

Artículo técnico sobre seguridad de la información

Conformidad con el RGPD

Introducción a la seguridad de la información

www.sharp.es

SHARP
Be Original.

Contenido

Introducción	3
Contexto	4
Recomendaciones	6
Conclusión	7
Glosario del RGPD	8
Referencias	9

Introducción

Todas las empresas modernas se enfrentan a desafíos para asegurarse de cumplir el Reglamento General de Protección de Datos (RGPD).

El Reglamento General de Protección de Datos (RGPD) ha traído consigo varios desafíos para las empresas europeas y de todo el mundo.

Si bien una parte importante del RGPD se centra en proteger los datos en línea, también se aplica a la forma en la que trabajan las empresas y en cómo almacenan los datos, lo que implica la necesidad de considerar qué ocurre con la información que capturan (a través de la digitalización de documentos o la entrada electrónica), almacenan y conservan, procesan, comparten, imprimen, copian, envían por fax y archivan documentos.

La normativa introduce categorías como datos identificables y personales, protección de datos, eliminación de datos, encargados del tratamiento, controladores de datos, responsables de la protección de datos, cumplimiento de normativas, autoridad de protección de datos, etc. (consulte el glosario del RGPD en la página 9).

Existen numerosas publicaciones dedicadas a interpretar el RGPD, las instancias que se verán afectadas y cómo introducir esta normativa en las empresas. Sin embargo, son pocos los documentos o artículos técnicos que aborden cómo traducir el RGPD en el idioma empresarial y todos los procesos vinculados con las actividades empresariales, especialmente los asociados a los datos personales.

Mediante la vinculación de los usuarios empresariales (empleados), los procesos empresariales (flujos de trabajo y prácticas recomendados) y los recursos empresariales (software y hardware), Sharp ha definido tres áreas independientes de la seguridad de las empresas que, al reunirse, pueden mejorar la seguridad general de las empresas para cumplir el RGPD.

Entorno de seguridad de Sharp



Estas tres áreas son:

- **Seguridad de las redes**
En relación con cualquier red utilizada por una empresa y mantenida por un departamento de TI, donde se haga énfasis en todos los periféricos conectados para fines de impresión, digitalización y envío de faxes.
- **Seguridad de las salidas**
En relación tanto con las salidas impresas y digitalizadas desde impresoras estándar o impresoras multifunción. Esta categoría incluye documentos en papel e imágenes de documentos en tránsito desde un PC hasta un dispositivo de impresión (incluido a través de servidores de impresión específicos), digitalización (incluido el envío de digitalizaciones a carpetas, digitalizaciones a correo electrónico y digitalizaciones a la nube) y envío por fax.
- **Seguridad de los documentos**
En relación con la información capturada desde documentos en papel hasta el proceso de digitalización, o las imágenes electrónicas de documentos almacenadas en sistemas

empresariales, como correos electrónicos, archivos electrónicos, formularios, etc.

relación directa con la seguridad de la red, la salida y los documentos.

Sharp puede ayudar a las empresas a cumplir el RGPD mediante la introducción y aplicación de un conjunto de herramientas y prácticas recomendadas en los procesos empresariales, en

Contexto

El RGPD es el mayor cambio introducido en el entorno de la protección de datos en más de 20 años y todavía quedan muchas preguntas por responder.

El RGPD introduce nuevos requisitos y define sanciones financieras por no aplicar las salvaguardias y medidas preventivas necesarias para protegerse contra las violaciones.¹. Pero se ofrece muy poca orientación sobre qué deben prever los propietarios de las empresas, los gestores de TI y los usuarios para cumplirlo. Se deja en manos de cada empresa la interpretación de las medidas que deben adoptarse.

El principal objetivo del RGPD es gestionar mejor y proteger el tratamiento de los datos identificables personalmente. Esto conlleva la obligación de gestionar adecuadamente toda la información personal existente en sus sistemas empresariales, desde los datos de contacto de los clientes y la empresa almacenados en las aplicaciones empresariales hasta los ajustes de red, la gestión de documentos y las cuentas de gestión para impresión, pasando por la documentación de RR. HH. sobre personal.

El cumplimiento del RGPD abarca dos capas principales:

- **Capa personal**
Todos los asuntos relacionados con el usuario, incluido su comportamiento, la forma de trabajar y la manera en la que se les aplican los sistemas y las reglas empresariales.
- **Capa organizativa**
Los procesos empresariales de una organización (incluidos los flujos de trabajo en papel y los flujos de trabajo electrónicos), activos (incluidos aquellos que ayudan a las empresas a compartir y comunicarse de forma electrónica o basada en papel) y la cultura, y cómo responde a los desafíos del mercado.

El cambio esperado en el comportamiento de los usuarios finales y la forma en la que trabajan y procesan todos los datos empresariales disponibles se puede establecer y gestionar mediante la introducción de estrategias y herramientas en un nivel organizativo. Como resultado, se logra una mejor comprensión de la forma en la que se procesan tanto los documentos como los datos identificables por el usuario.²

Por lo tanto, Sharp se centra en la capa organizativa (procesos, soluciones y hardware) y puede ayudar a desarrollar políticas de seguridad integrales y esenciales para toda la empresa.

Sharp ha esbozado los riesgos potenciales que podrían dar lugar a violaciones de seguridad si no se abordan, para lo cual se ha centrado en tres áreas de la seguridad de las empresas:

- **Riesgos relacionados con la red**
 - Las vulnerabilidades asociadas al movimiento de datos entre el formato en papel y el formato electrónico, y de vuelta al formato en papel.
 - La necesidad de proteger las impresoras estándar y las impresoras multifunción al mismo nivel que los servidores y la necesidad de una política de seguridad de la impresión planeada y unificada.
 - La necesidad de supervisar y gestionar dispositivos para sostener y actualizar, cuando es necesario, la política de seguridad en línea con las nuevas vulnerabilidades a lo largo del tiempo.
 - La necesidad de disponer de datos de forma segura y a tiempo.
- **Riesgos relacionados con la salida**
 - La necesidad de proteger el acceso a las impresoras multifunción y a los dispositivos de impresión para controlar la

salida y el direccionamiento de los datos confidenciales.

- La gestión del número y el tipo de salidas: copias, impresiones, faxes y digitalizaciones (incluida la digitalización de documentos a correo electrónico y la digitalización de documentos a carpeta).
 - La necesidad de una pista de auditoría y la responsabilidad de lo que se capturó e imprimió.
- **Riesgos relacionados con los datos**
 - Falta de definición y comprensión del ciclo de vida de los documentos en la empresa. Aquí se incluyen todos los pasos del ciclo

de vida de los documentos, desde su creación hasta su eliminación.

- Los almacenes de documentos no estructurados que dejan los sistemas de gestión de documentos abiertos a ataques y violaciones potenciales.
- Tareas manuales repetitivas vinculadas a documentos (electrónicos y en papel) en los que se podría añadir un destino erróneo por error y dar lugar a violaciones de la seguridad.
- Uso compartido no controlado de documentos esenciales para la empresa.
- Riesgo de corrupción de los datos sin control de versión.

Recomendaciones

Sobre la base del completo enfoque que aplicamos a la seguridad empresarial, Sharp puede garantizar el cumplimiento de las normativas más estrictas y crear soluciones que ayuden a las empresas a trabajar de forma más eficaz.

Sharp se ha propuesto garantizar el cumplimiento del RGPD en todos los aspectos de la seguridad de la información abordando las tres áreas principales de la seguridad empresarial: seguridad de las redes, seguridad de las salidas y seguridad de los documentos. Abarcamos los aspectos organizativos del tratamiento y la protección de los datos a través de nuestra completa cartera de productos y soluciones optimizadas, así como de los servicios profesionales relacionados de Sharp.

El desarrollo de una base sólida a través de toda la capa organizativa de una empresa nos permite influir en el comportamiento de los usuarios finales. Esto, junto con nuestros sistemas seguros y adecuadamente diseñados, ayuda a las empresas a cumplir el RGPD y ofrece las herramientas adecuadas para medir el riesgo, evitar los ciberataques y ofrecer conocimiento preciso relacionado con los usuarios.

Los servicios profesionales de Sharp abarcan todos los aspectos de la seguridad de los datos, incluida la forma en la que se gestiona la información identificable y personal en los sistemas empresariales, para ayudar a las empresas a cumplir el RGPD.

En la siguiente tabla se resumen las formas en la que Sharp puede ayudarle a cumplir el RGPD:

Reglamento General de Protección de Datos y Sharp		
Aspecto/área de seguridad	Productos y soluciones	Cumplimiento a través de
Seguridad de las redes	<ul style="list-style-type: none">• Impresoras multifunción de Sharp• Impresoras de Sharp• Gestor de dispositivos remotos de Sharp	<ul style="list-style-type: none">• Control de acceso de usuarios• Control de puertos• Control de protocolos• Control de servicios de red• Cifrado de datos• Sobreescritura de los datos
Seguridad de las salidas	<ul style="list-style-type: none">• Job Accounting II• PaperCut MF• SafeQ• Drive Image• Prism ScanPath	<ul style="list-style-type: none">• Control de acceso• Restricciones de funcionalidad• Registros de datos/informes de auditoría• Retención y supresión de registros de datos
Seguridad de los documentos	<ul style="list-style-type: none">• Cloud Portal Office• Drive DM• Docuware• Drive Image• Prism ScanPath	<ul style="list-style-type: none">• Control de acceso a bases de datos• Control de derechos de usuario• Seguimiento de versiones• Rastro de auditoría• Retención de documentos, incluida su eliminación• Registro de auditoría

Conclusión

Sharp puede ayudar a las organizaciones a establecer medidas de seguridad eficaces y metodologías de gestión efectivas para ayudar a cumplir el RGPD.

Entender, planificar, configurar y ejecutar las medidas y las funciones requeridas para cumplir el RGPD puede llevar mucho tiempo y presentar dificultades de implementación reales, especialmente porque cada empresa es diferente.

Sharp recomienda que los propietarios de las empresas y los gestores de TI dispongan de acceso a los documentos técnicos proporcionados en nuestra biblioteca para fines de orientación sobre las tres áreas de interés de la seguridad de la red, la seguridad de las salidas y la seguridad de los documentos:

www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/information-security.htm

En estos artículos se describirán los riesgos y cómo mitigarlos, y presentarán:

- Dispositivos de red seguros de Sharp
- Software de seguridad de Sharp que ayuda a proteger la captura de datos empresariales y la salida

- Software de seguridad de Sharp que ayuda a proteger los documentos electrónicos.

Por otra parte, los servicios profesionales de Sharp ofrecen asesoramiento y ayuda para desarrollar medidas de seguridad sólidas e introducir herramientas pertinentes para cada tipo de empresa y necesidad.

Para evitar posibles vulnerabilidades en otras áreas de su organización, podemos ayudarle a introducir medidas de seguridad adicionales desde la carpeta de Sharp, a fin de permitirle ofrecer protección de seguridad integral para cada aspecto de su empresa.

- Seguridad de las redes
- Seguridad de las salidas
- Seguridad de los documentos
- Conformidad con el RGPD

Glosario del RGPD³

Responsabilidad: el responsable del tratamiento vela por el cumplimiento sobre la base de los principios de protección de los datos. Deben ser capaces de demostrar los pasos que da la empresa para garantizar el cumplimiento.

Violación de la seguridad: cualquier destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a los datos de un interesado.

Responsable del tratamiento: el responsable es una persona jurídica, autoridad pública u otros organismos que, por si solos o en colaboración con otros, determina los fines y los medios del procesamiento de datos personales.

Supresión de datos: (también conocido como derecho al olvido) concede derecho al interesado para solicitar que el responsable del tratamiento borre sus datos personales.

Encargados del tratamiento de los datos: por «tratamiento» se entiende cualquier operación o conjunto de operaciones, realizadas sobre los datos personales o conjuntos de datos personales. El tratamiento abarca las operaciones realizadas con datos ya sean por medios automáticos o manuales. El tratamiento incluye las siguientes actividades: recopilación, registro, organización, uso, estructuración, almacenamiento, adaptación, recuperación, consulta, destrucción, etc. El encargado del tratamiento de los datos puede ser una organización o un proveedor externo que gestiona y trata los datos personales en nombre del responsable del tratamiento. Los encargados pueden tener obligaciones jurídicas, como el mantenimiento de los registros personales, y son responsables en caso de que se produzca una violación de los datos.

Autoridad de protección de datos: la autoridad nacional que protege la privacidad de los datos

Delegado de protección de datos: una persona designada que trabaja para asegurarse de que usted implementa y cumpla las políticas y los procedimientos establecidos por el RGPD.

Interesado: alguien cuyos datos personales son tratados por un responsable del tratamiento o encargado del tratamiento de los datos.

Datos personales: cualquier información directa o indirecta relacionada con una persona identificada que podría utilizarse como forma para identificarles, incluidos su nombre, número de ID, datos de ubicación o un identificador en línea.

Tratamiento: se refiere a cualquier actividad relacionada con los datos personales, desde la recopilación inicial hasta la destrucción final. Incluye la organización, alteración, consulta, uso, divulgación, combinación y conservación de los datos, ya sea de forma electrónica o manual.

Referencias

1. «UK firms could face £122bn in data breach fines in 2018», ComputerWeekly, octubre de 2016
2. «CEO Survey», PwC, 2017
3. «GDPR Glossary of Key Terms», High Speed Training, febrero de 2018

SHARP
Be Original.