2019

White paper series
Edición 6

– CLASIFICACIÓN –
DE DATOS

OEA Más derechos para más gente

aws

— CLASIFICACIÓN —
DE DATOS

CRÉDITOS

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Equipo técnico OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Kadri Kaska
Elsa Neeme
Klaid Mägi
Lauri Luht

Equipo técnico AWS

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTENIDO

— CLASIFICACIÓN —
DE DATOS

Introducción

1

Organizaciones, personas y miles de millones de dispositivos conectados generan, procesan y consumen todo tipo de datos, todos los días. Y cada día se crean más de 2.5 quintillones de bytes de todo tipo de información[1] nueva para ser analizada, procesada y almacenada. El abanico de datos también es diverso: desde unos y ceros que provienen de dispositivos simples del internet de las cosas (IoT, por sus siglas en inglés) que señalan un evento de encendido/apagado (por ejemplo, un sensor de movimiento), hasta el clima, el tráfico, las transacciones financieras, la salud y las redes sociales, entre otros. Del mismo modo, los gobiernos, que son el objeto de este documento, generan, gestionan y almacenan petabytes de datos. La diversidad de datos provoca que se examinen cuáles son las políticas correctas que debe seguir un gobierno para clasificar y almacenar los datos que posee. La respuesta de los gobiernos a esta pregunta ha sido el desarrollo de políticas de Clasificación de Datos, que son lineamientos específicos para las organizaciones gubernamentales sobre cómo deben clasificarse los diferentes tipos de datos, para luego protegerse, manejarse, almacenarse y procesarse en función de su clasificación.

La primera pregunta que surge con frecuencia es "¿por qué no protegemos todos los datos al más alto nivel y ahorramos tiempo?" Para los gobiernos, esto no solo no es factible financieramente, sino que prescindiría de algunos otros beneficios de clasificar y etiquetar adecuadamente los diferentes tipos de datos. Primero, los niveles más altos de protección de datos acarrean costos adicionales, y tienen el potencial de generar mayores gastos de lo que se merecen los datos. Otro aspecto es que si se les da el mismo trato a todos los datos y no se etiquetan correctamente, puede ser difícil implementar controles de acceso adecuados, lo que llevaría a que personas que no tienen una razón oficial para tener acceso a datos confidenciales podrían acceder a estos fácilmente. Y, por último, se pueden obtener eficiencias en la gestión y la presentación de informes sobre datos que están organizados, agrupados, asegurados y etiquetados adecuadamente, según la clasificación.

La clasificación de datos les permite a las organizaciones pensar en datos, fundados en la sensibilidad y el impacto comercial, lo que ayuda a la organización a evaluar los riesgos

1 Forbes: How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#49f394760ba9

asociados con diferentes tipos de datos. Las organizaciones de estándares prestigiosas, como la Organización Internacional de Normalización (ISO, por sus siglas en inglés) y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), recomiendan esquemas de clasificación de datos para que la información se pueda administrar y asegurar de manera más efectiva de acuerdo con su criticidad y riesgo relativo, aconsejando prescindir de prácticas que tratan todos los datos de la misma manera. A pesar del hecho de que cada organización procesa y clasifica los datos de acuerdo con sus respectivas necesidades, regulaciones e incluso capacidades, sigue existiendo una necesidad variable de establecer una línea base básica de controles de seguridad que brinden protección adecuada contra vulnerabilidades, amenazas y riesgos acordes con nivel de protección designado, especialmente en el sector público.

Los beneficios de que una organización cuente con una clasificación efectiva de datos son múltiples. Una organización no solo puede mejorar su accesibilidad y eficiencia organizativa, sino que también una clasificación de datos efectiva garantiza que la información reciba la protección adecuada de acuerdo con su sensibilidad, valor y criticidad, así como la naturaleza y el grado de riesgos que resultan de una divulgación indebida, daño o destrucción.

El objetivo de este whitepaper es proporcionar una orientación para el desarrollo de un sistema de clasificación de datos con el fin de garantizar el acceso y la protección de la información generada y procesada por los gobiernos. Es importante destacar que una política de clasificación de datos es necesaria, independientemente del tipo de infraestructura utilizada por una organización, ya sea en las instalaciones, en la nube o móvil. Una política de clasificación de datos les entrega pautas a las organizaciones sobre el nivel de seguridad y los procesos asociados para almacenar y administrar diferentes tipos de datos. Además, las recomendaciones contenidas en este whitepaper pueden emplearse independientemente del tipo de organización, pero su objetivo principal es ofrecerles a las entidades gubernamentales, que brindan servicios públicos, aspectos clave a tener en cuenta para este proceso.

|Estructura|

Este documento técnico busca entregar orientación para el desarrollo de un sistema de clasificación de datos con el fin de garantizar el acceso y la protección de la información generada y procesada por los gobiernos. El whitepaper examina los enfoques de clasificación de datos existentes a nivel nacional e internacional, con el fin de ofrecer la clasificación de datos como una herramienta funcional, y los medios para evitar riesgos potenciales como la clasificación de información excesiva o insuficiente.

El documento se divide en cuatro secciones: i.Principios de clasificación de datos e información; ii. ¿Cuáles son los modelos existentes del sector público? iii. Recomendaciones para establecer un sistema de clasificación de datos; y iv. Recursos recomendados, que entrega una visión general de los principios de clasificación de datos, así como recomendaciones para su establecimiento. Para ilustrar algunos de los modelos existentes del sector público, la Sección II analiza la experiencia de Estados Unidos, el Reino Unido y Argentina en su implementación y las reglamentaciones generales de clasificación de datos. Los estudios de caso de EE. UU. y el Reino Unido son particularmente relevantes dado su nivel de rigor y sofisticación. El caso argentino, por su lado, destaca la experiencia de un país en la región de América Latina y el Caribe. Más importante aún, las recomendaciones de este whitepaper deben aplicarse al contexto y las necesidades de su organización, cuando usted establezca una estrategia de datos.

Principios de clasificación de datos e información

2

La implementación de la gestión de la información en general, y la clasificación de datos en particular, varía según el tipo de organización e incluso puede ser diferente según cada organización. Sin embargo, existen ciertos principios fundamentales comunes entre los gobiernos, las organizaciones no gubernamentales y las organizaciones comerciales. A continuación se presenta una síntesis de seis principios que expresan fuentes legales nacionales (y regionales) y los instrumentos de las organizaciones internacionales para la gestión de la información. Los principios deben usarse como una guía, en vez de como un punto de referencia único y permanente cuando esté preparando la construcción y/o refinamiento de una estrategia de gestión de información y clasificación de datos.

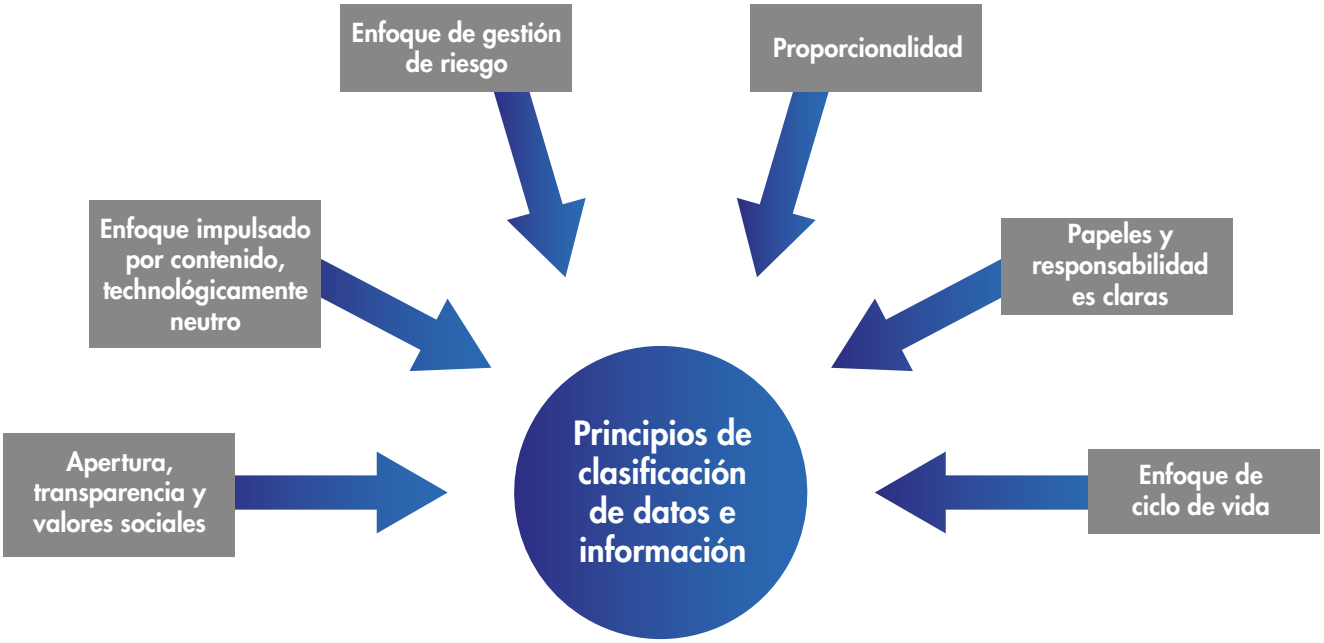

Figura 1- Principios de clasificación de datos e información

1. **Apertura, transparencia y valores sociales:** La clasificación debe usarse con precaución y de acuerdo con la sensibilidad, el valor y la criticidad de los datos. Las restricciones de acceso solo deben elegirse para los casos en que la divulgación de información sea perjudicial para los intereses legítimos y las obligaciones legales de la propia organización, su personal o terceros. En tales casos, deben observarse estrictamente los procedimientos especificados, para garantizar que la información no se vea comprometida ya sea a propósito o inadvertidamente. El desafío será no clasificar en exceso por efectos de conveniencia o practicidad, que resultaría en detrimento de la transparencia y la confianza pública, y así privaría a los interesados de ser los dueños de sus propias decisiones de gestión de riesgos.

2. **Enfoque basado en el contenido y tecnológicamente neutral:** La información debe clasificarse en función de su contenido y los riesgos asociados con el compromiso del contenido, independientemente de su formato, medios u origen. No se debe discriminar basado en el formato o los medios de la información, ya sea analógica (en papel) o digital; almacenado en un sistema de información, en medios de almacenamiento, en dispositivos móviles o en la nube. Del mismo modo, la decisión de clasificar la información debe depender del contenido en sí y no necesariamente derivarse automáticamente de la fuente de la información en la que se basa, a la que responde o hace referencia). Por ejemplo, confiar en fuentes públicas no debería determinar automáticamente que la información agregada debería revelarse públicamente.

3. **Enfoque de gestión de riesgos:** Se debe brindar protección a la información de acuerdo con el nivel de sensibilidad, valor y criticidad de esta. La protección generalmente se realiza con un enfoque graduado, basado en niveles correspondientes al valor y el riesgo. Un nivel de protección circunscribe el conjunto de medidas para reducir los riesgos a un nivel aceptable, es decir, la posible gravedad y probabilidad de que la información se vea comprometida. Al determinar el nivel de sensibilidad y el valor de la información, se deben tener en cuenta tanto el grado de daño potencial de compromiso (divulgación no autorizada, modificación o pérdida) como el valor potencial de los datos.

4. **Proporcionalidad:** La información se clasificará a un nivel apropiado que debe ser lo más bajo posible, pero tan alto como sea necesario.

5. **Papeles y responsabilidades claras:** Con respecto a la clasificación de datos, la política y los procesos deben asignarse para lograr la seguridad de la información dentro de la organización y confirmarse por el compromiso con y la conciencia de la seguridad de la información que tiene la gerencia.

6. **Enfoque del ciclo de vida:** Como parte de un sistema de gestión de la información, el sistema de clasificación debe tener en cuenta la información durante todo su ciclo de vida: desde la creación o recepción, almacenamiento, recuperación, modificaciones, transferencia, copia y transmisión hasta la destrucción. Además, la política de gestión de información/procesamiento de datos de una organización no debe estar escrita en piedra, sino evaluarse regularmente para garantizar que se corresponde con las necesidades y expectativas de la organización.

¿Cuáles son los modelos existentes del sector público?

3

La globalización ha marcado una tendencia hacia una convergencia en la terminología de clasificación de datos. Esta convergencia ha sido impulsada notablemente por el rigor de los estándares de la industria de las TIC (por ejemplo, el cumplimiento de las definiciones ISO/IEC, NIST), los desarrollos políticos y legales regionales consecuentes (en particular en la Unión Europea y sus estados miembros), pero principalmente la interacción e interdependencias entre dominios (por ejemplo, una creciente consideración de la ciberseguridad y la regulación de protección de datos entre sí). Por lo tanto, es aconsejable tener en cuenta estas mejores prácticas al desarrollar definiciones nacionales.

Estados Unidos (EE. UU.), el Reino Unido y Argentina han establecido esquemas de clasificación de datos para los datos para el sector público. Tanto los gobiernos de EE. UU. como del Reino Unido utilizan un esquema de clasificación de tres niveles, en la que la mayoría de los datos del sector público quedan clasificados en los dos niveles más bajos. Se ha incluido a Argentina como un estudio de caso para presentar un ejemplo regional sobre implementación y los desafíos enfrentados. La ciudad de Washington D. C. también podría ser un buen modelo para destacar y que ha sido celebrado ampliamente, por la convergencia de datos abiertos con clasificación de datos y sin un componente de seguridad nacional. Los esquemas de clasificación de datos tienen una lista corta de atributos y medidas o criterios asociados que ayudan a las organizaciones a determinar el nivel de categorización apropiado.[2]

|Estados Unidos de América (EE. UU.)|

El gobierno de EE. UU. utiliza un esquema de clasificación de tres niveles que fue actualizada según la Orden Ejecutiva 135261 y se basa en el impacto potencial para la seguridad nacional si se llegara a divulgar (es decir, asuntos de confidencialidad):

1.Confidencial—Información cuya divulgación no autorizada se estima que causaría daños a la seguridad nacional.

2.Secreta—Información cuya divulgación no autorizada se estima que causaría daños graves a la seguridad nacional.

3.Alto secreto— información cuya divulgación no autorizada se estima que causaría daños excepcionalmente graves a la seguridad nacional.

2 AWS Data Classification – Secure Cloud Adoption (June 2018)

Aunque no es una clasificación real, EE. UU. también usa el término "datos no clasificados" para referirse a cualquier dato que no esté incluido en los tres niveles oficiales de clasificación. Incluso en relación con datos no clasificados, existen algunas advertencias para la información delicada, como "Solo para uso oficial" (FOUO, por sus siglas en inglés) e "Información controlada no clasificada" (CUI, por sus siglas en inglés) que restringen la divulgación al público o a personal no autorizado. Sin embargo, esto no tiene en cuenta las diversas leyes de protección de datos basadas en márgenes más estrechos de tipos de datos, como datos de impuestos particulares, datos penales, datos de tarjetas de crédito, datos de atención médica y otros.

Debido al enfoque tan restrictivo del sistema de clasificación de EE. UU., que no incluye directamente la integridad y la disponibilidad de los datos entre sus niveles de clasificación–factores que se deberían solicitar al evaluar los requisitos de protección de la información–, el NIST desarrolló un esquema de categorización de tres niveles basado en el impacto potencial a la confidencialidad, integridad y disponibilidad de la información y los sistemas de información aplicables a la misión de una organización. La mayoría de los datos procesados y almacenados por las organizaciones del sector público se pueden clasificar en los siguientes:

- **Bajo—** Efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.

- **Moderado —** Efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.

- **Alto —** Efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.

Clasificación de datos	Clasificación del sistema de seguridad
No clasificado	Bajo a alto
Confidencial	Moderado a alto
Secreto	Moderado a alto
Alto secreto	Alto

Tabla 1 — Alineación de la clasificación de datos con la categorización de seguridad del sistema

Para muchos otros gobiernos nacionales, provinciales, estatales y locales, este sistema dual de clasificación y categorización puede ser demasiado complejo e innecesario para satisfacer las necesidades de aseguramiento de la información. En estas situaciones, una opción más simple puede ser fusionar los dos conceptos en un único término "clasificación", que es abordar la seguridad nacional (si corresponde) y la importancia de los tres pilares del aseguramiento de la información: confidencialidad, integridad y disponibilidad en la misión y los negocios de la organización. Por esta razón, el uso de la palabra "clasificación" en este documento significará el enfoque holístico de la categorización para la confidencialidad, integridad y disponibilidad en lugar del alcance más limitado del impacto en la seguridad nacional.

|Reino Unido|

El gobierno del Reino Unido recientemente simplificó su esquema de clasificación al reducir los niveles de seis a tres. Estos son:

1.Oficial:— Operaciones y servicios comerciales de rutina, algunos de los cuales podrían tener consecuencias perjudiciales si se perdieran, fueran robados o se publicaran en los medios de comunicación, pero ninguno se consideraría tener un perfil de amenaza elevado.

2.Secreto—Información muy sensible que justifica medidas de protección intensificadas para defenderse contra actores de amenazas muy resueltos y altamente capaces (por ejemplo, el compromiso podría dañar significativamente las capacidades militares, las relaciones internacionales o la investigación de la delincuencia grave y organizada).

3.Alto secreto— La información más confidencial que requiere los niveles más altos de protección contra las amenazas más graves (por ejemplo, el compromiso podría causar la pérdida generalizada de vidas o podría amenazar la seguridad o el bienestar económico del país o las naciones amigas).

El gobierno del Reino Unido ha categorizado tradicionalmente aproximadamente el 90 por ciento de sus datos como "Oficial"[3]. El Reino Unido utiliza un enfoque de acreditación flexible y descentralizado donde las agencias particulares definen los servicios en la nube adecuados para los datos "oficiales" basados en la garantía de seguridad de un proveedor de servicios en la nube (CSP, por sus siglas en inglés) contra 14 principios de seguridad en la nube[4]. La mayoría de las agencias del gobierno del Reino Unido han determinado que es apropiado usar las CSP de gran escala y de buena reputación cuando ejecutan cargas de trabajo con datos "oficiales".

El gobierno del Reino Unido estableció varias consideraciones para toda la seguridad de la información cuando se almacena usando la nube:

1.Oficial:— Toda la información y los activos clasificados como oficiales son adecuados para diferentes servicios de GCloud[5]. Sin embargo, se requiere que todos los propietarios de riesgos comprendan enteramente toda acreditación de GCloud. Todos los servicios de tecnología de la información y la comunicación (TIC) deben seguir el proceso de gestión de riesgos establecido en las Normas de Aseguramiento de la Información del gobierno del Reino Unido, además de seguir los enfoques arquitectónicos estándar que deben alojarse en el Reino Unido.

2.Secreto— Todos los servicios de TIC que tratan o almacenan información secreta deben acreditarse según corresponda de acuerdo con el modelo de amenaza secreta. Los patrones o consejos de diseño específicos deben provenir de la Autoridad Técnica Nacional para el aseguramiento de la información (CESG, por sus siglas en inglés). Una evaluación preliminar del riesgo y las implicaciones de habilitar la funcionalidad del intercambio de información fuera del nivel secreto estará altamente restringida y administrada, utilizando la capacidad acreditada compartida.

3. Alto secreto— Los sistemas de TIC diseñados deben estar acreditados según corresponda para poder contener materiales de Alto secreto. Puede ser necesario contar con asesoramiento arquitectónico personalizado.

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf

4 https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

5 El marco G-Cloud es un acuerdo entre el gobierno del Reino Unido y los proveedores que brindan servicios basados en la nube.

|Argentina|

Para el año 2004, el gobierno de Argentina comenzó a delinear los requisitos para formar e implementar una estrategia nacional de protección de datos. Esta estrategia inicial abarcó la creación de un modelo de política de seguridad, la formación de un comité de seguridad de la información, el establecimiento de sus funciones y la designación de un coordinador para supervisar el trabajo del comité. La política se formalizó en 2005 cuando la Oficina Nacional de Tecnologías de Información (ONTI), la entidad argentina responsable de la transformación e implementación de soluciones tecnológicas en el sector público, promulgó el Modelo de Política de Seguridad de la Información, Decreto N.° 378, que luego actualizó y modificó en 2014, en base a una serie de recomendaciones obtenidas de su revisión de 2013, que se convirtió en la Disposición 1/2015.[i]

La política designa las mejores prácticas para la protección y gestión de activos como parte de su gestión de riesgos. Los propietarios de los datos e información son responsables de clasificar la información, en función del grado de sensibilidad, documentar y actualizar la clasificación de la información, y definir qué usuarios deben tener acceso a la información en razón de sus funciones y papeles. Dentro de la clasificación, la política debe basarse en los siguientes tres factores: confidencialidad, integridad y disponibilidad. Cada uno de los tres factores tiene una escala de 0 a 3, que luego determina el grado de protección que debe recibir. La escala en la que se divide es la siguiente:

- **Baja criticidad: :** La información se clasifica como pública. La información es comúnmente conocida y utilizada por cualquier persona o empleado. Una modificación no autorizada puede repararse fácilmente y no compromete las operaciones de la organización.

- **Criticidad media:** La información se clasifica como reservada o para uso interno. La información puede ser conocida o utilizada por algunos empleados de la organización y algunas autoridades delegadas externas. Su uso podría causar leves riesgos o pérdidas para la agencia, el sector público nacional o terceros. Una modificación no autorizada podría repararse, aunque podría causar ligeras pérdidas para la agencia pública o terceros asociados. Su pérdida de un día o permanente podría causar daños significativos a las operaciones en la organización.

- **Alta criticidad:** La información se clasifica como confidencial o secreta. Esta información solo puede ser conocida por un grupo, o un grupo muy pequeño, de empleados, generalmente la alta dirección de la organización, y su divulgación o uso no autorizado podría causar serias pérdidas al sector público u otros terceros asociados. La pérdida permanente podría causar graves daños a la organización.

i http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Recomendaciones para establecer un sistema de clasificación de datos

4

Los sistemas de clasificación de datos existentes reconocen diferentes niveles de sensibilidad, valor y criticidad de la información, así como niveles variados de severidad y probabilidad de compromiso. A menos que los niveles de seguridad para ciertos datos estén prescritos por ley (por ejemplo, para información de seguridad nacional o privacidad) y/o requieran alineación con compromisos regionales o internacionales, la definición de los niveles de seguridad queda a discreción de la organización particular. Esto no significa necesariamente que el cumplimiento de los requisitos legales requiera una miríada de categorías de clasificación independientes. Cuando el riesgo y las protecciones requeridas son equivalentes, es factible acomodar las protecciones requeridas bajo un mismo nivel de clasificación.

La siguiente sección ofrece un resumen de las fases primarias del proceso de clasificación de datos. No sustituye la implementación sistemática de las normas de seguridad de la información o los requisitos legales que surgen de instrumentos específicos, pero sí pretende ofrecer una comprensión general de los pasos principales necesarios para desarrollar e implementar un sistema de clasificación de datos. Se define en cuatro pasos principales:

|Auditoría|

•Inventario de activos de datos

El primer paso para la clasificación de datos dentro de una organización es llevar a cabo un inventario de datos o una "auditoría de datos". Esta actividad debe proporcionar una comprensión amplia de los tipos de datos e información procesados dentro de la organización, su valor, sensibilidad y criticidad.

Este paso también implica la identificación de los requisitos legales que se aplican; y una auditoría de las políticas y procedimientos organizativos o administrativos existentes para la gestión de datos, incluidas las funciones y responsabilidades organizacionales existentes en el procesamiento de datos.

• Evaluación de riesgos

Después de la definición de las políticas de clasificación de datos, se puede implementar el sistema de clasificación de datos. El siguiente paso es realizar una evaluación de riesgos para los tipos de datos procesados que identifique y cuantifique los riesgos de gravedad y probabilidad, y priorice los riesgos en función de los criterios de aceptación de riesgos y objetivos relevantes para la organización. El resultado de este ejercicio

debe guiar y determinar la selección de medidas técnicas y organizativas apropiadas, así como las prioridades para la gestión de riesgos. Las evaluaciones de riesgos deben ser periódicas reconociendo que el entorno tecnológico y de amenazas, así como las prácticas de seguridad, evolucionan continuamente con el paso del tiempo y, preferiblemente, comparables[6].

La evaluación de riesgos es tarea del controlador de datos, en ciertos casos respaldado por requisitos legales, como se discutió en la sección anterior[7]. La ley aplicable podría exigir que el controlador pueda demostrar que el procesamiento cumple con los requisitos y restricciones establecidos (por ejemplo, el RGPD lo hace con respecto al procesamiento de datos personales). Véase el Anexo I para conocer algunas ideas sobre los factores de riesgo que podrían considerarse al emprender este proceso.

•Definición de los niveles de protección y su aplicación

Deben definirse los requisitos de protección apropiados, agrupados por categorías de clasificación, para cada tipo de activo de información.

La cantidad de niveles de clasificación de datos debe ser óptima para las necesidades de la organización. Un enfoque excesivamente matizado es difícil de administrar, podría resultar en datos inconsistentemente protegidos y un mayor riesgo, y podría confundir a los controladores y procesadores de datos. Un modelo demasiado simplificado presentaría el riesgo de ser una clasificación excesiva o insuficiente. Un enfoque de tres niveles tiende a cumplir tanto los estándares de seguridad de la información (ISO, NIST, estándares nacionales) como, en la mayoría de los casos, las expectativas de cumplimiento legal.

•Determinación de los papeles de gestión de datos

El siguiente paso es definir los papeles y responsabilidades de la organización y el personal con respecto a la clasificación y protección de la información. Además de los roles, se deben definir las obligaciones de gestión de riesgos apropiadas para cada papel. El objetivo es "traducir" lo anterior en rutinas organizacionales mediante políticas y procedimientos. Esta también es una buena fase para revisar y actualizar las regulaciones internas existentes, como parte de este proceso.

En última instancia, es la organización, como "controladora de datos", la responsable del cumplimiento y deberá poder demostrar dicho cumplimiento (rendición de cuentas).

|Implementación|

•Clasificación

En función de la evaluación de riesgos, se asigna el nivel de riesgo, considerando individualmente cada objetivo de seguridad (confidencialidad, integridad y disponibilidad). Se asigna una clasificación general a los datos según el valor más alto entre los tres factores[8]. Algunos sistemas también reconocen un nivel combinado (alta confidencialidad, integridad moderada, baja disponibilidad).[9]

•Consideraciones para tecnologías emergentes: nube, móvil e IoT

Se debe adoptar un enfoque basado en el riesgo

6 ISO 27000:2018; ISO/IEC 27005 proporciona orientación sobre gestión de riesgos de seguridad de la información, incluido asesoramiento sobre evaluación de riesgos, tratamiento de riesgos, aceptación de riesgos, informes de ries-gos, monitoreo de riesgos y revisión de riesgos. También se incluyen ejemplos de metodologías de evaluación de riesgos.

7 Véase, p. ej, preambulo RGPD, sección 75

8 Data Classification: Secure Cloud Adoption'. AWS, June 2018. https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf.

9 Por ejemplo, IT Grundschutz de Alemania https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html y el ISKE de Estonia, https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.cyber-security/it-baseline-security-system-iske.html.

para todas las evaluaciones e implementaciones técnicas, ya sean equipos tradicionales en las instalaciones, dispositivos móviles, en la nube o con dispositivos del Internet de las cosas (IoT). Las estrategias para adoptar tecnologías emergentes deberían estar influenciadas por la estrategia de riesgo organizacional, pero también proporcionar retroalimentación para actualizar la estrategia de riesgo de la organización a medida que van estando disponibles nuevas capacidades. Una evaluación de los activos de datos, los niveles de riesgo y los requisitos de confidencialidad, integridad y disponibilidad deben ofrecerle a la organización una comprensión de su tolerancia al riesgo, así como las combinaciones aceptables de implementación, modelos de servicio y ubicaciones que las tecnologías emergentes pueden brindar.

Por ejemplo, una de las tecnologías emergentes más incomprendidas hoy en día es la "nube". Cuando los gobiernos y las organizaciones carecen de un programa de clasificación de datos, procesos de gestión de riesgos y se centran en controles técnicos heredados en lugar de fijarse en los objetivos de seguridad de los datos, tiende a haber miedo, incertidumbre y duda (FUD, por sus siglas en inglés). Este FUD impide que la organización adopte tecnología emergente y se beneficie de nuevas capacidades, rendimiento y eficiencia de costos.

Un enfoque de "migración por etapas" puede ser útil con respecto a la adopción de tecnologías emergentes. En ese caso, se les asignan inicialmente 'macrocategorías' a los activos y servicios (por ejemplo, no sensibles y no críticos, medio sensibles y medio críticos, etc.) y se le asigna una clasificación detallada a cada activo y servicio a medida que se migra a la nube[10].

|Monitoreo|

•Supervisión y garantía de calidad
Se debe asignar una entidad apropiada para la supervisión, asesoramiento y consultoría, así como para la revisión de las decisiones de clasificación, p. ej. Director de información (CIO, por sus siglas en inglés), Director de datos (CDO, por sus siglas en inglés) o Director de seguridad de la información (CISO, por sus siglas en inglés) con la responsabilidad específica de la clasificación de datos, las decisiones de riesgo de datos y las medidas de protección requeridas. Esa entidad también debe estar facultada para avalar la garantía de calidad en la implementación de controles de seguridad, la idoneidad y lo adecuado de los controles existentes para satisfacer los objetivos de seguridad deseados y cualquier requisito de cumplimiento.

•Mejora continua y monitoreo
Una vez que se han clasificado los activos de datos, se deben implementar los procedimientos de seguridad con vistas a un monitoreo y evaluación constantes para continuar cumpliendo con los requisitos de cumplimiento y gestión de riesgos. Para continuar cumpliendo los objetivos de seguridad de la política, es aconsejable desarrollar estándares de seguridad y guías de implementación basadas en las capacidades técnicas y no técnicas actuales, que pueden actualizarse para adoptar nuevas innovaciones más fácilmente sin tener que actualizar la política.

|Revisión|

•Revisión y ajuste periódico
Más allá del monitoreo y la evaluación continuos, las revisiones sistemáticas periódicas permiten tener ajustes en el acceso a los datos y la revisión de datos clasificados. Una metodología de reclasificación y revisión puede garantizar que se

10 Security & Resilience in Governmental Clouds: Making an informed decision. ENISA 2011, https://www.enisa.europa.eu/publications/security-and-resilience...clouds/.../fullReport.

apliquen medidas de seguridad adecuadas a la tecnología actual y al entorno de amenaza/riesgo, pero también al valor y la sensibilidad cambiantes de los datos clasificados. La información clasificada debe revisarse regularmente para evitar que la información heredada se mantenga vigente, lo cual es costoso de almacenar y administrar. También es aconsejable revisar periódicamente las políticas y procedimientos de clasificación.

Figura 2- Recomendaciones para establecer un sistema de clasificación de datos

Recursos recomendados

5

Convenio del Consejo de Europa sobre acceso a los documentos públicos (2009) zhttps://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084826

Clasificación de datos para la preparación de la nube. Microsoft, abril de 2017. https://gallery.technet.microsoft.com/Data-Classification-for-51252f03

Clasificación de datos: adopción segura de la nube. AWS, junio de 2018. https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

Executive Order 13526 sobre clasificación y desclasificación de información sobre seguridad nacional (CT:IM-226; 10-31-2018). Oficina de origen: A/GIS/IPS https://fam.state.gov/fam/05fam/05fam0480.html; véase 5 FAM 482.5 para las categorías de clasificación.

Guía de buenas prácticas para la implementación segura de nubes gubernamentales. ENISA, 2013, https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

Reglamento general de protección de datos. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tra-tamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/EC. OJ L 119, 4.5.2016, p. 1–88, http://data.europa.eu/eli/reg/2016/679/oj

Política de protección de información de CPI, ICC/AI/2007/001. Boletín del Secretario General ST/SGB/2007/6 del 12 de febrero de 2007 sobre sensibilidad, clasificación y manejo, https://www.icc-cpi.int/resource-library/Vademecum/ICC%20Information%20Protection%20Policy%20-%202007.pdf

IT Grundshutz. Oficina Federal de Seguridad de la Información. https://www.bsi.bund.de/EN/

Topics/ITGrundschutz/itgrundschutz_node.html

Ley de información pública, Estonia https://www.riigiteataja.ee/en/eli/529032019012/consolide

Uso seguro de servicios en la nube en el sector financiero. Buenas prácticas y recomendaciones. ENISA, 2015 https://www.enisa.europa.eu/publications/cloud-in-finance

Ley de Secretos de Estado e Información Clasificada de Estados Extranjeros, https://www.riigiteataja.ee/en/eli/501042019009/consolide

Publicación especial del NIST 800-60 Rev. 1 (Volume 1, Volume 2), Guía para asignar tipos de información y sistemas de información a categorías de seguridad

Publicación 199 de las Normas federales de procesamiento de información del NIST: Normas para la categorización de seguridad de la información federal y los sistemas de información https://nvlpubs.nist.gov/nistpubs/FIPS/NIST. FIPS.199.pdf

Marco de gestión de riesgos del NIST (RMF) https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

Clasificaciones de seguridad del gobierno del Reino Unido https://www.gov.uk/government/publications/government- security-classifications

Organización Internacional de Normalización (ISO) 27001, Requisitos para los sistemas de gestión de seguridad de la información https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Asociación de Auditoría y Control de Sistemas de Información (ISACA) Objetivos de control para la Información y Tecnología Relacionadas (COBIT) http://www.isaca.org/cobit/pages/default.aspx

Blog de AWS sobre Cómo abordar la residencia de datos — https://aws.amazon.com/blogs/security/addressing-data- residency-with-aws/

Documentos técnicos de AWS — https://aws.amazon.com/whitepapers/

La seguridad física y centro de datos de AWS — https://aws.amazon.com/compliance/data-center/data-centers/

Clasificación de datos de AWS: adopción segura de la nube en junio de 2018 - https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf

Anexo I. Escenarios de riesgo

6

La siguiente categorización resume los escenarios de riesgo comúnmente reconocidos en los instrumentos incluidos en las secciones anteriores de este whitepaper. En lugar de un catálogo predeterminado de riesgos, este puede ofrecer orientación para desarrollar un sistema de clasificación de datos con el fin de gestionar los riesgos derivados de las violaciones a la seguridad de la información (es decir, confidencialidad, integridad o disponibilidad).

Riesgos para la persona	-Efecto del compromiso sobre la seguridad y protección física de una persona, incluida la amenaza directa o indirecta a la vida o la salud, independientemente de la relación del individuo con la organización (personal o terceros); -Efecto del compromiso de los derechos individuales no materiales (cuando el resultado podría ser la pérdida o violación de la privacidad, la discriminación, el daño a la reputación u otra desventaja social significativa, o cuando un interesado podría verse privado de sus derechos y libertades o impedido de ejercer control sobre sus datos personales); -Efecto del compromiso de los derechos e intereses materiales individuales (donde el resultado podría ser, por ejemplo, robo de identidad o fraude, pérdida financiera u otra desventaja económica significativa);
Riesgos para las operaciones de una organización	- Efecto del compromiso sobre la operación y administración efectivas de la organización y sus procesos; - Efecto del compromiso del proceso de toma de decisiones interno libre e independiente y las investigaciones (internas);

Riesgos para los activos o intereses comerciales de una organización	-Riesgo de pérdida financiera para la organización; efecto del compromiso sobre los intereses financieros de la organización o los de otras partes involucradas; -Efecto del compromiso sobre los socios de la organización, incluso sobre la información intercambiada con terceros bajo una expectativa de confidencialidad; -Efecto del compromiso de la información cubierta por el privilegio legal; -Efecto del compromiso de la organización en negociaciones comerciales o políticas; -Riesgo para la reputación, estabilidad o seguridad de la organización;
Riesgo para la seguridad nacional, el orden público o las relaciones exteriores	–Efecto del compromiso sobre la seguridad nacional y la capacidad de defensa (incluidos los asuntos tecnológicos y económicos relacionados con la seguridad nacional) o perjudicar las operaciones o actividades de seguridad; -Efecto del compromiso sobre el ejercicio de las relaciones exteriores (incluida la información de gobiernos extranjeros); -Efecto del compromiso sobre el orden público y el funcionamiento de las autoridades de seguridad. -Efecto del compromiso de la información sobre vulnerabilidades o capacidades de sistemas, instalaciones, infraestructuras, proyectos, planes o servicios de protección relacionados con la seguridad nacional; -Efecto del compromiso sobre la infraestructura y la protección de la información; -Efecto del compromiso de los intereses administrativos o judiciales, incluida una investigación o juicio; -Efecto del compromiso sobre la confianza pública de la organización y sus operaciones.

Fuentes y ejemplos:

RGPD, ISO/IEC, NIST, CPI, ley de seguridad nacional

(Estados Unidos, Estonia y países de la OTAN/UE)[11].

11 https://www.valisluureamet.ee/nsa/tables.html

OEA Más derechos para más gente

aws

– CLASIFICACIÓN –
DE DATOS

White paper series
Edición 6

2019