RESUMEN DE LA SOLUCIÓN
RGPD de la UE

Cumplimiento del RGPD: ¿cómo adaptarse al nuevo reglamento?

ca technologies

Las empresas han cumplido las directivas y los reglamentos en materia de protección de datos durante más de dos décadas; pero el Reglamento General de Protección de Datos (RGPD), una reforma de la legislación vigente de la Comisión Europea sobre la protección de datos, tiene como objetivo endurecer y unificar esas leyes para los ciudadanos de la Unión Europea (UE). Los objetivos principales del RGPD son devolver a los ciudadanos el control de sus datos personales y simplificar el entorno normativo para las empresas internacionales. ¿Qué deben hacer las organizaciones que ya acatan la Directiva 95/46/CE para cumplir con el RGPD en lo que respecta a la tecnología?

Sección 1:

Introducción al RGPD

A partir del 25 de mayo de 2018, cualquier organización que trate datos personales de ciudadanos de la UE deberá cumplir el RGPD. Este reglamento introduce nuevos requisitos de protección de datos que afectarán a la mayoría de las empresas de todos los sectores. Aquellas que no lo cumplan podrían enfrentarse a multas administrativas de hasta 20 000 000 € o hasta un 4 % de la facturación global, lo que sea mayor.

Aunque el RGPD ha elevado el listón en materia de protección de datos, también busca armonizar las leyes de privacidad en toda la Unión Europea, lo que debería, en cierta medida, ayudar a las empresas a adoptar políticas y procesos de protección de datos más normalizados.

En la siguiente tabla se clasifican los requisitos del RGPD de manera general:

Categoría	Requisitos
Derechos de los interesados	1. Los interesados (consultar la definición núm. 1) tienen derecho a: a. acceder a sus datos. b. rectificar y borrar los datos (derecho al olvido), así como a limitar su tratamiento (consultar la definición núm. 2). c. la portabilidad de sus datos. d. oponerse al uso de sus datos.
Responsabilidad	2. Aquellos que tratan datos personales están obligados a: a. implementar las medidas técnicas y organizativas correspondientes para garantizar y demostrar que el tratamiento se realiza de acuerdo con el RGPD. b. obtener el consentimiento del interesado para ciertas actividades de tratamiento. c. implementar las políticas y los procesos de protección de datos apropiados. d. mantener un registro de las actividades de tratamiento. e. notificar a la autoridad de control ciertas violaciones de la seguridad de los datos personales. f. informar al interesado sobre ciertas violaciones de la seguridad de los datos personales. g. designar a un delegado de protección de datos cuando se considere oportuno.
Protección desde el diseño y por defecto	3. Implementación de medidas técnicas y organizativas apropiadas que: a. estén destinadas a aplicar de manera eficaz los principios relativos a la protección de datos, como la minimización de estos y la seudonimización, y a integrar las medidas de seguridad necesarias para el tratamiento. b. por defecto, no permitan acceder a los datos personales a un número indefinido de personas físicas sin la intervención del individuo.
Notificación de violaciones de seguridad de los datos	4. En el caso de que se produzcan violaciones de la seguridad de los datos personales (consultar la definición núm. 7): a. los responsables del tratamiento deben informar de lo ocurrido a la autoridad de control en no más de 72 horas después de haber detectado la infracción. b. los encargados del tratamiento (consultar la definición núm. 8) avisarán al responsable del tratamiento sin demoras indebidas después de tener constancia de ello. c. se comunicarán las infracciones de datos al interesado (se aplican excepciones).

Categoría	Requisitos
Anonimato y seudonimización	5. Se deben aplicar técnicas de seudonimización y anonimización: a. al tratar datos personales como parte de los principios de la protección de datos desde el diseño y por defecto. b. en los datos archivados con fines estadísticos o destinados al interés público y la investigación científica o histórica.
Transferencias transfronterizas de datos y normas corporativas vinculantes	6. Los datos personales están sujetos a restricciones de transferencia: a. a países fuera del Espacio Económico Europeo (EEE). b. si no están registrados como "adecuados"; en este caso, las normas corporativas vinculantes (consultar la definición núm. 9) y las cláusulas contractuales tipo (o cláusulas modelo) emitidas por la Comisión Europea siguen siendo instrumentos válidos para cumplir con las restricciones de la UE en materia de transferencia de datos (consultar la definición núm. 10). c. como el escudo de la privacidad UE-EE. UU. (consultar la definición núm. 11).
Certificaciones, códigos de conducta y sellos	7. Las organizaciones podrán acogerse a mecanismos de certificación con el fin de demostrar la existencia de ciertas medidas de seguridad y el cumplimiento de estas.

Definiciones tomadas del RGPD

1. **Interesado:** persona física identificable, es decir, toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
2. **Limitación del tratamiento:** marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
3. **Responsable del tratamiento:** persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el derecho de la Unión o de los Estados miembros.
4. **Autoridad de control:** autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.
5. **Delegado de protección de datos:** será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.
6. **Seudonimización:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
7. **Violación de la seguridad de los datos personales:** toda violación de la seguridad 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.

8. **Encargado del tratamiento:** persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
9. **Normas corporativas vinculantes:** políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Definiciones adicionales que conciernen al RGPD

10. **Países adecuados:** los datos personales pueden circular de los 28 países de la UE y de tres países miembros de EEE (Noruega, Liechtenstein e Islandia) a un tercer país sin necesidad de tomar medidas de seguridad adicionales.

    Hasta ahora, la Comisión ha reconocido a **Andorra, Argentina, Canadá** (organizaciones comerciales), **Islas Feroe, Guernesey, Israel, Isla de Man, Jersey, Nueva Zelanda, Suiza y Uruguay** como países con protección adecuada. (Consulte http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

11. Para transferir datos personales de la UE a los EE. UU., se dispone de distintas herramientas, como las cláusulas contractuales, las normas corporativas vinculantes y el escudo de la privacidad. Para utilizar el escudo de la privacidad, las empresas estadounidenses deben primero afiliarse a este marco en el Departamento de Comercio de los EE. UU. Las obligaciones que contraen las empresas afiliadas al escudo de la privacidad se recogen en los "principios de privacidad". El citado Departamento es responsable de gestionar y administrar el escudo de la privacidad y de velar por que las empresas cumplan sus compromisos. Para poder obtener una certificación, las empresas deberán tener una política de privacidad acorde con los principios de privacidad y renovar su "autocertificación" en el escudo de la privacidad con carácter anual. De no hacerlo, dejarán de poder recibir y usar los datos personales de la UE con arreglo a ese marco. Se puede encontrar una lista de empresas que se autocertifican en el escudo de la privacidad en el sitio web del Departamento de Comercio (https://www.privacyshield.gov/welcome). También se puede consultar una lista de las empresas que han dejado de pertenecer al escudo de la privacidad.

Sección 2:

Requisitos

Derechos de los interesados

Este es uno de los temas más importantes de este reglamento. El listón se ha elevado y se han incluido nuevos derechos que afectarán profundamente a la forma en que el equipo de TI tendrá que tratar y controlar los datos personales. Es importante entender que el RGPD sustituye a la **directiva sobre protección de datos** (Directiva 95/46/CE) y su objetivo es endurecer y unificar la protección de datos para las personas dentro de la UE.

Aunque los derechos tradicionales de acceso (artículo 15), rectificación (artículo 16), supresión (artículo 17) y oposición (artículo 21) siguen siendo en gran medida los mismos, se ha incluido un nuevo derecho: el derecho a la portabilidad de los datos (artículo 20) y algunas modificaciones del derecho a la supresión al incluir el concepto "derecho al olvido" (artículo 17) y el derecho a la limitación (artículo 18). Estos derechos son fundamentales y universales en toda la UE. Según la directiva anterior, cada Estado miembro podía interpretarlos de manera diferente, lo que dificultaba que los interesados reivindicaran sus derechos.

Las organizaciones se encuentran con múltiples desafíos y alguno de los nuevos derechos, como la portabilidad de los datos, que permite a las personas obtener y reutilizar sus datos personales para sus propios fines en diferentes servicios, podría ser el más importante. De ahí la necesidad de adoptar un modelo que ayude a las empresas a satisfacer las necesidades actuales y futuras.

Cuando tenemos que hacer que las aplicaciones actuales que incluyen datos personales cumplan con este nuevo reglamento y, al mismo tiempo, evitar incurrir en el coste de modificar las aplicaciones existentes, solo existe una respuesta: las API.

La adopción de un modelo basado en API para acceder a los datos es la base de una arquitectura preparada para el futuro que permita a una organización adoptar tanto este como reglamentos futuros, precisamente porque las API se pueden proteger, controlar y mejorar implementando las soluciones de software apropiadas.

También se ha endurecido el requisito para obtener el consentimiento del interesado, por lo que las organizaciones deberán gestionar de una manera diferente su relación con él. Las identidades digitales y su gestión, la gobernanza y el control del acceso desempeñarán un papel importante para aquellos que deseen cumplir satisfactoriamente el reglamento.

Para adherirse al RGPD, las organizaciones tendrán que adoptar nuevos canales de comunicación con los interesados con el fin de garantizar que puedan ejercer correctamente sus derechos fundamentales. Esto significa que deben aplicarse medidas técnicas para permitir el acceso seguro y adecuado de los interesados a sus datos. También se deberán crear nuevos canales que permitan la portabilidad de los datos, de modo que los interesados puedan ejercer el derecho a esta e iniciar el proceso de transferencia de sus datos al tercero designado. Por lo tanto, es crucial implementar unas medidas de seguridad y unos controles de acceso adecuados en estas nuevas puertas de enlace que atravesarán los datos.

Aunque pueda parecer simple, se podría acceder a los datos personales a través de diversos sistemas de archivos y servidores, por lo que deben aplicarse medidas de descubrimiento, análisis y clasificación apropiadas en las infraestructuras de TI antes incluso de aplicar políticas de protección de datos.

Responsabilidad

Aparecen requisitos técnicos por todo el reglamento, pero todo se reduce a la responsabilidad del responsable o encargado del tratamiento de datos. En otras palabras: cuando ocurren accidentes, algo casi inevitable, la autoridad reguladora busca la prueba de que la empresa en proceso de investigación ha implantado los controles organizativos y técnicos adecuados para garantizar el tratamiento apropiado de los datos personales según el reglamento. Las organizaciones deben demostrar que han implementado los controles y medidas de TI requeridos por la norma; además, deben monitorizar todas las decisiones que se han tomado e informar sobre ellas en todo momento. No demostrar todo lo anterior determinará en gran medida la cuantía de las multas administrativas. Esto queda claramente subrayado en el artículo 83.

En el mundo híbrido de TI actual, no siempre resulta sencillo determinar a quién pertenecen determinados datos de nuestros sistemas. Esto podría suponer un problema para las organizaciones, que tendrán que explorar y encontrar datos personales en todo el espectro de plataformas existentes. Además, tendrán que implementar soluciones que ayuden no solo a identificar la información, sino que también favorezcan el control y el seguimiento del uso de estos datos personales durante todo el ciclo de vida. Lo más probable es que, en caso de accidente, no haber implementado controles técnicos avanzados en estas áreas haga que no se cuente con el beneplácito de la autoridad reguladora.

Protección desde el diseño y por defecto

En el considerando 2 del artículo 25, se establece: “El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas”. Asimismo, el artículo 30 ordena el registro de las actividades de tratamiento.

Además, en el artículo 32, “Seguridad del tratamiento”, sección (b), se precisa “(...) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento”. En la sección (d) se establece la existencia de “(...) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento”.

Este es un tema muy amplio que requerirá un enfoque holístico que incluya procesos de desarrollo de software, como pruebas, preguntas y respuestas, y lanzamientos de nuevas versiones. Todas estas disciplinas de TI requerirán una capa integrada de controles de seguridad para garantizar que únicamente las personas indicadas pueden acceder a los datos para los fines específicos para los que se recopilaron.

Notificación de violaciones de seguridad de los datos

Del principio de responsabilidad ya explicado se deriva la obligación de los responsables y encargados del tratamiento de los datos de denunciar determinadas infracciones que afecten a los datos personales. Los tipos de infracciones que requieren notificación se describen en los artículos 33 y 34.

En el artículo 33 se establece la obligación de notificar las violaciones de datos a la autoridad de control competente y en el artículo 34 se expone lo mismo en lo que respecta la comunicación al interesado. Es importante señalar que, de conformidad con el artículo 34.3, las organizaciones se encuentran exoneradas de la obligación de comunicar el accidente al interesado si:

- el responsable del tratamiento **ha adoptado medidas de protección técnicas y organizativas apropiadas** y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
- el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1.

La comunicación de una violación de la seguridad de los datos de un encargado a un responsable del tratamiento debe producirse sin demoras indebidas, y la de un encargado a la autoridad de control, en no más de 72 horas después de tener constancia de ella. La notificación debe incluir información sobre quién hizo qué y cuándo, así como las acciones y medidas tomadas para mitigar cualquier efecto adverso posible.

Anonimato y seudonimización

El RGPD introduce nuevos conceptos relacionados con los principios que deben aplicarse al gestionar y tratar datos personales. La protección de los datos personales y la devolución de su control al interesado son el principal objetivo del reglamento, por lo que en él se mencionan algunas técnicas de protección de este tipo de datos.

En el capítulo II (“Principios”), podemos ver que la intención es reforzar la manera en que se tratan los datos personales (“minimización de datos”) y mantenerlos de una forma que permita la identificación justa y necesaria del interesado. Además, los datos personales se deben tratar de una manera que garantice la seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, la destrucción o el daño accidentales, con las medidas técnicas y organizativas apropiadas (“integridad y confidencialidad”).

Transferencias transfronterizas de datos y normas corporativas vinculantes

Al igual que en la directiva, el artículo 45 del reglamento establece restricciones en las transferencias internacionales de datos personales a países no adecuados fuera de la UE. En el considerando 2 del artículo 46, se establecen las medidas de seguridad apropiadas que deben existir para la transferencia de datos sin una autorización específica de una autoridad de control.

Las normas corporativas vinculantes (artículo 47) y las cláusulas contractuales tipo (o cláusulas modelo) emitidas por la Comisión Europea siguen siendo instrumentos válidos para cumplir con las restricciones de la UE en materia de transferencia de datos. El uso de estos mecanismos de transferencia para fines intragrupo debería volverse una tarea más sencilla, ya que se han eliminado ciertos requisitos de autorización existentes. Consulte las definiciones 10 y 11 con respecto a las implicaciones del escudo de la privacidad UE-EE. UU.

El control de quién tiene acceso a los datos es fundamental para cumplir con este requisito. Las organizaciones tendrán que realizar campañas de certificación de acceso de manera regular para validar que los derechos de acceso de sus usuarios son correctos en cualquier momento. El delegado de protección de datos designado necesitará capacidades de generación de informes avanzadas en diferentes áreas de seguridad de TI para garantizar la conformidad.

Además, se necesitarán competencias para restringir el envío de documentación que contiene datos personales fuera de la organización con objeto de garantizar que nadie envía de forma involuntaria archivos considerados como relacionados con el GDPR a terceros que no están autorizados.

Certificaciones, códigos de conducta y sellos

Las organizaciones tienen derecho a acogerse a mecanismos de certificación con el fin de demostrar la adopción de las medidas de seguridad correspondientes. De hecho, en el artículo 42 se pide a los Estados miembros, a las autoridades de control y a otras instituciones de la UE que establezcan mecanismos de certificación, sellos y marcas de protección de datos con el fin de demostrar el cumplimiento del reglamento. En el artículo 42, también se menciona un futuro marco para una certificación común, el Sello Europeo de Protección de Datos, que garantizaría un estándar de certificación común en toda la UE, con el consiguiente aumento de la coherencia y la claridad para los ciudadanos.

Sección 3:

Cómo puede ayudar CA

El cumplimiento del reglamento requerirá un enfoque exhaustivo, que incluya la asistencia de los departamentos jurídicos y de TI y, en algunos casos, de las empresas consultoras, para las evaluaciones y revisiones íntegras del propio reglamento, así como para la comprobación de los procesos organizativos. Como una empresa de software innovadora y líder en la economía de las aplicaciones, CA Technologies está guiando a las organizaciones a través del proceso de la transformación digital y puede suministrar un amplio conjunto de soluciones de software para ayudar a las organizaciones a transitar por todos los caminos de la conformidad.

CA proporciona ayuda a las organizaciones tecnológicas para lograr el cumplimiento del RGPD y para implementar los controles necesarios exigidos por el reglamento para cumplir con la filosofía general del principio de seguridad desde el diseño y por defecto que en él se persigue.

Lo que distingue a CA de los proveedores de tecnología puntual es que nuestras soluciones de productos llegan a casi todos los puntos del ciclo de vida de los datos de una organización. Las organizaciones pueden usar la combinación de las soluciones de CA para proteger el acceso a los datos, gestionar y controlar el acceso de los usuarios, y prevenir el acceso no autorizado a datos personales de personas ajenas a la organización y del personal interno para garantizar el cumplimiento del nuevo reglamento protegiendo los derechos de los interesados. CA Technologies cuenta con las herramientas y la experiencia necesarias para guiar a las organizaciones a través de todo el proceso.

Además, ofrece una completa y segura estrategia de DevOps, que no solo aumenta la velocidad de desarrollo y entrega de aplicaciones, sino que garantiza la seguridad de estas y de todo el ciclo de vida de entrega de software. Nuestras completas soluciones de seguridad incluyen la gestión de API, la seguridad del mainframe y varios componentes de nuestro amplio conjunto de programas de seguridad de IAM. Para obtener más información sobre estas soluciones de seguridad de IAM, visite ca.com/iam.

CA Technologies en la clasificación y localización de datos

Aunque las organizaciones puedan creer que saben dónde se almacenan y controlan los datos personales, la realidad es que estos se distribuyen por toda la empresa y distintas personas acceden a ellos, los utilizan y los transforman ampliamente de diferentes maneras, por lo que los controles basados en aplicaciones no son suficientes para cumplir con el reglamento.

Además, la directiva anterior se centraba más en la protección de los ficheros que contenían datos personales y en el almacenamiento de la información, mientras que el nuevo reglamento se centra en el tratamiento de los datos. Este es el resultado de la nueva era digital, en la que los datos se transforman, se añaden, se alimentan y se tratan a velocidades muy altas. Con el análisis moderno de grandes datos, partes de datos en apariencia no relacionadas podrían combinarse con datos personales que quedan sujetos al reglamento.

Por eso es muy importante adoptar un enfoque de defensa en profundidad para la protección de los datos personales, de manera que podamos aplicarle diferentes niveles de control.

Empecemos con la identificación y clasificación de los datos, así como la comprensión de la ubicación de los datos personales en nuestra infraestructura. Si los datos personales circulan fuera de los canales y flujos asignados, es importante entender esto y evaluar el riesgo asociado.

Entender dónde se albergan los datos personales y quién en la organización dispone de acceso a ellos es uno de los principios fundamentales del RGPD.

CA Data Content Discovery

En la economía de las aplicaciones, el mainframe se encuentra cada vez más conectado con el resto del centro de datos, más disponible incluso para usuarios ocasionales y sujeto al reglamento de protección de datos. Los conjuntos de datos se copian de la producción para su desarrollo o prueba, luego se descartan; otros quedan huérfanos cuando sus dueños abandonan la empresa. Además, la inyección de datos no estructurados dirigida por el usuario a través de UNIX® System Services puede haber dejado grandes volúmenes de datos regulados o confidenciales ocultos en el mainframe, lo que representa el daño monetario y reputacional posible que sufriría la empresa si se pierde el control.

El mainframe aún alberga más del 70 % de los datos fundamentales. De hecho, si hoy usó su tarjeta de débito bancaria, compró un billete de avión o llamó por teléfono, es probable que haya pasado por un mainframe; sin embargo, la economía de las aplicaciones ha añadido nuevos riesgos al mainframe, está interconectada con casi todas las aplicaciones y las infracciones de datos se pueden ver con frecuencia en las noticias. Sería catastrófico para una organización que el mainframe y sus datos regulados o confidenciales quedasen en entredicho.

En el mundo híbrido de TI actual, no siempre resulta sencillo determinar qué datos de nuestros sistemas pertenecen al grupo afectado por el reglamento. Con el fin de hacerlo de una manera adecuada y sistemática, **CA Data Content Discovery** encuentra, clasifica y protege los datos confidenciales del mainframe con el fin de cubrir el espectro completo de las plataformas existentes. La solución incluye políticas predefinidas de datos personales que ayudan no solo a identificar la información, sino también a controlar y realizar el seguimiento del uso que le dan los usuarios, como se establece en varios artículos. El análisis se realiza 100 % en la plataforma del mainframe, por lo que los datos no se duplican fuera de esta para llevarlo a cabo. Esto permite a las organizaciones identificar y proteger con rapidez los datos antes de que se produzca una infracción.

CA Identity Suite

En el considerando 2 del artículo 25, se establece: “El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas”. Asimismo, el artículo 30 ordena el registro de las actividades de tratamiento. Esto significa que debe implementar una solución que gestione y controle el acceso apropiado de los empleados a los datos personales para reducir la exposición innecesaria de estos últimos.

CA Identity Suite le ayuda a gestionar y controlar el acceso de los usuarios a las aplicaciones empresariales y a los datos subyacentes. La solución es compatible con la conformidad total de este requisito, ya que proporciona informes sobre quién tiene acceso a qué, y puede realizar y gestionar campañas de certificación de acceso para ayudar a que la organización siga cumpliendo con el reglamento.

Un enfoque común para alcanzar la conformidad consiste en validar con asiduidad que los usuarios disponen de acceso adecuado a los recursos corporativos. Durante la certificación de acceso, los gestores deben revisar las listas de los privilegios de los informes directos y confirmar o denegar la necesidad de este acceso.

CA Identity Suite hace que este proceso sea simple e intuitivo, lo que aumenta la satisfacción y la productividad del usuario. La personalización de un proceso de certificación en relación con las necesidades específicas de una organización es fundamental para validar con eficacia el acceso y fomentar la participación en el proceso. CA Identity Suite puede solicitar la revisión desde varias perspectivas, por ejemplo, la de los gestores de usuarios, los propietarios de los recursos o los ingenieros de roles. Los procesos de certificación, conocidos como campañas, se pueden llevar a cabo para cada una de estas perspectivas mediante el uso de planificaciones, flujos de trabajo

y aprobadores distintos. Asimismo, se pueden llevar a cabo varias campañas al mismo tiempo, cada una de ellas centrada en partes de la organización (por ejemplo, los usuarios de una unidad de negocio específica) o resaltar tipos de accesos distintos (por ejemplo, solo las presuntas asignaciones o los accesos obtenidos fuera del modelo de roles). CA Identity Suite incluye flujos de trabajo y controles administrativos sólidos para contribuir a garantizar el progreso de las campañas de conformidad con los requisitos. Eso incluye notificaciones por correo electrónico, alertas de recordatorios y procesos de escalación para la solicitud de aprobaciones de gestores de nivel superior. Además, cuando se detectan diferencias y se precisan cambios en los derechos de acceso, los procesos de corrección se pueden activar asignando tickets de corrección a los propietarios adecuados o mediante la integración con CA Identity Manager.

En este reglamento, hay un actor clave, el responsable de la protección de datos; las organizaciones deben nombrar a esta figura. En este papel, serán cruciales las soluciones tecnológicas que sustentan y demuestran todos los controles de seguridad que la organización ha puesto en marcha para proteger los datos personales. Las funciones de generación de informes de las soluciones de CA ayudarán al responsable de la protección de datos a demostrar cómo cumple la organización el reglamento y serán relevantes para la elaboración de las evaluaciones de impacto sobre la protección de datos descritas en el artículo 35.

Asimismo, CA Identity Suite incluye análisis integrados de procesos de identidad que proporcionan información detallada y fácil de procesar que destaca el funcionamiento de los procesos de identidad clave (como la incorporación de usuarios). Estos análisis ayudan a identificar y solucionar los cuellos de botella, además de a garantizar que se cumple con los acuerdos de nivel de servicio. CA Identity Governance incluye un conjunto adicional de informes y cuadros de mandos listos para usar y admite consultas ad hoc para requisitos forenses. Los informes varían en el nivel de información comercial y técnica facilitada con el fin de satisfacer las necesidades de los distintos tipos de usuarios. Esto incluye informes separados para los gestores empresariales, los ingenieros de roles, los responsables de cumplimiento, los auditores y el personal de TI, por ejemplo.

CA Test Data Management

El reglamento lleva camino de engendrar amplias implicaciones para el tipo de datos que se pueden utilizar en entornos de no producción. Las organizaciones tendrán que entender exactamente qué datos tienen y quién los utiliza, y deben poder restringir su uso a las tareas para las que se ha dado consentimiento. Una manera de evitar la exposición de los datos personales a entornos de prueba es, en primer lugar, no proporcionarlos, incluso de forma enmascarada. La generación sintética de datos ofrece una técnica que podría permitir a las organizaciones transitar a entornos de pruebas totalmente virtualizados.

Al probar y desarrollar software, los datos pueden terminar extendiéndose a través de pruebas y desarrollos, así como en entornos complejos. Los probadores podrían copiar datos a su entorno para un uso determinado, pero las organizaciones deben saber cuánto tiempo se usan los datos y que se usan con consentimiento y con un propósito legítimo. La elaboración de perfiles de datos de **CA Test Data Manager** puede ayudar con este punto clave de la conformidad identificando exactamente dónde se almacenan los datos confidenciales en toda la empresa y usando el análisis estadístico para encontrar datos personales almacenados en múltiples formatos de archivo y aplicaciones. Con una vista de cubo para crear una imagen precisa de los datos, CA Test Data Manager identifica información confidencial reflejada en sistemas, componentes o aplicaciones relacionados. Los filtros personalizados, basados en las matemáticas, permiten filtrar los datos en un nivel granular para identificar cada petición de información relacionada con una persona. Estos datos pueden incluir números de tarjetas de crédito, direcciones de correo electrónico, direcciones de domicilios particulares e información similar, lo que ayuda a las organizaciones a cumplir con el derecho a la portabilidad de los datos. La detección de datos ofrecida por CA Test Data Manager es completamente verificable, por lo que las organizaciones pueden demostrar la aplicación de los controles adoptados para la conformidad.

CA API Management

Cuando tenemos que hacer que las aplicaciones actuales que incluyen datos personales sean compatibles con este nuevo reglamento, mientras que al mismo tiempo evitamos incurrir en el coste de modificar las aplicaciones existentes, solo existe una respuesta: las API.

El conjunto de programas de **CA API Management** simplifica el modo en el que las empresas se enfrentan a los retos del uso compartido de la información en la economía de las aplicaciones. La solución combina funcionalidades avanzadas para la integración de back-end, la optimización en dispositivos móviles, la organización de la nube y la gestión de desarrolladores, y es única en su capacidad de lidiar con la totalidad de estos requisitos de la gestión de API empresariales. Con el uso de CA API Management, las organizaciones pueden ayudar a demostrar el cumplimiento del reglamento sin necesidad de cambiar las aplicaciones actuales. Además, **CA Live API Creator** puede utilizarse para crear nuevas API que incluirán los controles adecuados y expondrán la información necesaria a terceros.

Por ejemplo, utilizando las soluciones de CA API Management, podemos evitar modificar aplicaciones, lo que es arriesgado y costoso, y será capaz de controlar los comportamientos desde una solución orientada a reglas y políticas. De esta manera, la organización puede incorporar reglas para obtener el consentimiento con el aviso a los usuarios sobre la información solicitada en los artículos 15 y 20 documentando, a través de **CA API Developer Portal**, cómo se puede acceder a los datos. **CA API Gateway** proporciona estos controles de acceso de seguridad.

Para comprender las ventajas de este enfoque, puede calcular el coste de modificar todas las aplicaciones que gestionan actualmente los datos personales en su organización, en comparación con el gasto de disponer de una interfaz única y estandarizada que también podría utilizarse para cumplir con otras normativas del sector.

CA Privileged Access Manager

La explotación de cuentas de usuario con privilegios constituye el factor de riesgo más frecuente en la mayoría de las infracciones de datos, tanto si se han obtenido de forma malintencionada como si las emplea un usuario válido de forma inadecuada. A medida que el entorno se hace cada vez más complejo, también lo hace el reto de defenderse contra ataques cada vez más sofisticados y dañinos. La gestión de accesos con privilegios de CA ofrece una solución completa, que proporciona controles basados en la red y en el host para la nube empresarial e híbrida.

Aunque las organizaciones puedan verse tentadas a creer que la protección del acceso a los datos a través de controles de acceso basados en aplicaciones podría ser suficiente, la realidad es que la mayoría de las infracciones de datos ocurren explotando cuentas de usuario con privilegios, de manera que rodean los controles de acceso válidos y los vuelve inútiles. Esta es la razón por la cual las empresas necesitan implementar controles de seguridad para gestionar y controlar el acceso con privilegios.

CA Privileged Access Manager (CA PAM) es una solución probada de implementación sencilla que permite gestionar el acceso con privilegios en entornos físicos y virtuales, además de en la nube. CA PAM está disponible como un dispositivo de hardware reforzado y montado en rack, un dispositivo virtual abierto (OVA) o una imagen de máquina de Amazon (AMI). Esta solución mejora la seguridad protegiendo las credenciales administrativas confidenciales, controlando el acceso de los usuarios con privilegios, aplicando políticas de forma proactiva, y monitorizando y grabando la actividad de los usuarios con privilegios en todos los recursos de TI.

Un componente de CA PAM, **CA Privileged Access Manager Server Control** proporciona una protección integral para sus servidores más importantes con controles potentes y exhaustivos sobre el acceso al sistema operativo y las acciones de los usuarios con privilegios. Es capaz de reforzar los controles de acceso en las potentes cuentas de superusuario nativas, como el usuario raíz de Unix y Linux® y el administrador de Microsoft® Windows®. Esta solución basada en host y que opera en el sistema controla, monitoriza y audita la actividad de los usuarios con privilegios, de manera que mejora la seguridad y simplifica la auditoría y la conformidad.

La combinación de CA Privileged Access Manager Server Control para la protección de los servidores con CA Privileged Access Management proporciona la solución más completa para gestionar usuarios con privilegios y el acceso de la organización.

CA Single Sign-On

La economía de las aplicaciones ha modificado la forma en que las empresas interactúan con sus clientes. Los usuarios exigen disponer de acceso a servicios y datos en línea en cualquier momento y lugar, y esperan disfrutar de una experiencia de usuario impecable y uniforme en diversos dispositivos y canales de acceso. Con respecto al RGPD, las organizaciones necesitan equilibrar la facilidad de acceso con los datos a los que se puede acceder. ¿Cómo se asegura de que solo las personas adecuadas están accediendo al contenido confidencial y exclusivamente cuando está legalmente permitido? Por ejemplo, un ciudadano de la UE tiene derecho a ver sus datos personales; sin embargo, ¿pueden acceder y ver sus datos si inician sesión desde un país fuera de los Estados Unidos? ¿Qué pasa con un empleado de la organización? Tal vez puedan acceder a estos mismos datos al iniciar sesión desde los Estados Unidos, pero no cuando accedan desde un país de fuera.

CA Single Sign-On puede gestionar estos retos proporcionando a los empleados, clientes, partners y proveedores un inicio de sesión único para las aplicaciones en línea, independientemente del lugar en el que se implementen, del tipo de dispositivo utilizado para acceder a ellas o de cómo se autentica el usuario en el sitio, directamente, a través de redes sociales o federados desde un sitio de partner. Además, la solución también mejora la seguridad gracias a un nivel de política común que reduce la posibilidad de que surjan deficiencias en las políticas de acceso.

El RGPD requiere que las organizaciones concedan acceso a los usuarios, pero que limiten el número de personas que puedan acceder a estos datos personales. Una solución de gestión de acceso integral como CA Single Sign-On puede proporcionar los controles de acceso web adecuados para ambos tipos de usuarios desde un punto centralizado. Externalizar esta seguridad desde dentro de las aplicaciones es compatible con el concepto de seguridad desde el diseño en las DevSecOps.

CA Directory

El RGPD presenta una revisión importante a la legislación vigente sobre la protección de datos, y aunque la mayoría de estos puedan existir en los mainframes de grandes empresas, una cantidad significativa de los datos también reside en directorios. Las organizaciones se están volviendo cada vez más dependientes de las aplicaciones para dispositivos móviles y en línea para proporcionar servicios importantes a los usuarios. Además, se enfrentan a retos de rendimiento y disponibilidad debido a problemas con la infraestructura de directorios subyacentes, entre los que se incluyen los siguientes:

- **El crecimiento explosivo:** el auge de las identidades de usuarios, los dispositivos y la habilidad de mantener la capacidad de respuesta necesaria para una experiencia de usuario superior desafía muchos repositorios heredados.
- **Las unidades aisladas de identidad:** diversos directorios se implementaron por diferentes unidades de negocio a lo largo del tiempo, lo que ahora está causando retos, entre los que se incluyen, sin que sirva de limitación, la experiencia insuficiente del usuario, el riesgo de seguridad y el aumento de los gastos de explotación.
- **Los nuevos requisitos:** los requerimientos de seguridad evolucionan desde la autenticación de usuario sencilla hasta el seguimiento del inicio de sesión pormenorizado y la información personalizada asociada a las operaciones empresariales dinámicas.

Como resultado, muchos clientes buscan elevar la infraestructura de la gestión de identidades y accesos, lo que les lleva a migrar a un servicio de directorio de última generación que ofrece un mejor rendimiento a un coste menor de propiedad. Pero el RGPD también añade otro giro interesante en sus criterios de evaluación. El servicio de directorio de última generación debería admitir la posibilidad de particionar el árbol de directorios en varios servidores, lo que permitiría a la organización almacenar físicamente los datos personales. Además, debería permitirle determinar de forma selectiva qué datos obtienen la replicación en diferentes nodos para prohibir que salgan de una región específica.

CA Cleanup

CA Cleanup identifica las cuentas que no se usan partiendo de un límite de tiempo específico y genera comandos que eliminan los ID de usuario, derechos, permisos y conexiones de grupo o perfil que los usuarios tienen, pero no usan. Estas soluciones ayudan de forma eficaz a resolver la acumulación de derechos de acceso excesivos y obsoletos que se producen en un archivo de seguridad con el tiempo (un requisito clave para cumplir con muchas normativas). CA Cleanup se implementa completamente en un día y puede:

- identificar y eliminar usuarios individuales, derechos y grupos de acceso que ya no se utilizan.
- reconocer los derechos (como permisos y reglas) que realmente se utilizan y crear comandos para eliminar los que no se usan. Esto incluye los recursos definidos por el usuario.
- determinar los ID de usuario realmente utilizados y crear comandos de eliminación para los que no se usen. Esto se basa en el uso real de la seguridad, no en las fechas de último uso notificadas, que a menudo no son fiables.
- producir informes que detallen tanto los derechos que se utilizan como los que no.
- generar comandos para ejecutar o restaurar la limpieza de la seguridad.

Al usar CA Cleanup con CA ACF2™, podrá identificar los ID de conexión activos frente a los inactivos, los conjuntos de reglas y las reglas. Esto incluye las clases de recursos definidas por el usuario, la fuente NEXTKEY y las reglas de destino. Al utilizar CA Cleanup con CA Top Secret®, podrá identificar los ACIDS activos frente a los inactivos, los permisos y las conexiones de perfil. Esto incluye recursos definidos por el usuario y el registro de todos los elementos. Al usar CA Cleanup con IBM® RACF®, podrá identificar los ID de usuarios activos o inactivos, los perfiles, los permisos, las conexiones de grupo y grupos de recursos IBM RACF. El uso del permiso se detecta a cada entrada específica de la lista de acceso, ya sea discreta, genérica o condicional.

CA Compliance Event Manager

CA Compliance Event Manager proporciona una monitorización proactiva de la seguridad a la vez que ayuda a reducir el coste, la complejidad y el esfuerzo requerido para monitorizar e informar sobre la seguridad y la conformidad del mainframe. Con múltiples componentes diseñados para procesar información sobre eventos externos del gestor de seguridad y monitorizar sin problemas los sistemas para realizar cambios en los recursos más importantes, CA Compliance Event Manager alerta, inspecciona y protege los datos esenciales del mainframe para proporcionar a los implicados clave notificaciones en tiempo real de posibles infracciones de la seguridad.

Una gran parte de la conformidad del RGPD se centrará en cómo se recopilarán los datos en el futuro; pero un énfasis sustancial recaerá en los negocios de los datos que ya tienen. Con tantos mainframes que contienen datos de generaciones anteriores, una auditoría manual de estos resulta totalmente irrealista. Ahí es donde entra en juego CA Compliance Event Manager, que ofrece tres funciones primordiales:

- **Alerta:** la solución supervisa sistemas completos de registros de seguridad, puntos de configuración de seguridad, conjuntos de datos del sistema y controles de configuración de IBM z/OS® con notificaciones inmediatas y en tiempo real de infracciones, accesos y actividades de cambio pertinentes a sistemas y recursos de seguridad fundamentales. Esto proporciona a los implicados información inmediata y esencial sobre el potencial y la magnitud de la exposición de los datos en el mainframe para prevenir de forma proactiva eventos de seguridad negativos.
- **Inspección:** una vez identificadas las amenazas de la exposición de los datos, CA Compliance Event Manager genera información avanzada de auditoría y conformidad que no se encuentra disponible en los informes de seguridad estándar. A través de la sofisticada recopilación de datos, la auditoría exhaustiva y la compatibilidad del almacén de datos, la solución permite a los usuarios reproducir todos los eventos de seguridad, realizar análisis forenses con registros de datos de seguridad sin procesar y buscar, filtrar y analizar datos históricos registrados con recuperación automática de cintas; todo esto proporciona información más detallada sobre cuestiones de seguridad y conformidad, y una postura frente al riesgo mejorada.
- **Protección;** una vez que haya recibido las notificaciones en tiempo real e inspeccionado las exposiciones de los datos para priorizar con rapidez cualquier problema, ha mejorado el control de los datos del mainframe y se encuentra mejor preparado para saber quién tiene acceso a los datos afectados por el RGPD, desde empleados hasta clientes y partners del negocio, tanto del pasado como del presente, y puede asegurarse de que se apliquen los permisos adecuados.

Sección 4:

Conclusión

El cumplimiento del RGPD se puede lograr a través de una combinación de personas, procesos y tecnología. En este documento se han descrito soluciones que pueden ayudar a las organizaciones con su periplo por el RGPD; sin embargo, puede extender esa protección y reforzar los controles de seguridad aún más mediante una autenticación fuerte y de riesgo o a través de la automatización de la carga de trabajo para la automatización del tratamiento de datos personales, lo que le ayuda a cumplir con el RGPD y mandatos similares. Las normativas tienden a establecer las normas mínimas que se requieren, pero en la economía de las aplicaciones, las empresas abiertas deben garantizar la debida diligencia para proteger uno de los activos más importantes y fundamentales: la información privada de los clientes.

Es importante no ver el RGPD de manera aislada, sino en el contexto de muchas otras leyes y reglamentos, entre los que se incluyen los específicos del sector, que se centran en proteger los datos en la economía de las aplicaciones. Los controles fuertes para la seguridad y la protección de los datos, y cómo se usan y se accede a ellos, serán fundamentales para las organizaciones que buscan cumplir con dichas leyes y normativas, independientemente del sector.

Consulte estos recursos para obtener más información sobre las soluciones de CA y el RGPD:

- Libro electrónico: "Complying with the EU General Data Protection Regulation. The Implications for Test Data Management".
- Libro blanco: "EU General Data Protection Regulation (GDPR): Are you ready for it?".

Comuníquese con CA Technologies en ca.com/es

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el núcleo de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA colabora con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles y entornos de mainframe y distribuidos. Para obtener más información, visite ca.com/es.

CS200-255926_0217