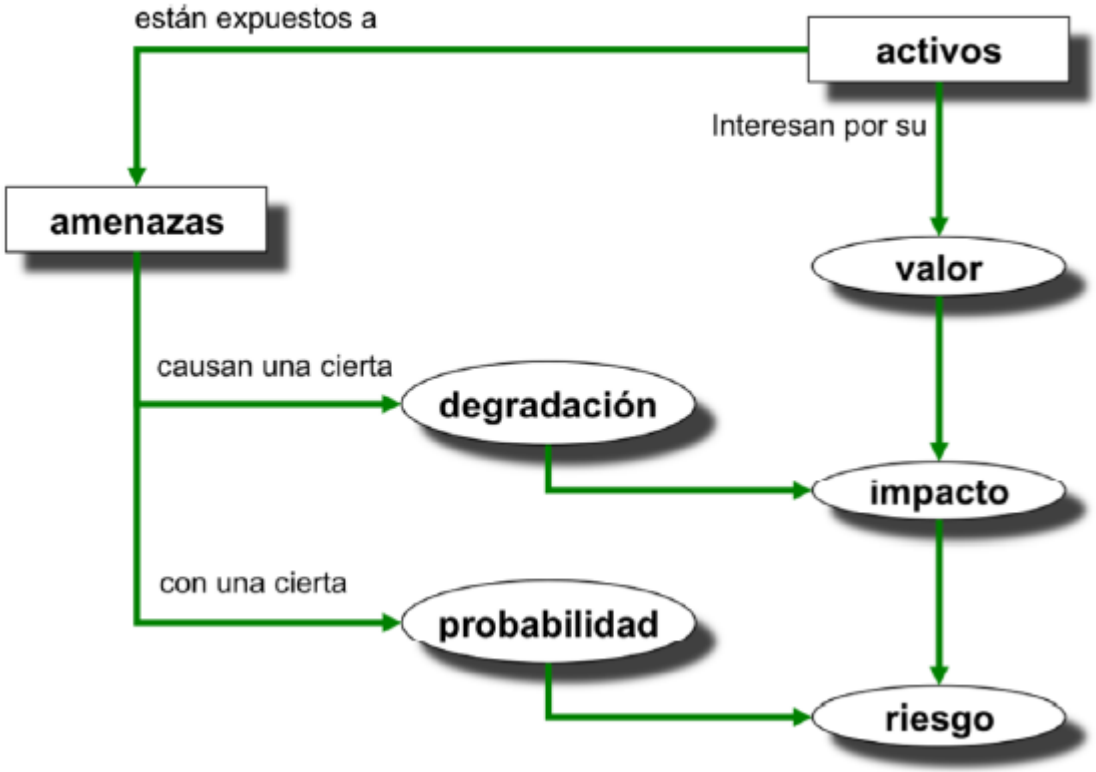


Pero el mapa de los ataques, que provocaron problemas
de acceso en sitios como Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud o The New York Times
entre otros, y su *modus operandi*, atacando servidores de DNS,

https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

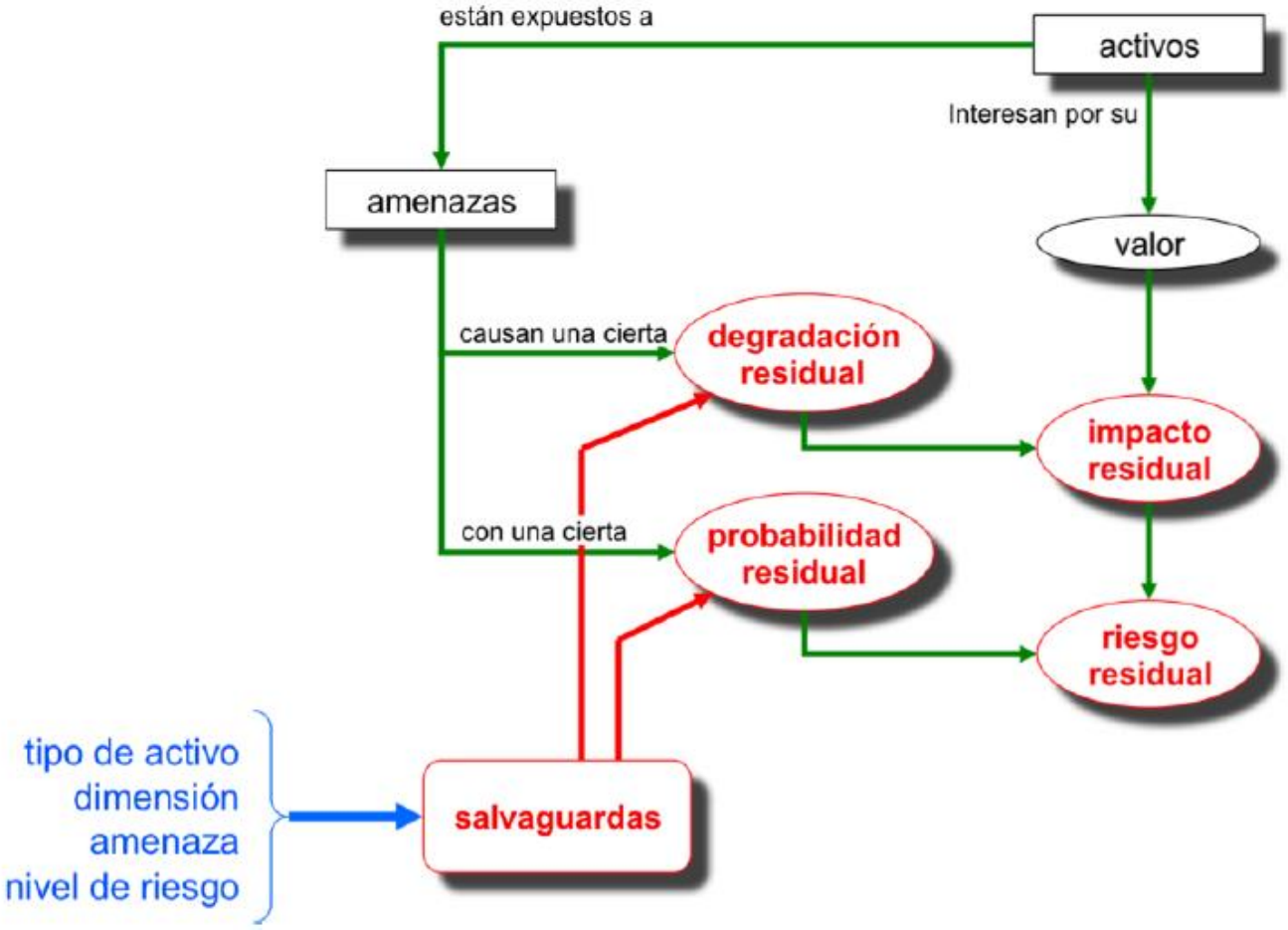
Gestión de riesgos y planes de seguridad

Gestión de riesgos



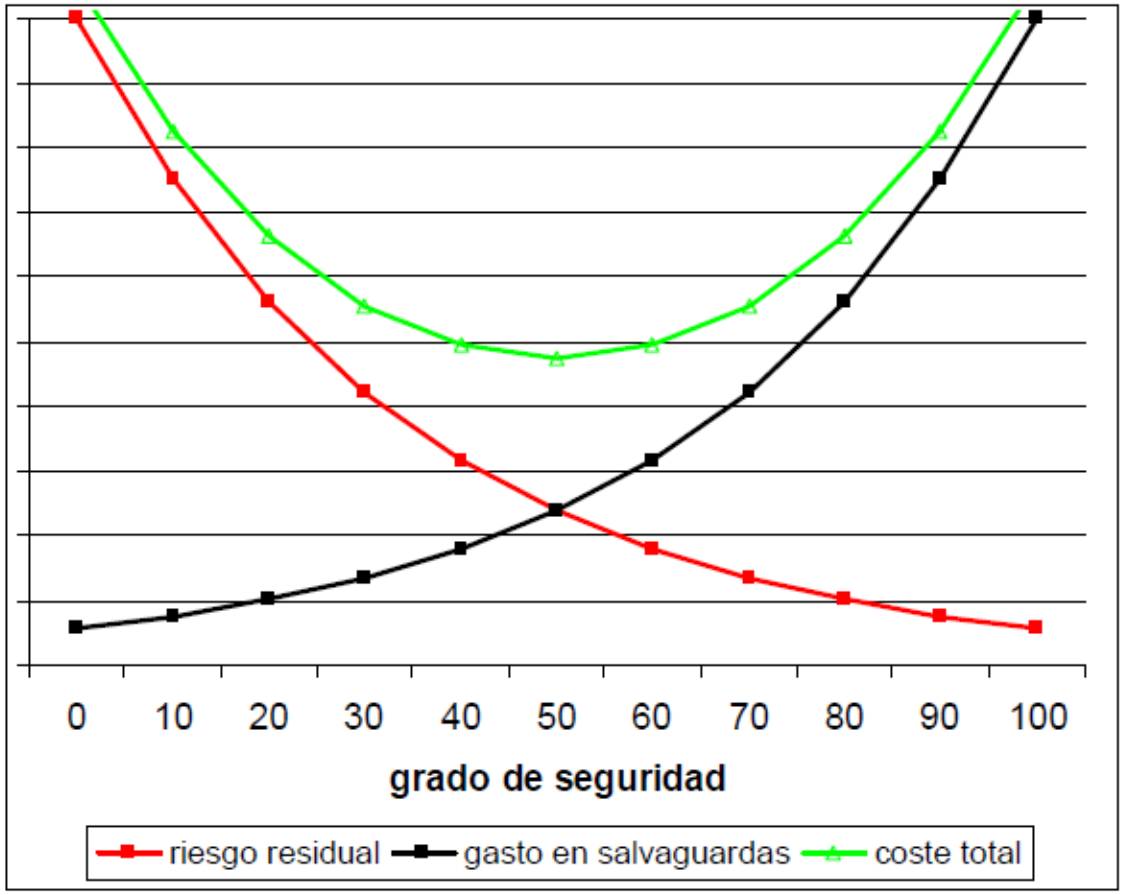
Gestión de riesgos y planes de seguridad

Gestión de riesgos



Gestión de riesgos y planes de seguridad

Gasto en seguridad y riesgo residual



Gestión de riesgos y planes de seguridad

¿Qué hacer con el riesgo?

- **Evitarlo**
  - **si se puede ... es la solución ideal**
  - **prescindir de activos**
- **Reducirlo | mitigarlo**
  - **ocurre menos**
  - **impacto limitado**
- **Transferirlo**
  - **se le pasa a otra organización**
  - **ya no es “mi problema”**
- **Asumirlo | aceptarlo**
  - **pasa a contabilizarse como gasto operacional**

Gestión de riesgos y planes de seguridad

Mapa de riesgos (amenazas x activo)

Consecuencias	Ocurrencia			
	Improbable	Posible	Probable	Muy pro-bable
Altas	4	8	12	16
Moderadas	3	6	9	12
Bajas	2	4	6	8
Insignificantes	1	2	3	4

Gestión de riesgos y planes de seguridad

Metodología MAGERIT y medidas ENS

control	current	ENS
[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)	L0-L3	L2-L3
[org] Marco organizativo	L2-L3 (L1-L3)	L2-L3
[org.1] Política de Seguridad	L3 (L2-L3)	L2-L3
[org.2] Normativa de seguridad	L2	L2-L3 (L2)
[org.3] Procedimientos de seguridad	L2	L2-L3 (L2)
[org.4] Proceso de autorización	L2 (L1-L2)	L2-L3
[op] Marco operacional	L1-L2 (L0-L2)	L2-L3
[op.pl] Planificación	L2	L2-L3
[op.acc] Control de acceso	L1-L2	L2-L3
[op.exp] Explotación	L1-L2 (L0-L2)	L2-L3
[op.ext] Servicios externos	L2	L2-L3
[op.cont] Continuidad del servicio	L1	L2
[op.mon] Monitorización del sistema	L1-L2 (L1)	L3 (L2-L3)
[mp] Medidas de protección	L0-L3	L2-L3
[mp.if] Protección de las instalaciones e infraestructuras	L2-L3	L3 (L2-L3)
[mp.per] Gestión del personal	L1-L2	L2-L3
[mp.eq] Protección de los equipos	L2	L2-L3
[mp.com] Protección de las comunicaciones	L1-L3	L3 (L2-L3)
[mp.si] Protección de los soportes de información	L0-L2	L2-L3
[mp.sw] Protección de las aplicaciones informáticas (SW)	L2	L2-L3
[mp.info] Protección de la información	L0-L2	L2-L3
[mp.s] Protección de los servicios	L2	L3 (L2-L3)

Gestión de riesgos y planes de seguridad

Metodología MAGERIT y medidas ENS (riesgo repercutido potencial, actual, objetivo)

activo	[D]	[I]	[C]	[A]	[T]
ACTIVC	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)
is	(4,2)	(5,0)	(5,0)	(5,0)	(5,0)

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(3,1)	(3,8)	(3,8)	(3,8)	(3,8)
is	(2,9)	(3,8)	(3,8)	(3,8)	(3,8)

activo	[D]	[I]	[C]	[A]	[T]
ACTIVO	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)
is [RRHH-GT] Gestión RRHH Gestrisam	(0,91)	(1,3)	(1,2)	(1,3)	(1,3)

Gestión de riesgos y planes de seguridad

Gestión de riesgos RGPD

Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos

https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd

agencia española protección datos

Gestiona EIPD

Asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos. Esta herramienta gratuita guía a las personas responsables y encargadas del tratamiento en los aspectos que se deben tener en cuenta, proporcionando una base inicial para una gestión adecuada

Con carácter general, el Reglamento General de Protección de datos (RGPD) exige al personal encargado de los tratamientos de datos personales la realización de análisis de riesgos y evaluaciones de impacto con el fin de llevar a cabo una gestión de los riesgos para los derechos y libertades de las personas físicas, por otra parte, la AEPD ha publicado la **lista de tratamientos** de datos personales que requieren una evaluación de impacto de acuerdo con lo previsto en el artículo 35.4 del RGPD.

GESTIONA_EIPD es una herramienta gratuita que guía a su usuario a través de los elementos básicos que deben ser tenidos en cuenta en los análisis de riesgos de los tratamientos y en las evaluaciones de impacto. GESTIONA_EIPD es algo más que una lista cerrada de elementos a tener en cuenta, y aporta a las personas responsables las bases mínimas para iniciar las actividades de análisis y gestión de riesgos en el ámbito del RGPD, incluyendo requisitos de cumplimiento normativo y medidas encaminadas a reducir o mitigar el riesgo del tratamiento. Tenga en cuenta que, en ningún caso, los requisitos de cumplimiento pueden reemplazarse por medidas alternativas técnicas u organizativas, para más información puede consultar el **Listado de elementos para el cumplimiento normativo** del RGPD.

Por tanto, **GESTIONA_EIPD** es una herramienta de ayuda y soporte a la decisión y cuya utilización genera la documentación básica sobre la cual hay que realizar un análisis y gestión del riesgo por parte de las personas responsables y encargadas para cumplir con lo previsto en el RGPD y la LOPDGDD. Esta documentación básica deberá ser completada y analizada por el personal responsable del tratamiento y, en su caso, la persona encargada, siguiendo las indicaciones establecidas en la **Guía práctica para las evaluaciones de impacto en la protección de datos personales**, con el fin de demostrar en todo momento que los tratamientos se llevan a cabo de conformidad con los requisitos que establece el RGPD y la LOPDGDD.

Gestiona_EIPD puede resultar especialmente útil para aquellas PYMES que necesitan iniciarse en la realización de evaluaciones de impacto en protección de datos personales.

Gestión de riesgos y planes de seguridad

Plan director de seguridad

https://www.youtube.com/watch?v=WkqLTbf1mEw

Gestión de riesgos y planes de seguridad

Análisis de riesgos práctico (¿Conoces tus riesgos?)

_https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD


Unión Europea
Fondo Social Europeo
El FSE invierte en tu futuro


DELPHOS
AGENCIA PÚBLICA ADMINISTRATIVA LOCAL


AYUNTAMIENTO
Rincón de la Victoria

Gracias.