PLASMAC

Plataforma en la nube para la mejora de la atención socioasistencial de la Macaronesia

Actividad 2.2.1: Auditorías de Calidad y Seguridad Tecnológica

Elementos de seguridad informática en la información y datos

Descripción de las consideraciones a destacar en materia de seguridad de la información y tratamiento de ésta, referida a sus dimensiones físicas, lógicas y jurídicas más destacables.

Descargo de Responsabilidad

Este documento ha sido preparado por el personal de Instituto Tecnológico y de Energías Renovables S. A. (ITER). ITER es una empresa pública con amplia experiencia en el desarrollo de proyectos relacionados con el uso de las TIC.

Este informe representa el mejor criterio de ITER a la luz de la información disponible. Se informa al lector que, dado el amplio alcance del proyecto, no toda la información se puede verificar o comprobar de forma independiente y que, por lo tanto, algunas afirmaciones en el informe pueden basarse en una única fuente de información. Aunque se usa el tiempo condicional para resaltar el grado de incertidumbre, el lector debe entender que el uso de la información contenida en este informe es responsabilidad del lector.

Glosario de términos

2FA (Two-factor authentication)	Autenticación de 2 factores
ADFS (Active Directory Federation Services)	Servicio de federación en directorio activo
APT (Advanced Persistent Threat)	Amenaza persistente avanzada
DoS (Denegation of Service)	Denegación de servicio (Ataque de)
DRM (Digital Rights Management)	Gestión de derechos digitales
IPS (Internet Prevention System)	Sistema de Prevención de Amenazas
IRM (Information Rights Management)	Gestión de derechos digitales
NAT (Network Address Translation)	Traducción de direcciones de red
NFGW (Next Generation Firewall)	Cortafuegos de nueva generación
OCRA	Algoritmo de respuesta a un desafío
OSI (Open System Interconnection)	Modelo de interconexión de sistemas abiertos
OTP (One time password)	Contraseña válida sólo para una autenticación
PAT (Port Address Translation)	Traducción de direcciones de puertos
RGPD	Reglamento General de protección de datos
TOTP (Time OTP)	OTP basado en tiempo
U2F (Universal 2nd Factor)	Autenticación de 2 factores universal
URL (Uniform Resource Locator)	Localizador de recursos uniforme
VPN (Virtual Private Network)	Red privada virtual
SMS	Servicio de mensajes simples
SMSOTP	OTP basado en SMS
SSH (Secure Shell)	Canal de acceso seguro
SSL (Secure socket layer)	Capa de puertos seguros
WiFi	Interconexión inalámbrica de dispositivos electrónicos

Tabla de contenido

1 Elementos de seguridad informática a nivel físico

A continuación se detallan, dentro del marco del proyecto PLASMAC, los principales elementos de seguridad informática a nivel físico.

1.1 Elementos de seguridad perimetral

Como dispositivos de seguridad perimetral se recomienda el uso de next-generation firewall (firewall de nueva generación) en dicha infraestructura de seguridad informática, ya que son capaces de detectar y bloquear ataques sofisticados mediante el uso de políticas de seguridad a nivel de aplicación, puerto y protocolo.

Las funciones avanzadas que caracterizan a estos firewall de nueva generación son:

- Conocimiento de las aplicaciones
- Sistemas integrados de prevención de intrusiones (IPS)
- Conciencia de identidad, control de usuarios y grupos
- Modo de funcionamiento como router y bridge
- Capacidad de usar fuentes de inteligencia externas

La mayoría de los firewalls de próxima generación integran al menos tres funciones básicas: capacidades de firewall empresarial, sistema de prevención de intrusos (IPS, Internet Prevention System) y control de aplicaciones.

Al igual que la introducción de la inspección de estado (stateful inspection) de los firewalls tradicionales, los NGFW (firewall de nueva generación) brindan un contexto adicional al proceso de toma de decisiones del firewall al proporcionarle la capacidad de comprender los detalles del tráfico de la aplicación web que pasa a través de él y de tomar medidas para bloquear el tráfico que pueda explotar vulnerabilidades

Las características de los firewall de nueva generación (NGFW), combinan muchas de las capacidades de los firewall tradicionales como la traducción de direcciones de red (NAT) y la traducción de direcciones de puertos (PAT), el bloqueo de URL y las redes privadas virtuales (VPN), con la funcionalidad de calidad de servicio (QoS) y Otras características que no se encuentran en los firewalls tradicionales. Esto incluye la prevención de intrusiones, la inspección de SSL y SSH, la inspección profunda de paquetes y la detección de malware basado en la reputación, así como el conocimiento de la aplicación. Estas capacidades específicas de la aplicación están destinadas a frustrar el número creciente de ataques de aplicación que tienen lugar en las Capas 4-7 de la pila de red OSI.

Los beneficios de los cortafuegos de nueva generación se basan en las capacidades para bloquear el malware antes de que ingrese en nuestra red, algo que antes no era posible. Además están mejor equipados para abordar las amenazas persistentes avanzadas (APT, Advanced Persistent Threat) porque pueden integrarse con los servicios de inteligencia de amenazas. Los NGFW también pueden ofrecer una opción de bajo costo para las empresas que

intentan mejorar la seguridad básica de los dispositivos mediante el uso de la conciencia de la aplicación, los servicios de inspección, los sistemas de protección y las herramientas de concienciación.

1.2 Cifrado de bases de datos de usuarios

Las diferentes bases de datos de usuarios deberían hacer uso del cifrado criptográfico de toda la información contenida en ellas. Ésto permite proteger dicha información al transformarla en datos ilegibles, textos cifrados, mediante el uso de una clave de cifrado.

Se le solicitará al usuario una contraseña que sirve para crear la clave de cifrado que encriptará los datos contenidos en la base de datos. El método de generación de esta clave de cifrado usando una contraseña de usuario comprobará que dicha contraseña cumple requisitos de longitud de contraseña. Se recomienda que la contraseña tenga entre 8 y 32 caracteres, que mezcle letras mayúsculas y minúsculas, que posea un número o carácter especial. El usuario crea la base de datos cifrada indicando la clave de cifrado en el proceso, posteriormente, para conectarse y utilizarla deberá ingresar dicha clave.

1.3 Soluciones avanzadas de punto final (endpoint) en equipos de usuario:

Se recomienda, a su vez, el uso de soluciones de punto final (endpoint) en equipos de usuario dentro de la infraestructura informática que proporcione el soporte correspondiente dentro de nuestro entorno. Un endpoint es un dispositivo informático remoto que se comunica de ida y vuelta con una red a la que está conectado. Ejemplos de puntos finales:

- ordenadores
- ordenadores portátiles
- teléfonos inteligentes
- tabletas
- servidores

- estaciones de trabajo

Los puntos finales representan puntos de entrada vulnerables clave para los ciberdelincuentes. Los puntos finales es donde los atacantes ejecutan código además de explotan vulnerabilidades, y donde hay activos para cifrar, exfiltrar o aprovechar. Debido a que los trabajadores de la organización se vuelven más móviles y los usuarios se conectan a recursos internos desde puntos finales fuera de las instalaciones en todo el mundo, los puntos finales son cada vez más susceptibles a los ataques cibernéticos. Los objetivos para acceder a los puntos finales incluyen, pero no se limitan a:

- Toma el control del dispositivo y úsalo en una red de bots para ejecutar un ataque DoS.
- Utilice el punto final como un punto de entrada en una organización para acceder a activos e información de alto valor.
- Acceda a los activos en el punto final para exfiltrar o mantener como rehenes, ya sea por rescate o simplemente por interrupción.

Durante varias décadas, las organizaciones han confiado en gran medida en el antivirus como un medio para asegurar los puntos finales. Sin embargo, los antivirus tradicionales ya no pueden proteger contra las amenazas modernas de hoy. Una solución avanzada de seguridad de punto final debería evitar el uso de malware y vulnerabilidades conocidas y desconocidas; incorporar automatización para aliviar las cargas de trabajo del equipo de seguridad; y proteger y habilitar a los usuarios sin afectar el rendimiento del sistema.

2 Elementos de seguridad informática a nivel lógico aplicables en el entorno del PLASMAC.

2.1 Políticas de contraseñas en cuentas de usuarios y seguridad informática

Las contraseñas de usuarios a utilizar como mecanismos de autenticación deben de ser robustas o muy difícil de vulnerar. Se definirán como fáciles de recordar, difíciles de adivinar y de descubrir por fuerza bruta (prueba de todas las posibilidades). Los requisitos en las contraseñas generadas por los usuarios serían:

- longitud mínima de 8 caracteres
- usarían concatenación de varias palabras (passphrases)
- no compuestas por datos propios que sean fácilmente adivinables
- no deben ser iguales a ninguna de las últimas contraseñas usadas
- se sustituirían por otras en caso de evidencias de haber sido comprometidas
- no permitido apuntar en papel dichas contraseñas
- mantenerse el carácter secreto de las contraseñas

- no usar la misma contraseña para distintos servicios web o para el acceso a distintos dispositivos
- cambio de contraseñas cada cierta periodicidad
- el sistema de verificación de las contraseñas se ha limitaría a un número de intentos de acceso sin éxito
- el sistema de verificación permitiría al usuario ver el contenido de su contraseña
- el sistema de verificación de contraseñas usaría algoritmos de cifrado autorizados, además de un canal protegido
- anular contraseñas con más de un año de antigüedad

2.2 Tratamiento de datos personales en información sensible mediante herramientas IRM- Information Rights Management (sistemas de protección de documentación) tipo SealPath

Es recomendable usar elementos de gestión de derechos de información (IRM, Information Rights Management) que es un subgrupo de herramientas de gestión de derechos digitales (DRM), tecnologías que protegen la información sensible de intentos de acceso a ésta no autorizados. También es referido algunas veces como E-DRM, gestión de derechos digitales a nivel empresarial.

IRM es una tecnología que permite controlar remotamente la información, mayormente en forma de documentos. Esto implica que esa información y su control puede ser ahora creada, vista, editada y distribuida de forma separada. IRM se aplica habitualmente a documentos y a correos electrónicos. Se utilizaría la encriptación para prevenir de accesos no autorizados, mediante uso de una clave o password como control de acceso al dato encriptado.

Una vez el documento es encriptado, se aplicaría ciertos permisos de acceso que permitan o denieguen a un usuario llevar a cabo acciones sobre una parte determinada de la información. Algunos de estos permisos estándar son los siguientes:

- protección robusta de uso tal como controlar la acción de copiar y pegar entre documentos, prevenir capturas de pantalla, la impresión, edición
- una política de derechos que permita el mapeo fácil de clasificaciones de negocios con información asociada
- uso fuera de línea que permita a los usuarios crear o acceder a documentos sellados IRM, sin necesidad de acceso de red para ciertos períodos de tiempo
- auditoría completa sobre el acceso a los documentos, así como cambios en la política o derechos para usuarios de los negocios

También permitiría a los usuarios cambiar o revocar permisos sin compartir el documento de nuevo.

Se recomienda, entre otras, la herramienta IRM: SealPath, que permite proteger los datos, controlar el acceso definiendo quién accede a esos datos, con qué permisos de acceso a los

datos (ver, editar, imprimir, etc). Además de prevenir la fuga de datos destruyendo el documento en remoto o revocando permisos asociados. Permite la compartición de documentos usando los medios habituales (DropBox, GoogleDrive, OneDrive, etc)

Se adjunta diagramas explicativos:

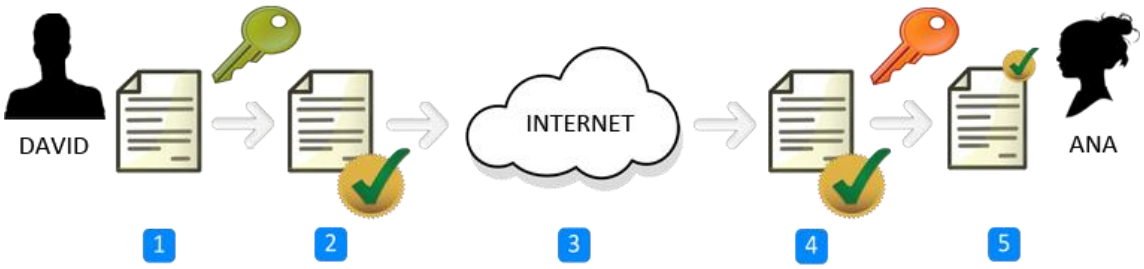
2.3 Uso de correo electrónico encriptado corporativo con herramientas tipo OpenPGP para evitar/reducir el phising email

Se aplicaría cifrado de mensajes email para proteger de ser leído el contenido por entidades a las que no se dirigen esos mensajes. Se aconseja usar software gratis y comercial y add-ons como: Gpg4win, que soportan el protocolo de cifrado de email: OpenPGP. Este sistema usa la criptografía asimétrica, que consta de dos claves, una pública y una privada. La pública la puede tener cualquier persona, sin embargo, la privada sólo la tiene nuestro usuario, que no se la entrega a nadie.

La pública se la podemos enviar a todo el que quiere comunicarse con nosotros. Esta clave pública permitirá a la gente crear mensajes cifrados que van dirigidos a nuestro usuario además de poder verificar la firma de nuestro correo electrónico usando estos medios. La clave privada, no será enviada a nadie, y permitirá firmar y descifrar los correos electrónicos.

Indicamos a continuación diagramas que explican lo expuesto anteriormente, a la firma y cifrado electrónico:

Ejemplo de firma



1. David redacta un mensaje.
2. David firma digitalmente el mensaje con su clave privada.
3. David envía el mensaje firmado digitalmente a Ana por Internet.
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la clave pública de David.
5. Ana puede leer el mensaje sabiendo que David es el remitente.

Ejemplo de cifrado

1. Ana redacta un mensaje.
2. Ana cifra el mensaje con la clave pública de David.
3. Ana manda el mensaje a David por Internet.
4. David recibe el mensaje cifrado y lo descifra con su clave privada.
5. David ya puede leer el mensaje original que le mandó Ana.

Mecanismos de autenticación fuerte para acceso a todo tipo de aplicaciones y recursos empresariales por parte de los usuarios, mediante tokens de seguridad de software virtual

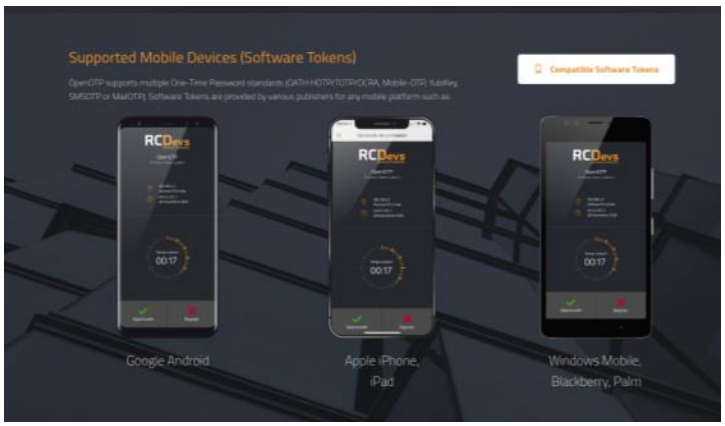
Un token de seguridad (también token de autenticación o token criptográfico) es un aparato electrónico para que el usuario autorizado de un servicio computerizado realice el proceso de autenticación en dicho servicio.

Existen muchos tipos de token. Los token generadores de contraseñas dinámicas “OTP” (One Time Password), permiten generar una contraseña en tiempo real de un solo uso para un servicio concreto.

Se aplicaría el uso de la solución OpenOTP Server, que es una solución de autenticación de usuario de grado empresarial basado en estándards abiertos. OpenOTP proporciona muchos esquemas de autenticación (altamente configurables) para tus usuarios del dominio. Soporta la combinación de acceso para usuarios de factor único y de multi-factor con Tecnologías de One-Time Password (OTP) y Segundo Factor Universal (FIDO-U2F).

La solución OpenOTP se compone de varios componentes que incluyen el servidor WebADM, OpenOTP RADIUS Bridge y las aplicaciones de autoservicio. Combinado con las integraciones de terceros de RCDev, OpenOTP admite VPN, Citrix, Web SSO, ADFS, Linux, Microsoft, Wifi, aplicaciones web y mucho más.

OpenOTP soporta múltiples estándard One-Time Password como: OATH HOTP/TOTP/OCRA, Mobile-OTP, YubiKey, SMSOTP o MailOTP. Los tokens software son proporcionados por varios publishers para cada plataforma móvil tales como:



2.4 VPN IPsec

Se recomienda usar el protocolo VPN (red privada virtual) bajo IPsec para comunicación entre usuarios remotos y plataforma web de PLASMAC. IPsec es un conjunto de protocolos que aseguran las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos de establecimiento de claves de cifrado. Los protocolos de IPsec se sitúan en la capa de red, capa 3 del modelo OSI. Otros protocolos de seguridad usados de forma extendida en internet como SSL, TLS y SSH operan en la capa de aplicación (capa 7 del modelo OSI). Esto hace que IPsec sea mucho más flexible, puesto que puede ser utilizado para proteger protocolos de la capa 4 del modelo OSI, incluyendo TCP y UDP.

IPsec está formado por protocolos criptográficos para permitir y asegurar el flujo de paquetes, garantizar la mutua autenticación y establecer los parámetros de criptografía.

La arquitectura de seguridad IP usa la asociación de seguridad (SA), que son el conjunto de algoritmos y parámetros (como las claves) que se usan para cifrar y autenticar un flujo determinado en una dirección. Para permitir el tráfico bidireccional en los dos sentidos, se define un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) se le encomienda al administrador de IPsec.

El protocolo de internet IP, no proporciona de forma intrínseca ninguna capacidad de seguridad, IPsec a nivel de seguridad nos permite obtener los siguientes servicios:

1. Cifrado del tráfico (no puede ser leído por nadie, salvo por el destinatario del mensaje al que va dirigido)
2. Integridad del mensaje (asegurar que el mensaje no es modificado en su trayecto)
3. Autenticación de los extremos (confirmar que el tráfico proviene de un extremo de confianza)
4. Anti-repetición (proteger ante repetición de sesión segura)

Se utilizaría las implementaciones de VPN IPsec propias de Windows según instrucciones indicadas en el siguiente enlace:

https://docs.microsoft.com/es-es/windows/security/identity-protection/vpn/vpn-connection-type

Para la configuración de VPN Ipsec sobre ubuntu, se implementaría según datos del siguiente enlace:

https://www.elastichosts.com/blog/linux-l2tpipsec-vpn-client/

Otra implementación de VPN Ipsec para Unix, gratuita, es el proyecto OpenBSD, también recomendada, del que adjuntamos el enlace:

http://www.openbsd.org/

3 Elementos de seguridad informática a nivel jurídico contemplados dentro de PLASMAC.

Normativa aplicable que regula el uso y tratamiento de información sensible relativa a datos personales de los usuarios de nuestros sistemas como: Esquema Nacional de Seguridad, Reglamento General de Protección de Datos, Directiva NIS.

3.1 Esquema Nacional de Seguridad como herramienta orientativa a seguir en materia de seguridad informática aplicable en nuestros sistemas de PLASMAC

El Esquema Nacional de Seguridad tiene por objeto establecer, precisamente, la política de seguridad en la utilización de medios electrónicos por relación a lo dispuesto en la legislación aplicable, esquema que deberá estar constituido por los principios básicos y requisitos

mínimos que permiten una protección adecuada de la información, en la comunicación electrónica de los ciudadanos con las Administraciones Públicas.

En desarrollo de tales previsiones normativas, se aprobó el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Tal y como reza el preámbulo del RD 3/2010, la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Entendemos, por tanto, que el Esquema Nacional de Seguridad es la normativa que se debería aplicar como marco de referencia en todos nuestros despliegues electrónicos del proyecto PLASMAC.

Los principales elementos en los que se fundamenta el Esquema Nacional de Seguridad son:

- Los principios básicos a considerar en las decisiones en materia de seguridad.
- Los requisitos mínimos que permitan una protección adecuada de la información.
- La categorización de los sistemas para la adopción de medidas de seguridad proporcionadas a la naturaleza de la información, del sistema y de los servicios a proteger y a los riesgos a los que están expuestos
- La auditoría de la seguridad que verifique el cumplimiento del Esquema Nacional de Seguridad

Respecto a los principios básicos, el ENS es de aplicación a las Administraciones Públicas y a las relaciones que puedan surgir entre estás y, entre éstas y los ciudadanos. El esquema está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Los principios básicos que rigen el Sistema Nacional de Seguridad son:

- Seguridad integral
- Gestión de riesgos
- Prevención, reacción y recuperación
- Líneas de defensa
- Reevaluación periódica
- Función diferenciada

La Política de Seguridad, que debe regir en cada administración, se debería establecer en base a los principios básicos indicados en el punto anterior y se desarrollaría aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad

- Análisis y gestión de los riesgos
- Gestión de personal
- Profesionalidad
- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos de seguridad
- Seguridad por defecto
- Integridad y actualización del sistema
- Protección de la información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

Para cumplir los anteriores requisitos mínimos establecidos en el real decreto: RD 3/2010 se aplicarían las medidas de seguridad teniendo en cuenta:

- Los activos que constituyen el sistema
- La categoría del sistema, según artículo 43 del RD 3/2010
- Las decisiones que se adopten para gestionar los riesgos identificados

Las medidas de seguridad son un conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Pueden ser medidas de prevención, de disuasión, de protección, de detección y de reacción, o de recuperación.

Para la selección de las medidas de seguridad apropiadas se seguirían los pasos siguientes:

1. Identificación de los tipos de activos presentes.
2. Determinación de las dimensiones de seguridad relevantes.
3. Determinación del nivel correspondiente a cada dimensión de seguridad.
4. Determinación de la categoría del sistema
5. Selección de las medidas de seguridad apropiadas, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

3.2 Marco legislativo en materia de protección de datos y privacidad aplicable en nuestro proyecto PLASMAC (RGPD, NIS)

El pasado 14 de abril del año 2016, tras varios años de negociación y de continuas revisiones legislativas, el Parlamento Europeo, aprobó formalmente el nuevo paquete regulatorio europeo en materia de protección de datos de carácter personal, en el que destaca el Reglamento General de Protección de Datos (en lo que sigue, “el Reglamento” o “RGPD”), y que deroga la actual Directiva 95/46/CE. Además, este nuevo paquete también incluye una

Directiva sobre transmisión de datos para cuestiones judiciales y policiales, que se aplicará al intercambio de datos transfronterizos dentro de la UE y establecerá estándares mínimos para el tratamiento de datos en cada país.

En términos generales, el nuevo RGPD presenta múltiples implicaciones para las entidades responsables de tratamiento, ya tengan éstas un carácter público o privado. Por último, se destaca la reciente aprobación también de la Directiva (UE) 2016/1148, de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (más conocida como Directiva NIS).

Ambas norma europeas (RGPD) y (Directiva NIS) se encuentran en fase de adecuación al ordenamiento jurídico español a través de la tramitación de sendos anteproyectos y proyectos de ley aprobados en este ámbito.

El nuevo RGPD implicará articular las siguientes actuaciones:

- Revisar y, en su caso, reforzar los procesos informativos y de transparencia respecto al usuario (principio de transparencia), quien ostenta un derecho a la información sobre las actuaciones de la empresa en lo que concierne al tratamiento de datos personales.
- Articular una estrategia adecuada para la correcta atención a los derechos del interesado, reconociéndose de forma expresa nuevos derechos tales como el derecho a la supresión (derecho al olvido), derecho a la portabilidad de los datos, o el derecho a la limitación en el tratamiento de los datos.
- Incorporar los principios de “privacy by design” y “privacy by default” en todo tipo de tratamientos y procesos corporativos con datos personales.
- Implementar el principio de “accountability”, que alude a la asunción de responsabilidad y de una actitud transparente por el responsable de tratamiento, sobre todo, en el caso de multinacionales que operan a escala global, en la adopción efectiva de medidas y políticas que garanticen el cumplimiento interno de principios y obligaciones en materia de protección de datos. Este principio se relaciona de forma directa con el llamado “Compliance Digital”.
- Establecer protocolos internos para prevenir y, en su caso, reaccionar en caso de violaciones de la seguridad de los datos o brechas de información personal, en orden a cumplir las obligaciones de notificación de cara a la autoridad de control y a los propios usuarios, así como minimizar los posibles efectos jurídicos y reputacionales asociados.

Según el artículo 33 del RGPD, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

Igualmente, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará, también se dirigirá al interesado sin dilación indebida. Es posible obviar esta específica obligación en determinados casos como, por ejemplo, cuando el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado (art.34 RGPD).

- Prever y contar con políticas claras en ordena la correcta identificación, contratación, control y auditoría de los encargados de tratamiento, en particular, cuando éstos operan fuera del Espacio Económico Europeo (EEE).
- Llevar un Registro de Actividades de Tratamiento: Esta obligación será obligatoria a empresas con más de 250 trabajadores, salvo que el tratamiento efectuado pueda entrañar riesgo para los derechos de los afectados, no sea ocasional o el tratamiento se refiera a determinadas categorías de datos indicados en el artículo 30.5 del RGPD. Tales registros se deberán llevar como una manera de demostrar el cumplimiento del RGPD tanto en calidad de responsable del tratamiento, cuanto en calidad de encargado del tratamiento.
- Revisar y adoptar medidas de seguridad adecuadas al tratamiento de datos personales actual o proyectado por la compañía, incluyendo, la seudonimización y el cifrado de datos personales, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.
- Realizar, si fuera necesario, las pertinentes Evaluaciones de Impacto en Protección de Datos (EIPD) de conformidad con el artículo 35 del RGPD. Destacar que la AEPD cuenta con una Guía previa a la aprobación del reglamento que, sin embargo, nos puede ayudar a orientar cómo enfocar estos procesos.
- Si así se considera, nombrar a un Delegado de Protección de Datos (DPO), que actuará como interlocutor de la empresa frente a la autoridad de control y frente a los usuarios, salvo que tal nombramiento tenga carácter obligatorio según dispone el artículo 37 del RGPD. En el caso de las entidades públicas es de nombramiento obligatorio. El DPO podrá formar parte de la plantilla del responsable o desempeñar sus funciones en el marco de un contrato de servicios.
- Revisar las transferencias internacionales o exportaciones de datos que se estén realizando fuera del EEE, a fin de adecuarlas a la nueva regulación europea. Si tales datos se están transfiriendo a EEUU se tendrá en cuenta el nuevo marco de actuación acordado (Privacy Shield).
- Conocer el nuevo régimen sancionador, que se endurece. Se introduce un nuevo e importante régimen sancionador que, según el tipo de infracción, puede implicar la imposición de multas por una cuantía equivalente a 20.000.000 EUR como máximo o,

tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.