Ley Orgánica de Protección de Datos,

Reglamento General de Protección de Datos y

Esquema Nacional de Seguridad

www.seguridadinformacion.com
www.esquemanacionaldeseguridad.com

➢ LOPD

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

  Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

  Desarrolla la LOPD y describe las medidas de seguridad en el tratamiento de datos, automatizados y no automatizados, para los distintos niveles de seguridad: Bajo, Medio y Alto.

➢ Reglamento General de Protección de Datos(RGPD)

- 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 personales y a la libre circulación de estos datos.

Establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

Entrada en vigor: 25 de Mayo de 2016, pero será aplicable a partir del 25 de mayo de 2018.

Hasta esa fecha sigue siendo de aplicación la LOPD y su Reglamento de Desarrollo.

Así, se disponía de un plazo de dos años de adaptación.

Esquema Nacional de Seguridad

- 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.

  Determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

- Real Decreto 951/2015, de 23 de octubre, de modificación del Esquema Nacional de Seguridad.

  Actualiza determinados puntos y requisitos del ENS.

RGPD: Principios relativos al tratamiento

- Tratamiento lícito, leal y transparente.
- Limitación de la finalidad.
- Datos adecuados, pertinentes y limitados a lo necesario.
- Exactos y, si fuera necesario, actualizados.
- Limitación en el plazo de conservación.
- Tratados de manera que se garantice su seguridad.
- El responsable del tratamiento será responsable del cumplimiento y capaz de demostrarlo («responsabilidad proactiva»).

Definiciones RGPD

➢ Datos personales

- Toda información sobre una persona física identificada o identificable («**el interesado**»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente.

➢ Tratamiento

- Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea **por procedimientos automatizados o no**, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

➢ Datos genéticos

- Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

➢ Datos biométricos

- Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Ambos tipos de datos se incluyen en las categorías especiales de datos personales.

Situación actual

- LOPD
  - Responsable del Fichero.
  - Responsable de Seguridad LOPD.
  - Administradores de los Sistemas.
- ENS
  - Responsable del Servicio.
  - Responsable de la Información.
  - Responsable de Seguridad ENS.
  - Responsable del Sistema.
  - Opcional: Administrador de la Seguridad del Sistema.

Marco organizativo

Fuente: Guía CCN STIC 801. Responsabilidades y funciones.

➢ Requisito RGPD

- ❑ Implantar medidas **técnicas y organizativas**, para garantizar la seguridad de los tratamientos.

- ❑ Delegado de Protección de Datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Propuesta

- Integrar las funciones de protección de datos en el marco organizativo del Esquema Nacional de Seguridad.
- Nombrar a un Delegado de Protección de Datos que:

  a) Tenga conocimientos especializados del Derecho y la práctica en materia de protección de datos.
  b) Rinda cuentas directamente al más alto nivel jerárquico del responsable.
  c) Informe y asesore en materia de protección de datos.
  d) Supervise el cumplimiento del RGPD.
  e) Asesore en la realización de Evaluaciones de Impacto sobre la Protección de Datos.
  f) Promueva la concienciación y formación sobre protección de datos.
  g) Coopere con las autoridades de control.
  h) Monitorice los riesgos asociados a los tratamientos de datos de carácter personal.

- Posible compatibilidad con el Responsable de Seguridad del Esquema Nacional de Seguridad, aunque dependerá mucho del funcionamiento interno de cada organización.

Registro de actividades de tratamiento

➢ Situación actual

- ❑ Inscripción de ficheros en el Registro General de Protección de Datos.

➢ Requisito RGPD

- ❑ Las entidades con más de 250 trabajadores o que realicen tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales, deberán mantener un registro de actividades de tratamiento.

- ❑ **Según el artículo 33 del Anteproyecto de LOPD, se hará público el inventario de actividades de tratamiento por medios electrónicos.**

Registro de actividades de tratamiento

➢ Requisito RGPD

- ❑ Mantener un registro de las actividades de tratamiento que incluya:
  - Nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
  - Fines del tratamiento.
  - Descripción de las categorías de interesados y de las categorías de datos personales.
  - Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
  - En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas.
  - Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos,
  - Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

- ❑ También se debe mantener un registro de los tratamientos realizados en concepto de encargado del tratamiento.

Registro de actividades de tratamiento

➢ Propuesta

- ❑ Tomar como referencia la actual inscripción de ficheros.
- ❑ Para cada fichero, identificar las operaciones que se realizan sobre el mismo.
- ❑ Para el inventario de tratamientos en concepto de encargado, partir del inventario de ficheros que debería estar incluido en el documento de seguridad.
- ❑ Recomendación: incluir, para cada actividad de tratamiento, la base de legitimación del mismo.

Adaptación al RGPD

-

Legitimación del tratamiento

www.seguridadinformacion.com
www.esquemanacionaldeseguridad.com

Legitimación del tratamiento

➢ Requisito RGPD

❑ El tratamiento de datos de carácter personal será lícito si:

a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
e) El tratamiento es necesario para el cumplimiento de una misión realizada en interés publico o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

❑ No implica cambios respecto a la actual LOPD.

Legitimación del tratamiento

➢ Propuesta

- Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos. Por ejemplo mediante la incorporación de esta información en el registro de actividades de tratamiento.

- Será de utilidad, por ejemplo, en los siguientes casos:

  - Para cumplir con el derecho de información, en el que se deberá incluir la legitimación del tratamiento.
  - Se deben especificar en los casos en que sea necesario llevar a cabo una Evaluación de Impacto sobre la Protección de Datos o en determinadas transferencias internacionales.

➢ Situación actual

- ❑ Se admiten el consentimiento tácito o por omisión:

> *"El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que* ***en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal****."*

Obtención del consentimiento

➢ Requisito RGPD

- El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, especifica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen.

- No se admite el consentimiento tácito o por omisión. Dejan de ser válidos métodos como por ejemplo, casillas marcadas.

- Además, el consentimiento debe ser explícito cuando:
  - Se traten categorías especiales de datos.
  - Se vayan a adoptar decisiones automatizadas.
  - Para la realización de transferencias internacionales.

- El consentimiento obtenido tácitamente o por omisión, dejará de ser válido a partir de la aplicación del RGPD.

Obtención del consentimiento

➢ Propuesta

- ❑ Identificar los casos en que se haya obtenido el consentimiento de manera tácita o por omisión.
- ❑ En estos casos:
  - Volver a obtener el consentimiento del interesado de acuerdo a los requisitos del RGPD.
  - Valorar la posibilidad de que el tratamiento pueda apoyarse en otra base de legitimación.

Información a los interesados

➢ Situación actual

- Los interesados deberán ser informados previamente a la recogida de datos de modo expreso, preciso e inequívoco.

➢ Requisito RGPD

- El responsable tomará las medidas oportunas para informar al interesado de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.
- Se debe incorporar información sobre:
  - Base jurídica del tratamiento.
  - Intención de realizar transferencias internacionales.
  - Datos del Delegado de Protección de Datos (si lo hubiere).
  - Elaboración de perfiles.

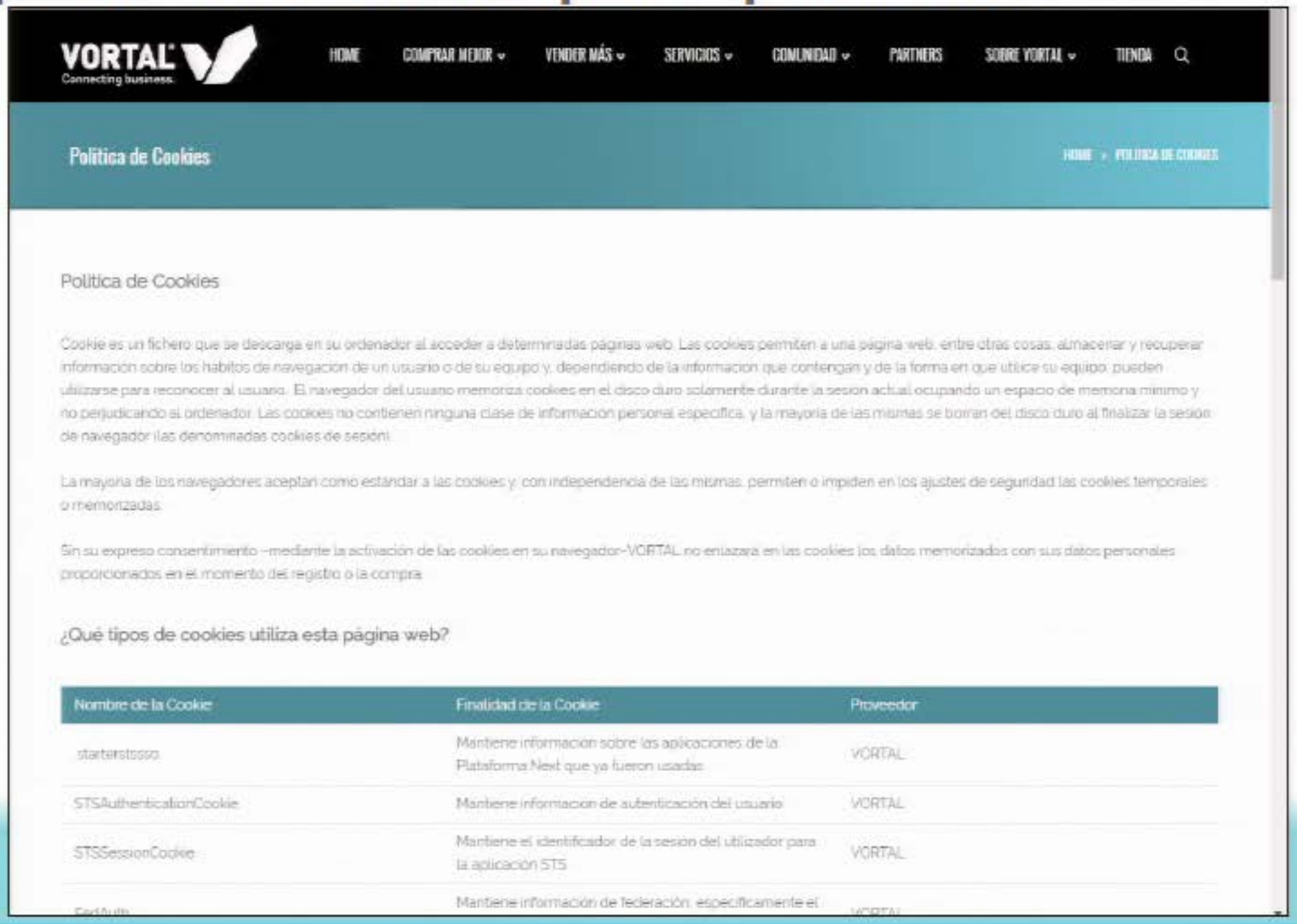
➢ Propuesta

❑ Información por capas:

- Presentar una **información básica** en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos.
  - Responsable
  - Finalidad
  - Legitimación
  - Destinatarios
  - Derechos
  - Información adicional
  - Procedencia, cuando no se hayan recabado del propio interesado.
- Remitir a la información adicional en un segundo nivel, donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo. Por ejemplo, como anexo a un formulario, mediante una página web específica, etc.

Información a los interesados

➢ Ejemplo de información por capas: cookies



VORTAL Connecting business.

HOME | COMPRAR MEJOR | VENDER MÁS | SERVICIOS | COMUNIDAD | PARTNERS | SOBRE VORTAL | TIENDA

Política de Cookies

HOME > POLITICA DE COOKIES

Política de Cookies

Cookie es un fichero que se descarga en su ordenador al acceder a determinadas páginas web. Las cookies permiten a una página web, entre otras cosas, almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo y, dependiendo de la información que contengan y de la forma en que utilice su equipo, pueden utilizarse para reconocer al usuario. El navegador del usuario memoriza cookies en el disco duro solamente durante la sesión actual ocupando un espacio de memoria mínimo y no perjudicando al ordenador. Las cookies no contienen ninguna clase de información personal específica, y la mayoría de las mismas se borran del disco duro al finalizar la sesión de navegador (las denominadas cookies de sesión).

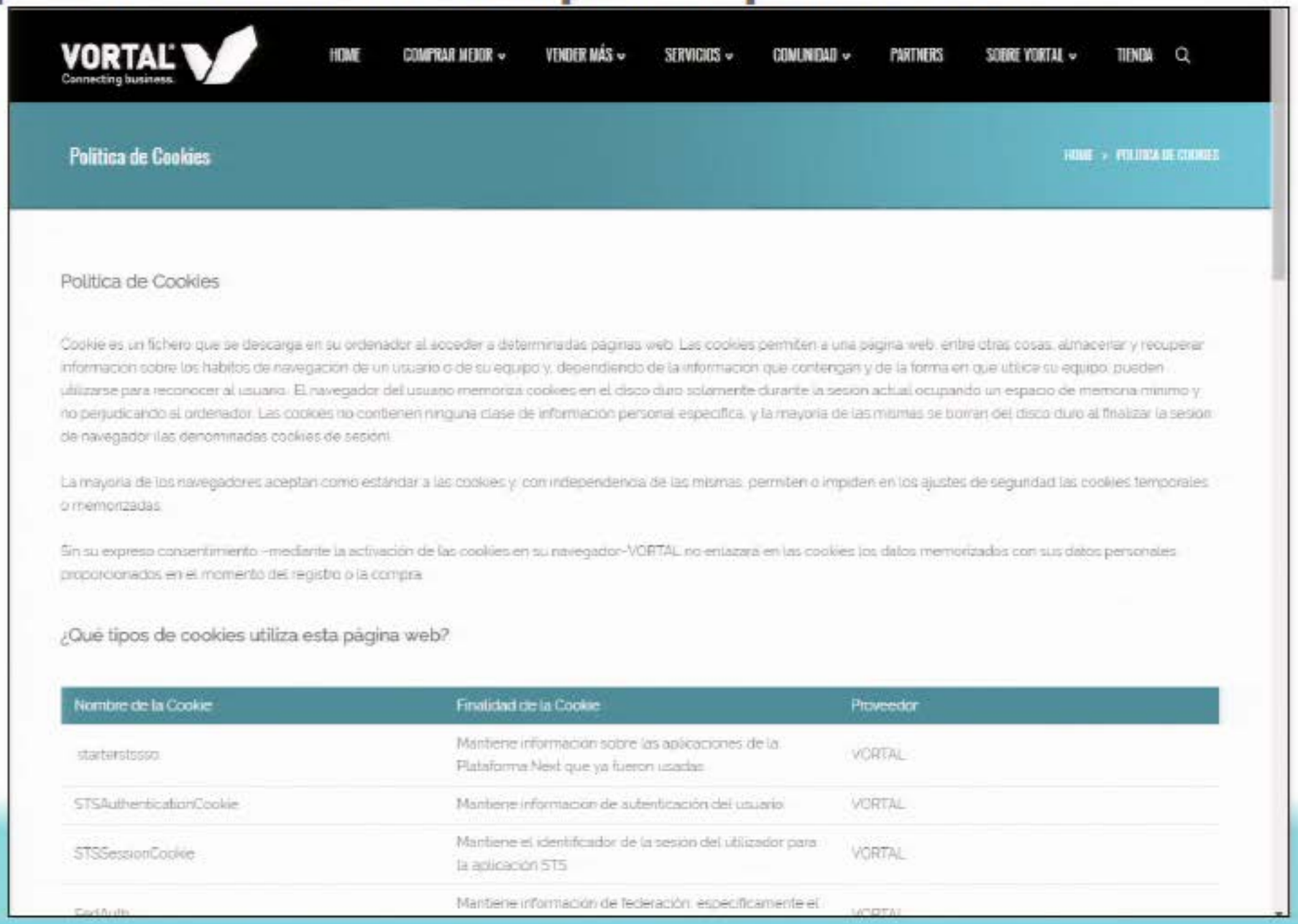
La mayoría de los navegadores aceptan como estándar a las cookies y, con independencia de las mismas, permiten o impiden en los ajustes de seguridad las cookies temporales o memorizadas.

Sin su expreso consentimiento –mediante la activación de las cookies en su navegador–VORTAL no enlazará en las cookies los datos memorizados con sus datos personales proporcionados en el momento del registro o la compra.

¿Qué tipos de cookies utiliza esta página web?

Nombre de la Cookie	Finalidad de la Cookie	Proveedor
starterststsso	Mantiene información sobre las aplicaciones de la Plataforma Next que ya fueron usadas	VORTAL
STSAuthenticationCookie	Mantiene información de autenticación del usuario	VORTAL
STSSessionCookie	Mantiene el identificador de la sesión del utilizador para la aplicación STS	VORTAL
FedAuth	Mantiene información de federación, especificamente el	VORTAL

Ejemplo de información por capas: cookies



Derechos

➢ Situación actual

- La LOPD establece y regula los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

➢ Requisito RGPD

- El RGPD establece y regula los derechos de Acceso, Rectificación, **Supresión (olvido)**, **Limitación del Tratamiento**, **Portabilidad de los Datos**, Oposición.

Derechos - Plazos

	Situación Actual	Requisito RGPD
Acceso	Resolver: 1 mes Efectivo: 10 días tras resolución	Efectivo: 1 mes Prorrogable 2 meses más por complejidad. En el primer mes se debe informar del motivo de la prórroga.
Rectificación	Resolver y Efectivo: 10 días	
Cancelación	Resolver y Efectivo: 10 días	
Oposición	Resolver y Efectivo: 10 días	
Limitación	N/A	
Portabilidad	N/A	

Derecho de Acceso

➢ Situación actual

- Deben facilitarse todos los datos de base del afectado, pero no copias o documentos (excepto en historia clínica).

➢ Requisito RGPD

- Se reconoce el derecho a obtener una copia de los datos personales objeto de tratamiento.

➢ Propuesta

- Se podrá facilitar el acceso remoto a un **sistema seguro** que ofrezca al interesado acceso directo a sus datos personales.

Derecho al Olvido

➢ Situación actual

- ❑ Derecho de cancelación: El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo.

➢ Requisito RGPD

- ❑ Derecho al olvido: Es una manifestación de los derechos de cancelación u oposición en el entorno on-line.

Derecho a la Limitación de Tratamiento

➢ Situación actual

- No se contempla.

➢ Requisito RGPD

- Concepto: marcado de los datos conservados con el fin de limitar su tratamiento en el futuro.
- Distinta naturaleza que el bloqueo de los datos: derecho del afectado / obligación del responsable.

Derecho a la Limitación de Tratamiento

➢ Requisito RGPD

❑ Se puede solicitar cuando:

- El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

❑ Mientras dure la limitación solo podrá tratar los datos:

- Con el consentimiento del interesado.
- Para la formulación, el ejercicio o la defensa de reclamaciones.
- Para proteger los derechos de otra persona física o jurídica.
- Por razones de interés publico importante de la Unión o del Estado miembro correspondiente.

Derecho a la Portabilidad

➢ Situación actual

- ❑ No se contempla.

➢ Requisito RGPD

- ❑ Es una forma avanzada del derecho de acceso por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica. Se podrá ejercer cuando:
  - El tratamiento esté basado en el consentimiento y además;
  - El tratamiento se efectué por medios automatizados.
- ❑ El interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
- ❑ No se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés publico o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Encargados del tratamiento

➢ Situación actual

- ❑ Se centra en las obligaciones de los responsables.

➢ Requisito RGPD

- ❑ Se establecen obligaciones concretas para los encargados:
  - Mantener un registro de actividades de tratamiento.
  - Determinar las medidas de seguridad aplicables a los tratamientos que realizan.
  - Designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.
- ❑ Los encargados pueden adherirse a códigos de conducta o certificarse en el marco de los esquemas de certificación previstos por el RGPD.

Encargados del tratamiento

➢ Situación actual

- ❑ Diligencia debida en la elección del encargado.

➢ Requisito RGPD

- ❑ El responsable deberá adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD.

- ❑ Aplicable también a los encargados del tratamiento cuando subcontraten actividades.

Adaptación al RGPD

-

Transferencias Internacionales

www.seguridadinformacion.com
www.esquemanacionaldeseguridad.com

Transferencias internacionales

- Las decisiones de adecuación que la Comisión ha adoptado con anterioridad a la aplicación del RGPD seguirán siendo validas, y por tanto, podrán seguir realizándose transferencias basadas en ellas, en tanto la Comisión no las sustituya o derogue.

- Las decisiones de la Comisión estableciendo clausulas tipo para los contratos en los que se establecen garantías para las transferencias internacionales seguirán siendo válidas hasta que la Comisión las sustituya o derogue.

- Las autorizaciones de transferencias que las autoridades nacionales de protección de datos hayan otorgado sobre la base de garantías contractuales seguirán siendo validas en tanto las autoridades no las revoquen.

- Las garantías sobre la protección que recibirán los datos en destino las debe ofrecer el exportador, que podrá ser tanto un responsable como un encargado de tratamiento.

- En los casos de Normas Corporativas Vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación, la transferencia no requerirá la autorización de las autoridades de supervisión.

Tratamiento de datos de menores

➢ Situación actual

- La edad a partir de la que el consentimiento de los menores es válido se fija en los 14 años con carácter general.

➢ Requisito RGPD

- La obtención del consentimiento en el ámbito de la oferta directa de servicios de la sociedad de la información, sólo será válido a partir de los 16 años, debiendo contar con la autorización de los padres o tutores legales por debajo de esa edad.

- Permite a los estados miembros establecer una edad inferior, siempre que no sea menor de 13 años.

- El anteproyecto de LOPD prevé que el consentimiento de un menor de edad sea válido cuando sea mayor de 13 años.

Medidas de seguridad

➢ Situación actual

- El Reglamento de Desarrollo de la LOPD determina con detalle y de forma exhaustiva las medidas de seguridad que deben aplicarse según el tipo de datos objeto de tratamiento (Bajo / Medio / Alto).

➢ Requisito RGPD

- Responsabilidad Activa. Los responsables y encargados establecerán las **medidas técnicas y organizativas apropiadas** para garantizar un nivel de seguridad adecuado **en función de los riesgos** detectados en un análisis previo.
- Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:

  - El coste de la técnica.
  - Los costes de aplicación.
  - La naturaleza, el alcance, el contexto y los fines del tratamiento.
  - Los riesgos para los derechos y libertades.

Protección de datos desde el Diseño y por Defecto

➢ Situación actual

- ❑ No se contempla este principio como tal.

➢ Requisito RGPD

- ❑ Estas medidas se incluyen dentro de las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

- ❑ Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o un servicio que implica el tratamiento de datos personales.

- ❑ Desde el inicio, los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD.

- ❑ Los responsables deben adoptar medidas que garanticen que sólo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Seudonimización de datos

➢ Anonimización de datos

- Eliminación de los elementos suficientes para que no pueda identificarse al interesado.
- La anonimización debe ser irreversible.

➢ Seudonimización de datos

- Sustitución de un atributo (normalmente un atributo único) por otro en un registro.
- Sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización **no garantiza un conjunto de datos anónimo**.
- Los datos resultantes continúan siendo datos personales.

Selección de técnicas

- Dictamen 05/2014 sobre técnicas de anonimización.
- Garantías a valorar:
  - **Singularización**: la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona.
  - **Vinculabilidad**: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas.

    Si el atacante puede determinar que dos registros están asignados al mismo grupo de personas pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.
  - **Inferencia**: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

Notificación de violaciones de seguridad de datos

➢ Situación actual

- No se contempla este requisito.
- Ley General de Telecomunicaciones:

> *"En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas."*

Notificación de violaciones de seguridad de datos

➢ Requisito RGPD

- Cualquier suceso que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Por ejemplo:

  - Pérdida de un ordenador portátil.
  - Acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) .
  - Borrado accidental de algunos registros.

- Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

- La notificación debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

Notificación de violaciones de seguridad de datos

➢ Requisito RGPD

- La notificación ha de incluir un contenido mínimo:
  - La naturaleza de la violación.
  - Categorías de datos y de interesados afectados.
  - Medidas adoptadas por el responsable para solventar la quiebra.
  - Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.
- Los responsables deben documentar todas las violaciones de seguridad.
- En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los **interesados**, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos, añadiendo recomendaciones sobre las medidas que puedan tomar.

Evaluación de Impacto sobre la Protección de Datos

➢ Situación actual

- ❑ No se contempla este requisito.

➢ Requisito RGPD

- ❑ Realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.

- ❑ Supuestos en los que se considera que puede haber un alto riesgo:

  - Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar.
  - Tratamientos a gran escala de datos sensibles.
  - Observación sistemática a gran escala de una zona de acceso público.

➢ Requisito RGPD

- ❑ Tratamiento a gran escala. A tener en cuenta:
  - El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población.
  - El volumen de datos y la variedad de datos tratados.
  - La duración o permanencia de la actividad de tratamiento.
  - La extensión geográfica de la actividad de tratamiento.

- ❑ La AEPD publicará listas de tratamientos que requerirán una Evaluación de Impacto sobre la Protección de Datos y que no lo precisarán.

Adecuación al ENS

www.seguridadinformacion.com
www.esquemanacionaldeseguridad.com

Adecuación al ENS

Adecuación al ENS

1. Política de Seguridad
2. Categorización de Sistemas
3. Análisis de Riesgos
4. Declaración de aplicabilidad
5. Plan de mejora de seguridad / Insuficiencias del sistema
6. Desarrollo de Normativa y Procedimientos
   Implantación
7. Mejora continua
8. Auditoría de certificación

Adecuación al ENS

1

- Política de Seguridad

- **Guías**
  - ✓ CCN-STIC-805 Política de Seguridad de la Información.
  - ✓ CCN-STIC-801 Responsabilidades y funciones.

- **Consideraciones**
  - ✓ Alcance.
  - ✓ **Marco organizativo. Nombramientos.**
  - ✓ Aprobación por el titular del órgano superior correspondiente.

RGPD

Adecuación al ENS

2

- Categorización de sistemas

Guías

- ✓ CCN-STIC-803 Valoración de sistemas en el Esquema Nacional de Seguridad.

Consideraciones

- ✓ Participación de Responsables de Servicio e Información.
- ✓ Dimensiones: Disponibilidad, Integridad, Confidencialidad, Autenticidad, Trazabilidad.
- ✓ Valoración razonable y razonada.
- ✓ **Incluir las actividades de tratamiento de datos de carácter personal.**

RGPD

Adecuación al ENS

3

- Análisis de Riesgos

➢ Guías

- ✓ MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- ✓ CCN-STIC-808 Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad.

➢ Consideraciones

- ✓ Identificación de activos de información y dependencias.
- ✓ Identificación y valoración de amenazas.
- ✓ Evaluación de medidas de seguridad.
- ✓ Herramienta PILAR. **En desarrollo adaptación al RGPD**.

RGPD

Adecuación al ENS

4

- Declaración de aplicabilidad

Guías

- ✓ CCN-STIC-806 Plan de Adecuación del Esquema Nacional de Seguridad.

Consideraciones

- ✓ Selección de **medidas técnicas y organizativas** en base a dimensiones y categorías.
- ✓ Justificar medidas compensatorias.
- ✓ Firmada por el Responsable de Seguridad.

Adecuación al ENS

5

- Plan de mejora de seguridad / Insuficiencias del sistema

Guías

- ✓ CCN-STIC-806 Plan de Adecuación del Esquema Nacional de Seguridad.

Consideraciones

- ✓ Incluir insuficiencias detectadas durante la evaluación de medidas de seguridad.
- ✓ Definir acciones de subsanación.
- ✓ Planificación realista.

Adecuación al ENS

6

- Desarrollo de normativa y procedimientos
- Implantación

Guías

- ✓ CCN-STIC-821 Normas de Seguridad en el ENS.
- ✓ CCN-STIC-822 Procedimiento de seguridad en el ENS.

Consideraciones

- ✓ Grado de detalle. Mantenibilidad.
- ✓ Aprobación formal y difusión.
- ✓ **Formación y concienciación.**

RGPD

Adecuación al ENS

7

- Mejora continua

Guías

- ✓ CCN-STIC-802 Auditoría del Esquema Nacional de Seguridad.
- ✓ CCN-STIC-815 Métricas e Indicadores en el Esquema Nacional de Seguridad.
- ✓ CCN-STIC-824 Informe del Estado de Seguridad.

Consideraciones

- ✓ Ciclo PDCA
- ✓ **Todo lo realizado debe mantenerse monitorizado y actualizado.**

RGPD

Mantenimiento del ENS

- **La gestión de la seguridad de la información es un proceso sujeto a cambios constantes:**
  - ❑ Cambios en la organización y su entorno.
    - **Nuevos servicios**
    - **Cambios organizativos**
    - **Cambio de suministradores**
  - ❑ Cambios en las amenazas.
    - **Nuevas variantes de ataques.**
    - **Descubrimiento de vulnerabilidades.**
  - ❑ Cambios en las tecnologías.
    - **Sistemas operativos.**
    - **Equipos.**
    - **Tecnología móvil**
  - ❑ Cambios en la legislación.
    - **Reglamento Europeo de Protección de Datos de Carácter Personal.**
    - **Actualizaciones del Esquema Nacional de Seguridad.**

Mantenimiento del ENS

- **Por ello es necesario implantar un proceso de actualización permanente, que conllevará, entre otras cosas:**
  - ❑ Revisión de la Política de Seguridad de la Información.
  - ❑ Revisión de los servicios e información y su categorización.
  - ❑ Actualización del análisis de riesgos, al menos anualmente.
  - ❑ Realización de auditorías, al menos bienal.
  - ❑ Revisión de las medidas de seguridad.
  - ❑ Revisión y actualización de procedimientos.

- **En definitiva, se trata de aplicar un ciclo de mejora continua, partiendo del trabajo realizado.**