Rev. 2022 03

SERVICIO DE EVALUACIÓN DE LA SEGURIDAD EN LA RED Y ADECUACIÓN LEGAL: *SECURE WEB*.

Prevención frente a las ciberamenazas acechantes en la red: *violación de datos, phising*, *malware*, *ransomware*, timos, etc.

FUENTE: INCIBE

CUMPLIMIENTO DE LOS PRINCIPIOS Y OBLIGACIONES RECOGIDOS EN EL REGLAMENTO (UE) 2016/679 (RGPD), EN LA LEY ORGÁNICA 3/2018 (LOPDGDD) Y EN LA LEY 34/2002, (LSSICE).

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid

Verificación de la seguridad reglamentaria SECURE WEB.

El Servicio de verificación de seguridad reglamentaria **SECURE WEB** de CONTROL ALT SUP, S.L., tiene como propósito verificar el cumplimiento de las medidas de seguridad esenciales legalmente y determinar las políticas de seguridad que se han de aplicar en la utilización de los medios electrónicos tales como páginas Web de la organización.

Base legal SECURE WEB.

- 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 (RGPD).
- LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, (LSSICE).

¿Qué es la verificación SECURE WEB?

Se trata de un Servicio de Evaluación de la Web, para verificación de seguridad reglamentaria regulada por la base legal y por tanto de obligado cumplimiento, cuyo objeto es el establecimiento de los principios y requisitos de las políticas de seguridad en la utilización de medios electrónicos y más concretamente de las Páginas Web de las organizaciones, que permita la adecuada protección de los activos de la información y de los datos, así como de los derechos de las personas usuarias y de la responsabilidad activa de la organización.

¿Cuál es la finalidad la verificación SECURE WEB?

La creación de las condiciones necesarias de confianza en el cumplimiento legal en el uso de los medios Web, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a las personas usuarias el ejercicio de derechos y el cumplimiento de los deberes legales de la organización a través de estos medios.

La verificación de seguridad reglamentaria ***SECURE WEB*** se necesita cuando se quiere saber si una Web es segura.

Si se ha de estar seguro de la Web, se han de verificar las medidas técnicas y los requisitos de cumplimiento de seguridad legal de los elementos y de los activos de información que los apoyan.

¿Cuáles son los elementos de la verificación?

El 95% de las incidencias de ciberseguridad se producen por un error humano, según un estudio de la compañía IBM, lo cual quiere decir que las personas usuarias de las herramientas digitales son la principal puerta de entrada para el ciberdelincuente y también puede convertirse en la principal barrera para frenarlos.

Por lo tanto disponer de los elementos de verificación adecuados en la Web, permite a la organización cumplir las exigencias reglamentarias y técnicas de seguridad, que una vez revisadas y conformes, proporcionan seguridad a las personas usuarias y al Cliente legalidad.

1. REVISIÓN DE LA SEGURIDAD DE LA URL.

La mayoría del tráfico de internet tiene lugar entre el navegador (Google, Firefox, Chrome, Opera…) y el servidor.

El servicio **SECURE WEB** verifica la parte del servidor, es decir, en la Web de la organización, el estándar de seguridad y marca del sello SSL o *Secure Sockets Layer*.

SSL o *Secure Sockets Layer* es un protocolo de seguridad de Internet basado en el cifrado. desarrollado por Netscape en 1995 para garantizar la privacidad, la autenticación y la integridad de los datos en las comunicaciones de Internet. SSL es el predecesor del cifrado TLS moderno que se utiliza hoy en día.

Los sitios web que implementan SSL/TLS tienen "HTTPS" en su URL en lugar de "HTTP". Si la URL no la tiene, la web podría no ser segura.

2. CONFIGURACIÓN DE LAS COOKIES.

Debido a la LSSICE establecida por el Real Decreto 13/2012, es de obligación obtener el consentimiento expreso del usuario de todas las páginas web que usan cookies prescindibles, antes de que éste navegue por ellas.

Las cookies y otras tecnologías similares tales como *local shared objects, flash cookies* o píxeles, son herramientas empleadas por los servidores Web para almacenar y recuperar información acerca de sus visitantes, así como para ofrecer un correcto funcionamiento del sitio.

Mediante el uso de estos dispositivos se permite al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etc.

El servicio **SECURE WEB** verifica que según el RGPD, las cookies que requieren el consentimiento informado por parte de las personas usuarias, son las cookies de analítica, las de publicidad y las de afiliación, quedando exceptuadas las de carácter técnico y las necesarias para el funcionamiento del sitio web o la prestación de servicios expresamente solicitados por el usuario.

La seguridad de la URL y la Configuración de las Cookies son los primeros pasos para que el Cliente disponga de la disposición de una Web segura y legalmente adecuada.

3. RASTREO DE LA URL EN BUSCA DE VIRUS Y AMENAZAS.

El servicio **SECURE WEB** utiliza analíticas online como medida de seguridad mediante herramientas que nos permiten rastrear una URL en busca de virus u otras amenazas.

Nuestros servicios pueden revisar una web muy rápidamente y asimismo podemos comprobar quién está detrás de una página concreta mediante herramientas d la Corporación de Internet para la Asignación de Nombres y Números (ICANN), de modo que informaremos al Cliente a quién pertenece la web, dónde y cuándo se registró, entre otros datos.

Cabe señalar que la UE reconoce únicamente servidores que están ubicados en lugares aceptados para la seguridad de la información, con un nivel adecuado a efectos del artículo 45 del RGPD, cuyo incumplimiento puede acarrear riesgos de seguridad y sanciones económicas y administrativas.

Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes:

https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00049

Fuente: AEPD.

4. ANÁLISIS Y VALORACIÓN DE RIESGOS.

El servicio SECURE WEB verifica los riesgos a los que está expuesta la Web para establecer las medidas necesarias a adoptar, para que no se hagan realidad.

Por ejemplo, al hacer un análisis de los posibles riesgos a los que están expuestas las bases de los datos personales de nuestros usuarios Web, podemos trazar un mapa de las acciones que debemos de emprender, para que ese riesgo no se materialice.

Si existe el riesgo de que la base de datos del Cliente se borre, para que no se materialice este riesgo, debería tener copias de seguridad. De esta manera, mediante análisis es factible deducir lo que tiene que hacer la organización para prevenir brechas de seguridad si las amenazas no tengan impacto ó bien que el riesgo sea menor.

El rastreo Web para buscar virus y amenazas es una medida técnica relevante para una Web segura.

Mediante análisis y valoración de los riesgos es factible deducir lo que tiene que hacer la organización para prevenir brechas de seguridad si las amenazas se materializan.

5. POLÍTICA DE PROTECCIÓN DE DATOS Y PRIVACIDAD.

La organización del Cliente ha de establecer una Política de Protección de Datos en su sitio web, siendo conforme su contenido y su enfoque de la información para cumplir con las exigencias reglamentarias.

Incorporar la política de privacidad web es obligatorio en el momento en que la página o sitio web recopila algún dato de carácter personal, por ejemplo, el registro de la IP por alguna cookie de terceros alojada en la web (como puede ser un botón de una red social o banner de publicidad).

Básicamente, cualquier página web, sea del tipo que sea, tiene la obligación de incorporar una página de política de privacidad en ella para cumplir con el RGPD y la LOPDGDD. Incluso un blog personal si tiene activados los comentarios, deberá contar con ella.

El servicio **SECURE WEB** realiza una revisión extensa de los elementos de la página web, revisando en especial las políticas de cookies, según lo señalado en el apartado anterior **2. CONFIGURACIÓN DE LAS COOKIES.**

Se deberá disponer en la página web de una cláusula informativa de primera capa o ventana emergente que debe perdurar hasta que el usuario acepte su uso o de su comportamiento se deduzca su aceptación de la política de cookies, así como el contenido de ambas, conforme a lo establecido en el artículo 22 de la LSSICE.

Asimismo el RGPD requiere que las páginas web cumplan con la obligación de están obligadas a establecer una política de privacidad completa, clara y actualizada, para lo cual se ha de verificar la política de privacidad web, qué incluir y su formulación.

Se verificarán elementos como los siguientes:

- Información del responsable del tratamiento o de su representante.
- Datos del responsable en materia de protección de datos.
- Información sobre la finalidad del tratamiento.
- Terceros destinatarios de los datos personales.
- Transferencias internacionales.
- Plazo de conservación de los datos.
- Derechos (**).
- Explicación sobre el uso de decisiones individuales automatizadas.

Por ejemplo su en la página web el Cliente basa decisiones en el tratamiento automatizado de datos que puedan afectar a las personas usuarias, como la que se produce con la elaboración de perfiles de usuario, en la política de privacidad web la organización debe explicar la lógica en la que se fundamenta para ello, para cumplir con el Artº. 22 del RGPD y explicar los efectos y el alcance que el proceso automatizado tiene sobre las personas usuarias.

(**)https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

La Política de Protección de Datos y Privacidad es necesaria para que el Cliente cumpla con el RGPD, la LOPDGDD y la LSSICE.

6. INTERLOCUCIÓN CON LAS PERSONAS USUARIAS.

El servicio **SECURE WEB** verifica los elementos Web de la interlocución con las personas de las que se puedan tratar datos personales, tales como el borrado y bloqueo de datos de las personas usuarias, la confidencialidad responsable y corresponsable y el formulario de contacto con el Cliente.

Para el borrado y bloqueo de datos de usuario, se ha de remitir a las personas interesadas una información documentada que, conforme a uno de los derechos que pueda ejercer, ha pedido que la organización borre sus datos personales de nuestra web, según lo señalado en el apartado **5. POLÍTICA DE PROTECCIÓN DE DATOS Y PRIVACIDAD.**

La organización por una imposibilidad técnica por ejemplo, quizás no pueda llevar a cabo este borrado de manera efectiva y es posible que resulte informáticamente muy difícil de garantizar que se dispone de todas las copias de las bases de datos, acceder a esos datos concretos, borrarlos y volver a hacer las copias exactamente como estaban antes.

En este caso hay que comunicarlo a la persona afectada y explicarle que puede estar tranquila en cuanto al ejercicio de sus derechos, ya que con el bloqueo de datos jamás podremos acceder a ellos.

Para la confidencialidad responsable, se ha de remitir a las personas interesadas una información documentada que tiene que estar firmada por el responsable de la organización, admitiendo así que su contenido está formulado, revisado y aprobado. En él se han de detallar las obligaciones legales que la organización ha de cumplir por guardar los datos de las personas usuarias.

Adicionalmente se ha de verificar que si existiera un corresponsable, existe una información documentada de confidencialidad corresponsable, que tiene que estar firmada por el corresponsable de la organización.

En cuanto a los formularios de contacto del Cliente, en el caso de que una persona usuaria de la organización ejerza cualquiera de sus derechos, se deberá tener asimismo preparada una información documentada como formulario que recopile los datos que se necesitan que rellene la persona usuaria para confirmar su identidad y al tiempo tener evidencia objetiva de su consentimiento.

Puede venir bien si no tiene la organización automatizado todos estos procesos, que llegado el momento se haya de hacer de manera manual. También puedes disponerse en un correo electrónico tipo lo cual facilita el tener que reenviarlo a otras personas que lo pidan.

Se han de verificar los elementos web de la interlocución con las personas de las que se puedan tratar datos personales, tales como el borrado y bloqueo de datos de las personas usuarias, la confidencialidad responsable y corresponsable y el formulario de contacto con el Cliente para una Web segura.

7. ASPECTOS REGLAMENTARIOS DEL RGPD DE APLICACIÓN EN LA WEB.

El servicio **SECURE WEB** verifica los elementos web de las exigencias generales del RGPD, tales como el Delegado de Protección de Datos (DPD/DPO), la Evaluación de Impacto de los Datos Personales (EIPD) y el Registro de Actividades de Tratamiento de los Datos Personales (RAT).

El Delegado de Protección de Datos (DPD ó DPO, *Data Privacy Officer*, por sus siglas en inglés) es una figura que aparece en el Artº. 37.1 del RGPD y en muchas empresas o sitios webs será necesario su nombramiento formal a la AEPD.

El DPD es una piedra angular de la responsabilidad, que facilita el cumplimiento a través de herramientas de rendición de cuentas, como las EIPD y la realización de auditorías, que actúa como intermediario entre las partes interesadas relevantes. El DPD también supervisa las políticas de privacidad y protección de datos para garantizar los procesos de esas políticas a través de las unidades organizativas y se asegura de que la organización lleva acabo el RAT de manera compatible.

Se ha de verificar su obligatoriedad y si se cumplen los requerimientos específicos, ya que de otro modo la organización no está obligada a su nombramiento. Se deberá en ese caso mediante información documentada, disponer del registro de que la organización no necesita el nombramiento del DPD.

Del mismo modo que antes, el servicio **SECURE WEB** verifica si la organización está obligada a llevar a cabo una EIPD, comprobando su obligatoriedad y si se cumplen los requerimientos específicos, ya que de otro modo la organización no está obligada a la EIPD. Se deberá en ese caso mediante información documentada, disponer del registro de que la organización no necesita llevar a cabo una EIPD.

Por ejemplo, la organización no está obligada a realizar una EIPD si el tratamiento de datos no entraña un riesgo para los derechos y libertades de las personas usuarias, lo cual es una tarea, muy técnica y compleja de realizar.

Se han de verificar los aspectos reglamentarios del RGPD de aplicación en la Web, tales como tales como el Delegado de Protección de Datos (DPD/DPO), la Evaluación de Impacto de los Datos Personales (EIPD).

Se ha de verificar su obligatoriedad y si se cumplen los requerimientos específicos, ya que de otro modo la organización no está obligada a su cumplimiento.

Se deberá en ese caso mediante información documentada, disponer del registro de que la organización no necesita DPD, ni EIPD, ni RAT.

El Registro de Actividades de Tratamiento de los Datos Personales (RAT) es una información documentada que también va dirigida a demostrar la responsabilidad activa, ya que por el volumen de datos que recoge la organización y la naturaleza de los mismos, puede estar obligada a llevar un RAT para poder acreditar la conformidad de su actuación con las exigencias legales de protección de datos.

El servicio **SECURE WEB** verifica la obligatoriedad de que cada organización que deberá llevar un RAT conforme a lo previsto en el Artº. 30 del RGPD, lo ejecute según el Artº. 30.1 del RGPD que recoge el contenido del RAT para el responsable de tratamiento y según el Artº.30.2 que indica el contenido del RAT que el encargado de tratamiento debe llevar, cuando se da alguno de estos requisitos:

- La organización o el autónomo tiene más de 250 empleados o bien con menos de 250 empleados realiza tratamientos que:
  - Puedan entrañar un riesgo para los derechos y libertades de los interesados.
  - No sean ocasionales.
  - De manera ocasional incluyan categorías especiales de datos personales.

De manera no ocasional, el Artº.9 del RGPD incluye categorías especiales de datos personales:

- Origen étnico o racial.
- Opiniones políticas.
- Convicciones religiosas o filosóficas.
- Afiliación sindical.
- Tratamiento de datos genéticos.
- Datos biométricos dirigidos a identificar de manera unívoca a una persona física.
- Datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

8. METADATOS.

Los metadatos (del griego μετα, *meta*, 'después de, más allá de' y latín *datum*, 'lo que se da', "dato") son datos que describen otros datos. Por ejemplo: en un departamento comercial, los metadatos serían las fichas donde se almacena información sobre clientes, suministradores, contratistas, etc., para buscar productos y servicios. Los metadatos permiten identificar más datos.

En el mundo digital podría ser información que aislada no aporte ninguna información sobre quién es el interesado o pudiera ser que sí y aunque ni el RGPD ni la LOPDGDD hacen referencia alguna a los metadatos, podrían ser considerados "datos" a los efectos del RGPD.

De hecho, el Considerando 17 RGPD, establece la obligación de requerir el consentimiento para tratar estos metadatos por parte de los proveedores de servicios, aunque en el Artª 6.2 establecen tres tipos de bases de legitimación diferentes para tratar metadatos, que son la obligación derivada de calidad de servicio, la facturación e impedir fraudes.

El servicio **SECURE WEB** verifica las obligaciones para tratar estos metadatos por los proveedores de servicios y además la supresión o anonimización de los mismos cuando ya no los use, según las exigencias del RGPD.