



# Anonimización de usuarios de WatchGuard y el Reglamento General de Protección de Datos de la UE

Resumen técnico

WatchGuard Technologies, Inc.

Fecha de publicación: mayo de 2016

## Introducción

El crecimiento de Internet ha provocado que los problemas de privacidad que giran en torno a los datos del usuario adquiera especial importancia. Son muchos los países implicados en el desarrollo de reglamentos que definan estándares que marquen cómo mover, almacenar, ver y generar informes de datos que contengan información personal de los usuarios, también conocida como PII.

La Unión Europea (UE) está sentando precedentes con los reglamentos de protección de los datos y de la privacidad más estrictos de todo el mundo. En abril de 2016, el Parlamento Europeo adoptó con carácter oficial el marco de trabajo del **Reglamento General de Protección de Datos**, o **GDPR**, cuya aplicación íntegra está programada para el 25 de mayo de 2018. Las obligaciones que marca el GDPR son muy significativas, y se establece la responsabilidad como un importante componente de conformidad, especialmente en lo que respecta a las plantillas de las empresas. Las amenazas internas siguen siendo uno de los principales motivos de vulneraciones de la información y de uso inadecuado de los datos. Una buena forma de ponerse manos a la obra es cifrarlo todo, pero las empresas deben acometer muchas otras tareas para cumplir con la futura ley.

Las empresas de la UE tendrán que demostrar el cumplimiento de las medidas del GDPR, entre las que se incluyen las siguientes:

- **Evaluar la repercusión de la protección de datos** antes de iniciar los procesos que conlleven más riesgos.

- **Implementar la protección de datos por diseño y de forma predeterminada:** en otras palabras, las organizaciones tendrán que diseñar la protección de datos para implementarla en sus infraestructuras de servicio y evaluar dichas implementaciones desde una perspectiva de responsabilidad.
- **Adoptar medidas técnicas y organizativas destinadas a los procesadores de los datos.**
  - Informar al controlador de posibles infracciones
  - Designar un responsable de protección de datos, también conocido como DPO\*
- **Pseudoanonimizar los datos personales:** es decir, la información personal se anonimiza hasta el punto que no puede atribuirse a su propietario durante ninguna fase del procesamiento.

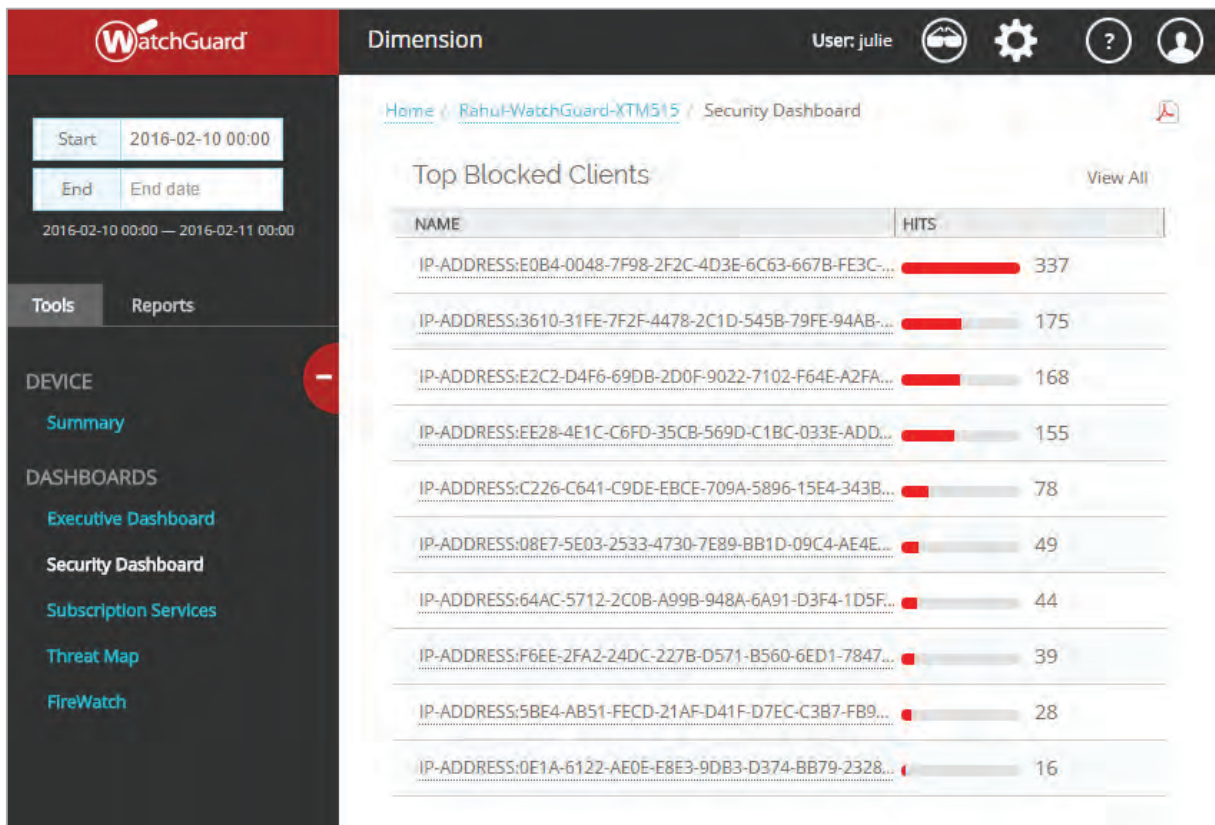
*\*A pesar de que no todas las empresas estarán obligadas a tener este cargo en su organigrama, la responsabilidad y una privacidad estricta para el usuario son elementos universales que se aplican a todos los encargados de procesar los datos.*

## Anonimización de usuarios de WatchGuard

La plataforma de visibilidad **WatchGuard Dimension™**, incluida con la compra de todos los dispositivos de seguridad WatchGuard Firebox, ofrece una nueva función de **anonimización de usuarios** que facilita a las organizaciones de la UE el cumplimiento del marco de regulatorio del GDPR. Esta característica funciona de un modo muy sencillo, es muy fácil acceder a ella y configurarla, y se diseñó para ayudar a garantizar el cumplimiento del GDPR y pensando en las amenazas internas.

### ¿Cómo funciona la anonimización de usuarios?

La anonimización de usuarios sustituye toda la información personal (PII) de los informes, paneles de control y páginas de resumen de Dimension por marcadores de posición de texto con algoritmos hash licados. Cuando se habilita, la anonimización de usuarios aplica algoritmos hash a los nombres de usuario, las direcciones IP, los nombres de host y los nombres de los dispositivos móviles mediante secuencias alfanuméricas exclusivas generadas de forma aleatoria. Las secuencias anonimizadas no solo son exclusivas en cada sesión anonimizada, sino también entre todas las sesiones anonimizadas. Por ello, al mismo elemento de datos de información personal anonimizado se le aplicará un algoritmo hash distinto en cada sesión, lo que bloquea la posibilidad de generar tendencias basadas en los datos de información personal en cada sesión y entre sesiones.



**Figura 1.** El modo anonimizado cifra únicamente en la plataforma de visibilidad. No cifra la base de datos.

Cuando los usuarios inicien sesión en Dimension con el modo anonimizado habilitado, verán una versión restringida de las páginas que pueden ver según sus roles de usuario. Además, cuando la función esté habilitada, no estarán disponibles ni los mensajes de registro ni los informes detallados. Los paneles de control de visibilidad de Dimension disponibles en el modo anonimizado son los siguientes:

- Panel de control ejecutivo
- Panel de control de seguridad
- Panel de control de servicios de suscripción
- Mapa de amenazas
- FireWatch

En cuanto a los informes, en el modo anonimizado solo hay disponibles informes de resumen. La opción «Ver detalles» profundiza en los informes de resumen, en los informes de cliente y en los informes detallados, pero solo está disponible cuando no está activado el modo anonimizado en Dimension.

### ¿Cómo puedo habilitar la anonimización de usuarios?

Al configurar Dimension en un dispositivo Firebox por primera vez, la anonimización de usuarios puede habilitarse en el Asistente de configuración de Dimension. Si ya se ha implementado Dimension, la anonimización de usuarios se puede habilitar desde las páginas de administración del servidor y de administración del acceso.

**Anonymize Reports**

Enable Anonymized Mode

In Anonymized Mode, user names, IP addresses, host names, and mobile device names are masked in reports, and log messages and detail reports are not available. You can add a local user account with Anonymization Officer privileges that can manage whether users can see data that has been anonymized.

After you enable Anonymized Mode and save your settings, you can add a local user account on the Access Management > [Users & Groups](#) page.

When the Anonymization Officer logs in to enable users to see anonymized data, a message appears with instructions. Specify the title and text of the message for the Anonymization Officer.

Message Title:

Message Text:

**Figura 2.** Configuración de la anonimización de usuarios tras la implementación de Dimension en un Firebox.

### ¿Cuál es el papel del responsable de anonimización?

El **responsable de anonimización** es una nueva función disponible en Dimension para apoyar el cumplimiento del GDPR. Equivale al responsable de protección de datos (DPO) introducido en el marco de trabajo del GDPR. La función de responsable de anonimización se creó de forma que empleados tanto con conocimientos técnicos como sin ellos puedan desempeñarla, y tiene como fin cumplir el enfoque de cuatro ojos o dos inicios de sesión para la autenticación. Por ejemplo, cuando un administrador informático deba cancelar la anonimización de Dimension, el administrador necesitará contar con la aprobación del responsable de anonimización. Esto evita aquellas situaciones en las que una sola persona ostenta el acceso a la información personal, sin control de responsabilidad ni verificaciones externas.

**Add Role(s)**

Select Role(s):

Super Administrator

Global Administrator  Global Monitor

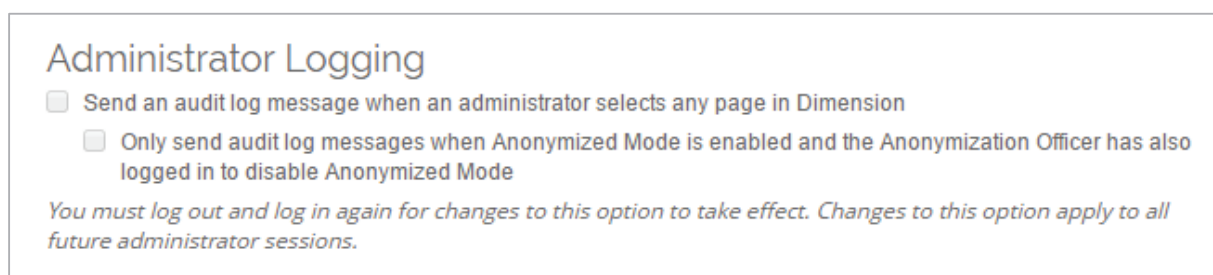
Report Administrator  Anonymization Officer

View All Logs  View All Reports

**Figura 3.** La anonimización de usuarios facilita la tarea de designar a un empleado como responsable de anonimización.

## Auditorías

Las auditorías se efectúan cuando se anula la anonimización de una sesión de Dimension. Dimension registrará toda la actividad que tiene lugar dentro de la propia aplicación para poder controlar las acciones del usuario, lo que permite a la organización controlar la responsabilidad del personal informático cuando tienen acceso a datos personales. Las auditorías pueden realizarse tanto cuando Dimension está anonimizado como cuando no, o puede limitarse únicamente a sesiones no anonimizadas cuando el modo anonimizado se encuentra habilitado.



**Figura 4.** Configure fácilmente si quiere crear un registro de auditoría de todas las acciones realizadas en Dimension o limitar el registro a solo cuando el modo anonimizado está habilitado pero no en funcionamiento.

Para obtener más información sobre la anonimización de usuarios y las potentes herramientas de visibilidad de WatchGuard Dimension, visite <http://www.watchguard.com/es/wgrd-international/products/user-anonymization>.

---

#### DIRECCIÓN:

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

#### WEB:

[www.watchguard.com](http://www.watchguard.com)

#### VENTAS EN

**NORTEAMÉRICA:**  
+1-800-734-9905

#### VENTAS INTERNACIONALES:

+1-206-613-0895

#### ACERCA DE WATCHGUARD

WatchGuard® Technologies, Inc. es un líder internacional en soluciones de seguridad empresariales multifuncionales e integradas que combinan de forma inteligente hardware estándar del sector, las mejores funciones de seguridad y herramientas de administración basadas en políticas. WatchGuard ofrece protección fácil de usar, pero de primer nivel, a cientos de miles de empresas de todo el mundo. WatchGuard tiene sede central en Seattle, Washington, y cuenta con oficinas en Norteamérica, América Latina, Europa y Asia Pacífico. Para obtener más información, visite [WatchGuard.com](http://WatchGuard.com).

No se otorgan garantías explícitas ni implícitas mediante el presente documento. Todas las especificaciones están sujetas a cambios y toda funcionalidad, característica o producto futuros previstos se suministrarán según su disponibilidad. ©2016 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, el logotipo de WatchGuard y WatchGuard Dimension son marcas registradas o comerciales de WatchGuard Technologies, Inc. en los Estados Unidos y/o en otros países. Las demás marcas o nombres comerciales son propiedad de sus respectivos propietarios. N.º de pieza WGCE66913\_052516