UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Autocheking sobre una auditoría de SI RGPD

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Villacorta Rivera, Monica Jazmin

Tutor/a: Gil Pechuán, Ignacio

CURSO ACADÉMICO: 2021/2022

Resumen

En las auditorías de seguridad se analizan los riesgos y vulnerabilidades que presentan las empresas, los puntos a cumplir son muchos y la frustración de las organizaciones por no superar estas auditorías es grande, ya que acaban por no entender qué es lo que necesitan realmente para poder disponer de una completa seguridad en sus sistemas de información. El presente trabajo de fin de grado (en adelante, TFG) pretende mostrar las principales amenazas y delitos a los que se exponen las organizaciones al no disponer de los correctos mecanismos, políticas, normas y procedimientos que garanticen la seguridad dentro de su negocio. Con la herramienta de autodiagnóstico, todas las entidades podrán saber en qué nivel de seguridad se encuentran y qué es lo que deben corregir o comenzar a implantar, garantizando así la continuidad en su negocio.

Palabras clave: seguridad, amenazas, delitos, políticas, medidas, auditoría, RGPD, AEPD, diagnóstico, ciberdelincuentes, incidentes.

Abstract

In security audits, the risks and vulnerabilities that companies present are analysed, the points to be fulfilled are many and the frustration of organisations for not passing these audits is great, as they end up not understanding what they really need in order to have complete security in their information systems. This Final Degree Project (hereinafter, TFG) aims to show the main threats and crimes to which organisations are exposed when they do not have the correct mechanisms, policies, standards and procedures to ensure security within their business. With the self-diagnosis tool, all entities will be able to know what level of security they are at and what they need to correct or begin to implement, thus guaranteeing the continuity of their business.

Keywords: security, threats, crime, policies, audit, GDPR, diagnosis, cybercriminals, incidents.

Agradecimientos

Al principio todo era un “no lo voy a conseguir”, “la carrera que has elegido es muy complicada”, etc., pero sin el apoyo de mis padres y su confianza en mí, todos esos comentarios y pensamientos no hubiera podido apartarlos tan fácilmente de mi mente. Sin la ayuda de ellos y sus constantes ánimos, no hubiera conseguido poder tener confianza en mí misma para superar esta carrera.

Gracias también a mis compañeros que estuvieron durante mis últimos años de carrera, ya que siempre es importante tener a alguien que se encuentre en la misma situación que tú y pueda ponerse en tu piel durante los momentos más complicados de la carrera (exámenes, trabajos, etc.) y también durante lo momentos buenos, para vivirlos y celebrarlos.

Agradecer también a mi tutor de TFG, que me ha ayudado mucho a orientar y decidirme en la temática, las ideas y su contenido. Asimismo, si no hubiera conocido su asignatura y lo que nos contaba en clase sobre el área de consultoría y auditoría informática, no hubiera conocido este mundo, ya que la informática siempre está muy enfocada a la programación y hay muchos campos desconocidos que si no te los llegan a explicar y contar no sabes ni que existen.

La experiencia vivida durante mi estancia en prácticas y los conocimientos obtenidos también me han ayudado mucho a llevar a cabo este TFG, por ello me gustaría agradecer a todo el equipo de Gesprodat, sin ellos no me hubiera dado cuenta de lo mucho que me gusta el mundo de la consultoría, auditoría y seguridad, ni podría haber desarrollado este TFG. Gracias por abrirme las puertas en vuestra empresa y haberme enseñado tanto en tan poco tiempo.

Por último y no menos importante, agradecer a mi hermana por su tiempo dedicado a ayudarme y aconsejarme a la estructuración y mejora de mi trabajo. Su experiencia en la realización y entrega de su TFG me ha servido de mucho.

Índice

1. Introducción 5
   1.1. Introducción a la seguridad 6
   1.2. La seguridad informática y su evolución 7
   1.3. Seguridad física y lógica 10
2. Amenazas y delitos 11
   2.1. Delitos informáticos 13
   2.2. Amenazas lógicas y humanas 14
   2.3. Ciberataques 15
      2.3.1. Ataque a contraseñas. 15
      2.3.2. Ataque por ingeniería social. 16
      2.3.3. Ataque por malware o código malicioso: 17
      2.3.4. Ataque a las conexiones: 18
3. Políticas de seguridad 19
   3.1 Puntos clave sobre el establecimiento de políticas 20
   3.2 Inexistencia o deficiencias en las políticas de seguridad 21
   3.3 Ejemplos de políticas de seguridad 21
4. La normativa legal en materia de seguridad 23
   4.1 El RGPD y los principios en los que se basa 24
   4.2 Adaptación de la LOPDGDD al RGPD 25
   4.3 Cumplimiento de las auditorías RGPD 26
      4.3.1 Dominios a revisar para el cumplimiento 27
   4.4 Integración de la auditoría de protección de datos en la auditoría de SI 29
5. Desarrollo de un prototipo previo al desarrollo de un plan de mejora de la SI 30
   5.1 Bloques del autodiagnóstico 33
      5.1.1 Gobierno de la privacidad 34
      5.1.2 Minimización y exactitud de los datos 34
      5.1.3 Responsabilidad proactiva 35
      5.1.4 Plazos de conservación 35
      5.1.5 Transparencia e información 36
      5.1.5.1 Transparencia e información: web 36
      5.1.5.2 Transparencia e información: videovigilancia 37
      5.1.6 Deber de secreto 37

5.1.7 Registro de actividades de tratamiento 37
5.1.8. Derechos de los interesados 38
5.1.9 Seguridad: violaciones de seguridad..... 38
5.1.10 Seguridad: medidas técnicas y medidas organizativas..... 39
5.1.12 Seguridad: Formación 40
5.1.14 Encargado de tratamiento 40
Conclusiones. 41
Motivación. 43
BIBLIOGRAFÍA 44
Anexos. 47
A. AutoAuditat Quiz.....47
A.1 Clave de respuesta 65
B. ODS (Objetivos del Desarrollo Sostenible) 67

1. Introducción

El mundo tecnológico está siempre en constante evolución, cada día surgen nuevas tecnologías. La innovación tecnológica ha hecho que vivamos en una sociedad más cómoda y sencilla, el día a día de las personas depende, fundamentalmente, de la tecnología ya que ponen en manos de esta, gran cantidad de información de carácter personal, la cual es necesaria proteger. No solamente crece la dependencia tecnológica, si no que a su vez aumentan también los riesgos a los ataques informáticos. Cualquiera puede ser víctima de un ciberataque, invertir en ciberseguridad es más que fundamental y es algo que se debería tomar más en consideración.

Es raro no toparse con una noticia sobre ataques informáticos, robo de información y/o identidad, etc. Las consecuencias de sufrir un ataque pueden ser muy graves, sobre todo para las grandes organizaciones, la mayoría de ellas se encuentran en un proceso de digitalización y pueden comprometer la seguridad de los datos que sus clientes, proveedores, socios y trabajadores, ponen en su tejado. Alguna de estas consecuencias puede ser: grandes costes económicos, pérdida de la confianza de los clientes y con ello, pérdida de reputación en la empresa.

Como ya se ha mencionado, las grandes empresas tienden a hacer uso de tecnologías cada vez más modernas, para mantenerse en constante crecimiento, con el fin de lograr acelerar sus procesos y mantener su competitividad en el mercado. De acuerdo con lo que dijo Alonso (2016) en la conferencia "Cómo gestionar la seguridad informática en las empresas" [1], no sirve de nada tener las medidas de seguridad más caras y modernas, si no se tienen implantadas las medidas básicas, como por ejemplo establecer medidas de complejidad para la definición de contraseñas como la combinación de caracteres y establecimiento de una longitud mínima. No sirve de nada gastarse millones de euros en ciberseguridad si como dice Alonso, no se empieza por lo básico.

A parte de las medidas de seguridad básicas a nivel informático, también existen leyes que regulan el tratamiento de datos personales de las personas físicas, así como la libre circulación de los mismos, en concreto la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD) que es la adaptación a la normativa del Reglamento General de Protección de Datos (en adelante, RGPD) y que pretende garantizar el respecto a los derechos digitales. En 1999 ya se disponía de una Ley Orgánica en materia de Protección de Datos (en adelante, LOPD), pero el uso de las tecnologías no estaba tan masificado como a día de hoy, el volumen de datos que circulaban de manera digital no era para nada comparable con la actualidad. Con la entrada en vigor de la LOPDGDD 3/2018 el 25 de mayo del 2018, la cual llegó a sustituir a la LOPD 15/1999, todas las entidades que manejaban datos de personas físicas se vieron obligadas a cumplir con la LOPDGDD y el RGPD.

Para garantizar que cumplían con estas normativas, comenzaron a realizar Auditorías de seguridad como mínimo una vez al año y con ello, comprobar qué puntos cumplían, incumplían o debían corregir. Cumplir con la normativa no es tarea fácil para todas las entidades, sobre todo para aquellas que manejan una gran cantidad de datos o datos muy sensibles o críticos.

[1]Chema Alonso (abril de 2016). Conferencia de Chema Alonso: Cómo gestionar la Seguridad Informática en las empresas. Recuperado el 13 de junio de 2022 de: https://www.youtube.com/watch?v=_PsB2e0U5FU

El servicio de diagnóstico previo de auditoría, se basa en un servicio dirigido a las empresas que desean conocer el estado puntual de implantación y eficacia de su sistema de Gestión en prevención de riesgos de sus sistemas de información, ya que una auditoría supondrá una herramienta verdaderamente útil para aquellas empresas cuyos sistemas de información son de reciente implantación o no han sido frecuentemente contrastados y deseen conocer una opinión profesional, basada en los aspectos técnicos y de procedimiento sobre la viabilidad del sistema y su capacidad para evitar riesgos, potenciales problemas y así conseguir los objetivos marcados.

Todo servicio previo de diagnóstico resulta de utilidad, para conocer el estado de cumplimiento de potenciales estándares, normativas, políticas y procedimientos; detectando carencias y debilidades del sistema, que pueden ser corregidos en fase temprana a través de un plan de acciones correctoras que servirá como preparación para una futura Auditoría de Sistemas de Información (o incluso de Certificación), ya que se comprueba el grado de cumplimiento por parte de la empresa, así como la capacidad del sistema y evitando de esta forma, llegar a la auditoría con las manos vacías.

Un diagnóstico comenzará en primera instancia conociendo la infraestructura tecnológica con la que cuenta una organización, que puede ser tan general o específica como se requiera, de un área concreta o tan amplia que pueda abarcar en su totalidad a una empresa, incluyendo todos sus procesos sin importar el área geográfica o forma que la comprendan.

En su contra, también debemos aclarar que si, en gran parte, la auditoría informática consiste en realizar el levantamiento de información, su clasificación y la evaluación de la misma, lo cual nos permite determinar si los procesos, los activos tecnológicos y la información, son congruentes y mantienen la integridad y la finalidad para los cuales originalmente fueron implementados y/o adquiridos, así como su cumplimiento de acuerdo a normas y reglas internas o corporativas, una herramienta de diagnóstico no puede sustituir esta posibilidad, ni lo pretende; únicamente persigue ayudar mediante el conocimiento y la aproximación de una situación real informada y una recomendación técnica fundamentada en normas y políticas, así como ayudar a las entidades a llevar un control sobre cada una de los aspectos importantes a proteger.

Este TFG pretende desarrollar una herramienta de autodiagnóstico, llamada “AutoAuditat” que permita a la empresa, de manera rápida, flexible y eficaz identificar las necesidades o áreas de oportunidad de la empresa para poder corregirlas y/o actualizarlas de manera oportuna, así como hacer más eficiente la misma, sin tener que esperar a la llegada de su auditoría anual y darse cuenta de sus carencias en el último momento.

1.1. Introducción a la seguridad

Para hablar de seguridad informática lo primero que hay que hacer es comprender el concepto de seguridad. La seguridad se refiere a la ausencia de peligro, riesgos y/o amenazas tanto internos como externos. Hay una gran variedad de tipos de seguridad, entre ellos: seguridad de la información, las personas, ambiental, económica, sanitaria, entre otras.

Castro, Morán, Navarrete, Cruzatty, Anzúles, Mero, Qumiz & Merino (2018)[2] señalan que cuando se pretenda realizar algo de forma segura, las acciones a tener en cuenta involucradas dentro del concepto de la seguridad, el cual se caracteriza por la gestión de los riesgos, son:

- prevenir,
- transferir,
- mitigar y
- aceptar.

Tal como define Castro, "cuando se está buscando hacer algo más seguro, estas acciones son algo que se debe de considerar sin importar el área, se aplica a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera" (Castro et al., 2018, p.12).

1.2. La seguridad informática y su evolución

Tal y como se ha mencionado al principio de este capítulo, la seguridad ha existido desde los principios de la historia y su evolución ha dado grandes avances. Del mismo modo, la evolución de la seguridad en las organizaciones tampoco se ha quedado atrás y esto ha sido impulsado principalmente por los avances tecnológicos.

Como cuenta INCIBE (2015) en su artículo "La seguridad vista desde sus inicios"[3], la seguridad ha tenido su punto de partida en la década de los setenta. En esta época lo más común dentro de una organización era toparse con trabajadores poco conocedores de los riesgos asociados a la información que manejaban: en las organizaciones no se realizaba ningún tipo de copia de seguridad y las medidas de seguridad física que se aplicaban eran totalmente inadecuadas.

Con la aparición de los primeros virus informáticos en los años ochenta, debido a la popularización de los ordenadores, se desarrollaron las primeras herramientas de ciberataque. Esto hizo que la tecnología diera un paso a la comercialización de los sistemas antivirus, de los cuales se hablará más adelante.

La protección en la red comenzó a aplicarse a partir de los primeros ataques a través de Internet que surgieron a principios de los años noventa. Los trabajadores hacían un mal uso de Internet, la dependencia hacia los proveedores, sin establecer medidas de seguridad adecuadas era cada vez más fuerte y la información se almacenaba en dispositivos externos con insuficientes medidas de protección.

[2]Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Vol. 46). 3Ciencias. Recuperado el 10 de febrero de 2022 en: Seguridad-informática.pdf (3ciencias.com)

[3]INCIBE (11 de marzo de 2015). La seguridad vista desde sus inicios. Recuperado el 10 de abril de 2022 de: https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

El uso masivo de las redes sociales en la década del 2000 hizo que la seguridad de la información cobrara más vida; los ataques comenzaron a dirigirse a las herramientas encargadas de proteger la información y la red corporativa, cada vez se producían más fraudes online. Durante la década del 2010 el malware se volvió indetectable, esta situación dio paso a la elaboración de planes sólidos de concienciación de los empleados sobre seguridad de la información y el establecimiento de un mayor control relacionado con la privacidad de la información para evitar su fuga, y a esto se le sumó el uso de herramientas de cifrado de información a nivel corporativo y en algunos casos, personal.

Cabe destacar, que, pese a ese largo camino hacia un futuro seguro, las empresas no se han rendido y son cada vez más conscientes de la importancia de la seguridad para el buen funcionamiento y prospección de su negocio, pero quedan muchas organizaciones que aún tienen muchos pasos por delante para situarse en un buen nivel de concienciación. La forma de afrontar la política de ciberseguridad ha cambiado mucho a lo largo de los años, no solo las empresas han cambiado su forma de actuar si no que también los desarrolladores y fabricantes de soluciones de seguridad.

Sin embargo, dentro del concepto de la seguridad informática, primero debemos distinguir y entender dos puntos clave que derivan de esta: la seguridad de la información y la protección de datos personales.

La seguridad de la información se enfoca en construir un sistema (controles) que trate todos los posibles riesgos que puedan afectar a la seguridad de la información. Por lo tanto, como indica Castro et al. (2018)[4], estos controles tienen que estar basados en tres principios básicos de la seguridad: **disponibilidad**, **integridad** y **confidencialidad** de la información. Estos tres principios son los que subyacen a todos los programas e infraestructura: disponibilidad de los recursos (equipo, comunicaciones, personal, datos, información y cifras), integridad de la información (la veracidad y certeza de los datos capturados por el personal interno) y la confidencialidad de esta (acceso y consulta por las personas/usuarios autorizados para ello). El objetivo principal de la seguridad de la información son los datos, es decir, evitar su pérdida y la modificación no autorizada de los mismos. Esta protección deberá garantizar los tres principios nombrados anteriormente. Por lo tanto, un sistema se considerará seguro siempre que esté garantizado en todo momento:

1. **Disponibilidad**: los usuarios tendrán disponible los datos cuando sea necesario, es decir, los datos deben poder ser recuperados correctamente en el momento en que lo desee el usuario.
2. **Integridad**: asegurará que el contenido y los datos estén siempre completos y correctos, solamente podrán ser modificados y/o actualizados por aquellos usuarios que estén autorizados. Para poder asegurarla, según Castro et al. se deberá tener en cuenta lo siguiente:
    - Controlar el tráfico de la red para detectar posibles intrusiones;
    - Realizar auditorías en los sistemas para implementar políticas de auditorías en las que se registren quién hace cada cosa, cómo, cuándo y con qué información (Castro et al., 2018, p.26).

[4]Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Vol. 46). 3Ciencias. Recuperado el 10 de febrero de 2022 en: Seguridad-informática.pdf (3ciencias.com)

3. **Confidencialidad**: únicamente los usuarios autorizados podrán acceder los recursos, datos e información. En este punto Castro resalta que, para poder garantizar la confidencialidad, generalmente se recurre a tres recursos:
    - Autenticación de los usuarios;
    - Gestión de privilegios;
    - Cifrado de información (Castro et al., 2018, p.26).

En la figura se puede ver los tres pilares fundamentales nombrados.

Figura 1. Principios básicos de la seguridad de la información.

Fuente: (Castro et al., 2018, p.25). Recuperado el 10 de febrero de 2022 de Seguridad-informática.pdf (3ciencias.com)

Sin embargo, hay otros puntos que también deben ser considerados, como son: la autenticidad, responsabilidad, no repudio y fiabilidad. De acuerdo con Castro et al. (2018), si alguno de estos puntos clave mencionado es fácilmente vulnerable, entonces se perderá seguridad en la información.

Por otra parte, el objetivo principal de la protección de datos no son los datos, sino el contenido sobre las personas y evitar así un uso abusivo. La norma jurídica que regula el tratamiento de datos de carácter personal es la LOPDGDD, la cual se explicará con más profundidad en otro capítulo.

Cabe destacar, que, aunque haya que distinguir estos dos puntos, las medidas de protección que se han de implementar serán las mismas. Una vez definidas las ramas que se desprenden de la seguridad informática, conviene definir qué se entiende por seguridad informática.

De este modo, según define Costas Santos: “la seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización” (Costas Santos, 2011, p.19).

La seguridad informática puede considerarse como un aspecto derivado de la seguridad de la información, ya que la seguridad de la información además de abarcar los controles de seguridad informática también abarca los controles de seguridad física (los accesos a las instalaciones, la gestión de los recursos humanos, la protección legal, la organización de la empresa, los procesos y los activos de información en todos estos procesos de la organización).

Castro et al. (2018)[5], destaca que aquello que tampoco hay que olvidar dentro del área de la seguridad, se puede separar en los siguientes puntos:

- **Usuarios**, considerados el punto débil debido a que pueden ocasionar más daños a la seguridad. Con esto se quiere decir, que una persona es muy complicada de controlar, ya que un día puede ocasionar un incidente de poca gravedad y otro día puede olvidar cómo se gestionaban ciertas cosas y echar a perder todo el trabajo (por ejemplo, los empleados de una organización).
- **Información**, considerada la base para cumplir con la seguridad informática, ya que es el centro de lo que se quiere proteger.
- **Infraestructura**, puede decirse que es uno de los medios que corre menos riesgos y se encuentra más controlado, ya que dependerá de los procesos de protección que se establezcan (esto no quiere decir que no corra riesgos).

1.3. Seguridad física y lógica

Es necesaria una aproximación seria y objetiva a la seguridad de la información que nos permita determinar de manera fiable los riesgos a los que estamos expuestos, en qué medida lo estamos y cuáles son las consecuencias. La seguridad informática puede entenderse desde dos enfoques los cuales deberán ir de la mano: el punto de vista físico y lógico.

Muchas de las definiciones encontradas sobre qué son exactamente la seguridad física y lógica son muy similares. Por tanto, la seguridad física se podría definir como "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial" (Costas Santos, 2011, p.50).

De modo que, la seguridad física es uno de los aspectos más importantes al momento de realizar un diseño de un sistema informático; es aquella que intenta proteger el hardware (equipos, cableado, servidores y todos activos físicos de la organización) de los posibles desastres naturales (incendios, inundaciones, terremotos, entre otros). Mediante esta se evita el acceso no autorizado, daños o intromisiones en instalaciones y a la información de la organización.

[5]Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Vol. 46). 3Ciencias. Recuperado el 10 de febrero de 2022 en: Seguridad-informática.pdf (3ciencias.com)

No obstante, generalmente los ataques suelen ir contra la información que se encuentra dentro de los equipos, ya que el activo más crítico y el que más hay que proteger es la información. Por lo tanto, se pude puede decir que la seguridad lógica complementa a la seguridad física, "la superposición entre los dos es cada vez mayor, ya que los sistemas que proporcionan seguridad lógica tienen algunas medidas de seguridad física" [6].

Por ende, se entiende por seguridad lógica, "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo" (Costas Santos, 2011, p.90).

Es decir, persigue proteger el software de los equipos informáticos, prohibiendo el acceso a datos y programas a usuarios no autorizados. En ella se hace uso de una serie de mecanismos para protección, algunos de ellos son:

- Cesión de los privilegios adecuados, mínimos y necesarios a todos los usuarios según sus roles en el sistema, evitando así otorgar permisos de más.
- Permisión de acceso exclusivamente a ciertos programas o ficheros de archivo cifrando los accesos o haciendo uso de claves.

Para finalizar este capítulo, una cita que podemos destacar es la siguiente:

> "todo lo que no está permitido debe estar prohibido y esto es lo que debe asegurar la seguridad lógica" (Costas Santos, 2011, p.90).

2. Amenazas y delitos

Los datos de todas las personas físicas valen mucho, toda la información personal que se encuentra en Internet, redes sociales, en la nube o en los propios equipos de los usuarios, tiene un gran valor en el área de la delincuencia digital. En concordancia con lo que dice Gesprodat en su artículo "¿Cómo usan los ciberdelincuentes tus datos?", "la información vale dinero porque es la puerta para ganar todavía más dinero"[7]. Y es que puede que muchos delincuentes ataquen por el simple hecho de divertirse o satisfacer sus ganas de robar y/o atacar, pero la mayoría de ellos lo hacen con el fin de beneficiarse para obtener dinero, bien para quedárselo ellos mismos o para negociar con terceros y ganar de esta forma, aún más dinero.

En 2020 con el aumento del trabajo y educación de forma remota y con ello, el crecimiento de la cantidad de dispositivos conectados a internet, el uso de las redes sociales, aplicaciones y servicios web, hizo que los ciberdelincuentes no se quedaran atrás en sus movimientos, y es que estos se encuentran siempre al acecho y pensando en nuevas maneras de atacar.

[6]Ayudaley. Seguridad lógica en informática. ¿En qué consiste? Recuperado el 29 de mayo de 2022 de: Seguridad lógica en informática. ¿En qué consiste? (ayudaleyprotecciondatos.es)
[7]Gesprodat (3 de mayo de 2022). ¿Cómo usan los ciberdelincuentes tus datos? Recuperado el 19 de junio de 2022 de: https://gesprodat.com/como-usan-los-ciberdelincuentes-tus-datos/

La presencia de las organizaciones en la nube ha supuesto el riesgo de ataques a través del robo de credenciales y de la explotación de vulnerabilidades y malas configuraciones de la nube y sus programas. Asimismo, el creciente uso de las redes sociales tanto en el ámbito privado como profesional ha hecho que los usuarios se hagan cada vez más dependientes de los pagos móviles (compras a través de internet), con esto los ciberdelincuentes aprovechan el momento para defraudar a los internautas mediante el envío de mensajes de tipo *phishing*, urgentes o *smishing*, los cuales se explicarán en breve.

Llegar a comprender la seguridad y su importancia no requiere de un gran esfuerzo ni grandes conocimientos por parte de las personas, lo más importante es el interés que se muestre en aprender para saber cómo actuar y hacer frente a la enorme variedad de amenazas a las que nos exponemos. Todo esto dependerá sobre todo del nivel de madurez que se tenga dentro de la empresa, tal y como explica Alonso (2016) en la conferencia "Como gestionar la Seguridad Informática en las empresas".

> "Las empresas inmaduras todavía creen que pueden proteger sus sistemas contra cualquier ataque, error, esto es como si siendo padres pensáis que vais a ser capaces de evitar todos los problemas a vuestros hijos. Las empresas más maduras balancean la inversión entre prevenir y detectar, detectar que los malos están dentro, monitorizar, hacer análisis continuos de código, hacer análisis contiguo de vulnerabilidades, etc. Y las más maduras, como el caso de Tesla motors, ya vienen diseñadas pensando que vamos a hacer el día que tengamos un fallo de seguridad, […]".[8]

Es esencial conocer a fondo las amenazas y ser conscientes de ellas, ya que pueden ocurrir en cualquier momento y es importante estar siempre preparados ante los posibles daños e incidentes que puedan causar, evitando así daños más significativos. La gran cantidad de información que manejan las empresas las convierte en un atractivo para los ladrones de identidad e información, ya que frecuentemente existen importantes vacíos en su seguridad mostrados en el registro de ataques y violaciones a la seguridad reflejados por INCIBE en 2022 donde el 80% se origina desde personal interno, por la falta de controles administrativos.

Zambrano & Valencia (2017)[9] cuentan que los primeros virus informáticos no surgieron precisamente con el objetivo de provocar daños en los activos informáticos, si no como experimentos en las universidades, juegos o con el fin de causar daños. Actualmente, el malware se propaga rápidamente, sobre todo por la cantidad de puertas abiertas que existen como: Internet, redes sociales, correo electrónico.

Las amenazas suelen llegar a través de programas dañinos o maliciosos que son instalados en un dispositivo o se introducen por medio de la nube o vía remota (por ejemplo, los hackers que se conectan a Internet y acceden a diversos sistemas informáticos). Son uno de los principales problemas que ponen en riesgo la seguridad de la información en las organizaciones.

[8]Chema Alonso (abril de 2016). Conferencia de Chema Alonso: Cómo gestionar la Seguridad Informática en las empresas. Recuperado el 13 de junio de 2022 de: https://www.youtube.com/watch?v=_PsB2e0U5FU

[9]Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, *3*(3), 676-688. Recuperado el 8 de mayo de 2022 de: Seguridad en informática: consideraciones - Dialnet (unirioja.es)

Así pues, una amenaza puede describirse en términos generales como:

> "cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que lo procesan" (Tarazona, T., & Cesar, H., 2007, p.2).

Del mismo modo, en AMBIT BST (2020) se considera amenaza informática "toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático" [10] y relacionado a este concepto, es preciso destacar que "las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber consecuencia sin la presencia conjunta de éstas" (Tarazona, T., & Cesar, H., 2007, p.1).

Sin embargo, no todas las amenazas que se producen están relacionadas con delitos informáticos, los cuales se explicarán a continuación con más detalle.

2.1. Delitos informáticos

Los ciberdelincuentes cada vez tienen más fuerza para atacar y salirse con la suya, cuanto más difícil se lo ponemos más fuerza ganan para conseguir lo que quieren. Como relata Rinali en LeVPN[11], la evolución del delito cibernético coincide con la evolución de Internet. El Centro Estadístico de Observación y Monitoreo de ciberdelitos[12] declara que, los delitos que se cometían a principios de la década de los setenta eran habitualmente a través de líneas telefónicas.

Dada la intencionalidad de este apartado, conviene definir primero qué se entiende por delito informático. Pero en conformidad con lo que declara Posada, R. E., & Somellera, R. (1998) y con la búsqueda de un significado exacto sobre el delito informático, resulta complicado llegar a un acuerdo sobre su definición. Basándonos en el concepto mencionado por Posada, R. E., & Somellera, R., se puede decir que es un "acto en el cual interviene un sistema de cómputo como utensilio en la producción de un hecho criminológico, en donde se atenta contra los derechos y libertades de los ciudadanos" (Posada, R. E., & Somellera, R., 1998, p.3).

Hay que recalcar que existen una serie de elementos comunes dentro de la acción de delito informático. El primer aspecto por considerar es la conducta fraudulenta; en segundo lugar, se encuentra el instrumento con el que se comete el delito; en tercer lugar, está la finalidad; y, por último, y no menos relevante está el resultado, referido al daño que se ocasiona al usuario o usuarios.

---

[10] AMBIT BST (10 de noviembre, 2020). Tipos de Vulnerabilidades y Amenazas informáticas. Recuperado en 19 de marzo de 2022 de: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

[11] LEVPN. ¿De dónde viene el delito cibernético? Origen y evolución del delito cibernético. Recuperado el 5 de junio de 2022 de: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

[12] Centro Estadístico de Observación y Monitoreo de Ciberdelitos. Historia del Cibercrimen. Recuperado el 5 de junio de 2022 de: https://ogdi.org/historiadelcibercrimen#:~:text=La%20primera%20persona%20en%20ser,llamadas%20gratis%20en%20horas%20pico

La Instrucción 2/2011 dictada por la fiscalía general del Estado informa que los delitos informáticos se encuentran estructurados en tres categorías:

- Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs, entre ellos:
  - ✓ daños, sabotaje informático y ataques de denegación de servicios,
  - ✓ acceso sin autorización a datos,
  - ✓ descubrimiento y revelación de secretos.
- Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs, entre estos:
  - ✓ acoso a menores de 13 años,
  - ✓ corrupción de menores o de personas discapacitadas o relativas a pornografía infantil.
- Delitos en los que la actividad criminal, entraña especial complejidad en su investigación que demanda conocimientos científicos en la materia, como:
  - ✓ falsificación documental;
  - ✓ apología o incitación a la discriminación, el odio y la violencia.[13]

De los delitos nombrados y los descritos también por Acurio del Pino. S[14], algunos de ellos Acurio del Pino. S los detalla de la siguiente manera:

- Ataques de denegación de servicio, "estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a muchos usuarios" (Acurio del Pino, S., 2016, p.27).
- La llave maestra, "es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador" (Acurio del Pino, S., 2016, p.29).
- Datos falsos o engañosos, "manipulación de datos de entrada al computador con el finde producir o lograr movimientos falsos en transacciones de una empresa […]" (Acurio del Pino, S., 2016, p.23).

2.2. Amenazas lógicas y humanas

Las brechas de seguridad informática se pueden agrupar en dos bloques:

- **Amenazas físicas**, son conocidas por robo, vandalismo y catástrofes ambientales. Estas pueden clasificarse en:

[13]Instrucción nº2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías. *Boletín Oficial del Estado, 2, de 11 de octubre de 2011*. Recuperado el 17 de abril de 2022: https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf

[14]Acurio Del Pino, S. (2016). Delitos informáticos: generalidades. Recuperado el 19 de junio de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

- ✓ Acceso físico, por ejemplo, tomas de conexión a la red informática no controladas.
- ✓ Desastre del entorno y daños del hardware, entre ellos, pico de sobretensión que pueden quemar componentes y provocar apagones de los servidores;
- ✓ Radiaciones electromagnéticas;
- ✓ Desastres naturales.

- **Amenazas lógicas**, son aquellas que pueden provocar los sistemas software, datos o red sin dañar realmente el hardware. Estas pueden distinguirse en dos tipos:
  - ✓ Malware;
  - ✓ Bugs o errores de programación, software mal diseñado.

2.3. Ciberataques

Como muchos otros términos, el ciberataque ha sido definido de distintas maneras. La empresa de consultoría Gesprodat describe en su artículo "El riesgo más común de la red: los ciberataques", el ciberataque como:

> "[…] asalto o intromisión en los dispositivos electrónicos de un particular una empresa o una institución por parte de personas no autorizadas, es decir, de forma ilegal. El propósito de estas intromisiones puede ser adverso"[15]

Y sumándole lo indicado por la empresa multinacional estadounidense, IBM.

> "Los ciberataques son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos"[16].

De acuerdo con la clasificación proporcionada por OSI[17] en su guía sobre ciberataques y en común con los mencionados por IBM, los ciberataques pueden dividirse en los siguientes: ataques a contraseñas, ataques por ingeniería social, ataque a las conexiones y ataques por malware. A continuación, se explicará en qué consiste cada uno de ellos.

2.3.1. Ataque a contraseñas.

Dentro de los ataques a contraseñas existen diversas técnicas y herramientas con las que los ciberdelincuentes pueden atacar los credenciales o contraseñas de acceso a aplicaciones, páginas, webs, plataformas sociales o herramientas informáticas. El objetivo de estos es conseguir la mayor información posible almacenada en ellas. Los usuarios suelen facilitar este tipo de ataques por la falta de políticas de complejidad a la hora de crear las contraseñas, como:

[15]Gesprodat (31 de agosto de 2021). El riesgo más común de la red: los ciberataques. Recuperado el 19 de junio de 2022 de: https://gesprodat.com/el-riesgo-mas-comun-de-la-red-los-ciberataques/
[16]IBM. ¿Qué es un ataque cibernético? Recuperado el 17 de junio de 2022 de: https://www.ibm.com/es-es/topics/cyber-attack
[17]OSI. Guía de ciberataques. Recuperado el 10 de abril de 2022 de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

- contraseñas débiles sin ninguna complejidad (combinación de caracteres, mayúsculas y minúsculas, longitud mínima),
- hacer uso de información personal en la creación de contraseñas (fecha de nacimiento, apellidos, nombre propio o de familiares),
- guardar las contraseñas en el navegador, los navegadores guardan las claves en una lista sin cifrar, por lo que significa que las contraseñas que se guarden en el navegador no se encuentran protegidas frente a los intrusos.

Estos tipos de patrones pueden favorecer el acceso y el uso no autorizado de los datos y servicios.

De entre las técnicas existentes, OSI destaca las siguientes dentro de este ataque: fuerza bruta y ataque por diccionario.

- Fuerza bruta: "Consiste en adivinar nuestra contraseña a base de ensayo y error. Los atacantes comienzan probando diferentes combinaciones con nuestros datos personales, en caso de conocerlos por otras vías. Luego, continúan haciendo combinaciones de palabras al azar, conjugando nombres, letras y número, hasta que dan con el patrón correcto" (OSI, p.5).
- Ataque por diccionario: "Los ciberdelincuentes utilizan un software que, de forma automática, trata de averiguar nuestra contraseña. Para ello, realiza diferentes comprobaciones empezando con letras simples como 'a', 'AA' o 'AAA' y, progresivamente, va cambiando a palabras más complejas" (OSI, p.5).

2.3.2. Ataque por ingeniería social.

Este tipo de ataque se basa en las técnicas de manipulación psicológica y suelen utilizarse como paso previo a un ataque por *malware* (elaborados por ciberdelincuentes con el fin de tener el control de medios informáticos ajenos y conseguir que los usuarios revelen información personal).

INCIBE[18] plantea dos maneras diferentes en las que se caracteriza un ataque de este tipo, estas dependerán fundamentalmente de la cantidad de comunicaciones que deberá ejecutar el ciberdelincuente hasta alcanzar su meta:

- ***Hunting***: "mediante una única comunicación los ciberdelincuentes buscan obtener su propósito. Generalmente la técnica del *hunting* es utilizada en ataques de *phishing* o campañas de distribución de *malware*" (INCIBE, p.10).
- ***Farming:*** "en este caso los ciberdelincuentes emplean más de una comunicación con la víctima hasta conseguir su objetivo […]" (INICIBE, p.11).

INCIBE a su vez muestra tres formas en las que se divide este ataque:

- **Recolección de información**. En esta fase el objetivo principal del ciberdelincuente será recolectar toda la información posible sobre las futuras víctimas.

[18] INCIBE. Ciberamenazas contra entorno empresariales. Recuperado el 10 de abril de 2022 de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

- **Manipulación.** El modo de atacar de estos ciberdelincuentes es fingiendo ser una entidad de confianza a través de un cebo. Esto puede ser con un mensaje urgente o una promoción atractiva que invita a hacer clic en algún hipervínculo que en realidad no es seguro, incluso llegando a suplantar la identidad de una persona u organización de confianza.
- **Salida.** Una vez el ciberdelincuente ha conseguido alcanzar su objetivo, este tratara de no ser descubierto. Esta será la fase final del ataque.

Por otro lado, OSI[19] describe distintos tipos de ataques basados en ingeniería social, entre ellos los más conocidos por su nombre son:

- *Phishing*, *vishing* y *smishing*: "el ciberdelincuente enviará un mensaje suplantando a una entidad legítima, como puede ser un banco, una red social, un servicio técnico o una entidad pública, con la que nos sintamos confiados, para lograr un objetivo. Estos mensajes suelen ser de carácter urgente o atractivo, para evitar que apliquen el sentido común y se lo piensen dos veces" (OSI, p.8).

  El *phishing* suele llevarse a cabo mediante el correo electrónico, redes sociales o aplicaciones de mensajería instantánea. Por otra parte, el *vishing* suele realizarse mediante llamadas telefónicas y, por último, el canal que se utiliza para el *smishing* son los sms.

- *Spam*: "consiste en el envío de grandes cantidades de mensajes o envíos publicitarios a través de Internet sin haber sido solicitados, es decir, se trata de mensajes no deseados" (OSI, p.13).

Otros menos escuchados son: *bating* o gancho, *shoulder surfing* y *dumpster diving*.

La mejor forma de prevenir este tipo de ataques es desconfiar; es decir, desconfiar por ejemplo de todo tipo de correo electrónico que induzca a urgencia o este fuera de lo común, como puede ocurrir en el caso de recibir un correo en otro idioma o traducido automáticamente.

2.3.3. Ataque por malware o código malicioso:

OSI[20] señala que estos ataques se realizan a través de programas maliciosos con el propósito de realizar acciones perjudiciales a los sistemas informáticos o nuestra privacidad. Buscan dañar los equipos, robar información, obtener un beneficio económico y hacerse con el control del equipo o sistema.

Hay distintos tipos de malware, de los cuales los más comunes y conocidos por su nombre son:

- *Spyware*: "código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador (tendencias de navegación), para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercadeo, o para robar información personal (p.ej. número de tarjetas de crédito)" (Tarazona, T., & Cesar, H., 2007, p.2).

[19]OSI. Guía de ciberataques. Recuperado el 8 de junio de 2022 de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf
[20]OSI. Guía de ciberataques. Recuperado el 10 de abril de 2022 de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

- *Troyanos, virus y gusanos:* "son programas de código malicioso, que de diferentes maneras se alojan en los computadores con el propósito de permitir el acceso no autorizado a un atacante, o permitir el control de forma remota de los sistemas. El virus adicionalmente tiene como objetivo principal ser destructivo, dañando la información de la máquina, o generado el consumo de recursos de manera incontrolada para bloquear recursos" (Tarazona, T., & Cesar, H., 2007, p.2).

Las mejores prácticas para evitar estos códigos maliciosos son:

- Evitar la instalación de programas y/o aplicaciones de fuentes de origen inseguro. Es recomendable comprobar siempre que el sitio web es seguro, esto es fácil saberlo si se observa que el hipervínculo de la página web empieza por https y contiene un candado cerrado, esto significa que la página web dispone de un certificado de seguridad;
- Mantener actualizado el sistema operativo;
- Hacer uso de un buen sistema de protección (antivirus y antispyware, cortafuegos firewall, cifrado de disco y equipos).

2.3.4. Ataque a las conexiones:

Como se indica en la guía de ataques de OSI[21], es una práctica común de los ciberdelincuentes de atacar las conexiones inalámbricas a través de software y herramientas con las que saltarse las medidas de seguridad. Su finalidad es monitorizar remotamente la actividad de los usuarios para extraer información y robar datos bancarios, de las redes sociales o correo electrónico. Existen diversos tipos, algunos de ellos son:

- **Redes trampa:**

Consiste en la creación de redes inalámbricas falsas (copia de una red wifi, con el mismo nombre o similar a la original configurada con los mismos patrones que la original), su principal objetivo es hacer que los usuarios confíen en que se trata de una red segura y hacer que se conecten, robando así información personal cuando estos acceden a redes sociales, cuenta bancaria u otro tipo de cuentas personales.

- **Ataque a cookies:**

Su principal objetivo es robar la identidad y credenciales, alterar los datos almacenados en una *cookie* y obtener información sin autorización. Los ciberdelincuentes aprovechan la falta de protocolos de cifrado en las sesiones de navegación (protocolo HTTPS, o protocolo HTTP seguro).

[21]OSI. Guía de ciberataques. Recuperado el 10 de abril de 2022 de: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

- **Ataque de adware:**

"El adware es un tipo de software malicioso cuyo objetivo es mostrar anuncios publicitarios a su víctima con el fin de generar ingresos a los ciberdelincuentes" (INCIBE, p.62)[22].

Un tipo de *adware* es el *malvertising*, su modo de atacar es ocultando *malware* en la publicidad mostrada en las páginas webs a las que acceden los usuarios. Al contrario que el adware su principal meta es infectar cualquier dispositivo que esté a su alcance con *malware*, para posteriormente poder llevar a cabo cualquier tipo de ataque.

3. Políticas de seguridad

Actualmente existe una gran diversidad de políticas de seguridad con las que se ayuda a las empresas a poner en práctica los procesos internos con el fin de mejorar y mantener una buena seguridad, con ello concienciar y dar a conocer a los empleados sobre los riesgos que pueden surgir si no se siguen correctamente las pautas de actuación establecidas por la organización. Así pues, se entiende como política de seguridad, "pautas y procedimientos que dan soporte a la seguridad conforme a requisitos legales y de negocio" (Postigo Palacios, 2020; p.5).

Se puede decir que se basan en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de los datos y minimizar así, los riesgos que le afecten. Recalcar que las políticas que se apliquen deberán ser revisadas, monitorizadas y conocidas por todo el personal de la organización, así como redactadas en documentos que estén a disposición de todos.

En conformidad con lo que subraya Postigo Palacios (2020), estas normas, pautas y directrices consistirán en mecanismos diseñados para evitar y revelar la intrusión, es decir, anticipación ante posibles amenazas y garantizando así la recuperación del sistema en caso de incidentes. Postigo Palacios (2020), fragmenta en tres estos mecanismos:

- Mecanismos de protección lógicos: se establecen medidas de protección para evitar la entrada de intrusos al sistema (ej.: programas antivirus, firewall, cortafuegos).
- Mecanismos de detección: dispositivos que se ejecutan para detectar si se han producido o no cambios en el sistema, controlando de esta forma si se ha llevado a cabo algún intento de intrusión (ej.: sistemas de vigilancia, software de detección de intrusos).
- Mecanismos de recuperación: herramientas que se pondrán en acción una vez se haya producido el ataque (ej.: copias de seguridad).

[22] INCIBE. Ciberamenazas contra entornos empresariales. Recuperado el 10 de abril de 2022 de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

3.1 Puntos clave sobre el establecimiento de políticas

De acuerdo con el Departamento de Tecnología Organización Inca[23], los elementos esenciales que se deben considerar dentro de una política son los siguientes:

- Alcance, en el cual se mencionarán las facilidades, los sistemas y el personal encargado de la política;
- Objetivos y descripción de los elementos o sistemas involucrado en la misma;
- Responsabilidades establecidas sobre los usuarios (trabajadores) con respecto a la información a la que tienen acceso;
- Descripción de violaciones y sanciones por no cumplir con las políticas;

Anudado a esto, es importante que estas políticas estén redactadas con un lenguaje sencillo (libres de tecnicismos, términos claros) y entendible para todas aquellas personas a las que se les deba informar sobre la existencia de estas.

Otro elemento clave es la necesidad de la actualización periódica (como se ha mencionado antes), ya que las entidades normalmente están en continuos cambios para innovar y mantener una continuidad en su negocio, se amplía el personal, uso de nuevas tecnologías, desarrollo de nuevos procesos y servicios, u otras modificaciones. Por tal razón, se requerirá marcar el periodo de validez de cada una de las políticas.

En conformidad con lo que el Departamento de Tecnología Organización Inca[24] menciona, es necesario también que a la hora de elaborar las políticas se tengan en cuenta los siguientes elementos:

- Generar un análisis de riesgos para poder valorar los activos que contienen información relevante y con esto identificar los riesgos a los que está propensa a sufrir la organización y el impacto que puede tener esto internamente. La identificación de los riesgos ayudará a la organización a evitar las posibles amenazas y daños que se puedan producir, implantando de esta manera las correctas medidas de seguridad para poder controlar los riesgos detectados en el análisis.
- Reunirse con los departamentos a los que les impliquen cada una de las políticas para poder establecerlas correctamente;
- Documentar con detalle el alcance y propósito de cada una de las políticas, dejando establecidos los mecanismos de seguridad que correspondan a cada una.

[23]Departamento de Tecnología Organización Inca. Política de seguridad informática (PSI). Recuperado el 11 de junio de 2022 de: https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf
[24]Departamento de Tecnología Organización Inca. Política de seguridad informática (PSI). Recuperado el 11 de junio de 2022 de: https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

3.2 Inexistencia o deficiencias en las políticas de seguridad

Seguir las pautas mencionadas previamente es fundamental para llevar a cabo una buena implantación y definición de las políticas de seguridad y procedimientos de seguridad de acuerdo con las necesidades de la organización. De entre las vulnerabilidades citadas por Vieites, Á. G.[25] en su libro, se pueden destacar las siguientes:

- Información crítica o sensible que se guarda sin cifrar en el sistema;
- Escaso control en los tratamientos realizados por proveedores, terceros (ej. Empresa de informática encargada del mantenimiento, empresa de destrucción de información, etc.),
- Falta de control en el acceso a los recursos, usuarios con permisos elevados a los necesarios por su puesto de trabajo;
- Inexistencia de procedimientos para la realización de copias de seguridad, despreocupación por el almacenamiento de la información y posibilidad de recuperación de la misma en caso de incidentes.

3.3 Ejemplos de políticas de seguridad

Si se tuvieran que nombrar la cantidad de políticas de seguridad existentes, no habría fin, ya que cada organización establece las suyas propias. Sin embargo, muchas de ellas son muy comunes, las cuales pueden dividirse en medidas técnicas, organizativas y legales.

INCIBE[26] ha puesto a disposición de todos, una serie de políticas y entre ellas se encuentran las más típicas y esenciales para que las organizaciones puedan poner en marcha.

Clasificación de la información, el objeto es asegurar que la información recibe un nivel de protección adecuado con su importancia en la organización. Esta política es esencial que la apliquen todos los usuarios de la corporación que manejen documentación en soporte papel para el cumplimiento de sus labores.

- Elaborar un listado con la tipología de documentos clasificados.
- Establecer los criterios de seguridad con los que se clasificarán los activos de información.
- Definir qué usuarios pueden tener acceso.

[25] Vieites, Á. G. (2011). *Auditoria de seguridad informática (MF0487_3)*. Grupo Editorial RA-MA. Recuperado el 18 de junio de 2022 de: Recuperado de: https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&as_vis=1&q=Auditor%C3%ADa+de+Seguridad+Inform%C3%A1tica+%28MF0487_3%29&btnG=#d=gs_cit&t=1655550603809&u=%2Fscholar%3Fq%3Dinfo%3AgOkaAAheJfcJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Des

[26] INCIBE. Políticas de seguridad para la pyme. Recuperado el 4 de abril de 2022: https://www.incibe.es/protege-tu-empresa/herramientas/politicas

Concienciación y formación, adoptar las medidas necesarias para que el personal conozca, entienda y cumpla las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. Algunos de los controles que se han de tener en cuenta para revisar el cumplimiento de la política son:

- Llevar a cabo un plan formativo con el objetivo de aumentar el nivel de conocimientos de los empleados sobre la seguridad a aplicar dentro de la organización, a través de cursos y/o charlas de concienciación cada cierto tiempo, adaptados a los puestos de trabajo de cada trabajador;
- Controlar que los empleados han asimilados correctamente todo lo aprendido sobre la seguridad de la información.

Relación con proveedores, es decir, mantener un control de todas las relaciones que se tienen con proveedores y en concreto, aquellos que tienen acceso a datos de la empresa, con el fin de asegurarse de que se encuentra totalmente protegida. Esta política ha de contener los siguientes puntos:

- Contrato de encargo de servicios con tratamiento de datos personales, a firmar con todos aquellos proveedores que acceden a datos de carácter personal de manera directa o indirecta;
- Contrato de encargo de servicios sin acceso a datos personales (como es el caso de la empresa de seguridad y limpieza).

Control de acceso, el objeto es autorizar accesos sólo a aquellos datos y recursos que el usuario del sistema de información precise para el desarrollo de sus funciones en su puesto de trabajo. Las medidas y normas relativas al control de acceso lógico y físico del personal autorizado para acceder a los datos personales pueden ser entre ellas:

- Establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos a los autorizados;
- Definir los permisos de los usuarios en función del puesto de trabajo y del tipo de información al que podrán acceder;
- Definir un protocolo para llevar a cabo las altas y las bajas de los usuarios o modificación de sus cuentas.

Copias de seguridad, tiene por objeto describir los requisitos de los procedimientos para la copia y recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Esto implica:

- Documentación de la política de copias de seguridad, en el que se indique: ¿de qué se hace la copia de seguridad?, ¿cuándo se realiza?, ¿quién se encarga o supervisa?, ¿en qué programas se configuran? y ¿cómo se realizan exactamente y de qué forma se restauran?
- Cifrado de las copias de seguridad que contengan información confidencial y sensible.

Antimalware, el objeto de esta política es establecer y adecuar las medidas de protección frente a virus informáticos y otro tipo de software malintencionado, en los equipos para tratamientos de información con el fin de garantizar la seguridad y protección de los datos. Entre las medidas a adoptar están:

- Contar con un antivirus instalado y actualizado;
- Mantener actualizado el sistema operativo y las aplicaciones;
- Establecer un procedimiento de respuesta ante una posible infección.

No hay que olvidar que la violación de la política de seguridad significa que el sistema este sujeto a amenazas, esto se conoce como brechas de seguridad. Las brechas de seguridad son todas aquellas violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra manera, o la comunicación o acceso no autorizados a dichos datos.

4. La normativa legal en materia de seguridad

Este es el último punto que abarca la seguridad informática, y que cubre los aspectos mencionados anteriormente, entre ellos: la seguridad física y lógica, amenazas y ciberataques, todos los temas explicados hasta ahora. En el presente capítulo se tratará la normativa desde el punto de vista del RGPD y la LOPDGDD.

El 25 de mayo de 2016 se publicó el RGPD y dos años después, el 25 de mayo de 2018 las organizaciones que no tuvieran aplicada esta norma ya podían ser sancionadas por la falta de cumplimiento. El RGPD, "órgano de la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal, con miras de hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados la norma que vela por la protección de datos de carácter personal de las personas" (López, P. A., 2010; p.213), es considerada una evolución de la LOPD, pero obliga a llevar a cabo una seguridad extrema y una revisión continua sobre la misma.

Por otro lado, la LOPDGDD el 6 de diciembre de 2018 se publicó en el Boletín Oficial del Estado, nueva Ley Orgánica 3/2018 de 5 de diciembre y entrando en vigor al día siguiente. Es considerada una adaptación al territorio español del RGPD que se aplica a nivel europeo. La mayoría de las novedades, tal y como indica su nombre, se deben a cambios producidos por la evolución de las nuevas tecnologías y la necesidad de abordar dicha progresión legislativamente.

Estas normas afectarán a todas las empresas y microempresas, autónomos, comunidades, que traten datos personales de ciudadanos europeos, aquellas a las que los ciudadanos les hayan cedido datos y las que traten datos de terceros.

Antes de pasar a explicar los principios que establece el RGPD y como se ha de cumplir, conviene saber que se entiende como datos personales.

> "Los datos personales son aquellos que están relacionados con una persona identificada o identificable, es decir, son datos personales los identificadores online como direcciones IP, nombre de usuario, correo electrónico, etc." (INCIBE, p.10).

No obstante, es importante tener en cuenta que los tratamientos pueden ser de dos tipos, de bajo o alto riesgo, tal y como apunta INCIBE[27].

Por una parte, se considera que un tratamiento es de alto riesgo cuando se tratan datos de categoría especial. Se entiende por dato de categoría especial toda información de una persona física relacionada con los datos biométricos (huella dactilar, reconocimiento facial, datos dirigidos a identificar a una persona de forma unívoca), datos de salud, vida u orientación sexual, origen étnico o racial, opiniones políticas, afiliación sindical, datos genéticos y convicciones religiosas o filosóficas. Asimismo, el tratamiento de datos masivos como en el caso de los bancos, colegios y empresas de comunicaciones, también es considerado un tratamiento de alto riesgo.

Por otra parte, será de bajo riesgo cuando solo se traten datos de contacto de trabajadores, clientes, proveedores y cualquier otra persona que ceda datos a la entidad.

Con carácter general, los datos personales serán tratados siguiendo los principios que establece el RGPD, los cuales se explicarán en el siguiente apartado.

4.1 El RGPD y los principios en los que se basa

La normativa de protección de datos está construida sobre un conjunto de principios jurídicos, estos forman los pilares conforme a los cuales realizar un correcto tratamiento sobre los datos personales. Estos principios van más allá de los fundamentos por los que regir la elaboración, interpretación y aplicación de la normativa de protección de datos. Tienen una doble base, por una parte, configuran y constituyen derechos para los titulares de los datos; y, por otra parte, obligaciones para los responsables y encargados del tratamiento, que deberán respetar y cumplir los principios establecidos por el RGPD e indicados en la AEPD (2022)[28]:

- **Licitud, lealtad y transparencia**: se prohíbe la recogida de datos de forma fraudulenta, desleal e ilícita.
- **Limitación de la finalidad**: los datos personales solamente deberán ser tratados para fines determinados, explícitos y legítimos.
- **Minimización de datos**: solamente se recabarán aquellos datos que sean estrictamente necesarios para la finalidad para la que se solicitaron, esto supone que sean pertinente y no excesivos.
- **Exactitud de datos**: los datos deberán reflejar la realidad de las personas, esto significa que deberán estar actualizados y su inexactitud implicará la supresión o modificación de los mismos.
- **Limitación del plazo de conservación de los datos**: los datos se mantendrán el tiempo necesario para la finalidad para la que fueron originalmente recabados, no pueden conservarse de forma ilimitada.

[27] INCIBE. Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario. Recuperado el 12 de mayo de 2022 de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-ganar-competitividad-cumpliendo-rgpd-metad.pdf

[28] AEPD (14 de junio de 2022). Principios. Recuperado el 3 de abril de 2022 de:https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios

- **Seguridad**: quienes traten los datos deberán llevar a cabo un análisis de riesgos orientado de determinar las medidas organizativas y técnicas necesarias con el fin de garantizar la integridad, disponibilidad y confidencialidad de los datos. La seguridad y la protección deberán estar asegurados por el responsable contra el tratamiento no autorizado, su pérdida, destrucción y daños accidentales.

4.2 Adaptación de la LOPDGDD al RGPD

Aunque la base de este trabajo sea principalmente la normativa del RGPD, no es de más el destacar las novedades que aplica la nueva LOPDGDD sobre el RGPD, ya que también se tendrán en cuenta. Esta destaca sus cambios sobre todo en lo que se refiere a sus siglas "GDD" (Garantía de los Derechos Digitales).

Entre las novedades a mencionar se encuentran las siguientes:

- Se eleva la edad de consentimiento de un menor de 13 a 14 años;
- Se aumenta la cantidad de personas que pueden acceder a los datos de fallecidos;
- Se impone la obligatoriedad de designar un delegado de protección de datos en caso de que:

    1. el procesamiento de datos se realice a través de una autoridad u organismo público,
    2. si las actividades del organismo incluyen seguimiento continuado y a gran escala,
    3. las operaciones del organismo o la autoridad en cuestión tienen relación con el procesamiento y seguimiento a gran escala de datos referentes a delitos y condenas judiciales.

- Reconocimiento de una carta de derechos digitales, de entre la lista de derechos digitales se hace una división entre derechos digitales de carácter personal y ámbito laboral:

    ✓ Ámbito personal:
    - Neutralidad de internet;
    - Acceso universal a la red;
    - Seguridad digital;
    - Educación digital y protección de menores;
    - Derecho al olvido;
    - Portabilidad;
    - Testamento digital.

    ✓ Ámbito laboral:
    - Derecho a la intimidad y utilización de dispositivos digitales;
    - Derecho a la desconexión digital;
    - Intimidad sobre la utilización de dispositivos de videovigilancia en el puesto de trabajo y sobre el uso de geolocalizadores.

4.3 Cumplimiento de las auditorías RGPD

Normalmente, el punto de partida de una entidad para adecuarse a la normativa de protección de datos es comenzar por realizar una toma de datos; esta consiste en realizar una reunión con un consultor (generalmente externo) que empezará por conocer la empresa y recabar toda la información posible sobre los datos que se recopilan (clientes, proveedores, socios, trabajadores, posibles clientes, posibles trabajadores, cualquier dato que se recabe de una persona física) y revisará si se aplican los textos legales (cláusulas, políticas y procedimientos) sobre protección de datos y las medidas de seguridad (técnicas, legales y organizativas) adecuadas. Este proporcionará a la empresa toda la documentación necesaria para poder iniciar una adecuación a la normativa, desde generar cláusulas necesarias para facturas, presupuestos, correo electrónico, toda la documentación en la que se soliciten datos a las personas, hasta políticas y procedimientos a implantar en la organización (en caso de que no las tengan). Una vez hecho este recorrido, el siguiente paso por parte del consultor será revisar que las medidas y recomendaciones dadas, se han llevado a cabo por el coordinador RGPD de la entidad. Una vez cubiertos todos los puntos importantes, es responsabilidad del coordinador haber seguido las directrices indicadas por su consultor y tener toda la documentación preparada y correcta para la realización de la auditoría de protección de datos.

Una auditoría de protección de datos se basa en el cumplimiento de las medidas de seguridad exigidas por el RGPD y la LOPDGDD. Cabe destacar que la LOPDGDD no establece una obligación para los responsables del tratamiento de realizar auditorías de cumplimiento de la normativa de protección de datos. Sin embargo, en el principio de responsabilidad proactiva (artículo 5.2 del RGPD), se indica que los responsables y encargados del tratamiento de los datos no solamente se harán responsable de cumplir con los principios del RGPD, mencionados anteriormente, sino que también deberán ser capaces de demostrarlo. Con ello se hace referencia a la necesidad de que el responsable y encargado del tratamiento apliquen las medidas técnicas, legales y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento es conforme a la norma.

Las medidas de seguridad se han de implantar en función del riesgo. Para saber el riesgo lo primero que hay que hacer es llevar a cabo un análisis del riesgo, es decir, evaluar si las medidas de seguridad que están implementadas en la organización son suficientes para poder garantizar que, ante la posible pérdida, robo o la destrucción de los datos de carácter personal que se están tratando, podrán salvar este tipo de incidentes. El objetivo principal es tener presente si el tratamiento de la información puede llevar a consecuencias negativas.

Antes de evaluar el riesgo, es esencial contar con un registro de actividades de tratamiento, “medida que obliga a las empresas y otras entidades a documentar los flujos de datos personales que circulan dentro de ellas”[29]. El registro de actividades de tratamiento se considera obligatorio siempre que en la organización disponga de más de 250 personas o se realicen tratamiento que puedan generar grandes daños a la privacidad o tratamiento de datos de alto riesgo. La elaboración del registro de actividades de tratamiento es el primer paso para cumplir con la normativa vigente en materia de privacidad y protección de datos. Generalmente es elaborado por una consultoría u entidad especializada en ello, además, este debe mantenerse actualizado.

[29]Ayudaley. Registro de Actividades de tratamiento en el RGPD. Recuperado el 15 de mayo de 2022: https://ayudaleyprotecciondatos.es/2017/11/27/registro-actividades-rgpd/

Finalmente, una vez obtenidos los resultados de la auditoría, el auditor deberá analizar y valorar el nivel de cumplimiento basándose en las distintas evidencias. A veces, el nivel de cumplimiento depende de quién tiene que aplicar la norma, frente a la persona que lo audita. Como declara la guía de buenas prácticas de ISMS FORUM (2020)[30], para poder evitar esta discordancia, se deberán tener en cuenta un conjunto de indicadores (dominios), los cuales permitirán marcar si se está cumpliendo o incumpliendo la norma.

El análisis y valoración del grado de cumplimiento suele estar vinculado con las evidencias y los documentos obtenidos en cada una de las entrevistas que realiza el auditor con cada área involucrada. Generalmente, el porcentaje de aprobación de la auditoría se basa en diferentes factores (número de cumplimientos positivos o negativos, sensibilidad y riesgos de los tratamientos, opinión profesional del equipo auditor, entre otros.).

Normalmente, los rangos de puntuación suelen darse entre los siguientes valores: auditoría denegada (0% a 39,99%), desfavorable (40% a 74,99%), favorable con salvedades (75% a 89,99%) y favorable (90% a 100%). Estos rangos pueden varias dependiendo del equipo auditor que lo lleve a cabo.

4.3.1 Dominios a revisar para el cumplimiento

Para verificar el nivel de cumplimiento del RGPD de cualquier entidad, tal y como recomienda la guía de buenas prácticas en auditorías de ISMS FORUM y siguiendo el listado proporcionado por la AEPD (2018)[31], los dominios que se recomiendan tener en cuenta son los siguientes:

- **Gobierno de la privacidad:** Política de privacidad interna, procedimientos organizativos, roles y funciones de la privacidad, identificación de la autoridad de control, revisión de inspecciones y sanciones, códigos de conductas y/o certificaciones, normas corporativas vinculantes.
- **Minimización y exactitud de los datos:** Cumplimiento del artículo 5 del RGPD.
- **Responsabilidad proactiva:** Cumplimiento del artículo 5, 25 y 35 del RGPD. Privacidad desde el diseño y por defecto, Evaluación de impacto relativa a la protección de datos y Análisis de riesgos para la privacidad.
- **Corresponsabilidad:** Cumplimiento del artículo 5 y 26 del RGPD. Escenarios de corresponsabilidad, revisión de acuerdos de corresponsabilidad, coordinación entre los corresponsables.
- **Plazos de conservación:** Cumplimiento del artículo 5 del RGPD.
- **Licitud del tratamiento:** Cumplimiento del artículo 6 del RGPD.
- **Transparencia e información:** Cumplimiento del artículo 13 y 14 del RGPD. Cláusulas informativas y consentimientos.
- **Limitación de la finalidad:** Cumplimiento del artículo 5 y 6 del RGPD.
- **Deber de secreto:** Cumplimiento del Artículo 5 del RGPD y LOPDGDD. Principio de integridad y confidencialidad.

[30]ISMS FORUM (28 de mayo de 2020). Guía de buenas prácticas en auditorías. Recuperado de 3 de abril de 2022 de:https://www.ismsforum.es/ficheros/descargas/guia-de-buenas-practicas-en-auditorias.pdf
[31]AEPD (13 de abril de 2018). Listado de cumplimiento normativo. Recuperado el 9 de abril de 2022 de: https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf

- **Registros de actividades de tratamiento:** Revisión, adecuación y actualización de los distintos tratamientos de datos.
- **Derechos de los interesados:** Cumplimiento de los artículos 15 al 22 del RGPD. Revisión de procedimientos, sistemas de información de los derechos de los usuarios, formulario de solicitud, canales de comunicaciones, roles intervinientes, revisión de su efectiva aplicación.
- **Notificación de violaciones de seguridad:** Cumplimiento del artículo 23 del RGPD.
- **Medidas de seguridad**, tanto técnicas como organizativas:
  - ✓ **Medidas técnicas:** Revisión de medidas de seguridad de carácter técnico (sistemas de autenticación, cifrado, gestión de usuarios, activos informáticos, controles de acceso físico, copias de seguridad) vinculadas a los tratamientos de datos personales en todo su ciclo de vida dentro de la organización.
  - ✓ **Medidas organizativas:** Revisión de medidas de seguridad de carácter organizativo (almacenamiento seguro, transporte confidencial, destrucción irrecuperable, clasificación coherente, custodia diligente) vinculadas a los tratamientos de datos personales en todo su ciclo de vida dentro de la organización.

- **Formación:** Medidas y controles del cumplimiento, planes de formación y concienciación.
- **Encargados del tratamiento:** "Persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste" (AEPD, 2018, p.4). Cumplimiento del Artículo 28 del RGPD: modelos de contratos, procedimientos de verificación del cumplimiento con proveedores, revisiones de encargados de tratamiento, adhesiones a certificaciones o códigos de conducta.

Al conjunto de dominios recomendados por ISMS FORUM (2020)[32] se pueden nombrar también otros puntos de los que, en ocasiones, no aplican a muchas organizaciones pero que no se han de olvidar, estos son:

- **Delegado de Protección de Datos (DPD):** Cumplimiento del artículo 5 y 37 del RGPD.
- **Transparencia e información, web:** Cumplimiento del artículo 13 y 14 del RGPD. Política de privacidad y Política de cookies de la página web.
- **Transparencia e información, videovigilancia:** Cumplimiento del artículo 13 del RGPD y artículo 22 de la LOPDGDD.
- **Tratamiento de menores de edad:** Cumplimiento del artículo 7 de la LOPDGDD.
- **Categorías especiales de datos:** Cumplimiento del artículo 9 del RGPD y LOPDGDD.
- **Transferencias internacionales:** Cumplimiento del artículo 44 y 49 del RGPD. Identificación de las transferencias internacionales a terceros fuera del Espacio Económico Europeo, confirmación de distintos niveles de protección adecuadas, excepciones reguladas conforme el RGPD. Como se indica en la guía de buenas prácticas de ISMS FORUM, implica:

  - ✓ Identificación de transferencias internacionales.

[32] ISMS FORUM (28 de mayo de 2020). Guía de buenas prácticas en auditorías. Recuperado el 3 de abril de 2022 de: https://www.ismsforum.es/ficheros/descargas/guia-de-buenas-practicas-en-auditorias.pdf

- ✓ Confirmación de destinos con nivel de protección adecuada o transferencias mediante garantías adecuadas (artículo 46).
- ✓ Entre otros.

Las razones por las que en ocasiones puede que no apliquen para algunas entidades pueden ser varias, bien sea porque en esa organización no se requiere de un delegado de protección de datos (por ejemplo, no se tratan datos sensibles a grandes dimensiones), no se dispone de página web ni sistemas de videovigilancia, no se tratan datos de menores, no se tratan datos de categoría especial o no se realizan transferencias internacionales fuera del espacio económico Europeo, es decir, no se hace uso de programas como *Mailchimp* para el envío de comunicaciones comerciales.

4.4 Integración de la auditoría de protección de datos en la auditoría de SI

Una auditoría de sistemas de información es una rama especializada de la auditoría que promueve y aplica conceptos de auditoría en el área de sistemas de información. En esta se evalúan los sistemas y aplicaciones, así como las medidas de seguridad de las que está dotada la organización a la que audita y la eficacia de las mismas.

Actualmente, aunque los datos sean o no personales, se consideran activos de información con un importante valor para el desempeño y la operativa de la organización. Por ello, los resultados que se obtengan de una auditoría de sistemas de información pueden ser perfectamente aprovechados por una auditoría de protección de datos, esto permitirá evaluar la eficacia de las aplicaciones y bases de datos en las que residen los datos de carácter personal que se tratan en la organización auditada.

Las ventajas más destacables que se obtendrán al integrar la auditoría de protección de datos en una auditoría de SI[33], son la obtención de un conjunto de resultados que aportarán más valor y el ahorro en el tiempo de realización de auditorías.

Finalmente, cabe decir que la forma de realizar una auditoría dependerá de factores como el tipo de organización que vaya a ser auditada, así como el contexto, momento o la persona que se vaya a encargar de llevarla a cabo. En general, todas aquellas organizaciones que traten datos de carácter personal tendrían que realizar una auditoría para la protección de estos datos, ya que es muy probable que no se hayan tomado todas las medidas correctas y necesarias para poder garantizar la disponibilidad, integridad y confidencialidad de la información tratada. Estas malas acciones pueden conducir a la empresa a grandes sanciones por parte de la AEPD, estas pueden ir desde un conjunto de advertencias, limitaciones, la prohibición del tratamiento de datos, ordenamiento de la supresión de datos hasta la imposición de multas de millones de euros.

[33]Sistemas de Información.

5. Desarrollo de un prototipo previo al desarrollo de un plan de mejora de la SI

A pesar de los distintos avances en el campo de la tecnología, el pilar fundamental para poner en marcha una buena seguridad lo representa la figura del coordinador de la empresa, pues de este dependerá que el personal en plantilla y todas aquellas personas que manejan datos de personas físicas, hagan una buena gestión de la información. El coordinador deberá controlar que todo el personal cumple con todas las directrices indicadas (políticas, procedimientos y medidas de seguridad). Por ello, aunque el coordinador sea un agente relevante dentro de la empresa, el principal elemento para garantizar la seguridad en una organización es el empleado, ya que podemos aplicar todo tipo de medidas, pero al fin y al cabo el empleado es quien gestiona la información en la empresa y si este no es consciente ni muestra interés alguno por todo lo que hay que llevar a cabo para mantener la seguridad y evitar así ataques e intrusiones, las medidas de seguridad elaboradas, no servirán de nada. Se evidencia, de este modo, la necesidad de generar una concienciación y cultura de seguridad en las empresas, de forma fácil y autosuficiente, resulta esencial. Como menciona INCIBE[34], la falta de preparación en ciberseguridad en las empresas y microempresas, afectan principalmente a la continuidad del negocio. Para saber desde dónde empezar a mejorar es necesario conocer el punto de partida y para ello es esencial comenzar a analizar cómo se encuentra la organización, se necesitará por tanto hacer uso de distintos puntos de comprobación y controles.

El camino explicado en los capítulos anteriores, desde que el consultor revisa que el coordinador ha implantado correctamente las medidas indicadas hasta que se realiza la auditoría en materia de protección de datos, normalmente se hace extenso. A lo largo de este, pueden surgir diferentes transformaciones dentro de la entidad y los coordinadores pueden no darse cuenta de que, al implantar ciertos cambios, están dejando vulnerabilidades, tales como la creación de una nueva página web sin sus correspondientes textos legales o implantación de cámaras de videovigilancia sin su correspondiente cartel informativo, entre otros.

Este capítulo final se analizará el autodiagnóstico elaborado y la utilidad del mismo, este autodiagnóstico ha sido denominado “AutoAuditat”, tal y como se mencionó al principio. Con AutoAuditat todas las grandes empresas, microempresas, autónomos y comunidades, podrán hacer un seguimiento, análisis rápido y eficaz sobre los posibles riesgos a los que se enfrentan, garantizando así que se aplican las correctas medidas de seguridad.

[34]INCIBE. Kit de concienciación. Recuperado el 31 de mayo de 2022 de: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

AutoAduitat es una herramienta que será de utilidad para que cualquier entidad, pública o privada (entidades de todos los sectores), pueda realizar una autocomprobación acerca del nivel de cumplimiento respecto de sus obligaciones en materia de protección de datos y, además, poder llevar a cabo una autoevaluación inicial del riesgo de seguridad de su negocio en función de cómo hacen uso de la tecnología y la información tratada. De este modo, todas las empresas podrán saber desde dónde empezar a reconstruir sus bases para gestionar la seguridad de su negocio y garantizar así, una persistencia.

Para el desarrollo de este prototipo se han probado varios tipos de software, *plugins* en WordPress, formularios de Google, LimeSurvey e iSpring Quiz Maker 10, viendo cuales eran las ventajas y desventajas de cada uno de ellos. El proceso se inició probando a realizar la encuesta a través de LimeSurvey; después, se procedió a probar el *plugin* H5P de *WordPress* y otra serie de *plugins*, entre ellos: *QuizMaker*, *Forminator* y *QSM*. Sin embargo, todo ello no satisfacía los objetivos planteados en relación con el formato deseado para el cuestionario y, además, las funciones que se requerían para esta tarea no estaban disponibles.

La finalidad principal era generar un autodiagnóstico en el que las preguntas se dividieran por categorías, que cada pregunta tuviera su valor de puntuación y que, dependiendo de la respuesta dada, que el usuario obtuviera un texto o comentario con una serie de recomendaciones o recordatorios y pasos a implantar. Los puntos fundamentales a cubrir eran: establecimiento de una puntuación en cada pregunta, estructuración de las preguntas por categorías, visualización de comentarios o recordatorios para cada respuesta dada y una puntuación final global.

Finalmente, se optó por el empleo de iSpring QuizMaker 10, software descargable para Windows. De las opciones nombradas anteriormente, LimeSurvey y H5P son las dos en las que más tiempo se invirtió, con el fin de comprobar si los objetivos. Cada uno tenía sus ventajas y desventajas, entre ellos no eran nada similares, ya que el diseño y forma en que se llevaba a cabo el cuestionario cambiaba significativamente.

Una de las ventajas que para mí tenía LimeSurvey eran que permitía establecer condiciones sobre las preguntas que no se quisiera que fueran visibles, en caso de que no aplicaran para la organización y las preguntas siguientes a la primera que se hacía no aparecían, es decir, la pregunta se elaboraba de tal manera que si el usuario respondía “No dispongo de …”, entonces las siguientes preguntas no se mostraban. Sin embargo, no permitía establecer ninguna puntuación sobre las respuestas seleccionadas, ni comentarios y, además, el informe que permitía descargar solamente se trataba de un documento que contenía las respuestas dadas, sin ninguna puntuación final. Asimismo, se generaban unas estadísticas las cuales eran visibles solo para el autor del cuestionario y lo que se pretendía era que el usuario que realizara la encuesta pudiera ver por si mismo su reporte final.

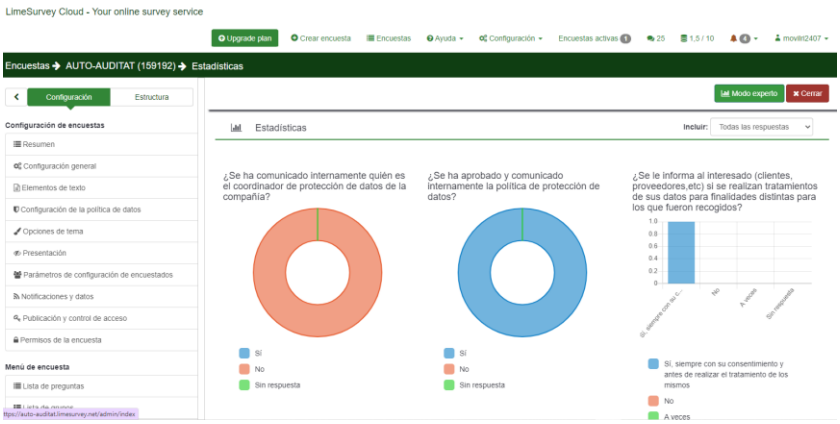


Figura 2: Estadísticas de LimeSurvey.

Fuente: captura de pantalla propia realizada el 25 de junio de 2022.

Por otra parte, de H5P cabe hacer mención a la posibilidad que nos ofrecía para generar un cuestionario de distintas maneras, desde uno simple hasta un libro interactivo con distintas características. Con él se obtiene un cuestionario con un buen diseño, el cual permite establecer puntuaciones sobre cada respuesta correcta o incorrecta, entre otros aspectos. A pesar de ello, las conclusiones finales nos llevaron a confirmar que este *plugin* esta más enfocado a preguntas sencillas, para cursos, formaciones, exámenes pequeños o similares.

Con iSpring Quiz Maker 10 se han obtenido resultados destacables en relación con las expectativas acerca de AutoAuditat. Con este programa también se pudo generar un diseño libre (es similar o igual a la creación de *power points* de *Office*), sin restricciones como por ejemplo en LimeSurvey en el que solamente permitía escoger tres o cuatro tipos de diseños simples de los que disponía la herramienta. Finalmente, tras probar con todas esas herramientas he decidido realizar este autodiagnóstico con iSpring Quiz Maker 10. Entre las ventajas que he visto con este ha sido varias, entre ellas: se puede generar una puntuación a cada pregunta y/o sobre cada respuesta, sobre cada respuesta seleccionada se puede mostrar también un mensaje al usuario, el usuario puede ver fácilmente sus respuestas junto con los comentarios nada más terminar el *quiz* y también la puntuación final con un mensaje de aprobación o suspenso.

En definitiva, el fundamento de este autodiagnóstico eran las preguntas y su correspondiente autoevaluación, por ello el uso de un software sencillo. Las cuestiones generadas, son cuestiones mínimas que se han de tener en cuenta para los tratamientos de datos, servirán como una referencia de apoyo al cumplimiento, aunque luego cada entidad puede considerar otros puntos importantes a valorar.

La elaboración de estas preguntas no ha sido tarea fácil, para ello me he apoyado mucho en mi trabajo actual como consultora. Con las distintas reuniones que realizo en mi día a día he ido apuntándome y analizando cuales eran los puntos más débiles que tenían en común las empresas de las que yo soy su consultora, así como los puntos principales a cumplir. A medidas que iba viendo esas vulnerabilidades, he tratado de plasmar en el cuestionario las preguntas que normalmente hago en las reuniones. Por otra parte, para estructurar el cuestionario se han tomado como referencia tanto en los dominios que se mostraban en la guía de buenas prácticas de IMSFORUM como la estructura en la que en la empresa en la que trabajo, Gesprodat, se generan las actas tras realizar una reunión de revisión.

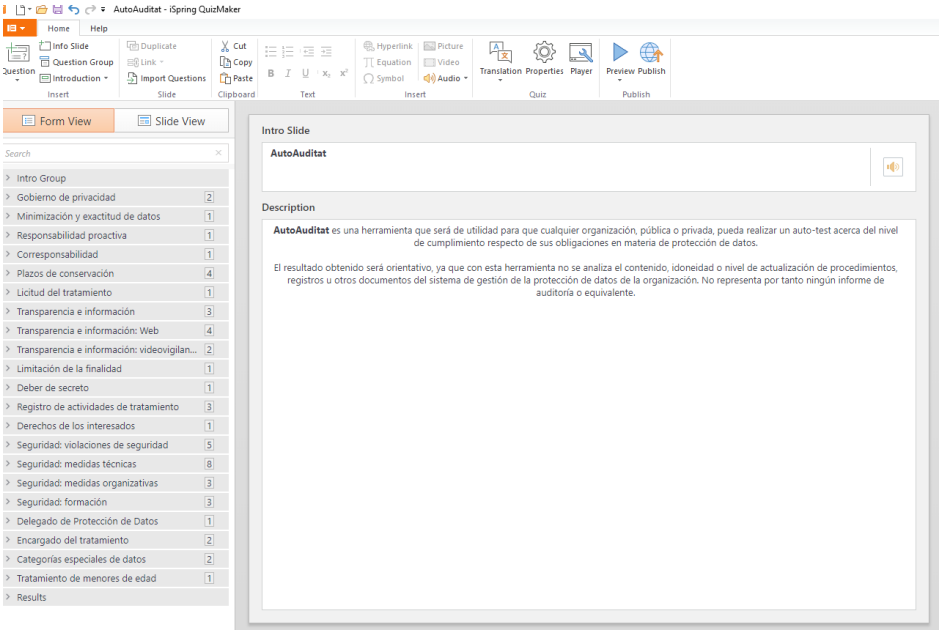


Figura 3: Estructura del *quiz*.
Fuente: captura de pantalla propia realizada el 25 de junio de 2022.

He de recalcar que el resultado obtenido de este autotest será orientativo, ya que con esta herramienta no se analiza el contenido, idoneidad o nivel de actualización de procedimientos, registros u otros documentos del sistema de gestión de la protección de datos de la organización. No representa por tanto ningún informe de auditoría o equivalente, pero sí que puede ser un primer paso para preparar a las organizaciones ante una futura auditoría.

5.1 Bloques del autodiagnóstico

Este autotest consta de 50 preguntas divididas en 21 bloques:

1) Gobierno de la privacidad;
2) Minimización y exactitud de los datos;
3) Responsabilidad proactiva;
4) Corresponsabilidad;
5) Plazos de conservación;
6) Licitud del tratamiento;
7) Transparencia e información;
8) Transparencia e información: web;
9) Transparencia e información: videovigilancia;
10) Limitación de la finalidad;
11) Deber de secreto;
12) Registro de actividades de tratamiento;
13) Derechos de los interesados;
14) Seguridad: violaciones de seguridad;
15) Seguridad: medidas técnicas y medidas organizativas;
16) Seguridad: formación;
17) Delegado de Protección de Datos;

18) Encargado de tratamiento;
19) Categorías especiales de datos;
20) Tratamiento de menores de edad.

A continuación, se destacará y explicará de manera amplia el porqué de haber incluido alguno de estos apartados.

5.1.1 Gobierno de la privacidad

La AEPD define la gobernanza de datos como: "proceso por el que se definen políticas y procedimientos para garantizar una gestión de datos proactiva y efectiva. Además, la adopción de un marco de gobierno de datos permite la colaboración de todos los niveles de la organización, nivel estratégico, táctico y operativo, para gestionar datos de toda la entidad, y proporciona la capacidad para alinear los datos con los objetivos corporativos".[35]

Este primer bloque de preguntas es importante para poder gestionar de la mejor forma posible toda la información que se maneja dentro de la empresa. Para ello, la manera más efectiva y eficiente de realizarlo es definir los roles y las responsabilidades de las personas que formarán parte de este proceso, sobre todo un coordinador de protección de datos que sea responsable de establecer las políticas y procedimientos, y con esto garantizar una buena gestión de la información y los datos que se tratan. Esto implica mantener un control de los cambios que surgen en la organización, actualizando así las medidas de seguridad que correspondan. Será necesario que estas políticas sean aprobadas por los departamentos a los que les impliquen y comunicadas a todo el personal en plantilla, con el objetivo de que todos sean conscientes de cómo tratar adecuadamente los datos sin generar ningún tipo de incidente.

5.1.2 Minimización y exactitud de los datos

En este segundo bloque se pretende recalcar la importancia de tratar los datos con la finalidad para la que fueron recogidos y tratar el menor número de datos, con esto se evitará acumular datos innecesarios y los titulares de los datos se encontrarán más tranquilos sobre el tratamiento de sus datos. Por otra parte, llevar un control sobre los datos para mantenerlos actualizados conforme a la realidad, evitará que sean incorrectos e inexactos. La mejora de la veracidad de los datos tendrá diversos beneficios, entre ellos: la confianza del cliente aumentará, mejorará la imagen de la empresa, se asegurará la toma de decisiones exacta, con esto la continuidad del negocio.

[35]AEPD. Gobernanza y política de protección de datos. Recuperado el 12 de junio de 2022 de: https://www.aepd.es/es/prensa-y-comunicacion/blog/gobernanza-y-politica-de-proteccion-de-datos

5.1.3 Responsabilidad proactiva

El RGPD describe el principio de responsabilidad proactiva como la necesidad que tiene el responsable de tratamiento de aplicar medidas técnicas, legales y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento esta conforme a la normativa. Las medidas establecidas por el RGPD e indicadas en la AEPD[36] para garantizar los derechos y libertades de las personas cuyos datos son tratados son:

- Registro de actividades de tratamiento;
- Análisis de riesgos;
- Medidas de seguridad;
- Evaluaciones de impacto;
- Autorización previa o consultas previas;
- Establecimiento del delegado de protección de datos;
- Notificación de las violaciones de seguridad.

Se dependerá de los apartados que vienen a continuación, para saber que se cumple de forma correcta este punto. Garantizar el principio de responsabilidad proactiva beneficiará a todas las empresas y asegurará su mejora continua, esto implica:

- Evitar ataques a *ransonware*;
- Disponer de una correcta protección de los datos en cada servidor;
- Llevar a cabo un buen aprovechamiento de los datos.

5.1.4 Plazos de conservación

Los plazos de conservación sobre los datos deben establecerse principalmente para evitar acumular información dentro de la organización. Guardar datos innecesarios que no aportan ningún valor a la empresa, provocará perdidas de información realmente importantes, además de problemas con los titulares de los datos sobre sus derechos.

El principio de limitación del plazo de conservación genera siempre mucha inseguridad a la hora de cumplir con la normativa de protección de datos, ya que el RGPD no establece plazos concretos para la conservación, por tanto, lo que se deberá tener en cuenta es el principio básico de conservarlos el tiempo que se considere razonable, teniendo en cuenta cuál será el objeto del tratamiento de los datos. Por ello, cuando ya no se necesiten los datos para el objeto del tratamiento y tampoco sea de interés público, lo mejor será suprimirlos.

El Responsable deberá definir los plazos de retención o conservación de los datos según la legislación se lo determine (legislación laboral, fiscal o correspondiente a otras materias del Derecho) o se lo exija como responsabilidad (contractual, civil, penal, etc.). También podrá definir criterios propios que equilibren un plazo razonable de conservación responsable, frente a unos datos de calidad (veraces y exactos).

[36]AEPD (14 de junio de 2022). Medidas de cumplimiento. Recuperado el 12 de junio de 2022 de: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento

5.1.5 Transparencia e información

La clave de este capítulo es la transparencia y claridad de la información que se proporciona a los interesados. Es decir, mantener informados a los interesados siempre que se traten datos suyos, evitando tecnicismos, haciendo uso de un lenguaje claro y sencillo.

La información se podrá dar a través de distintos medios, bien mediante cláusulas informativas, formularios, contratos, cualquier otro documento que se entregue. Pero como dice el RGPD[37], deberá facilitarse de forma escrita, incluyendo los medios electrónicos cuando esto sea apropiado.

5.1.5.1 Transparencia e información: web

Tener una página web implica cumplir con dos leyes importantes, RGPD y LSSI CE[38]. El incumplimiento de estas puede incurrir a sanciones de miles de euros. Por esta razón y otras, se ha dado importancia a la inclusión de este capítulo de preguntas y aunque la entidad que realice el autodiagnóstico no disponga de página web corporativa, es importante que este informada sobre los puntos más esenciales a garantizar.

El prestador de servicios está obligado a ofrecer cierta información en su página web, esta información quedará dividida en los siguientes textos legales:

- Aviso legal;
- Política de privacidad;
- Política de cookies.

Sin embargo, si existe la venta de bienes o servicios, se deberá incluir también las condiciones de venta. Cabe destacar, que estos textos legales deberán ser claramente visibles y de acceso directo (mediante un hipervínculo por cada texto legal) durante toda la navegación de los usuarios.

No solo se considera sanción el no disponer de los correspondientes textos legales, sino también el no informar a los usuarios al acceder por primera vez a la página web sobre las cookies de las que se hacen uso (mediante un *banner* informativo), permitiéndoles descargar las cookies que deseen en su equipo. Para cumplir con esto, será necesario disponer de un configurador de cookies que permita a los usuarios activar o desactivar las cookies no necesarias.

En conclusión, es muy importante que nuestra página web, cómo imagen pública de la empresa, disponga de un cumplimiento real y actualizado de las normativas relacionadas con el tratamiento de la información de los usuarios.

[37]AEPD (22 de mayo de 2018). Guía RGPD para responsables de tratamiento. Recuperado el 12 de junio de 2022 de: https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf
[38]Ley 24/2002, de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico.

5.1.5.2 Transparencia e información: videovigilancia

Este capítulo se considera importante en especial para aquellas empresas que dispongan de sistemas de videovigilancia, pero también para las que no, ya que es esencial que se mantengan al tanto de los puntos a cumplir en caso de que implanten en algún momento estos sistemas, previniendo así posibles sanciones. Las entidades que no informen sobre la disposición de estos sistemas pueden buscarse problemas con aquellas personas con las que no desean ser grabadas.

El cumplimiento de este punto implica disponer, colocar e informar sobre la implantación de estos sistemas mediante un cartel informativo, que deberá estar ubicado en los espacios en los que estén instaladas las videocámaras, un lugar claramente visible y, en todo caso, en las entradas de la entidad. La información mínima que debe contener este cartel es:

- Datos del responsable del tratamiento de datos;
- Ejercicio de derechos, medio por donde el interesado pueda ejercer sus derechos (correo electrónico y/o dirección postal);
- Apartado con más información informando sobre: la finalidad, el plazo de conservación de los datos, las posibles comunicaciones o cesiones de datos, entre otros.

5.1.6 Deber de secreto

El pilar del deber de secreto se basa en la no revelación de los datos de carácter personal que se tratan dentro de la organización a personas ajenas a ella, se conoce como deber de secreto profesional. Esto implicará que todo profesional (personal laboral de la empresa) que tenga acceso a los datos de carácter personal como consecuencia del desempeño de sus funciones en la organización, asumirá la confidencialidad y el deber de guardar sigilo incluso tras finalizar la relación laboral, esto se garantizará mediante la firma del acuerdo de confidencialidad, este acuerdo suele firmarse junto al contrato de empleo, todo el personal deberá estar informado y haber firmado este acuerdo. Así como otros puntos mencionados anteriormente, el incumplimiento del mismo puede con llevar a enormes sanciones por parte de la AEPD, ya que es una de las infracciones consideradas como graves en la LOPDGDD.

5.1.7 Registro de actividades de tratamiento

El registro de actividades de tratamiento es uno de los principales puntos a implantar para poder cumplir con la normativa vigente en materia de protección de datos y aparte, es una obligación para los responsables el mantenimiento de estos registros. Este es el punto base para el cumplimiento de la normativa.

El formato en el que debe estar el registro puede ser en físico o electrónico, pero lo importante es que siempre este a disposición del responsable o encargado del tratamiento, ante posibles controles por parte de la AEPD.

Los puntos mínimos en los que deberá dividirse este registro son:

- Finalidad del tratamiento;
- Base jurídica: consentimiento, ejecución de un contrato, interés legítimo, obligación legal, interés público y/o protección de intereses vitales;
- Origen de los datos: el propio interesado o su representante legal, registros públicos, entidad privada, administraciones públicas y/u otras personas físicas;
- Procedimiento de recogida: medios digitales o en soporte papel;
- Datos de carácter identificativo;
- Datos de categoría especial;
- Destinatarios de cesiones;
- Nivel de seguridad, básico o alto;
- Nivel de tratamiento: manual, automático o mixto;
- Transferencias internacionales, sí o no;
- Medidas técnicas;
- Medidas organizativas;
- Plazos de conservación.

5.1.8. Derechos de los interesados

La protección de datos es un derecho que tenemos todos y el ejercicio de todos los derechos es y debe ser gratuito.

Los procesos en los cuales se tratan los datos no dejan de ser una situación donde se está tratando con un bien de los interesados el cual les pertenece, y aunque te permitan utilizarlo, no deja de ser un bien privativo. Por todo esto, sus derechos son esenciales para guardar su seguridad y la de sus datos. Los responsables del tratamiento de los datos estarán obligados a permitir ejercer los derechos en el plazo de un mes y también deberán informar de los medios que se emplean para hacerlos valer. Es decir, para que los interesados puedan ejercer sus derechos deberá existir un medio habilitado donde los interesados puedan solicitar el ejercicio de sus derechos de forma fácil y sencilla. Un medio puede considerarse un correo electrónico (o una página web), en el que solamente se reciban solicitudes y se gestione su respuesta con la mayor brevedad posible.

5.1.9 Seguridad: violaciones de seguridad

Las violaciones de seguridad pueden provocar la pérdida de confianza de los titulares de los datos y una gran pérdida económica dentro de la entidad, se perderá la reputación y se dará a entender que la organización no dispone de la mayor seguridad para gestionar datos de personas físicas. Sin embargo, tener un procedimiento para gestionar las brechas de seguridad, hará que se eviten un mayor número de incidentes y se tendrá la tranquilidad de los titulares de los datos, al ver que la entidad sabe actuar de manera rápida y eficiente ante inesperados incidentes, ya que muchos de ellos pueden no ser por falta de seguridad si no por ataques tan grandes que no se ven venir o nunca se han producido y se desconoce la forma de actuar ante ellos.

El procedimiento para gestionar las brechas de seguridad se basa en la comunicación a la AEPD dentro del plazo establecido, pero puede haber casos en los que, debido a la complejidad de identificación del incidente, este plazo puede no cumplirse. En estos casos es posible realizarla posteriormente al incidente, pero siempre acompañado de una explicación contundente y adecuada, indicando los motivos de su retraso. En cambio, no siempre se trata de la comunicación, si no que puede haber casos en los que no sea necesario siempre que el responsable tome las medidas de seguridad apropiadas previamente a la violación de seguridad, tal y como indica la AEPD[39].

La importancia de disponer de un procedimiento conlleva el ahorro de multas de miles o millones de euros por el simple hecho de haber notificado la violación ante la autoridad de control y al interesado afectado. A esto se suma la importancia de la existencia de organismos o figuras (como el DPD) que asuman la responsabilidad y sepan solucionar los retos y amenazas que acechan en las empresas.

5.1.10 Seguridad: medidas técnicas y medidas organizativas

Con este aspecto se garantizará la seguridad de los datos que se tratan, los responsables y encargados del tratamiento serán los que tendrán la misión de establecer las medidas técnicas y organizativas para disponer de una buena seguridad.

Ambas medidas deberán estar documentadas e informadas a todo el personal, pero antes que nada es necesario que sean revisadas y aprobadas por el departamento correspondiente. La implementación de medidas técnicas implicará disponer de la mayor seguridad en los equipos informáticos en los que se guarden datos personales (copias de seguridad, sistemas antivirus, seguridad de los servidores, cifrado de los datos, identificación y autenticación, entre otros). Por otra parte, el establecimiento de medidas organizativas implica llevar un control de la documentación que se trata y el almacenamiento seguro de esta.

Se requiere hacer estas cuestiones debido a que con esto la entidad podrá asegurarse de que se producirán los menores incidentes posibles. Es decir, que este apartado estará claramente relacionado con el anterior, ya que, si no se tienen implementadas las medidas técnicas y organizativas apropiadas, esto dará pie a que se tengan más puertas abiertas a los ciberdelincuentes y con ello, brechas de seguridad.

[39]AEPD. ¿A quién hay que notificar las brechas de datos personales? Recuperado el 12 de junio de 2022 de: https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/11-brechas-de-datos-personales/FAQ-0233-a-quien-hay-que-notificar-las-brechas-de-datos-personales

5.1.12 Seguridad: Formación

Es esencial que los responsables informen y formen a todos los empleados sobre el buen uso de los medios informáticos y el correcto tratamiento de los datos. Para ello es imprescindible recordar y llevar a cabo estas formaciones de manera periódica, bien mediante cursos, recordatorios (infografías, píldoras informativas u otras comunicaciones).

Cuando se trata de la protección de datos, la formación de los trabajadores es necesaria. Muchas veces el desconocimiento en esta materia les hace responsables de la producción de ciberataques que causan enormes daños a la seguridad de la empresa. Estos incidentes muchas veces ocurren de forma inocente, ya que no siempre se trata de que los trabajadores lo hagan a propósito, si no que puede que no sean conscientes de los efectos que pueden derivar de su conducta.

5.1.14 Encargado de tratamiento

El propósito de hacer hincapié en este punto es que, al disponer de un encargado de tratamiento, es fundamental escoger uno con el que se pueda garantizar que se aplicarán las medidas de seguridad apropiadas, es decir, que los datos se tratarán conforme a lo establecido por el responsable de tratamiento. Lo que une al responsable y encargado de tratamiento es un contrato de encargo, será el punto clave a tener en cuenta, este contrato deberá firmarse con todos los proveedores que tengan acceso a los datos de la organización. La mayoría de las entidades disponen de un informático externo, asesoría que se encarga de gestionar las nóminas de los trabajadores, empresa de limpieza, seguridad, consultoría, empresa de formación, entre otros.

Muchas veces se tienen muchos proveedores que acceden o pueden tener acceso a los datos de la organización, aumentando así la vulnerabilidad de los datos. La responsabilidad del responsable de tratamiento de tratar datos de un gran número de personas implica garantizar que cuando estos datos se ceden a personas externas a la organización, sean tratados de forma segura y sin ocasionar modificaciones ni alteraciones, manteniéndolos de acuerdo al principio de exactitud de los datos.

Conclusiones.

A día de hoy, la mayoría de los datos se encuentran digitalizados debido al uso masivo de Internet, las redes sociales e información subida a la nube. La protección de datos y la seguridad de la información debe ser una prioridad establecida por todas las empresas y autónomos. Se debe saber que toda empresa (grande, mediana o pequeña) y autónomos, recaban datos de un modo u otro para su posterior tratamiento. El tratamiento de estos datos puede ser por obligación legal, consentimiento y/o contrato, pero siempre debe estar basando en alguna de estas tres bases legitimadoras, tal y como menciona el principio de licitud del tratamiento. Regular el uso de estos datos es esencial para garantizar el honor, la privacidad (intimidad), los derechos, la seguridad y tranquilidad de las personas físicas. El correcto tratamiento de datos será beneficioso para cualquier negocio, la satisfacción de los clientes es un punto clave para la reputación, imagen y progresión de toda empresa. Su incumplimiento puede llevar a la empresa a grandes problemas, como multas de millones de euros.

Por este motivo, es importante conocer previamente la Ley que aplica al tratamiento de datos de carácter personal y en caso de que no se sepa cómo tratar los datos de forma correcta, lo mejor será asesorarse mediante una consultoría especializada en ello y seguir las directrices que se marquen. En el peor de los casos, lo mejor será no llevar a cabo esa responsabilidad y ponerla en manos de alguien especializado en ello. Por esto, resulta importante realizar una correcta elección del responsable del tratamiento de los datos, ya que una mala gestión puede perjudicar tanto a los titulares de los datos como a las personas que trabajan en la organización, estos pueden perder su trabajo por el cierre de la empresa.

Por mi experiencia durante mi estancia en prácticas y mi continuidad en una empresa de consultoría especializada en derechos de las nuevas tecnologías, he podido observar a primera vista que es muy difícil toparse con una empresa que cumpla de primera mano los principales principios del RGPD. Es necesario mantener un control periódico, en el que se revise como mínimo cada año los cambios que hayan surgido en la organización para poder aplicar las correctas medidas de seguridad (técnicas, legales y organizativas), y para ello es crucial la implicación de la organización y el interés de todo el personal, sobre todo del coordinador, para que toda la plantilla pueda seguir las mismas directrices y con ello un buen camino hacia la adecuación de la normativa vigente en materia de protección de datos.

No obstante, hay casos en los que el total cumplimiento puede verse afectado por terceras personas, como proveedores que tengan acceso a datos de la organización u otros prestadores de servicios. Esto puede ser el caso de un informático externo encargado del mantenimiento de los sistemas de la organización, una empresa de destrucción documental, la agencia encargada del mantenimiento de la página web, entre otros proveedores. Por esa razón, es necesario escoger proveedores que ofrezcan garantías suficientes conforme con los requisitos del RGPD y que garanticen la protección de los derechos del interesado, como se ha explicado anteriormente. Pero no todos los responsables de tratamiento de los datos están al tanto de las normativas y principios que han de cumplir para poder llevar a cabo un buen tratamiento de los mismos, las normas van cambiado y es complicado estar al día de todas las novedades, la AEPD sube siempre pequeños cambios en su página, de lo que es importante estar al día. Aunque la ciberseguridad absoluta no existe, es necesario tratar de reducir al máximo los riesgos.

Personalmente, me he topado con entidades que meses antes de su auditoría no saben que es lo que deben tener en mano o listo para pasar con éxito, y muchos de ellos hasta que no realizan la auditoría y se les da un tiempo para entregar la documentación pedida por el auditor como evidencia, no se dan cuenta de cuál es la documentación u otro tipo de evidencia importante a presentar para garantizar que están haciendo lo correcto dentro de su negocio. Asimismo, en el momento en que les llega un informe de auditoría desfavorable, es cuando reaccionan y alguno de ellos lo hace de mala manera, en ocasiones pueden haber malentendidos pero lo mejor es mostrar una buena actitud para mejorar. Sin embargo, aunque se les dé un plazo para la entrega de la documentación a veces no muestran el interés y la implicación que se debe demostrar para prosperar hacia un buen camino. Por esto, resulta esencial hacer saber a todas las empresas que se encuentran desubicadas en este ámbito, que documentos, procedimientos, medidas, cláusulas y políticas deben tener en su punto de mira para llevar un control de los mismos.

Muchas empresas quieren cumplir al pie de la letra con las medidas de seguridad que establece el RGPD, pero la mayoría de ellas no son capaces de conseguirlo y esto no es siempre por falta de interés, si no que a veces es debido a la falta de conocimientos y recursos. Sin embargo, el desconocimiento de la Ley no excluye a nadie de su cumplimiento.

Por esta razón, encuentro conveniente y esencial proporcionar este autodiagnóstico que ayude a todas las entidades, ya que es una evaluación básica e importante al estar basada en la normativa vigente (RGPD), la cual afecta a muchas personas. El alivio que generará un autodiagnóstico previo a la auditoría será fundamental y motivará a todas las organizaciones a llevar una gestión adecuada de los datos, ya que con unos minutos dedicados a la autoevaluación sabrán en que aspectos deberán comenzar a centrarse de manera más profunda. Muchas veces la consultoría que se tenga contratada no puede darte una solución al momento, bien porque tienen otras consultas urgentes que atender o porque la solución a ese problema les llevará más tiempo de lo normal, y esto hace que muchas empresas vayan dejando de lado las vulnerabilidades o problemas que tengan, acumulando así una montaña de incidencias.

Con esta autoevaluación puede que se consiga formar a todas aquellas empresas que la realicen, concienciándolas de la importancia de cumplir con la normativa y aumentando así sus conocimientos en protección de datos con las recomendaciones y recordatorios que se indica en cada respuesta seleccionada. Con los resultados obtenidos se pretenderá asegurar una adecuada identificación de las amenazas a las que esta expuesta cada actividad del tratamiento de los datos que lleva a cabo la organización.

Motivación.

Aquello que me ha llevado a realizar este TFG, ha sido principalmente mi interés por el mundo de la auditoría y consultoría en materia de protección de datos. La asignatura que se da en cuarto de carrera denominada “Gestión de Servicio de SI TI” fue la que me hizo conocer esta área. Por otra parte, haber podido conseguir unas prácticas sobre algo que me gusta y que tenía ganas de aprender y conocer más a fondo, ha sido una suerte, sobre todo el poder haber recibido tanta ayuda para aprender cada día más sobre esto. Poder haber vivido desde primera línea que se hace exactamente y cómo, me ha ayudado mucho a poder redactar este trabajo y poder llevar a cabo el cuestionario de autoevaluación, el cuál pienso que será de gran apoyo para las pequeñas empresas que se encuentran perdidas dentro del área de la protección de datos y también para las grandes empresas que manejan una enorme cantidad de documentos, y que consideran un fastidio o requieren de tiempo para poder sentarse junto con su consultor para implantar las correctas medidas de seguridad y cumplir así con la normativa en su organización.

BIBLIOGRAFÍA

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades. Recuperado de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

AEPD (13 de abril de 2018). Listado de cumplimiento normativo. Recuperado de: https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf

AEPD (16 de mayo de 2018). Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. Recuperado de: https://www.aepd.es/es/documento/guia-directrices-contratos.pdf

AEPD (2022). ¿Cuál es el contenido del contrato de encargado de tratamiento? Recuperado de: https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/12-encargados-de-tratamiento/FAQ-0238-cual-seria-el-contenido-del-contrato-de-encargo-de-tratamiento

AEPD (2022). ¿Qué es el Registro de actividades de tratamiento? Recuperado de: https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/8-registro-de-actividades/FAQ-0220-que-es-el-registro-de-actividades-de-tratamiento

AEPD (22 de mayo de 2018). Guía del Reglamento General de Protección de Datos para responsables de tratamiento. https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf

AEPD (29 de junio de 2018). Guía sobre el uso de videocámaras para seguridad y otras finalidades. Recuperado de: https://www.aepd.es/es/documento/guia-videovigilancia.pdf

AEPD (8 de noviembre de 2019). Guía sobre el uso de cookies. Recuperado de: https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

AMBIT BST (10 de noviembre, 2020). Tipos de Vulnerabilidades y Amenazas informáticas. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Vol. 46). 3Ciencias. Recuperado de: Seguridad-informática.pdf (3ciencias.com)

Cookiebot (18 de enero de 2022). Consentimiento de cookies, en resumen. Recuperado de: https://www.cookiebot.com/es/consentimiento-cookie/

Costas Santos, J. (2011). Seguridad informática. *Bogotá: Ra-ma Editorial*. Recuperado de: https://books.google.es/books/about/Seguridad_Inform%C3%A1tica_GRADO_MEDIO.html?id=7I6fDwAAQBAJ&redir_esc=y

DATADEC (2017). Consejos para una correcta gestión de incidencias. Recuperado de: https://www.datadec.es/blog/consejos-para-correcta-gestion-de-incidencias

EKON (2019). Cómo hacer una política de protección de datos. Recuperado de: https://www.ekon.es/blog/hacer-politica-proteccion-datos/

ESET. Guía sobre el Reglamento General de Protección de Datos. Recuperado de: https://gdpr.eset.es/pdf/ESET_Guia_sobre_el_reglamento_general_de_proteccion_de_datos_GDPR.pdf

Grupo Atico34 (2022). "He leído y acepto" ¿Qué asumimos al aceptar las Políticas de privacidad? Recuperado de: https://protecciondatos-lopd.com/empresas/he-leido-y-acepto-la-politica-de-privacidad/

Grupo Atico34 (2022). Protección de datos en currículums: La gestión de datos personales de candidatos. Recuperado de: https://protecciondatos-lopd.com/empresas/curriculums-datos-personales-candidatos/#:~:text=Si%20bien%2C%20respecto%20al%20CV,su%20lectura%2C%20o%20su%20eliminaci%C3%B3n.

Grupo Atico34 (2022). Textos legales web 2022 obligatorios para cumplir con la LOPDD y el RGPD. Recuperado de: https://protecciondatos-lopd.com/empresas/textos-legales-web/

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf

INCIBE (11 de marzo de 2015). La seguridad desde sus inicios. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

INCIBE (2018). Copias de seguridad: una guía de aproximación para el empresario. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

INCIBE (2020). Políticas de seguridad para la pyme: contraseñas. Recuperado de: https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf

INCIBE. Ciberamenzas contra entornos empresariales: una guía de aproximación para el empresario. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

INCIBE. Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-ganar-competitividad-cumpliendo-rgpd-metad.pdf

Instrucción nº2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías. *Boletín Oficial del Estado, 2, de 11 de octubre de 2011*. https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf

ISMS FORUM (28 de mayo de 2020). Guía de buenas prácticas en auditorías RGPD. Recuperado de: https://www.ismsforum.es/ficheros/descargas/guia-de-buenas-practicas-en-auditorias.pdf

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (1999). *Boletín Oficial del Estado, 298, de 14 de diciembre de 1999.* https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (2018). *Boletín Oficial del Estado, 294, de 6 de diciembre de 2018*, 119788 a 119857. https://www.boe.es/eli/es/lo/2018/12/05/3/dof/spa/pdf

López, P. A. (2010). *Seguridad informática*. Editex. Recuperado de: https://d1wqtxts1xzle7.cloudfront.net/54078418/Seguridad_informatica_UD01_1-with-cover-pagev2.pdf?Expires=1652025327&Signature=CwZbCGnz3DkZYtHb9LBzH2R9gzHrhNoGMMrMISdn6htkUeKGoG1sO25OB1JxB62eKYXSeM~mLMuD525nI4L4IfCJ8tMXwB1Gkm9tg1cB5s58jPVi8mH2nqVxy9rQCNjBgbyZqProwbih8qNBkp8or8FbZWq8p6B6pz4nVqpJAU-Admy5uvsfXd3RySeveER3HAUR7FmVCMKrhurNdyW8QmNGvQxSX2KHHF7LmI58TMpjsv1tenYJpUOCmGoSKiHb5PXthrnhdHE185MTfmQp7VhG2pwzSP7Bbry3kmW1dTfdp~eCm6cxmETX~bnlaEeKVpKh8bfO2b22Xpt29pPA__&Key-PairId=APKAJLOHF5GGSLRBV4ZA

Montenegro, D. B. N. (2015). El delito informático y su clasificación. *Revista UNIANDES Episteme*, *2*(2), 158-173. Recuperado de:https://dialnet.unirioja.es/descarga/articulo/6756355.pdf

Posada, R. E., & Somellera, R. (1998). Delitos informáticos. *Informática y derecho: Revista iberoamericana de derecho informático*, (27), 423-442. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/248204.pdf

Postigo Palacios, A. (2020). *Seguridad informática (Edición 2020)*. Ediciones Paraninfo, SA. Recuperado de: https://books.google.es/books/about/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020.html?id=UCjnDwAAQBAJ&printsec=frontcover&source=kp_read_button&hl=es&redir_esc=y#v=onepage&q&f=false

Reglamento (UE) 2016/679 DEL Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personal y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *Diario Oficial de las Comunidades Europeas*, 4 de mayo de 2016, núm. 119. Recuperado de: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Tarazona, T., & Cesar, H. (2007). Amenazas informáticas y seguridad de la información. *Derecho penal y criminología*, *28*, 137. Recuperado de:https://dialnet.unirioja.es/descarga/articulo/3311853.pdf

Vieites, Á. G. (2011). *Auditoria de seguridad informática (MF0487_3)*. Grupo Editorial RA-MA. Recuperado de: https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&as_vis=1&q=Auditor%C3%ADa+de+Seguridad+Inform%C3%A1tica+%28MF0487_3%29&btnG=#d=gs_cit&t=1655550603809&u=%2Fscholar%3Fq%3Dinfo%3AgOkaAAheJfcJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Des

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, *3*(3), 676-688. Recuperado de: Seguridad en informática: consideraciones - Dialnet (unirioja.es).

Anexos.

A. AutoAuditat Quiz

AutoAuditat

AutoAuditat es una herramienta que será de utilidad para que cualquier organización, pública o privada, pueda realizar un auto-test acerca del nivel de cumplimiento respecto de sus obligaciones en materia de protección de datos.

El resultado obtenido será orientativo, ya que con esta herramienta no se analiza el contenido, idoneidad o nivel de actualización de procedimientos, registros u otros documentos del sistema de gestión de la protección de datos de la organización. No representa por tanto ningún informe de auditoría o equivalente.

¿Tu organización está adaptada al RGPD y a la LOPDGDD?

¿No sabes en qué punto de cumplimiento se encuentra tu empresa y quieres asegurarte si cumple adecuadamente con la Ley Orgánica de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)?

...

¡Vamos a ello!

Gobierno de la privacidad:

Política de privacidad interna, procedimientos organizativos, roles y funciones de la privacidad, identificación de la autoridad de control, revisión de inspecciones y sanciones, códigos de conductas y/o certificaciones, normas corporativas vinculantes.

1. ¿Se ha comunicado internamente quién es el coordinador de protección de datos de la compañía?

A) No

B) Sí

2. ¿Se ha aprobado, establecido y comunicado internamente la política de protección de datos?

A) No lo sé

B) Sí

C) No

Minimización y exactitud de datos:

Cumplimiento del artículo 5 del RGPD.

Minimización: verificar el tratamiento de los datos indispensables para su finalidad (en formularios, en registros, etc.), y no datos en exceso.

Exactitud: verificar que los datos se mantienen al día, bien desde la propia entidad, bien porque el propio interesado puede poner sus datos al día (desde su cuenta, desde su perfil, etc.). Verificar que no existen bases de datos duplicadas o bases de datos no centralizadas que pueden dar lugar a datos inexactos

3. ¿Se le informa al interesado (clientes, proveedores, titulares de los datos) si se realizan tratamientos de sus datos para finalidades distintas para los que fueron recogidos?

A) Sí, siempre con su consentimiento y antes de realizar el tratamiento de los mismos

B) No

C) A veces

Responsabilidad proactiva:

Cumplimiento del artículo 5, 25 y 35 del RGPD.

Privacidad desde el diseño y por defecto, Evaluación de impacto relativa a la protección de datos y Análisis de riesgos para la privacidad.

4. Cuando surge un nuevo tratamiento o proyecto que utilizará datos personales, ¿se realiza un análisis previo por las implicaciones de la protección de datos (se pone en conocimiento del responsable de protección de datos)?

A) Se informa al responsable para que intervenga, analice y asesore inicialmente en los puntos correspondientes a la privacidad

B) No

C) No lo sé

Corresponsabilidad:

Cumplimiento del artículo 5 y 26 del RGPD.

Escenarios de corresposabilidad, revisión de acuerdos de corresponsabilidad, coordinación entre los corresponsables.

5. ¿Se tiene un protocolo para llevar a cabo la implementación de la corresponsabilidad ?

A) Se firma de un acuerdo de corresponsabilidad, se fijan las responsabilidades para el cumplimiento de las obligaciones y se informa al interesado sobre los aspectos esenciales del acuerdo

B) No lo sé

C) No

D) No sé que hay que hacer

Plazos de conservación:

Cumplimiento del artículo 5 del RGPD.

Plazos por Ley general, plazos por ley específica, plazos por alguna responsabilidad, plazos basados en criterios propios y sistema de destrucción tras vencimiento de plazos.

6. ¿Se han determinado plazos de conservación de datos, basados en: obligación o imperativo legal, responsabilidad (civil, penal, etc.) o criterio interno objetivo y válido?

A) Sí

B) No lo sé

C) No

7. Con carácter general, ¿cuánto tiempo se conserva la documentación de los clientes y trabajadores? (Por ejemplo: facturas, contratos, albaranes, ficha laboral, entre otros)

A) Se eliminan cuando dejan de ser necesarios para la finalidad para la cual fueron recabados o registrados

B) De forma indefinida, no se tiene un plazo establecido

C) No lo sé

8. ¿Durante cuánto tiempo se conservan los datos de un extrabajador?

A) Se conservan durante el plazo establecido por la legislación aplicable

B) No lo sé

C) No se tiene un plazo establecido, se guardan por si acaso se necesitaran en un futuro

9. ¿Tiene establecido un plazo de conservación sobre los currículos?

A) 1 año

B) Más de 1 año

C) Indefinido, no se tiene un plazo establecido

D) No lo sé

Licitud del tratamiento:

Cumplimiento del artículo 6 del RGPD.

Argumentación/ análisis de los tratamientos basados en interés legítimo, revisión de: consentimientos, contratos, cláusulas informativas.

10. ¿Los tratamientos de datos personales cuentan al menos con una base legitimadora de conformidad con el RGPD (consentimiento, obligación legal y/o ejecución de un contrato)?

A) Ninguno

B) Consentimiento del interesado

C) No lo sé

D) Ejecución de un contrato

E) Obligación legal

Transparencia e información:

Cumplimiento del artículo 13 y 14 del RGPD.

Cláusulas informativas y consentimientos.

11. ¿Ha establecido una nota legal***** sobre protección de datos en los correos electrónicos de la organización?

*******Nota legal: cláusula informativa en el pie de firma relativa al tratamiento de los datos personales en la que se informa sobre: i**dentidad del responsable, finalidad del tratamiento, legitimación o base jurídica, destinatarios de los datos, derechos de usuarios y cómo ejercerlos, procedencia y plazo de conservación de los datos.***

A) Una cláusula en el pie de firma

B) No

C) No lo sé

12. Indique si utiliza actualmente algún tipo de documento para solicitar datos personales (formulario, encuesta, contrato, entre otros documentos) que no contenga un aviso, cláusula o texto informativo sobre protección de datos.

A) Todos mis documentos para solicitar datos personales contienen una aviso, cláusula o texto informativo sobre protección de datos

B) Ninguno de los documentos que se utilizan contienen textos o cláusulas sobre protección de datos

C) No lo sé

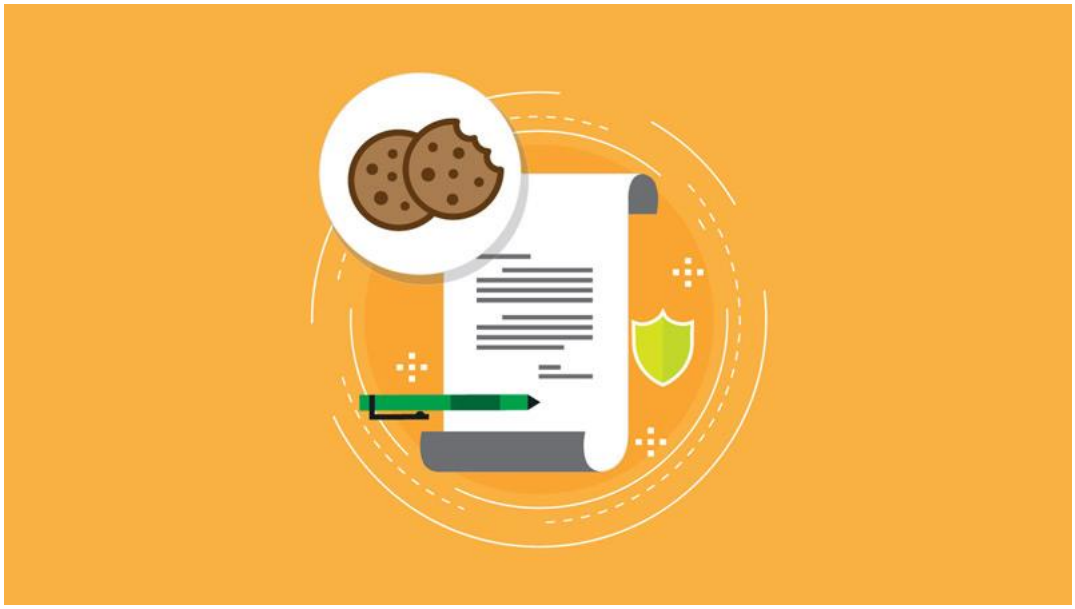
13. ¿Se toman medidas para facilitar al interesado toda la información relativa al tratamiento de sus datos?

A) Se realiza de forma escrita, incluidos los medios electrónicos (cuando sea apropiado)

B) No

C) A veces

Web:



Cumplimiento del artículo 13 y 14 del RGPD.

Política de privacidad y Política de cookies de la página web.

14. En su página web corporativa, ¿de qué manera se permite a los usuarios aceptar, rechazar y/o seleccionar las cookies que desean instalar en su equipo?

A) Botón de aceptar, rechazar y un hipervínculo a un panel de configuración (permite al usuario activar/ desactivar las cookies no necesarias)

B) Botón aceptar y rechazar

C) Botón aceptar y configurar

D) Botón aceptar

15. ¿Se han implementado los textos legales***** que necesita su página web?

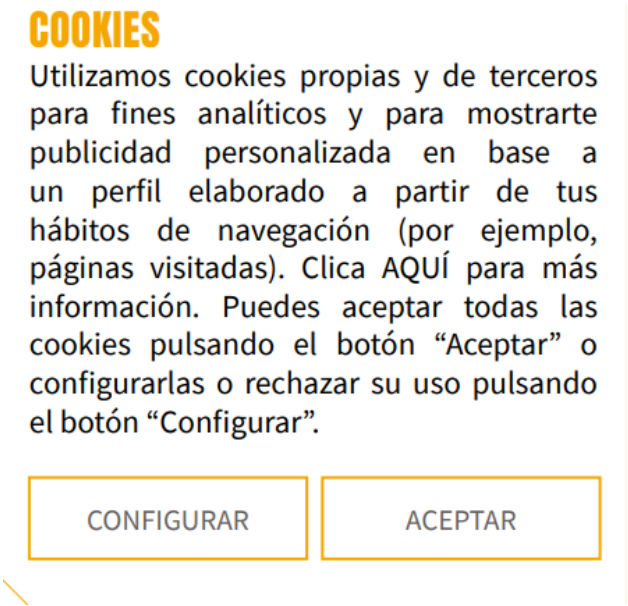
***** política de privacidad, aviso legal, política de cookies.

A) Política de privacidad, política de cookies y aviso legal

B) Ninguno

C) No lo sé

16. ¿La página web dispone de un banner informativo relativo al tipo de cookies de las que se hacen uso?



A) Sí, es visible al acceder por primera vez a la página web

B) No

C) No lo sé

17. ¿Los formularios que se encuentran en la página web, (formulario de contacto, envío de CV, newsletter u otros) cuentan con una casilla de verificación para controlar que los usuarios de la web han leído la política de privacidad previamente al tratamiento de sus datos personales a través del formulario?

A) Se dispone de una cláusula informativa sobre el tratamiento de datos y debajo de esta se ubica la casilla de verificación de la política de privacidad

B) No

C) No lo sé

Videovigilancia:

Cumplimiento del artículo 13 del RGPD y 22 de la LOPDGDD.

Señalización de las zonas videovigiladas, ubicación del cartel de videovigilancia.

18. ¿Ha implantado los controles relativos a señalización e información?

A) No

B) Dispongo del cartel informativo con la información mínima correspondiente

19. ¿Dónde se encuentra ubicado el cartel de videovigilancia?

A) En la entrada, en un lugar suficientemente visible

B) Se coloca donde hay hueco, en cualquier lugar

Limitación de la finalidad:

Cumplimiento del artículo 5 y 6 del RGPD.

Verificar que los datos no se usan para otra finalidad que no hayan sido informadas y verificar que cuando se usen los datos para otras finalidades que sí hayan sido informadas, si procede separar las finalidades para obtener consentimientos individuales, así se ha realizado y no se ha englobado en un todo.

20. ¿Los tratamientos de datos, en general, se están utilizando para otros fines distintos de los lícitos e informados a los interesados?

A) No lo sé

B) A veces, cuando no se consigue dar con el titular de los datos

C) No, pero en caso de que fuera necesario se le informaría de nuevo al interesado esperando su autorización

D) Sí

Deber de secreto:

Cumplimiento del artículo 5 del RGPD y LOPDGDD.

Principio de integridad y confidencialidad.

21. ¿Se ha firmado el deber de confidencialidad con los trabajadores?

A) Sí, durante la firma del contrato laboral

B) No

C) No lo sé

Registro de actividades de tratamiento y análisis de riesgos:

Cumplimiento del artículo 31 de la LOPDGDD.

Revisión, adecuación y actualización de los distintos tratamientos de datos.

22. ¿Se lleva a cabo un Registro de las Actividades de Tratamiento?

A) Desconozco que es el Registro de Actividades de Tratamiento

B) Sí, a través de una consultoría u organización especializada en ello

C) No lo considero necesario

23. ¿Se dispone de un protocolo para actualizar periódicamente el Registro de Actividades de Tratamiento?

A) Sí

B) No

24. ¿Ha elaborado y mantiene actualizado su análisis de riesgos?

A) No

B) Sí, a través de una consultoría u organización especializada en ello

Derechos de los interesados:

Cumplimiento de los artículos 15 al 22 del RGPD.

Revisión de procedimientos, sistemas de información de los derechos de los usuarios (acceso, rectificación, supresión, limitación, portabilidad y oposición), formulario de solicitud, canales de comunicaciones, roles intervinientes, revisión de su efectiva aplicación.

25. Si el titular de los datos quiere cancelar la información de sus datos, ¿existe un medio para notificarlo?

A) Un correo electrónico específico para los derechos de protección de datos (Por ejemplo, rgpd@xxxxx.com)

B) Se utiliza el mismo medio para cualquier solicitud

C) No tengo ningún medio habilitado para esto

Violaciones de seguridad:

Cumplimiento del artículo 23 del RGPD.

Revisión de procedimientos de violaciones de seguridad, evaluación de brechas, revisión de procesos de investigación, revisión de notificaciones realizadas ante la Autoridad de Control y afectados.

26. ¿Es conocedor de el significado de quiebra, brecha o violación de seguridad?

A) Sí

B) No

27. ¿Se han producido algunas de estas incidencias a nivel informático?

A) Virus

B) Robo de identidad

C) Ataque de servidores

D) Robo de información

E) No se ha producido ningún incidente

F) Otro:

28. En caso de que en se haya producido algún incidente o se produzca en un futuro, ¿se dispone de un protocolo para gestionar las brechas de seguridad?

**Un protocolo de brechas de seguridad se refiere a un plan de respuesta rápida y eficiente a incidentes, define cómo actuar en caso de que se produzca una violación de los datos, con el fin de asegurar una reacción responsable y oportuna.*

A) Disponemos de una política para la gestión de brechas y se notifica a la Agencia de Protección de Datos

B) No

29. ¿Se tiene un procedimiento para registrar las incidencias informáticas?

A) Se almacenan en la base de datos de la organización con el fin de que no se vuelva a repetir la misma incidencia

B) No se realiza nada

30. ¿Se dispone de algún sistema para detectar intrusos en la red WiFi? (Por ejemplo: aplicación de escaneo de red, analizador de WiFi, etc.)

A) Aplicación de escaneo de red

B) Analizador WiFi

C) No lo sé

D) Ninguno

E) Otro:

Medidas técnicas:

Revisión de medidas de seguridad de carácter técnico (sistemas de autenticación, cifrado, gestión de usuarios, activos informáticos, controles de acceso físico, copias de seguridad) vinculadas a los tratamientos de datos personales en todo su ciclo de vida dentro de la organización.

31. ¿Qué sistemas de protección existen en los equipos?

A) Antivirus

B) Firewall (cortafuegos)

C) Cifrado de disco y equipos

D) Ninguno

E) Otro:

32. ¿Con que frecuencia realiza copias de seguridad de sus equipos, sistemas y del correo electrónico?

A) Nunca

B) Una vez a la semana

C) No lo sé

D) Una vez al mes

E) Otro:

33. ¿Se cuenta con copias de seguridad en unidades de almacenamiento externo (discos duros externos, USB, etc.)?

A) Sí, y en ocasiones se dispone de una segunda unidad externa como dispositivo de respaldo

B) No

34. Cuando un trabajador se incorpora a la empresa, ¿cómo se gestiona su alta en el servidor?

A) Se encarga el área de sistemas y se le asignan los permisos de acuerdo a su puesto de trabajo

B) No lo sé

C) De cualquier manera

35. ¿Se lleva a cabo un cambio de contraseña periódico?

A) Sí, con el objetivo de garantizar la confidencialidad de las contraseñas

B) No, se mantiene siempre la misma contraseña

C) No lo sé

36. ¿Existen condiciones o requisitos de complejidad para la definición de contraseñas?

A) No se permite la utilización de contraseñas anteriores

B) Se deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos) y deben contener al menos ocho caracteres

C) No existe ningún requisito

D) No lo sé

37. En caso de contraseña errónea “n” veces, ¿qué ocurre después?

A) Se bloquea al usuario

B) Nada, no existe ningún límite de intentos

C) No lo sé

38. ¿Se hace uso de alguno de estos sistemas de autenticación de doble factor?

A) Huella dactilar _____

B) Reconocimiento facial _____

C) Token USB _____

D) Código adicional que se genera de forma aleatoria y que el usuario recibe a través de otro canal _____

E) Ninguno

F) Otro: _____

Medidas organizativas:

Revisión de medidas de seguridad de carácter organizativo (almacenamiento seguro, transporte confidencial, destrucción irrecuperable, clasificación coherente, custodia diligente) vinculadas a los tratamientos de datos personales en todo su ciclo de vida dentro de la organización.

39. ¿Existe alguna política para deshacerse de la información, los soportes y sistemas que no se vayan a utilizar más en la organización?

A) Destrucción física del dispositivo

B) Trituradora de papel

C) Destrucción manual o por especialistas en destrucción certificada de información

D) No se realiza nada, se conserva todo en la organización

E) Otro: _____

40. ¿Existe un inventario de los dispositivos informáticos que se extraen fuera de la organización?

A) Se dispone de un listado de todos los activos de la organización, tanto de los que se extraen como de los que se quedan dentro de la organización

B) No

C) No lo sé

41. ¿Aloja sus propios servidores de datos en un espacio seguro (sala cerrada, rack o armario de servidores, etc.)?

A) Están seguros físicamente

B) Se encuentran en una sala compartida

C) Están en una zona de paso

D) No lo sé

Formación:

Medidas y controles de cumplimiento, planes de formación y concienciación, acreditación de la formación realizada y de la asistencia la misma.

42. ¿Se ha formado a los empleados en protección de datos?

A) No lo sé

B) Se realizan cursos cada cierto tiempo, se envían recordatorios, se les mantiene continuamente informados

C) No se realiza nada

43. ¿Se ha desarrollado formación con los trabajadores y se les ha informado de una política de buenos usos de los medios informáticos?

A) Sí, y se realiza al menos una vez al año para recordar y enseñar nuevos conceptos que hayan surgido

B) No

44. ¿Permite a sus trabajadores utilizar sus dispositivos particulares para llevar a cabo su trabajo?

A) Está prohibido y se les ha informado al respecto a través de una política sobre el uso de los dispositivos corporativos

B) Sí, son libres de ello

Delegado de Protección de Datos (DPD):

Cumplimiento del artículo 5 y 37 del RGPD.

Análisis de la necesidad de DPD, canales de comunicación interno y externos, nombramiento y difusión de los responsables de privacidad, análisis de compatibilidad/incompatibilidad de funciones y revisión de funciones.

45. En caso de que su organización en algún momento requiera obligatoriamente la designación de un Delegado de Protección de Datos, ¿se tiene un plan para formalizar y regularizar dicha situación?

A) Se formalizará un contrato con el DPD en caso de ser una figura externa, se notificará a la Agencia de Protección de Datos la designación, se documentarán sus funciones y obligaciones, entre otros

B) No sé qué es lo que se debe hacer

C) No lo sé

Encargado del tratamiento:

Cumplimiento del artículo 28 del RGPD.

Modelos de contratos, procedimiento de verificación del cumplimiento con proveedores, revisiones de encargados de tratamiento, adhesiones a certificaciones o códigos de conducta.

46. ¿Se escoge cualquier proveedor o se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y que garanticen la protección de los derechos del interesado?

A) Se escoge cualquiera, en caso de necesidad extrema

B) Se escogen los proveedores que ofrezcan las garantías suficientes de protección en la organización

C) El que mejor presupuesto nos dé para llevar a cabo el trabajo

D) No lo sé

47. ¿Ha identificado a los proveedores con acceso a datos (servicios externalizados), los ha clasificado según su criticidad y ha gestionado la firma de los contratos de protección de datos, así como las garantías adicionales de cumplimiento?

***Por ejemplo: informático, asesoría, auditor, etc.*

A) A todos y dispongo de una lista con la identificación de cada uno de ellos, la cual se mantiene actualizada

B) Sólo con algunos

C) A ninguno

D) No lo sé

Categorías especiales de datos

Cumplimiento del artículo 9 del RGPD y LOPDGDD.

48. ¿Se dispone de un procedimiento para llevar a cabo el correcto tratamiento sobre los datos sensibles? (datos de salud, biométricos, vida sexual, origen étnico o racial, opiniones políticas, afiliación sindical, datos genéticos y convicciones religiosas o filosóficas)

A) No

B) Se aplican medidas de seguridad superiores

C) No lo sé

49. ¿Conoce el concepto de Informe de Evaluación de Impacto en la Privacidad (EIPD), cómo determinar si es necesario realizar un EIPD, cómo realizar este tipo de informes y qué acciones tomar tras su elaboración?

A) Lo desconozco

B) Sí, y siempre me apoyo de la lista proporcionada por la AEPD sobre los tipos de tratamiento de datos que requieren un EIPD

Tratamiento de menores de edad:

Cumplimiento del artículo 7 de la LOPDGDD. Consentimiento basado en la patria potestad o tutela.

La LOPDGDD exige una edad mínima de 14 años para otorgar el consentimiento, con excepción de los supuestos en que la "ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento". El tratamiento de los datos de menores de 14 años (basado en el consentimiento), solo será considerado lícito si hay consentimiento del titular de la patria potestad o tutela y dentro del alcance del mismo.

50. ¿Se dispone de un protocolo para solicitar datos de niños menores de 14 años?

A) Se verifica o se solicita el consentimiento (en caso de no disponerlo) a los padres o tutores legales

B) No

C) No lo sé

A.1 Clave de respuesta

Pregunta	Respuesta
1	B
2	B

Pregunta	Respuesta
26	A
27	E

Pregunta	Respuesta
3	A
4	A
5	A
6	A
7	A
8	A
9	A
10	B D E
11	A
12	A
13	A
14	A C
15	A
16	A
17	A
18	B
19	A
20	C
21	A
22	B
23	A
24	B
25	A

Pregunta	Respuesta
28	A
29	A
30	A B E
31	A B C E
32	B D
33	A
34	A
35	A
36	A B
37	A
38	A B C D F
39	A B C E
40	A
41	A
42	B
43	A
44	A
45	A
46	A
47	A
48	B
49	B
50	A

B. ODS (Objetivos del Desarrollo Sostenible)

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Procede**
ODS 1. **Fin de la pobreza.**				**x**
ODS 2. **Hambre cero.**				**x**
ODS 3. **Salud y bienestar.**				**x**
ODS 4. **Educación de calidad.**				**x**
ODS 5. **Igualdad de género.**				**x**
ODS 6. **Agua limpia y saneamiento.**				**x**
ODS 7. **Energía asequible y no contaminante.**				**x**
ODS 8. **Trabajo decente y crecimiento económico.**				**x**
ODS 9. **Industria, innovación e infraestructuras.**				**x**
ODS 10. **Reducción de las desigualdades**.				**x**
ODS 11. **Ciudades y comunidades sostenibles**.				**x**
ODS 12. **Producción y consumo responsables.**				**x**
ODS 13. **Acción por el clima.**			**x**	
ODS 14. **Vida submarina.**				**x**
ODS 15. **Vida de ecosistemas terrestres.**		**x**		
ODS 16. **Paz, justicia e instituciones sólidas.**				**x**
ODS 17. **Alianzas para lograr objetivos.**				**x**

Generalmente las tecnologías digitales contribuyen de una forma muy amplia a la aceleración del cumplimiento de los 17 Objetivos del Desarrollo Sostenible. De los 17, el presente TFG puede contribuir con los siguientes objetivos extraídos del acuerdo de la ONU:

"Objetivo 15. Gestionar sosteniblemente los bosques, luchar contra la desertificación, detener e invertir la degradación de las tierras, detener la pérdida de biodiversidad". Se considera que se puede cooperar con este objetivo por el uso del cuestionario online y no en formato físico. Actualmente todo a nuestro alrededor se encuentra en continua evolución hacia la digitalización, sobre todo en las empresas que buscan el desarrollo de su negocio. En las empresas consultoras, lo que anteriormente era un informe (o cualquier otro tipo de documento) con más de 10 páginas o menos a entregar a los clientes, ahora la mayoría de esta información se encuentra normalmente ubicada en la nube y siempre a disposición de los usuarios. Esto implica el no tener que imprimir de nuevo la información en caso de pérdida o extravío, con ello el ahorro de papel.

En este caso, para los resultados que obtendrá la persona que realice el autodiagnóstico proporcionado, nada más se finalice el mismo el usuario podrá ver los resultados desde este y descargarlos en formato PDF, con esto se hace innecesaria la necesidad de malgastar folios que luego a la larga pueden olvidarse de su existencia y perderse. En síntesis, con este objetivo, se

ayudará a los bosques, reduciendo de este modo la tala de árboles (no utilizando o reduciendo y evitando el uso de papel).

Exactamente se pretenderá dar apoyo al cumplimento de la meta 15.2 que dice lo siguiente: “15.2 Para 2020, promover la gestión sostenible de todos los bosques, poner fin a la deforestación, recuperar los bosques degradados e incrementar la forestación y la reforestación a nivel mundial”. El aseguramiento de esta meta podrá implicar también el cumplimiento del objetivo 15.b: “15.b Movilizar un volumen apreciable de recurso de todas las fuentes y a todos los niveles para financiar la gestión forestal sostenible […]”.

Aunque hay otro objetivo que puede que no se garantice del todo, pero al que se puede hacer referencia, este es el objetivo 13.

“Objetivo 13. Adoptar medidas urgentes para combatir el cambio climático y sus efectos”.

Con la realización del autodiagnóstico las empresas no tendrán que ir presencialmente a su consultora y con ello, se ahorrarán el uso de transporte, ayudando así a la cooperación con el cambio climático, evitando emisiones de gases de efecto invernadero y con esto la reducción de la temperatura global, la cual es una de las mayores preocupaciones actuales. Esta reducción de estos gases hará que se pierda menos masa de hielo en los polos y a su vez se reducirá el aumento de los niveles del mar, el aumento del mar genera inundaciones y amenazas en los litorales. Como se observó durante la pandemia, la reducción del uso de transportes mejoró el cambio climático, por eso el trabajo de forma remota es un gran beneficio para todos.

En síntesis, se evitará generar una huella de carbono por cada reunión online que se hubiera mantenido de forma presencial con el consultor y/o auditor.