LLEGAR A LA META DEL GDPR

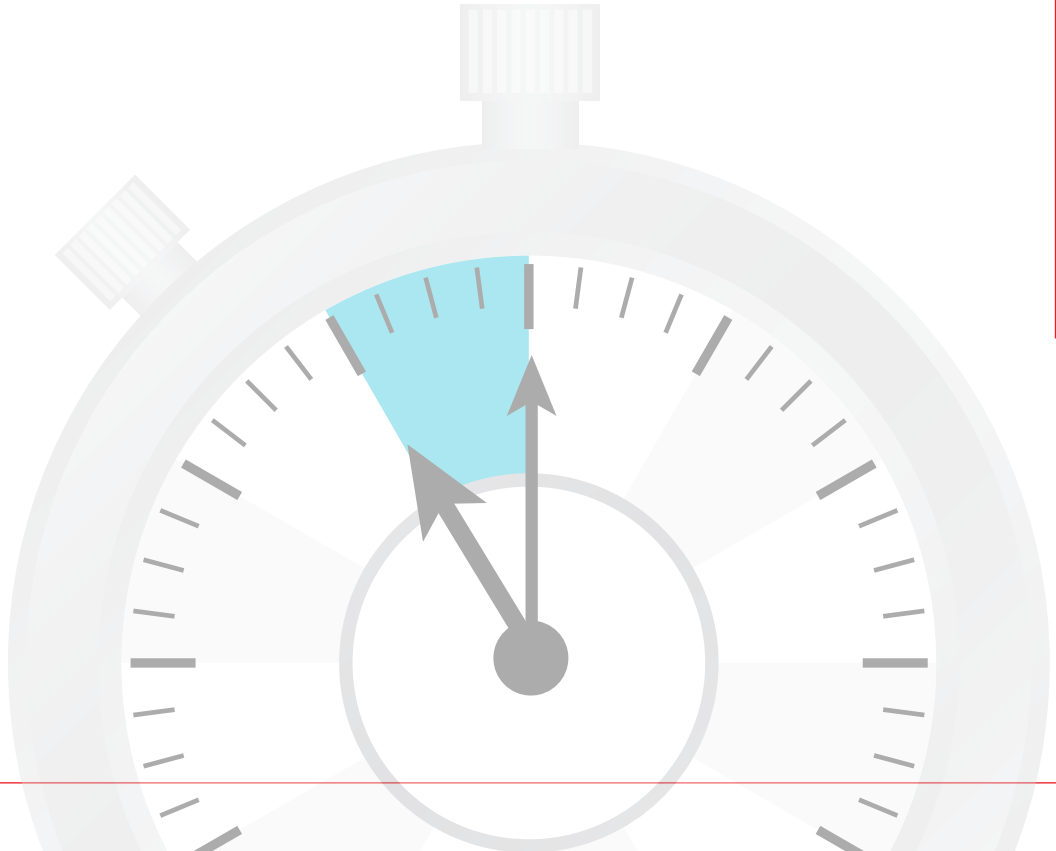
WatchGuard®

Índice

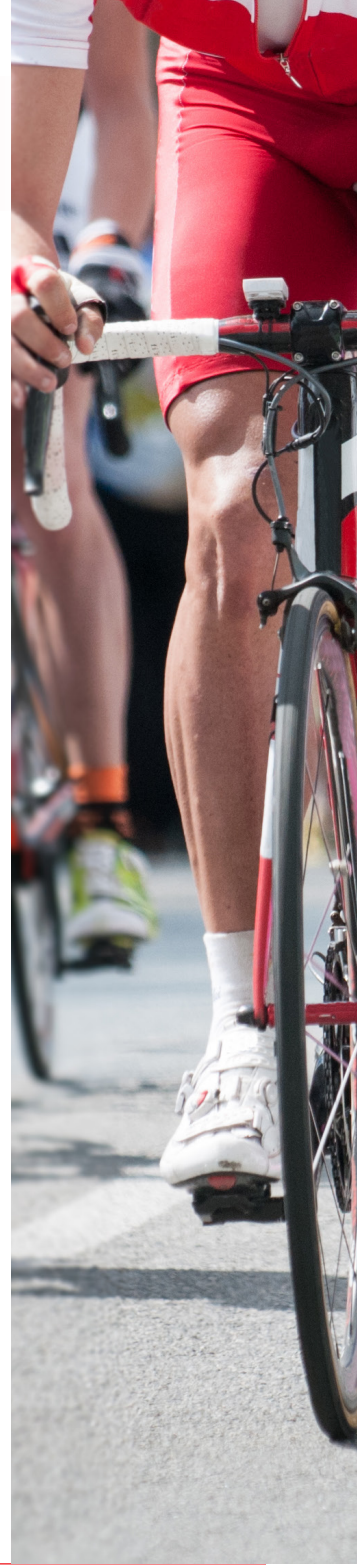
Carrera contrarreloj

Con la adopción de (EU) 2016/679 en abril de 2016, normalmente conocido como el Reglamento General de Protección de Datos (General Data Protection Regulation, GDPR), las compañías como la suya están ahora en una carrera para lograr el cumplimiento antes de que el reglamento entre en vigencia el **25 de mayo de 2018**; de lo contrario, posiblemente tengan que enfrentar enormes multas y posibles demandas. Este esfuerzo es mayor y más difícil porque este Reglamento expande considerablemente el alcance de la responsabilidad en comparación con la Norma de protección de datos de 1995 (Norma 95/46/EC) que estaba en vigencia anteriormente.

Pero hay una buena noticia: **¡no está solo!** Como el pelotón en una carrera de bicicletas, la mayoría de las compañías se encuentra aproximadamente en el mismo nivel en el proceso de cumplimiento y alcanzaremos la meta más rápido y fácil si colaboramos.



El Reglamento General de Protección de Datos entra en vigencia el **25 de mayo de 2018**



¿Quiénes participan en la carrera?

Por lo tanto, este libro electrónico comparte información clave sobre el GDPR y ofrece soluciones para guiar su iniciativa de cumplimiento y mejorar la seguridad de sus datos.

Las organizaciones que recopilan, almacenan o procesan información personal deben cumplir con el GDPR si:

- ofrecen bienes o servicios a ciudadanos de la UE que viven en la UE;

  O

- monitorear el comportamiento de ciudadanos de la UE que viven en la UE.

Esto incluye organizaciones que no tienen sede ni presencia en la UE y también incluye a aquellas que tienen empleados en la UE pero no tienen clientes en la UE. Si manipula algún tipo de información personal relativa a ciudadanos naturalizados de la UE, esto también rige para usted.

Todas las organizaciones que cumplen estos criterios deben demostrar el cumplimiento. Si procesa datos a gran escala, debe cumplir un set de requerimientos más extenso.

El Reglamento hace referencia a las organizaciones que deben cumplir con el GDPR como "controladores" o "procesadores". Los controladores son entidades que determinan los propósitos, las condiciones y las formas de procesar los datos personales; mientras que los procesadores son las entidades que procesan los datos personales en representación del controlador.

> Por ejemplo, una clínica de atención médica puede tercerizar su trabajo de laboratorio a otra instalación. La clínica tendría que compartir cierta cantidad de información personal que ha recopilado con el servicio de laboratorio para entregar los resultados al paciente correcto. En esta situación, el proveedor de atención médica es el controlador y el proveedor del laboratorio es el procesador a los fines del GDPR. Existen algunas diferencias en los requisitos del Reglamento para cada papel y, por lo tanto, querrá determinar si se aplica uno o ambos a su organización.

¿Qué se considera como datos personales?

El GDPR interpreta la definición de datos personales de manera amplia. Se considera como datos personales cualquier tipo de información que se pueda usar para identificar directa o indirectamente a una persona. Puede ser cualquier cosa, desde un nombre, una foto, una dirección de correo electrónico, los detalles bancarios, el número de identificación nacional, las publicaciones en sitios web de redes sociales, la información médica e incluso la dirección IP de una computadora que esté vinculada con la cuenta o el dispositivo de un usuario específico.

A modo de ejemplo, si dirige una carrera y registra o asigna números a los competidores en un sistema informático, en el cual los números de los competidores se asocian con una persona específica, entonces esta información se consideraría como datos personales. Además, esos números con frecuencia establecen una referencia cruzada con datos personales como el nombre del inscrito, la dirección, la foto, los exámenes médicos previos a la carrera y otra información.

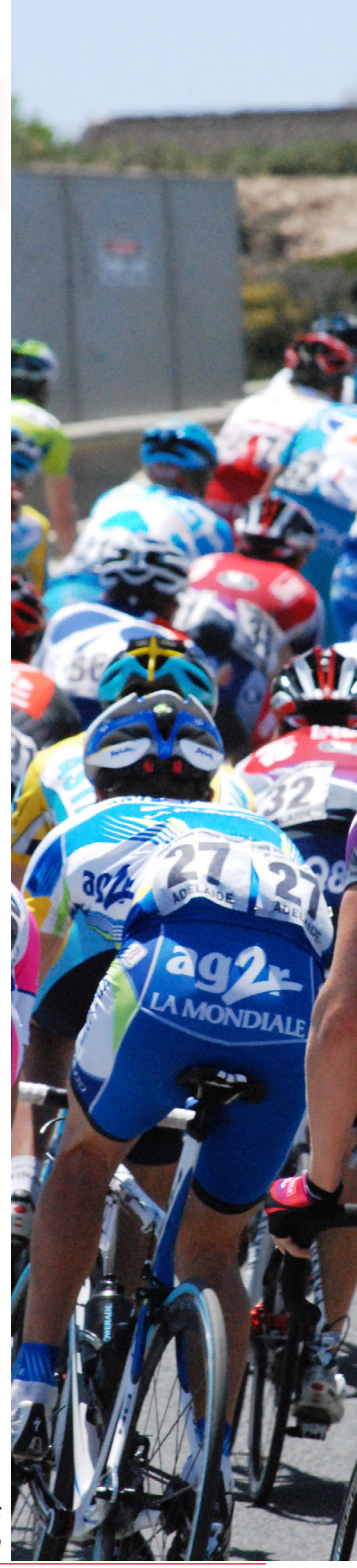


Foto del pelotón: Sue Hixson

Cuidado con los peligros en el camino

El GDPR incluye un número de elementos que no formaban parte de la Norma de protección de datos anterior y pueden confundirlo si no está preparado. A continuación, se incluye una descripción de algunos de los requisitos nuevos más significativos, pero debe consultar el Reglamento para obtener detalles completos y una lista completa.

- **NOTIFICACIONES POR PÉRDIDAS DE DATOS:** Actualmente, se requiere que los controladores y procesadores informen a las autoridades de supervisión dentro de las 72 horas del conocimiento de una pérdida y que informen a las personas a quienes se aplican los datos (sujetos a quienes pertenecen los datos) "sin demora indebida".

Se debe tener en cuenta que una pérdida de **datos cifrados** se **excluye específicamente** de los requisitos de notificación y, por lo tanto, puede considerarse para su estrategia de cumplimiento.

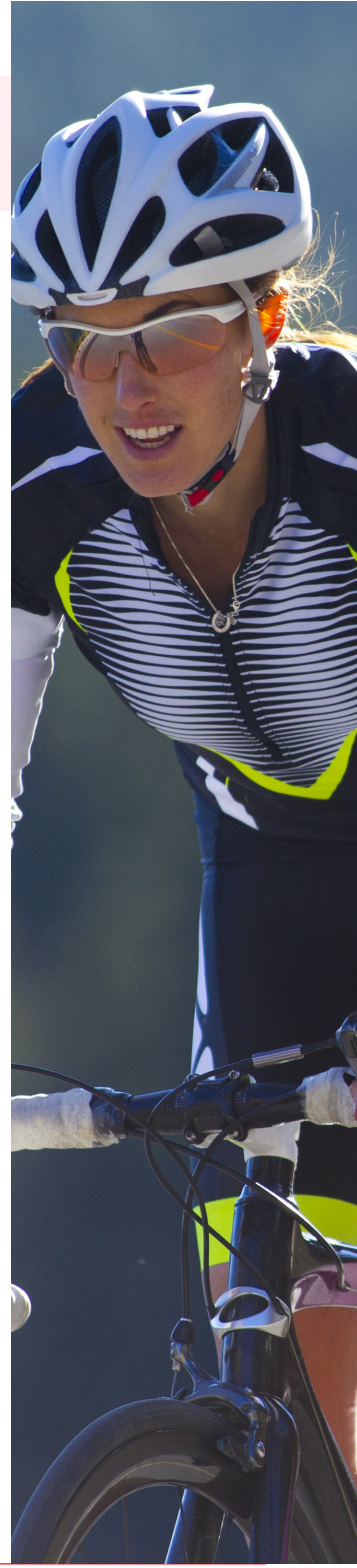
- **CONSENTIMIENTO EXPLÍCITO:** El GDPR requiere que cuando se recopilen los datos personales, el sujeto a quien le pertenecen los datos debe otorgar consentimiento explícito. Esto significa que las organizaciones ya no pueden esconder el consentimiento genérico en un formulario largo lleno de jerga legal. Por el contrario, las organizaciones deben ofrecer información específica sobre qué datos se recopilan, cómo se almacenarán y procesarán y deben usar lenguaje claro y sencillo. En este contexto, nada menos de "decidir participar" cubrirá de manera satisfactoria la reglulación. Además, se debe poder revocar el consentimiento con la misma facilidad con la que se lo proporciona.

- **TRANSFERENCIA DE DATOS FUERA DE LA UE:** Los datos personales no pueden salir de la UE, a menos que se cuente con aprobación de la Autoridad de supervisión o si se informa al sujeto a quien le pertenecen los datos sobre la transferencia de datos y los riesgos asociados y autoriza la transferencia.

- **DESIGNACIÓN DE UN OFICIAL DE PROTECCIÓN DE DATOS (DPO):** Si procesa datos a gran escala, debe designar a (contratar, asignar o firmar un contrato con) un DPO para su organización. El DPO es su representante frente a las Autoridades de supervisión que controlan y garantizan el cumplimiento del Reglamento. Esta persona también es el contacto para cualquier solicitud o queja de los sujetos a quienes les pertenecen los datos. Además, dirigen sus actividades de cumplimiento, como lo requiere la Evaluación del impacto de la protección de datos (Data Protection Impact Assessment, DPIA), y manejan la comunicación sobre políticas de seguridad, las evaluaciones, el cumplimiento, las solicitudes de los sujetos a quienes les pertenecen los datos y las notificaciones de pérdidas, entre otras cosas. De acuerdo con el reglamento, el DPO notifica al gerente ejecutivo, su designación es por dos años y puede extenderse.

Se pueden imponer multas de hasta **20 millones de euros** o el **4 %** de los ingresos mundialesa las organizaciones.

- **SANCIONES/COSTOS POR INCUMPLIMIENTO:** Se pueden imponer multas de hasta 20 millones de euros o el 4 % de las ganancias mundiales a aquellas empresas y organizaciones que no cumplen con el GDPR. Las multas son escalonadas, se imponen incluso por primeras infracciones y pueden incluir una multa del 2 % de los ingresos mundiales por no tener los registros en regla (Artículo 28), por ejemplo. Además, las organizaciones pueden incurrir en gastos adicionales, incluidos los honorarios de abogados y las compensaciones por orden judicial si los ciudadanos de la UE sienten que se han violado sus derechos, presentan una demanda por daños y ganan la causa.



La estrategia ganadora

El cumplimiento del GDPR requiere un esfuerzo significativo prácticamente para todas las empresas y, sin duda alguna, incluirá la incorporación de lo siguiente:

- Medidas para la protección de datos **mediante la tecnología de seguridad de red más reciente y eficaz** que permite lo siguiente:
  - **Proteger los datos** durante el almacenamiento y la transmisión.
  - Garantizar **el conocimiento situacional** de riesgos.
  - Permitir **medidas preventivas, correctivas y atenuantes en tiempo casi real** contra vulnerabilidades o incidentes detectados que podrían significar un riesgo para los datos.
  - Proporcionar **herramientas para evaluar** la efectividad de las políticas de seguridad.
- Mecanismo de recuperación de datos que restablece el acceso a los datos cuando un incidente interrumpe la disponibilidad.
- Procesos nuevos o mejorados y estructuras de generación de informes para supervisar el consentimiento, la notificación de pérdidas y el cumplimiento.

También debería considerar aquellos lugares en los que tenga la oportunidad de reducir el alcance/riesgo del impacto del GDPR, de modo que se reduzca la carga asociada con la supervisión, el mantenimiento de registros y las actividades de cumplimiento relacionadas con el GDPR.
Por ejemplo:

- **Reducir** el número de campos de datos personales recopilados/procesados.
- **Reducir** el tiempo en el que se mantienen/procesan los datos personales.
- **Cifrar los datos** en el almacenamiento y durante la transmisión.
- **Ocultar las direcciones IP** y anonimizar otros tipos de información del usuario.
- **Reducir** el número de personal autorizado que puede acceder a los datos personales.
- **Aumentar** su capacidad de impedir y corregir amenazas a los datos personales.

Se incluye una Lista de comprobación de planificación del GDPR al final de este libro electrónico que es útil para comenzar a planificar el cumplimiento del GDPR.
La lista de comprobación y las preguntas de referencia le permiten realizar una evaluación de las políticas actuales y las prácticas de seguridad, de modo que pueda notar el alineamiento y las brechas con respecto al Reglamento.

¡Cruzar la meta!

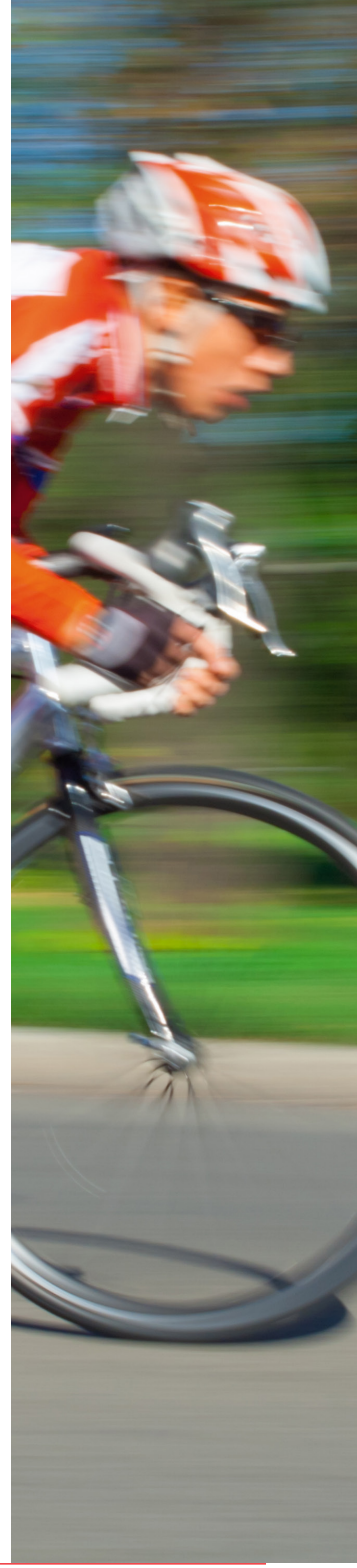
Ahora que cuenta con algunas buenas ideas sobre cómo comenzar a construir una organización que cumpla con el GDPR, sin duda debe estar tratando de cubrir brechas y deficiencias con las respuestas rápidas y fáciles que satisfacen el Reglamento e intentando completar esta gran labor a tiempo. WatchGuard puede ayudarlo a lograr el cumplimiento mediante tecnología y prácticas de seguridad de datos altamente eficaces.

Además, facilitamos la tarea. WatchGuard tiene la actualización de seguridad de datos necesaria para cumplir con las medidas de seguridad de datos del GDPR y todo se incluye en un paquete fácil de usar con nuestro Total Security Suite. Mediante la proporción de seguridad sólida de nivel empresarial, un dispositivo de seguridad Firebox® de WatchGuard con Total Security Suite aborda 16 de los 20 Principales Controles de Seguridad Crítica de SANS (v6) y, por lo tanto, ofrece el producto integral necesario para el cumplimiento del GDPR.

Un dispositivo de seguridad Firebox de WatchGuard con Total Security Suite aborda **16** de los 20 Principales **Controles** de **Seguridad Crítica** de SANS

Los 20 Principales Controles de Seguridad Crítica de SANS (V6)

CS1	Inventario de Dispositivos Autorizados y No Autorizados	*Sí*
CS2	Inventario de Software Autorizado y No Autorizado	*Sí*
CS3	Configuración Segura del Hardware y Software en Dispositivos Móviles, Computadoras Portátiles, Estaciones de Trabajo y Servidores	*Sí*
CS4	Evaluación de Vulnerabilidad y Corrección Continuas	*Sí*
CS5	Uso Controlado de Privilegios Administrativos	*Sí*
CS6	Mantenimiento, Supervisión y Análisis de Registros de Auditorías	*Sí*
CS7	Protecciones de Correo Electrónico y Explorador Web	*Sí*
CS8	Defensas contra Malware	*Sí*
CS9	Limitación y Control de los Puertos de Red, Protocolos y Servicios	*Sí*
CS10	Capacidad de Recuperación de Datos	*No*
CS11	Configuraciones Seguras para Dispositivos de Red como Firewalls, Enrutadores y Conmutadores	*Sí*
CS12	Defensa de Límites	*Sí*
CS13	Protección de Datos	*Sí*
CS14	Acceso Controlado Basado en la Necesidad de Conocimiento	*Sí*
CS15	Control de Acceso Inalámbrico	*Sí*
CS16	Supervisión y Control de Cuentas	*Sí*
CS17	Evaluación de Habilidades de Seguridad y Formación Adecuada para Cubrir Brechas	*N/C*
CS18	Seguridad de Software de Aplicación	*Sí*
CS19	Gestión y Respuesta ante Incidentes	*N/C*
CS20	Pruebas de Penetración y Ejercicios de Equipos de Red	*N/C*

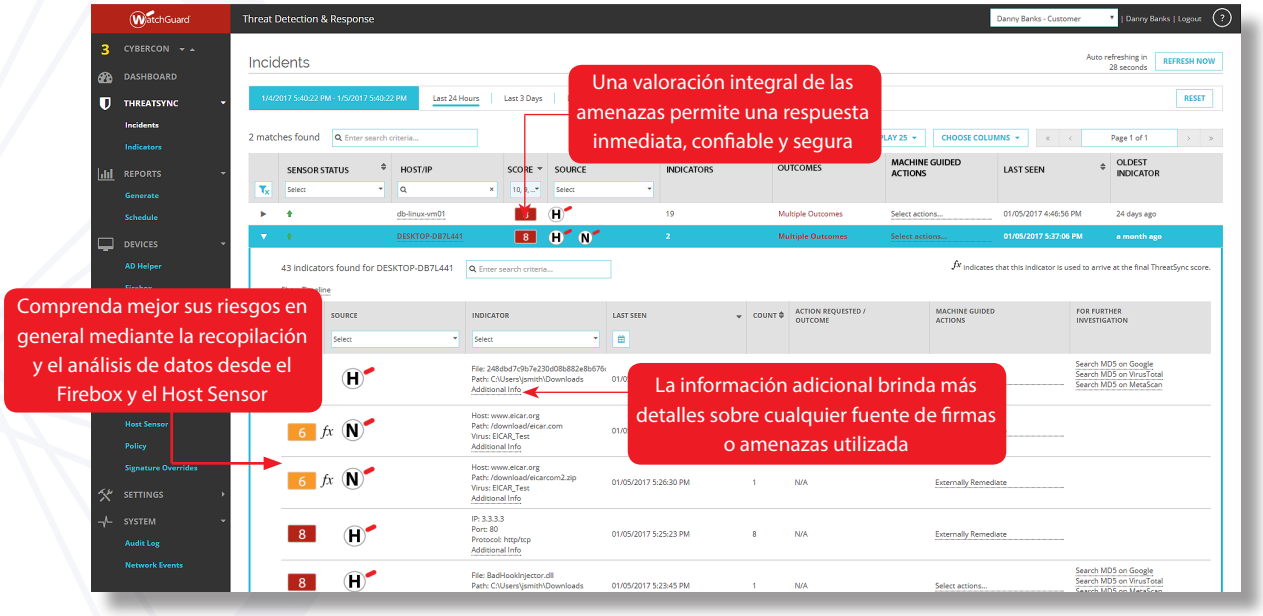


¡Cruzar la meta!

Nuestro Total Security Suite brinda soluciones exclusivas para abordar de manera específica los requisitos del GDPR que incluyen lo siguiente:

Threat Detection and Response: El GDPR requiere "conocimiento situacional", el cual es proporcionado por WatchGuard mediante nuestra funcionalidad característica ThreatSync. ThreatSync correlaciona la información de seguridad de los dispositivos de red y endpoint para que note la presencia de incidentes de seguridad en aumento en un panel de control fácil de decodificar.

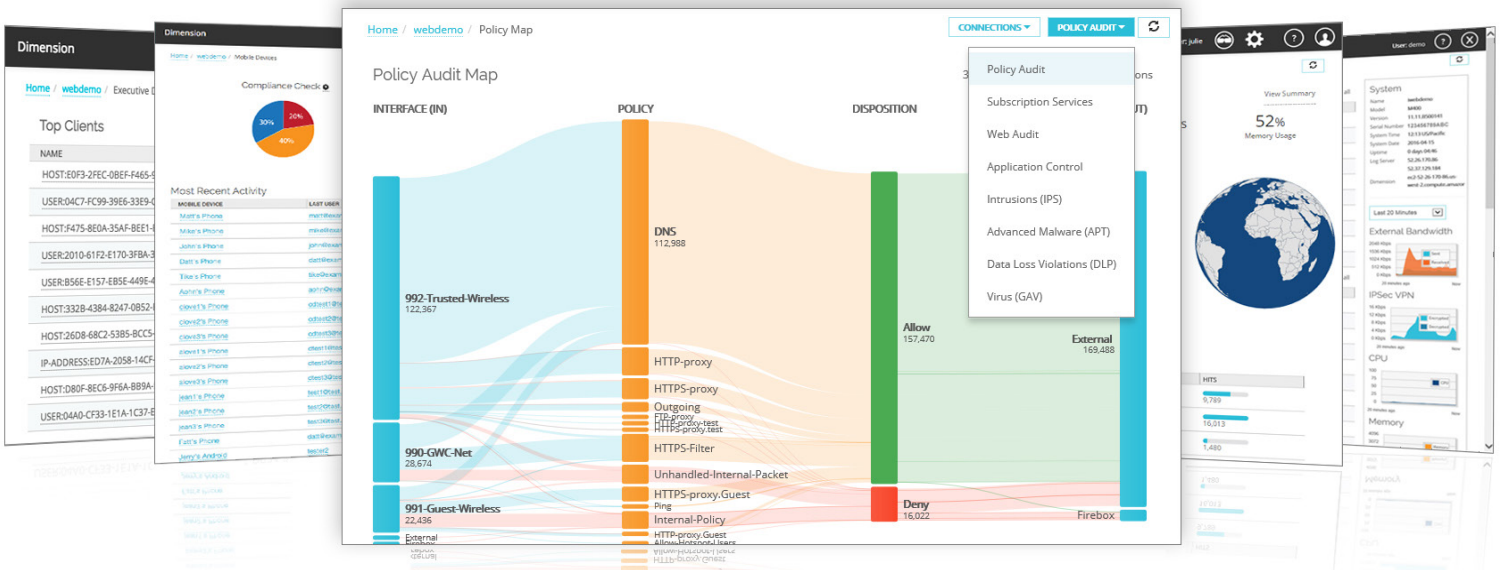
Además, puede crear políticas para corregir incidentes "importantes" de manera automática y no solo cumplir con el requisito de "medidas preventivas, correctivas y atenuantes en tiempo casi real". Aún mejor, una vez que se corrige una amenaza, la información se comparte con nuestra fuente de inteligencia sobre amenazas para que la identifique y evite que vuelva a ingresar a su red. A su vez, debido a que TDR es un servicio basado en la nube, puede optar por almacenar sus datos en la UE para cumplir con el artículo de transferencia de datos del Reglamento.



Threat Detection and Response

WatchGuard Dimension™: Dimension proporciona una solución rápida y eficaz para los requisitos del GDPR que se enfocan en el acceso inmediato a datos de registro e informes valiosos que demuestren el cumplimiento. Brinda herramientas de generación de informes y visibilidad de grandes datos que identifica y extrae de manera exclusiva tendencias y problemas clave de seguridad de red, de modo que se acelera la capacidad para combatir amenazas, generar informes sobre toda la actividad de seguridad de red y establecer políticas importantes de seguridad en toda la red.

Además, Dimension incluye una funcionalidad potente de Anonimización del Usuario que puede reemplazar toda la información de identificación personal (personally identifiable information, PII) en informes, paneles de control y páginas de resumen de Dimension con texto de marcador de posición cifrado. Cifra nombres de usuarios, direcciones IP, nombres de servidores y nombres de dispositivos móviles con secuencias alfanuméricas generadas al azar que no se repiten nunca para garantizar que se oculten los datos en tránsito.



WatchGuard Dimension

¡Cruzar la meta!

Data Loss Prevention (DLP): GDPR se trata sobre la protección de los datos y nuestro servicio de DLP ayuda a prevenir las pérdidas accidentales de datos mediante la detección y el bloqueo de archivos con información personal para que no salgan de la red. Busca información privada, como números de seguridad nacional, detalles de cuentas bancarias y registros de pacientes de acuerdo con las reglas que usted autoriza.

Cifrado y VPN: Mantener los datos personales cifrados en el almacenamiento y durante el tránsito es una estrategia fundamental para el éxito del cumplimiento, ya que reduce significativamente los requisitos de notificación después de que ocurre una pérdida de datos. Las soluciones de Gestión Unificada de Amenazas (Unified Threat Management, UTM) Firebox de WatchGuard incluyen la creación de VPN con "drag-and-drop" entre sucursales y la oficina central. Además de la configuración rápida y fácil, nuestros VPN tienen gran durabilidad y se conocen por su estabilidad, lo cual es primordial cuando su empresa confía en la disponibilidad uniforme de datos.

Al considerar todas las robustas funcionalidades de seguridad y de VPN, la visibilidad y la anonimización del usuario de Dimension, y el conocimiento situacional y la corrección automática de Threat Detection and Responsee, Firebox de WatchGuard con Total Security Suite es claramente la opción que puede ayudarle a alcanzar la meta a tiempo para el cumplimiento del GDPR.

El primer hombre que atravesó el Eurotúnel en bicicleta
Foto: Chris Froome

Total Security Suite de WatchGuard

SERVICIOS DE SEGURIDAD FUNDAMENTALES

INTRUSION PREVENTION SERVICE (IPS)

SERVICIO REPUTATION ENABLED DEFENSE (RED)

SPAMBLOCKER

GATEWAY ANTIVIRUS (GAV)

FILTRADO DE URL WEBBLOCKER

NETWORK DISCOVERY

APPLICATION CONTROL

ADVANCED SECURITY SERVICES

APT BLOCKER: PROTECCIÓN AVANZADA CONTRA MALWARE

DATA LOSS PREVENTION (DLP)

THREAT DETECTION AND RESPONSE

DIMENSION COMMAND

Lista de Comprobación de Planificación del GDPR

Nuestra Lista de comprobación de planificación del GDPR lo ayuda a comenzar a evaluar e implementar medidas para el cumplimiento del GDPR. Este recurso no representa una lista exhaustiva de los requisitos y se debe usar junto con otros recursos para crear un plan integral de cumplimiento.

☑ Identifique los campos de datos personales que está recopilando de ciudadanos naturalizados de la UE.

- ¿Qué datos personales se recopilan o procesan?
- ¿En dónde se almacenan o transmiten? ¿Por cuánto tiempo?
- ¿Qué políticas o procesos de retención se aplican a estos datos? ¿Se puede reducir esto?
- ¿Está bajo su control o bajo el control de un contratista?
- ¿Estos datos permanecen en la UE en todo momento?

☑ Describa la información y los procesos de consentimiento que existen cuando se recopilan estos datos.

- ¿Se solicita con claridad el consentimiento explícito para recopilar y procesar los datos de los sujetos a quienes les pertenecen?
- ¿Se otorga consentimiento cuando se realiza la recopilación?
- ¿La comunicación de consentimiento identifica y proporciona información de contacto para el controlador, procesador y DPO (cuando corresponde)?
- ¿Describe el propósito del procesamiento, la seguridad del procesamiento y el fundamento legal?
- ¿Proporciona el período de almacenamiento de los datos?
- ¿Nombra a los destinatarios o a la categoría de destinatarios de los datos?
- ¿Explica el derecho de los sujetos a quienes les pertenecen los datos a acceder, rectificar, solicitar, corregir o hacer que sus datos sean transferibles, como también su derecho a quejarse ante una autoridad de supervisión?
- ¿Indica la intención de transferir los datos fuera de la UE?
- ¿Estipula si la recopilación de datos es obligatoria u opcional, como también las consecuencias de no proporcionar dichos datos?
- ¿Se puede revocar el consentimiento con la misma facilidad con la que se lo proporciona?

☑ Describa la capacidad de comunicación con los sujetos a quienes les pertenecen los datos.

- ¿De qué manera los sujetos a quienes les pertenecen los datos acceden, rectifican, hacen que se borren y extraen sus datos para la transferencia?
- ¿Cómo revocan el consentimiento los sujetos a quienes les pertenecen los datos?
- ¿Cómo se comunica la organización con los sujetos a quienes les pertenecen los datos para notificar un incumplimiento?

Determine si las medidas actuales para llevar los registros y las políticas de procesamiento de datos son adecuadas.

- ¿Hay un registro de datos sujetos a respuesta para aprobación?
- ¿Hay un registro o seguimiento de los eventos de procesamiento de datos que involucran datos personales?
- ¿Estos registros son seguros y admiten consultas, búsquedas o informes del personal autorizado?
- ¿Se mantienen actualizadas las políticas que describen cómo se realiza el procesamiento de datos de conformidad con el Reglamento?
- Si un controlador se encuentra fuera de la UE, ¿hay un representante designado dentro de la UE y se documenta esto?
- Si se contratan los servicios de procesamiento de datos, ¿el acuerdo legal incluye las cláusulas necesarias para garantizar la seguridad y manipulación adecuadas de los datos personales para cumplir con el GDPR?
- ¿Hay suficiente control de acceso a los servidores y edificios para impedir que personas no autorizadas tengan acceso a los datos personales?

Determine si las prácticas de seguridad de datos y la tecnología son adecuadas para cumplir con los requisitos del GDPR.

- ¿Se toman las medidas técnicas y organizacionales adecuadas para garantizar que los datos se protegen de la destrucción, pérdida o modificación accidental o ilegal y el almacenamiento, el procesamiento, el acceso o la divulgación no autorizada o ilegal?
- ¿La política de seguridad aborda lo siguiente?
  - La manera de proteger los datos durante el almacenamiento y la transmisión.
  - La manera de restablecer el acceso a los datos cuando un incidente interrumpe la disponibilidad.
  - La manera de garantizar el conocimiento situacional de riesgos y permitir medidas preventivas, correctivas y atenuantes en tiempo casi real contra vulnerabilidades o incidentes detectados que podrían significar un riesgo para los datos.
  - La descripción del proceso para evaluar con frecuencia la efectividad de las políticas de seguridad.
- ¿Existe un proceso para proporcionar notificaciones de incumplimiento en 72 horas?
- ¿Existe un registro de una Evaluación del impacto de la protección de datos (Data Protection Impact Assessment, DPIA) que evalúe si es posible que las operaciones de procesamiento presenten riesgos específicos? ¿Se completó en los dos últimos años o de inmediato cuando hubo un cambio en los riesgos específicos de las operaciones de procesamiento?
- ¿Hay un Encargado de Protección de Datos (DPO) designado?

Las respuestas a estas preguntas de la lista de comprobación deberían ayudarlo a identificar en dónde puede tener deficiencias para abordarlas antes de quedarse sin tiempo.

Visite **www.watchguard.com** para obtener más información.

Oficina central mundial
Estados Unidos
Tel.: +1.206.613.6600
Correo electrónico: sales@watchguard.com

Oficina central de Europa
Países Bajos
Tel.: +31(0)70.711.20.85
Correo electrónico: sales-benelux@watchguard.com

Oficina central de Asia, el Pacífico y el Sudeste Asiático
Singapur
Tel: +65.6536.7717
Correo electrónico: inquiry.sea@watchguard.com

WatchGuard®

1. http://www.eugdpr.org/
2. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
3. https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf