Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1058

(03/2017)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la información y de las redes – Gestión de la seguridad

Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a la protección de la información de identificación personal

Recomendación UIT-T X.1058

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	**X.1050–X.1069**
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319

Para más información, véase la Lista de Recomendaciones del UIT-T.

NORMA INTERNACIONAL ISO/CEI 29151
RECOMENDACIÓN UIT-T X.1058

Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a la protección de la información de identificación personal

Resumen

El número de organizaciones que llevan a cabo el procesamiento de la información de identificación personal (PII, *Personally Identifiable Information*) aumenta sin cesar, del mismo modo que la cantidad de PII que tratan esas organizaciones. Al mismo tiempo, las expectativas de la sociedad respecto de la protección de la PII y la seguridad de los datos personales también están aumentando. Numerosos países incrementan su legislación para hacer frente al número cada vez mayor de graves violaciones a la seguridad de los datos.

En esta Especificación se establecen objetivos de control, controles y directrices para la implementación de controles con la finalidad de cumplir los requisitos identificados por la evaluación de los riesgos e incidencias vinculados a la protección de la información de identificación personal (PII). En particular, en la presente Especificación se describen directrices basadas en ISO/CEI 27002, teniendo en cuenta los requisitos necesarios para el procesamiento de la PII que puedan ser aplicables en el contexto de uno o más entornos de riesgo para la seguridad de la información de una organización.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	
1.0	ITU-T X.1058	2017-03-30	17	11.1002/1000/13182

Palabras clave

Código de prácticas, control, directrices de implementación, PII.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Introducción

El número de organizaciones que llevan a cabo el procesamiento de la información de identificación personal (PII) aumenta sin cesar, del mismo modo que la cantidad de PII que tratan esas organizaciones. Al mismo tiempo, las expectativas de la sociedad respecto de la protección de la PII y la seguridad de los datos personales también están aumentando. Numerosos países incrementan su legislación para hacer frente al número cada vez mayor de graves violaciones a la seguridad de los datos.

A medida que aumenta el número de violaciones de la PII, las organizaciones que llevan a cabo la recopilación o el procesamiento de la PII necesitarán cada vez más directrices relativas a la forma de protegerla con objeto de reducir el riesgo de violación de la privacidad y disminuir la incidencia de las infracciones en la organización y en las personas afectadas. Esta Especificación describe ese tipo de directrices.

La presente Especificación ofrece directrices para los controladores de PII en una amplia gama de controles de la seguridad de la información y la protección de la PII que se aplican de forma habitual en diferentes organizaciones encargadas de la protección de la PII. Los textos restantes que corresponden a la familia de normas internacionales de la familia ISO/CEI, enumeradas a continuación, facilitan directrices o describen requisitos con respecto a otros aspectos del proceso general de protección de la PII:

- ISO/CEI 27001 describe un proceso de gestión de la seguridad de la información y requisitos asociados, que podrían servir de base para la protección de la PII.
- ISO/CEI 27002 facilita directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta uno o más entornos de riesgo para la seguridad de la información de una organización.
- ISO/CEI 27009, que describe los requisitos de utilización de ISO/CEI 27001 en un determinado sector (campo, zona de aplicación o sector de mercado), explica cómo incluir requisitos adicionales a los de ISO/CEI 27001, cómo reformular cualquiera de los requisitos de ISO/CEI 27001 y cómo incluir controles o conjuntos de controles, además de los indicados en Anexo A de ISO/CEI 27001.
- ISO/CEI 27018 da orientaciones a las organizaciones que cumplen la función de procesadores de PII cuando ofrecen capacidades de procesamiento como servicios en la nube.
- ISO/CEI 29134 facilita directrices para la identificación, el análisis y la evaluación de los riesgos para la privacidad, si bien ISO/CEI 27001 e ISO/CEI 27005 describen una metodología destinada a identificar, analizar y evaluar dichos riesgos.

Convendría que la elección de los controles se efectuara teniendo en cuenta los riesgos identificados como resultado de un análisis, con objeto de elaborar un sistema integral y coherente de controles. Los controles deberían adaptarse al contexto del procesamiento particular de la PII.

Esta Especificación contiene dos partes: 1) el texto principal, integrado por las cláusulas 1-18; y 2) un anexo normativo. Esta estructura refleja la práctica normal para la elaboración de ampliaciones de ISO/CEI 27002 propias del sector.

La estructura del texto principal de esta Especificación, comprendidos los títulos de las cláusulas, corresponde al texto principal de ISO/CEI 27002. La introducción y las cláusulas 1 a 4 proporcionan información general sobre la utilización de esta Especificación. Los encabezamientos de las cláusulas 5 a 18 son similares a los de ISO/CEI 27002, y ponen de manifiesto que esta Especificación se basa en directrices indicadas en ISO/CEI 27002, a las que se añaden nuevos controles específicos para la protección de la PII. Numerosos controles descritos en ISO/CEI 27002 no necesitan amplificación en el contexto de los controladores de la PII. Sin embargo, en ciertos casos son necesarias directrices de implementación adicionales, que figuran en el encabezamiento correspondiente (y en el número de cláusula) de ISO/CEI 27002.

El Anexo normativo contiene un amplio conjunto de controles específicos para la protección de la PII que complementan los indicados en ISO/CEI 27002. Esos nuevos controles para la protección de la PII, con sus directrices asociadas, se dividen en 12 categorías, que corresponden a la política de privacidad y los once principios de privacidad enumerados en ISO/CEI 29100:

- consentimiento y elección;
- legitimidad y especificación de la finalidad;
- restricciones en materia de recopilación;
- minimización de datos;
- restricciones en materia de utilización, retención y divulgación;
- exactitud y calidad;
- apertura, transparencia y notificación;

- participación y acceso individual;
- rendición de cuentas;
- seguridad de la información; y
- cumplimiento de la privacidad.

En la Figura 1 se describe la relación entre esta Especificación y la familia de normas ISO/CEI.

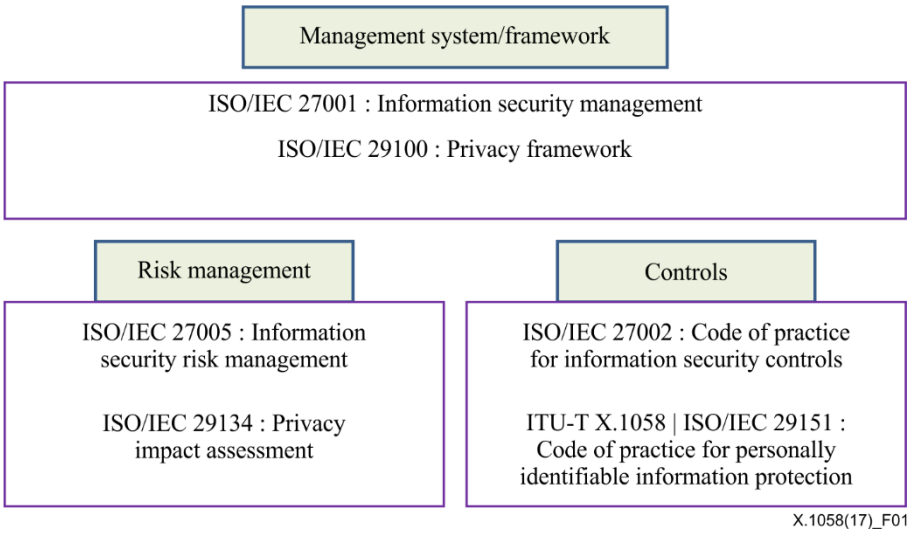

Figura 1 – Relación entre esta Especificación y la familia de normas ISO/CEI

Esta Especificación incluye directrices basadas en ISO/CEI 27002, que adapta, llegado el caso, para tener en cuenta las necesidades de protección de la privacidad que plantea el procesamiento de la PII:

a) En dominios de procesamiento diferentes, por ejemplo:
   - servicios en la nube públicos;
   - aplicaciones de redes sociales;
   - dispositivos conectados a Internet en el hogar;
   - búsqueda, análisis;
   - ataques a la PII con fines de publicidad y propósitos similares;
   - programas de análisis de *big data*;
   - empleo;
   - gestión comercial en ventas y servicio (planificación de recursos de empresa, gestión de la relación con los clientes).

b) En diferentes ubicaciones, por ejemplo:
   - en una plataforma de procesamiento personal (tarjetas inteligentes, teléfonos inteligentes y sus aplicaciones, medidores inteligentes, dispositivos llevables.);
   - en redes de transporte y recopilación de datos (cuando los datos de localización del teléfono móvil son creados operativamente mediante el procesamiento de la red, que pueden ser considerados PII en algunas jurisdicciones);
   - dentro de la propia infraestructura de procesamiento de una organización;
   - en la plataforma de procesamiento de un tercero.

c) Según características de recopilación, por ejemplo:
   - recopilación única de datos (al registrar un servicio);
   - recopilación permanente de datos (control frecuente de parámetros de salud realizado mediante sensores o en el cuerpo de una persona, recopilaciones de datos múltiples utilizando tarjetas de pago sin contacto, sistemas de recopilación de datos de contadores inteligentes, etc.).

NOTA – La recopilación permanente de datos puede contener o arrojar datos de comportamiento, de localización y otros tipos de PII. En esos casos, habrá que tener en cuenta la utilización de controles para la protección de la PII que permitan la gestión del acceso y la recopilación según el consentimiento y el control adecuado del titular de la PII sobre ese tipo de acceso y recopilación.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a la protección de la información de identificación personal

1 Ámbito de aplicación

En esta Recomendación | Norma internacional se establecen objetivos de control, controles y directrices para la implementación de controles con la finalidad de cumplir los requisitos identificados por la evaluación de los riesgos e incidencias vinculados a la protección de la información de identificación personal (PII, *Personally Identifiable Information*).

En particular, en esta Recomendación | Norma internacional se describen directrices basadas en ISO/CEI 27002, teniendo en cuenta los requisitos necesarios para el procesamiento de la PII que puedan ser aplicables en el contexto de uno o más entornos de riesgo para la seguridad de la información de una organización.

En esta Recomendación | Norma internacional es aplicable a todos los tipos y tamaños de organizaciones que cumplen la función de controladores de la PII (como se indica en ISO/CEI 29100), incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que llevan a cabo el procesamiento de la PII.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Especificación. En la fecha de esta publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y Normas son objeto de revisión, por lo que se insta a las partes en acuerdos fundados en esta Especificación a que estudien la posibilidad de aplicar la edición más reciente de las Recomendaciones y Normas que se indican a continuación. Los miembros de la CEI y de la ISO mantienen un registro actualizado de las Normas Internacionales vigentes. La Oficina de Normalización de las Telecomunicaciones publica periódicamente una lista de las Recomendaciones UIT-T vigentes.

– ISO/CEI 27002:2013, *Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a los controles para la seguridad de la información*.

– ISO/CEI 29100:2011, *Tecnología de la información – Técnicas de seguridad – Marco de privacidad.*

3 Definiciones y abreviaturas

3.1 Definiciones

A los efectos de esta Especificación, se aplicarán los términos y definiciones que se indican en ISO/CEI 27000:2016 e ISO/CEI 29100 y los que se presentan a continuación.

La Plataforma de navegación en línea de ISO, la *Electropedia de la CEI* y los Términos y definiciones de la UIT son bases de datos terminológicas que se utilizan en la normalización.

3.1.1 director responsable de la privacidad (CPO): Alto cargo directivo encargado de la protección de la PII en la organización.

3.1.2 proceso de desidentificación: Proceso de eliminación de la asociación entre un conjunto de datos de identificación y los datos principales mediante técnicas de desidentificación.

3.2 Abreviaturas

En esta Especificación se aplican los siguientes acrónimos:

BCR Regla de empresa vinculantes (*binding corporate rule*)

CCTV Televisión en circuito cerrado (*closed circuit television*)

CPO Director responsable de la privacidad (*chief privacy officer*)

PBD Privacidad por diseño (*privacy by design*)

PDA Asistente personal digital (*personal digital assistant*)

PET Tecnología que refuerza la privacidad (*privacy enhancing technology*)

PIA Evaluación de la incidencia en la privacidad (*privacy impact assessment*)

PII Información de identificación personal (*personally identifiable information*)

RFID Identificación por radiofrecuencias (*radio frequency identification*)

USB Bus serie universal (*universal serial bus*)

4 Visión general

4.1 Objetivo de la protección de la PII

En esta Especificación se describe un conjunto de controles para la protección de la PII. El objetivo de la protección de la PII es permitir que las organizaciones pongan en práctica un conjunto de controles como parte de su programa general de protección de la PII. Estas pueden utilizarse en un marco para el mantenimiento y mejora de la observancia de las leyes y disposiciones reglamentarias que guardan relación con la privacidad, la gestión de los riesgos para la privacidad y el cumplimiento de las expectativas de los titulares de la PII, reguladores o clientes, con arreglo a los principios de privacidad descritos en ISO/CEI 29100.

4.2 Requisitos para la protección de la PII

Una organización debe identificar sus requisitos en materia de protección de la PII. Para hacerlo, se aplican los principios de privacidad descritos en ISO/CEI 29100. Las tres fuentes principales de requisitos de protección de la PII son las siguientes:

- Requisitos jurídicos, estatutarios, reglamentarios y contractuales relativos a la protección de la PPI, comprendidos, por ejemplo, los requisitos en materia de PII que debe cumplir una organización, sus socios comerciales, sus contratistas y sus proveedores de servicio.
- Evaluación de los riesgos (esto es, riesgos para la seguridad y riesgos para la privacidad) para la organización y el titular de la PPI, teniendo en cuenta la estrategia comercial general de la organización y sus objetivos.
- Políticas institucionales: una organización también puede optar voluntariamente por no limitarse a los criterios que emanan de los requisitos anteriores.

Asimismo, las organizaciones deberían tener en cuenta los principios (esto es, los principios de privacidad definido en ISO/CEI 29100), los objetivos y los requisitos comerciales del procesamiento de la PII que se han elaborado en apoyo de sus actividades.

Habría que seleccionar los controles de protección de la PII (incluidos los controles de seguridad) teniendo en cuenta la evaluación de los riesgos. Los resultados de una evaluación de la incidencia en la privacidad (PIA), p.ej., como se especifica en ISO/CEI 29134, contribuirán a orientar y determinar el procesamiento adecuado y las prioridades en materia de gestión de los riesgos para la protección de la PII y la implementación de controles seleccionados para la protección contra esos riesgos.

Una especificación PIA, como la descrita en ISO/CEI 29134, puede proporcionar directrices sobre la evaluación de los riesgos para la privacidad, incluido el asesoramiento sobre la evaluación de los riesgos, el plan de tratamiento de riesgos, la aceptación de riesgos y el examen de los riesgos.

4.3 Controles

Una evaluación de los riesgos para la privacidad puede ayudar a las organizaciones a identificar los riesgos específicos de violaciones de la privacidad procedentes de procesamiento ilícito o de recorte de los derechos del titular de la PII involucrado en una operación prevista. Las organizaciones deberían determinar e implementar controles para el tratamiento de los riesgos identificados por el proceso de incidencia de riesgos. Los controles y los tratamientos tendrían luego que ser documentados, si fuera posible de forma separada en un registro de riesgos independiente. Ciertos tipos de procesamiento de la PII pueden justificar la aplicación de controles específicos, cuya necesidad sólo salta a la vista una vez que la operación prevista se ha analizado detenidamente.

4.4 Selección de controles

Los controles se pueden seleccionar a partir de la presente Especificación (que incluye por referencia los controles de ISO/CEI 27002, creando un conjunto combinado de controles de referencia). En caso necesario, los controles también pueden seleccionarse a partir de otros conjuntos de controles, o pueden diseñarse otros nuevos para atender a necesidades concretas, según proceda.

La selección de controles depende de las decisiones adoptadas por la organización teniendo en cuenta criterios respecto de las opciones de tratamiento del riesgo y el enfoque general de gestión de riesgos, aplicado a la organización y, mediante acuerdos contractuales, a sus clientes y proveedores, y debería estar además sujeta a todas las leyes y disposiciones reglamentarias nacionales e internacionales aplicables.

La selección e implementación de controles depende también del papel que cumple la organización en la prestación de infraestructura o servicios. Muchas organizaciones diferentes pueden participar en la prestación de infraestructura y/o servicios. En algunas circunstancias, los controles seleccionados pueden ser exclusivos de una determinada organización. En otros casos, pueden compartir el papel ejercido en la implementación de controles. Los acuerdos contractuales deberían especificar claramente las responsabilidades en cuanto a la protección de la PII de todas las organizaciones que participan en la prestación o utilización de los servicios.

Los controles descritos en esta Especificación pueden ser utilizados como referencia en organizaciones que llevan a cabo el procesamiento de la PII y están destinados a aplicarse en todas las organizaciones que cumplen la función de controladores de la PII. Las organizaciones que ejercen de procesadores de PII deberían hacerlo con arreglo a las instrucciones del controlador de la PII. Los controladores de la PII tendrían que garantizar que sus procesadores de PII estén en condiciones de implementar todos los controles necesarios contemplados en su acuerdo de procesamiento de la PII, de conformidad con el propósito del procesamiento de la PII. Los controladores de la PII que utilizan servicios en la nube como procesadores de PII pueden revisar la norma ISO/CEI 27018 para identificar los controles pertinentes que deben implementarse.

Los controles indicados en esta Especificación se explican con más detalle en las cláusulas 5 a 18, junto con directrices de implementación. La implementación puede ser más sencilla si se han tenido en cuenta los requisitos para la protección de la PII en el diseño del sistema de información, los servicios y las operaciones de la organización. Se trata de un elemento del concepto que suele conocerse como "privacidad por diseño (PdD)". En ISO/CEI 29134 puede hallarse una información más completa sobre la selección de controles y otras opciones en materia de tratamiento del riesgo. En la bibliografía se enumeran otras referencias de interés.

4.5 Elaborar directrices propias de una organización

Esta Especificación puede considerarse un punto de partida para la elaboración de directrices propias de una organización. No todos los controles y directrices descritos en la presente Especificación son aplicables a todas las organizaciones.

Por otra parte, pueden ser necesarios controles y directrices adicionales no contemplados en la presente Especificación. Cuando se elaboran estos documentos que contienen directrices o controles adicionales, puede ser de utilidad incluir referencias cruzadas en las cláusulas de la presente Especificación, llegado el caso, para facilitar a auditores y asociados comerciales la verificación del cumplimiento.

4.6 Consideraciones relativas al ciclo de vida

La PII tiene un ciclo de vida natural, desde la creación u origen, la recopilación, a través del almacenamiento, utilización y transferencia, hasta su eventual eliminación (por ejemplo, destrucción segura). El valor de la PII y los riesgos que afronta pueden variar durante su ciclo de vida pero, en cierta medida, la protección de la PII sigue siendo importante en todas las etapas y todos los contextos de su ciclo de vida.

Los sistemas de información tienen también ciclos de vida en el marco de los cuales se conciben, se especifican, se diseñan, se elaboran, se ponen a prueba, se implementan, se utilizan, se mantienen y, finalmente, se retiran del servicio y se eliminan. También habría que tener en cuenta la protección de la PII en cada una de esas etapas. La evolución de los nuevos sistemas y los cambios introducidos en los sistemas existentes ofrecen a las organizaciones la oportunidad de actualizar y mejorar los controles de seguridad y los controles para la protección de la PII, teniendo en cuenta los incidentes reales y los riesgos para la privacidad y la seguridad actuales y previstos.

4.7 Estructura de esta Especificación

La presente Especificación contiene dos partes normativas principales.

La primera parte, integrada por las cláusulas 5 a 18, contempla directrices de implementación adicionales y otras informaciones relativas a ciertos controles existentes de interés descritos en ISO/CEI 27002. En el formato de esta

primera parte se utilizan los encabezamientos y numeraciones pertinentes de las cláusulas de ISO/CEI 27002 que permiten realizar referencias cruzadas a esa Norma Internacional.

La segunda parte contempla un conjunto específico de controles para la protección de la PII especificados en el Anexo A. Se utiliza el mismo formato de ISO/CEI 27002, que especifica los objetivos de control (texto en un recuadro), seguidos de uno o más controles que pueden aplicarse. Las descripciones de los controles tienen la siguiente estructura.

Control

El texto en este encabezamiento define la declaración de control específica para cumplir el objetivo de control.

Directrices de implementación para la protección de la PII

El texto en este encabezamiento proporciona información más detallada para respaldar la implementación del control y el cumplimiento de los objetivos de control. Las directrices descritas en esta Especificación quizá no se adaptan completamente a todas las situaciones o son insuficientes, y pueden no cumplir los requisitos de control propios de una organización. En consecuencia, pueden resultar adecuados controles alternativos o adicionales, u otras formas de tratamiento del riesgo (evitar o transferir riesgos).

Otras informaciones para la protección de la PII

El texto en este encabezamiento proporciona información adicional que quizá sea necesario tener en cuenta, como las consideraciones de carácter jurídico y las referencias a otras normas.

5 Políticas en materia de seguridad de la información

5.1 Orientación de gestión para la seguridad de la información

5.1.1 Introducción

Se aplica el objetivo especificado en el apartado 5.1 de ISO/CEI 27002:2013.

5.1.2 Políticas para la seguridad de la información

Se aplican el control 5.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de aplicación relativas a la protección de la PII

Las políticas de seguridad de la información deberían incluir declaraciones adecuadas de medidas de seguridad para la protección de la PII. La información sobre la protección de PII está disponible en 18.1.4 de ISO/CEI 27002:2013.

Al diseñar, implementar y examinar la política de seguridad de información, las organizaciones deberían considerar los requisitos de protección de la privacidad descritos en ISO/CEI 29100.

Las organizaciones deben especificar los elementos de protección de PII no relativos a la seguridad como una política de privacidad separada. Véase la directriz en la cláusula A.2.

5.1.3 Examen de las políticas para la seguridad de la información

Se aplican el control 5.1.2 y las directrices de implementación especificadas en ISO/CEI 27002.

6 Organización de la seguridad de la información

6.1 Organización interna

6.1.1 Introducción

Se aplica el objetivo especificado en el apartado 6.1 de ISO/CEI 27002.

6.1.2 Funciones y responsabilidades en materia de seguridad de la información

Se aplican el control 6.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las funciones y responsabilidades para la protección de la PII se deben definir claramente, documentar adecuadamente y comunicar convenientemente, concretamente:

a) la responsabilidad de proteger la PII debería atribuirse a un alto dirigente claramente identificado (en ocasiones denominado Director encargado de la privacidad) de la organización;

b) la responsabilidad de coordinar las funciones de seguridad de la información dentro de la organización debería atribuirse a una o varias personas claramente identificadas (a saber, la función de protección de la PII); y

c) todas las personas que participan en el procesamiento de la PII (incluidos los usuarios y el personal de apoyo) deberían cumplir con los requisitos de protección de la PII señalados en su descripción de empleo.

La función de protección de la PII establecida debería estar estrechamente relacionada con otras funciones para el procesamiento de la PII, la función de seguridad de la información, que implementa requisitos de seguridad que incluye los dispuestos en la legislación en materia de protección de la PII, así como la función jurídica, que ayuda a interpretar leyes, reglamentos y cláusulas contractuales, y a manejar fallos en la seguridad de los datos.

La organización debería estudiar la necesidad de crear un consejo o comité polivalente integrado por altos funcionarios encargados de las funciones de procesamiento de la PII, y establecerlo según proceda. Habida cuenta de que la protección de la PII constituye una función multidisciplinaria, dicho grupo contribuiría de manera proactiva a identificar las posibilidades de mejora, identificar nuevos riesgos y ámbitos en los que realizar evaluaciones de la incidencia para la privacidad, planificar medidas preventivas, tomar medidas de detección y de reacción ante cualquier fallo, etc. Se recomienda que dicho grupo se reúna periódicamente y esté presidido por la persona encargada de la protección de la PII señalada en el apartado a).

El controlador de PII debería exigir a su(s) procesador(es) de PII que designaran un punto de contacto al que se puedan enviar preguntas acerca de la tramitación de la PII en el marco del contrato de procesamiento de la PII.

Las personas encargas de las funciones de protección de la PII deberían informar a un Director encargado de la privacidad para asegurarse de que tienen la suficiente autoridad para ejercer sus responsabilidades.

6.1.3 Segregación de tareas

Se aplican el control 6.1.2 y las directrices de implementación asociadas especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las tareas y el ámbito de competencia relativos a la protección de la PII deberían ser independientes de los relativos a la seguridad de la información. Si bien se reconoce la importancia de la seguridad de la información para la protección de la PII, es importante que las tareas y el ámbito de competencia de la seguridad y de la protección de la PII sean lo más independientes posible. De ser necesario o útil, en aras de la protección de la PII, se debería facilitar la coordinación y cooperación entre los responsables de la seguridad de la información y de la protección de la PII.

Las organizaciones deberían adoptar el principio de segregación de las tareas al asignar derechos de acceso para el procesamiento de la PII, sobre todo en el procesamiento considerado de alto riesgo.

El acceso a la PII que se está procesando y el acceso a los ficheros de registro relativos a dicho procesamiento deberían ser tareas diferenciadas.

El acceso a la información sobre la recopilación de la PII con objeto de atender a las solicitudes de los titulares de la PII debería diferenciarse de todas las demás formas de acceso a la PII. El acceso debería limitarse a las personas cuyas competencias incluyen responder a las solicitudes de titulares de la PII.

6.1.4 Contacto con las autoridades

Se aplican el control 6.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Cuando corresponda, las organizaciones deberían contar con procedimientos que especificasen cuándo y quién debería ponerse en contacto con las autoridades (incluidas las autoridades de protección de datos), por ejemplo, para señalar una violación de la privacidad o informar de detalles de procesamiento.

6.1.5 Contacto con grupos de interés especial

Se aplican el control 6.1.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

6.1.6 Seguridad de la información en la gestión de proyectos

Se aplican el control 6.1.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Antes de iniciar cualquier proyecto nuevo, se debería realizar al menos un análisis umbral para determinar si es necesario realizar una PIA. Cabe señalar que el término "proyecto" abarca todos los incidentes que pueden producirse cuando una organización implanta o modifica una tecnología, un producto, un servicio, un programa, un sistema de información, un proceso o un proyecto nuevo o existente.

Pueden obtenerse orientaciones adicionales en la PIA especificada en ISO/CEI 29134.

6.2 Dispositivos móviles y teletrabajo

6.2.1 Introducción

Se aplica el objetivo especificado en el apartado 6.2 de ISO/CEI 27002:2013.

6.2.2 Política acerca de los dispositivos móviles

Se aplican el control 6.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían limitar estrictamente el acceso a la PII desde los dispositivos portátiles y móviles, como ordenadores portátiles, teléfonos celulares, dispositivos USB y PDA, que suelen estar más expuestos a riesgos más importantes que los dispositivos que no son portátiles (por ejemplo, los ordenadores de sobremesa instalados en la organización), dependiendo de la evaluación del riesgo.

Las organizaciones deberían limitar estrictamente el acceso remoto a la PII y, cuando el acceso remoto es inevitable, asegurarse de que las comunicaciones por acceso remoto están encriptadas, los mensajes están autenticados y la integridad está protegida.

6.2.3 Teletrabajo

Se aplican el control 6.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

7 Seguridad de los recursos humanos

7.1 Anterior al empleo

7.1.1 Introducción

Se aplica el objetivo especificado en el apartado 7.1 de ISO/CEI 27002:2013.

7.1.2 Selección

Se aplican el control 7.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

7.1.3 Condiciones de empleo

Se aplican el control 7.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

7.2 Durante el empleo

7.2.1 Introducción

Se aplica el objetivo especificado en el apartado 7.2 de ISO/CEI 27002:2013.

7.2.2 Responsabilidades de gestión

Se aplican el control 7.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

7.2.3 Concienciación, educación y formación en materia de seguridad de la información

Se aplican el control 7.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Deberían establecerse medidas para concienciar al personal pertinente sobre las consecuencias que puede tener para el controlador de PII (por ejemplo, consecuencias jurídicas, pérdida del negocio, o daños causados a la marca o a la reputación), para los miembros del personal (por ejemplo, consecuencias disciplinarias) y para el titular de la PII (por ejemplo, consecuencias físicas, materiales y emocionales) la violación de las normas y los procedimientos de privacidad o seguridad, especialmente aquellos que intervienen en el procesamiento de la PII.

Al igual que la concienciación, educación y formación en materia de seguridad de la información, las organizaciones deberían asegurarse de que se imparten cursos de formación, educación y concienciación sobre la protección y el procesamiento de la PII.

7.2.4 Proceso disciplinario

Se aplican el control 7.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían adoptar una política disciplinaria oficial. Esta política, en caso de violación de la privacidad, debería comunicarse claramente a las personas afectadas. Las organizaciones deberían velar por la aplicación de esta política en todos los casos de violación de la privacidad.

7.3 Terminación y cambio de empleo

7.3.1 Introducción

Se aplica el objetivo especificado en el apartado 7.3 de ISO/CEI 27002:2013.

7.3.2 Terminación o cambio de responsabilidades de empleo

Se aplican el control 7.3.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

8 Gestión de activos

8.1 Responsabilidad de los activos

8.1.1 Introducción

Se aplica el objetivo especificado en el apartado 8.1 de ISO/CEI 27002:2013.

8.1.2 Inventario de activos

Se aplican el control 8.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían establecer, mantener y actualizar un inventario de activos, por ejemplo, con la información procedente del informe PIA, en su caso, tal y como se especifica en ISO/CEI 29134. Se deberían incluir los activos PII y todos los sistemas que procesan PII.

Al desarrollar y mantener el inventario, las organizaciones deberían extraer los siguientes elementos de información de las PIA relativos a los sistemas de información que procesan PII. A continuación se muestra una lista de ejemplo (se pueden añadir o suprimir elementos en las listas finales aplicadas):

a) nombre y acrónimo de cada sistema identificado;

b) tipos de PII procesada por dichos sistemas;

c) clasificación (véase 8.2.2) de todos los tipos de PII, tanto como elementos de información individuales como elementos combinados en dichos sistemas de información;

d) nivel de incidencia posible, para el titular de la PII y la organización, de cualquier fallo en la seguridad de la PII;

e) finalidad(es) para la recopilación de la PII;

f) si el procesamiento de la PII se va a subcontratar a un procesador de PII;

g) si la PII se transmite a otros controladores de PII, y, en su caso, a quién (o a qué grupo de destinatarios);

h) periodo de retención de la PII;

i) zona geográfica en que se recopiló o procesó la PII; y

j) si se trata de una transferencia de datos transfronteriza.

Las organizaciones deberían proporcionar actualizaciones periódicas del inventario de la PII a la persona encargada de la protección de la PII para apoyar el establecimiento de controles de seguridad adecuados para todos los sistemas de información nuevos o actualizados que procesan PII.

8.1.3 Propiedad de los activos

Se aplican el control 8.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

8.1.4 Utilización aceptable de los activos

Se aplican el control 8.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían proteger los activos que soportan PII de los accesos no autorizados, las modificaciones no autorizadas, las supresiones no autorizadas, las pérdidas o destrucciones, los procesamientos incorrectos o ilegales, etc.

8.1.5 Devolución de los activos

Se aplican el control 8.1.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

8.2 Clasificación de la información

8.2.1 Introducción

Se aplica el objetivo especificado en el apartado 8.2 de ISO/CEI 27002:2013.

8.2.2 Clasificación de la información

Se aplican el control 8.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían clasificar toda la información con PII utilizando una categoría de clasificación existente (llamada grupo de información en ISO/CEI 27002) o categorías de clasificación creadas recientemente. Las nuevas categorías de clasificación deberían incluir, entre otras, categorías generales como las PII sensibles y no sensibles. Un esquema de clasificación también podría incluir categorías más específicas como PHI, PFI. Si las organizaciones crean nuevas categorías de clasificación, los niveles de protección para ellas también deberían definirse. Las categorías que se utilicen realmente deberán depender también de factores como los requisitos definidos en la legislación y reglamentación pertinentes sobre protección de datos, otras obligaciones jurídicas (por ejemplo, contractuales), la naturaleza y el grado de confidencialidad de la información, y el riesgo que supondría un fallo.

Cierta PII clasificada como no confidencial en un país puede considerarse confidencial en otro, según las leyes de protección de datos aplicables.

Para poder clasificar un elemento de PII puede ser necesario reevaluarlo y modificarlo cuando está asociado con uno o más atributos adicionales. Deberían establecerse directrices y procedimientos adecuados.

8.2.3 Marcado (etiquetado) de la información

Se aplican el control 8.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplica la siguiente directriz adicional.

Directriz de aplicación para la protección de PII

Cuando una organización no clasifica PII a una categoría de clasificación, la organización debe velar por que la gente bajo su control conozca la definición de PII y cómo reconocer si la información es PII.

8.2.4 Utilización de los activos

Se aplican el control 8.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplica la siguiente directriz adicional.

Directriz de aplicación para la protección de PII.

Si las organizaciones permiten a su personal omitir el etiquetado de información para la categoría de clasificación a PII, deberán velar por que el personal maneje toda la información con PII como información de la categoría de clasificación asignada.

8.3 Utilización de soportes

8.3.1 Introducción

Se aplica el objetivo especificado en el apartado 8.3 de ISO/CEI 27002:2013.

8.3.2 Gestión de los soportes amovibles

Se aplican el control 8.3.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Algunas jurisdicciones pueden requerir que los soportes amovibles con PII estén encriptados. Independientemente de que lo exija la legislación, el encriptado se recomienda para reducir el riesgo de filtraciones de PII.

Si bien es cierto que la confidencialidad e integridad de los datos son consideraciones importantes, las técnicas criptográficas deberían utilizarse para proteger la PII en soportes amovibles. Se debería realizar una evaluación de los riesgos para identificar el nivel de protección requerido que, a su vez, permitirá determinar el tipo, la intensidad y la calidad del algoritmo criptográfico que se necesita utilizar.

En el punto 10.1 se ofrecen orientaciones adicionales sobre el uso de los controles criptográficos.

8.3.3 Eliminación de soportes

Se aplican el control 8.3.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Los procedimientos de eliminación segura de soportes con PII deberían ser proporcionales a la confidencialidad de la información así como al nivel de incidencia que tendría un procesamiento inadecuado de dicha información. Algunas jurisdicciones pueden imponer criterios a los procedimientos que se emplean para eliminar soportes que contienen PII o determinados tipos concretos de PII (por ejemplo, datos sobre salud, datos financieros, etc.).

8.3.4 Transferencia de soportes físicos

Se aplican el control 8.3.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Cuando se utilicen soportes físicos para transferir información, se debería establecer una medida para registrar los soportes físicos entrantes y salientes que contienen PII, incluido el tipo de soporte físico, los números de identificación (por ejemplo, los números de serie o los números de inventario), los expedidores/destinatarios autorizados, la fecha y hora, el número de soporte físico, y los tipos de PII que contienen para detectar la pérdida de soportes físicos. La

finalidad y el alcance de la transferencia, la persona encargada de autorizarla y la base jurídica/contractual de la misma también deberían estar documentadas. También debería estudiarse la posibilidad de hacer una referencia explícita al principio de minimización de datos.

9 Control de acceso

9.1 Prescripciones comerciales en materia de control de acceso

9.1.1 Introducción

Se aplica el objetivo especificado en el apartado 9.1 de ISO/CEI 27002:2013.

9.1.2 Política de control de acceso

Se aplican el control 9.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002:2013.

9.1.3 Acceso a redes y servicios de red

Se aplican el control 9.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.2 Gestión del acceso de los usuarios

9.2.1 Introducción

Se aplica el objetivo especificado en el apartado 9.2 de ISO/CEI 27002:2013.

9.2.2 Registro y cancelación del registro de usuarios

Se aplican el control 9.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Los procedimientos para el registro y la cancelación del registro de usuarios, así como para la gestión del ciclo de vida del usuario, deberían prever medidas sobre el compromiso de control de acceso de los usuarios, como la corrupción o el compromiso respecto de las contraseñas o demás información de registro de los usuarios (por ejemplo, como consecuencia de una divulgación involuntaria).

9.2.3 Suministro de acceso a los usuarios

Se aplican el control 9.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían otorgar a los usuarios derechos de acceso adecuados a los sistemas de información que procesan PII según el principio de minimización de datos descrito en ISO/CEI 29100.

Las organizaciones deberían restringir el acceso a los sistemas de información que procesan PII a un número mínimo de personas necesarias para perseguir los propósitos especificados para dicho procesamiento con arreglo al principio de minimización de datos descrito en ISO/CEI 29100.

Las organizaciones deberían adoptas métodos de autenticación sólidos para determinada PII y tipos de procesamiento de la PII (por ejemplo, datos sobre la salud).

9.2.4 Gestión de los derechos de acceso privilegiado

Se aplican el control 9.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

El procesamiento de la PII a gran escala (por ejemplo, consulta, modificación, exportación y supresión en bloque) aumenta el riesgo de incidentes a gran escala. Las organizaciones deberían prestar especial atención al otorgar derechos de acceso para realizar esas operaciones privilegiadas. A fin de evitar el mal uso de la PII, los derechos de acceso privilegiado para el procesamiento de la PII (en particular, el procesamiento de la PII de alto riesgo) deberían atribuirse

de manera estrictamente limitada. También deberían concederse de modo que contribuya a reducir el riesgo de colusión entre dos o más personas. La atribución y utilización de esos derechos debería quedar registrada en los ficheros de registro pertinentes. Todos los derechos de acceso deberían aprobarse por un periodo determinado. Las organizaciones deberían examinar periódicamente todas las aprobaciones y, según proceda, renovarlas, revocarlas o suprimirlas.

9.2.5 Gestión de la información de autenticación secreta de los usuarios

Se aplican el control 9.2.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.2.6 Examen de los derechos de acceso de los usuarios

Se aplican el control 9.2.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.2.7 Supresión o ajuste de los derechos de acceso

Se aplican el control 9.2.6, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.3 Responsabilidades de los usuarios

9.3.1 Introducción

Se aplica el objetivo especificado en el apartado 9.3 de ISO/CEI 27002:2013.

9.3.2 Utilización de la información de autenticación secreta

Se aplican el control 9.3.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.4 Control de acceso al sistema y las aplicaciones

9.4.1 Introducción

Se aplica el objetivo especificado en el apartado 9.4 de ISO/CEI 27002:2013.

9.4.2 Restricción de acceso a la información

Se aplican el control 9.4.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Antes de permitir a las personas, por ejemplo a los operadores y administradores, utilizar lenguajes de consulta que permiten extraer de manera masiva y automatizada PII de las bases de datos que contienen PII, las organizaciones deberían estudiar la necesidad de utilizar esos lenguajes al procesar la PII.

Cuando la utilización de lenguajes de consulta sea compatible con el requisito de protección, las organizaciones deberían establecer medidas técnicas para limitar el uso de dichos lenguajes al mínimo necesario para cumplir con los propósitos previstos.

Esto se traduce, por ejemplo, en que las restricciones de acceso limitan la utilización de lenguajes de consulta a unos pocos campos confidenciales predefinidos de los registros.

Cuando las personas necesitan acceder a ámbitos para los que normalmente no tienen autorización (por ejemplo, el ámbito operativo), deberían crearse mecanismos de aprobación sólidos. Las organizaciones deberían mantener un registro de todas esas aprobaciones.

9.4.3 Procedimientos de conexión seguros

Se aplican el control 9.4.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Cuando los titulares de la PII pueden solicitar cuentas a un controlador de PII, el controlador de PII debería proporcionar procedimientos de conexión seguros a dichas cuentas, en función de los resultados de un análisis de los riesgos.

9.4.4 Sistema de gestión de contraseñas

Se aplican el control 9.4.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.4.5 Uso de programas de utilidad privilegiados

Se aplican el control 9.4.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

9.4.6 Control de acceso al código fuente de los programas

Se aplican el control 9.4.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

10 Criptografía

10.1 Controles criptográficos

10.1.1 Introducción

Se aplica el objetivo especificado en el apartado 10.1 de ISO/CEI 27002:2013.

10.1.2 Política de uso de los controles criptográficos

Se aplican el control 10.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

10.1.3 Gestión de claves

Se aplican el control 10.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11 Seguridad física y del entorno

11.1 Zonas de seguridad

11.1.1 Introducción

Se aplica el objetivo especificado en el apartado 11.1 de ISO/CEI 27002:2013.

11.1.2 Perímetro de seguridad

Se aplican el control 11.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.1.3 Controles de acceso físico

Se aplican el control 11.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.1.4 Asegurar oficinas, salas y equipos

Se aplican el control 11.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.1.5 Protección contra las amenazas externas y del entorno

Se aplican el control 11.1.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.1.6 Trabajar en zonas seguras

Se aplican el control 11.1.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.1.7 Zonas de entrega y carga

Se aplican el control 11.1.6, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2 Equipos

11.2.1 Introducción

Se aplica el objetivo especificado en el apartado 11.2 de ISO/CEI 27002:2013.

11.2.2 Situación y protección de los equipos

Se aplican el control 11.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.3 Soporte de las utilidades

Se aplican el control 11.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.4 Seguridad del cableado

Se aplican el control 11.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.5 Mantenimiento de los equipos

Se aplican el control 11.2.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.6 Eliminación de activos

Se aplican el control 11.2.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.7 Seguridad de los equipos y activos fuera de los límites de la organización

Se aplican el control 11.2.6, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.8 Seguridad de los equipos abandonados o reutilizados

Se aplican el control 11.2.7, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

A efectos de garantizar la seguridad de los equipos abandonados o reutilizados, los equipos con soportes de almacenamiento que pueden contener también PII deberían destruirse físicamente o la PII se debería destruir, suprimir o sobrescribir utilizando técnicas aprobadas, de conformidad con procedimientos bien definidos y documentados, para que la PII original sea irrecuperable en lugar de utilizar la función clásica de borrado o formato. En el caso de los equipos que contienen soportes de almacenamiento con posible PII encriptada, tal vez sea suficiente destruir de manera controlada las claves de descifrado y/o los soportes de claves (como las tarjetas inteligentes).

11.2.9 Equipos de los usuarios sin vigilancia

Se aplican el control 11.2.8, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

11.2.10 Política de recogida y limpieza de despachos y pantallas

Se aplican el control 11.2.9, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12 Seguridad de las operaciones

12.1 Procedimientos operacionales y responsabilidades

12.1.1 Introducción

Se aplica el objetivo especificado en el apartado 12.1 de ISO/CEI 27002:2013.

12.1.2 Modos operatorios documentados

Se aplican el control 12.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.1.3 Gestión del cambio

Se aplican el control 12.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.1.4 Gestión de la capacidad

Se aplican el control 12.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.1.5 Separación de los entornos vinculados al desarrollo, a las pruebas y a las operaciones

Se aplican el control 12.1.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Los entornos vinculados al desarrollo, a las pruebas y a las operaciones deberían estar, como es lógico y en la medida de lo posible, físicamente separados. Deberían implantarse controles de acceso adecuados para velar por que el acceso se limite a las personas debidamente autorizadas. Si las redes o los dispositivos de pruebas o desarrollo requieren un acceso a la red operacional, deberían imponerse sólidos controles de acceso.

Las organizaciones deberían evaluar el riesgo que supone utilizar soportes amovibles y dispositivos con PII con capacidades inalámbricas, independientemente del entorno en que se utilizan.

Cuando la ley no lo permita o el titular de la PII no lo consienta explícitamente, la PII no debería utilizarse para fines de desarrollo y pruebas sin asegurar previamente la anonimización.

12.2 Protección contra los programas maliciosos

12.2.1 Introducción

Se aplica el objetivo especificado en el apartado 12.2 de ISO/CEI 27002:2013.

12.2.2 Controles contra los programas maliciosos

Se aplican el control 12.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.3 Copia de seguridad

12.3.1 Introducción

Se aplica el objetivo especificado en el apartado 12.3 de ISO/CEI 27002:2013.

12.3.2 Copia de seguridad de la información

Se aplican el control 12.3.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Los sistemas de información que procesan PII deberían introducir mecanismos adicionales o alternativos como copias de seguridad externas para protegerse frente a la pérdida de PII y garantizar la continuidad de las operaciones de procesamiento de la PII y la posibilidad de restablecer operaciones de procesamiento de la PII tras un evento perturbador, solamente si es estrictamente necesario.

NOTA 1 – Transcurre cierto tiempo entre el momento en que se realiza la copia de seguridad y las operaciones de recuperación. La PII almacenada en una copia de seguridad puede dejar de estar actualizada en el momento de acceder a ella para poder restablecerla. Las operaciones basadas en PII obsoleta pueden producir resultados incorrectos y suponer un riesgo para la privacidad.

12.4 Registro y control

12.4.1 Introducción

Se aplica el objetivo especificado en el apartado 12.4 de ISO/CEI 27002:2013.

12.4.2 Registro de eventos

Se aplican el control 12.4.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Siempre que sea posible, en el registro de eventos se debería registrar a qué PII se ha accedido, qué se ha hecho con la PII (por ejemplo, leer, imprimir, añadir, modificar, suprimir), cuándo y quién, especialmente en el caso de determinados tipos de PII (por ejemplo, los datos sobre la salud). Cuando varios proveedores de servicios participan en la prestación de servicios, puede haber funciones variadas o compartidas al aplicar estas directrices.

Se debería establecer un proceso para examinar el registro de eventos con una periodicidad especificada y documentada, con el fin de identificar irregularidades y proponer soluciones.

El controlador de PII debería definir procedimientos con respecto a si, cuándo y cómo se puede dar a conocer la información de registro al administrador o si, cuándo y cómo éste puede utilizarla para los fines de control de la seguridad y de diagnóstico operacional.

12.4.3 Protección de la información de registro

Se aplican el control 12.4.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

La información de registro registrada para fines de control de la seguridad y de diagnóstico operacional puede contener PII. Se deberían implantar medidas, como el control de acceso (véase 9.2.3), para garantizar que la información de registro se utilice únicamente para los fines previstos. También se deberían tomar medidas para velar por la integridad de los ficheros de registro.

12.4.4 Diarios de los administradores y operadores

Se aplican el control 12.4.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deberían vigilar el acceso privilegiado (por ejemplo, por los administradores del sistema y los operadores) a la PII y todo procesamiento ulterior realizado por esas personas. Dicho control debería formar parte del control global de los sistemas de información que procesan PII.

Las organizaciones deberían definir lo que consideran una actividad anómala y deberían aplicar procedimientos automatizados para informar de dicha actividad a las personas pertinentes dentro de la organización.

12.4.5 Sincronización de los relojes

Se aplican el control 12.4.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.5 Control de los programas informáticos operacionales

12.5.1 Introducción

Se aplica el objetivo especificado en el apartado 12.5 de ISO/CEI 27002:2013.

12.5.2 Instalación de programas informáticos en sistemas operativos

Se aplican el control 12.5.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.6 Gestión de las vulnerabilidades técnicas

12.6.1 Introducción

Se aplica el objetivo especificado en el apartado 12.6 de ISO/CEI 27002:2013.

12.6.2 Gestión de las vulnerabilidades técnicas

Se aplican el control 12.6.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.6.3 Restricciones en la instalación de programas informáticos

Se aplican el control 12.6.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

12.7 Consideraciones sobre la auditoría de los sistemas de información

12.7.1 Introducción

Se aplica el objetivo especificado en el apartado 12.7 de ISO/CEI 27002:2013.

12.7.2 Control de auditoría de los sistemas de información

Se aplican el control 12.7.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

13 Seguridad de las comunicaciones

13.1 Gestión de la seguridad de red

13.1.1 Introducción

Se aplica el objetivo especificado en el apartado 13.1 de ISO/CEI 27002:2013.

13.1.2 Controles de red

Se aplican el control 13.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

13.1.3 Seguridad de los servicios de red

Se aplican el control 13.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

13.1.4 Segregación en las redes

Se aplican el control 13.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

13.2 Transferencia de la información

13.2.1 Introducción

Se aplica el objetivo especificado en el apartado 13.2 de ISO/CEI 27002:2013.

13.2.2 Políticas y procedimientos de transferencia de información

Se aplican el control 13.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Deben adoptarse las medidas adecuadas para reducir el riesgo de filtraciones de PII en la transferencia de información. La solución consiste, en general, en la encriptación de los datos, otras medidas previas pueden incluir la desidentificación, el enmascaramiento o la ocultación.

13.2.3 Acuerdos de transferencia de información

Se aplican el control 13.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

13.2.4 Mensajería electrónica

Se aplican el control 13.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

13.2.5 Acuerdos de confidencialidad y de no divulgación

Se aplican el control 13.2.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deben especificar las condiciones bajo las cuales se puede realizar el procesamiento externo de la PII. Estas condiciones deben formar parte de un acuerdo adecuado (es decir, contrato, acuerdo de confidencialidad o de no divulgación).

14 Adquisición, desarrollo y mantenimiento de los sistemas

14.1 Necesidades de seguridad de los sistemas de información

14.1.1 Introducción

Se aplica el objetivo especificado en el apartado 14.1 de ISO/CEI 27002:2013.

14.1.2 Análisis y especificación de las necesidades de seguridad

Se aplican el control 14.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Cuando se desarrolla o realiza cambios significativos en los sistemas de información que procesan PII, se debe realizar una evaluación de consecuencias para la privacidad (PIA, *privacy impact assessment*). Las directrices para la realización de la evaluación pueden encontrarse en el Documento ISO/CEI 29134. Los resultados de la PIA deben utilizarse para determinar los controles para el tratamiento de los riesgos identificados durante proceso de PIA.

14.1.3 Seguridad de los servicios de aplicación en las redes públicas

Se aplican el control 14.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.1.4 Protección de las transacciones de los servicios de aplicación

Se aplican el control 14.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2 Seguridad de los procesos de desarrollo y de soporte técnico

14.2.1 Introducción

Se aplica el objetivo especificado en el apartado 14.2 de ISO/CEI 27002:2013.

14.2.2 Política de desarrollo seguro

Se aplican el control 14.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.3 Procedimientos de control de cambios en el sistema

Se aplican el control 14.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.4 Revisión técnica de las aplicaciones después de realizar cambio en la plataforma operativa

Se aplican el control 14.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.5 Restricciones a los cambios en los paquetes de software

Se aplican el control 14.2.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.6 Principios de ingeniería de los sistemas seguros

Se aplican el control 14.2.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.7 Entorno de desarrollo seguro

Se aplican el control 14.2.6, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.8 Desarrollo subcontratado

Se aplican el control 14.2.7, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.9 Pruebas de la seguridad del sistema

Se aplican el control 14.2.8, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

14.2.10 Pruebas de aceptación del sistema

Se aplican el control 14.2.9, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las pruebas de aceptación del sistema deben incluir también pruebas de los requisitos de protección de la privacidad.

14.3 Datos de las pruebas

14.3.1 Introducción

Se aplica el objetivo especificado en 14.3 de ISO/CEI 27002:2013.

14.3.2 Protección de los datos de las pruebas

Se aplican el control 14.3.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Los datos operativos que contengan PII no deben utilizarse normalmente para desarrollo y pruebas. La utilización de PII real en estos entornos incrementa el riesgo de poner en peligro la información. En su lugar, las organizaciones deben utilizar datos simulados o adoptar medidas para "esconder" (es decir, enmascarar, ocultar, desidentificar, etc.) cualquier dato real utilizado.

15 Relaciones con los proveedores

15.1 Seguridad de la información en las relaciones con los proveedores

15.1.1 Introducción

Se aplica el objetivo especificado en 15.1 de ISO/CEI 27002:2013.

15.1.2 Política de seguridad de la información en las relaciones con los proveedores

Se aplican el control 15.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

En el caso de que una organización necesite utilizar los servicios de un procesador de PII, la evaluación de los procesadores de PII debe realizarse en función de la experiencia, la fiabilidad y su capacidad para alcanzar los requisitos de protección de la PII definidos en la legislación aplicable, la reglamentación o en contratos u otros acuerdos legales.

La organización que actúa como controlador de PII debe disponer de un contrato firmado con cualquier proveedor que actúe como procesador de PII. El contrato debe definir claramente las funciones y responsabilidades entre el controlador de PII y el procesador de PII, y debe incluir las clausulas adecuadas relativas a la protección de la PII de manera a hacer al procesador de PII responsable del procesamiento realizado.

El controlador de PII debe asegurar al menos:

- una declaración adecuada de la escala, la naturaleza y los fines del procesamiento contratado;
- apoyo a las obligaciones del procesador de PII de dar a los titulares de la PII la posibilidad de acceder y revisar su PII y de atender todas las quejas de los titulares de la PII (véase la cláusula A.10);
- las medidas organizativas adicionales necesarias para cumplir con los requisitos legales o reglamentarios;
- la autorización del controlador de PII para realizar auditorías en las instalaciones del procesador de PII;
- las obligaciones de informar en los casos de filtración o pérdida de datos, de procesamiento no autorizado o de cualquier incumplimiento de los términos y condiciones del contrato, y de identificar las personas de contacto de cada parte;
- un método de envío de las instrucciones del controlador de PII al procesador de PII;
- las medidas aplicables a la terminación del contrato, en particular en lo relativo al borrado seguro de la PII en las instalaciones o la devolución de la PII y los soportes físicos.

El controlador de PII debe asegurar que sus procesadores de PII no realizan subcontrataciones adicionales del procesamiento (es decir, no utilizan subprocesadores) sin la aprobación previa del controlador de PII. El controlador de PII debe atenerse a toda la legislación y reglamentación relevante sobre este tema.

El controlador de PII debe asegurar que los procesadores de PII no procesan la PII para ningún fin diferente de los especificados en el contrato o en otro acuerdo legal.

El controlador de PII debe asegurar que los procesadores de PII se deshacen de las PII de manera segura de acuerdo con las políticas del controlador de PII u otras directrices (por ejemplo, los requisitos específicos de una agencia).

15.1.3 La seguridad en los acuerdos con los proveedores

Se aplican el control 15.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

15.1.4 Cadena de suministro de las tecnologías de la comunicación y la información

Se aplican el control 15.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

15.2 Gestión de la entrega de los servicios de los proveedores

15.2.1 Introducción

Se aplican el objetivo especificado en el apartado 15.2 de ISO/CEI 27002:2013.

15.2.2 Control y revisión de los servicios de los proveedores

Se aplican el control 15.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

15.2.3 Gestión de cambios en los servicios de los proveedores

Se aplican el control 15.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

16 Gestión de los incidentes relativos a la seguridad de la información

16.1 Gestión de los incidentes relativos a la seguridad de la información y mejoras

16.1.1 Introducción

Se aplica el objetivo especificado en el apartado 16.1 de ISO/CEI 27002:2013.

16.1.2 Responsabilidades y procedimientos

Se aplican el control 16.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deben ser capaces de responder (y de estar preparadas para responder) de manera organizada y eficaz a un incidente relativo a la privacidad. Las organizaciones deben por lo tanto elaborar e implementar un plan de respuesta a los incidentes relativos a la privacidad.

El plan de respuesta a los incidentes relativos a la privacidad de una organización debe incluir:

a) la definición de incidente de privacidad y el ámbito de aplicación de la respuesta ante un incidente así;

b) el establecimiento de un equipo transversal de respuesta a los incidentes relativos a la privacidad que elabora, implementa, prueba, ejecuta y revisa el plan de respuesta a los incidentes contra la privacidad (la aprobación del plan debe realizarse por la dirección de la empresa);

c) funciones, responsabilidades y autoridad claramente definidas para todos los miembros del plan de respuesta a los incidentes relativos a la privacidad;

d) procedimientos para aclarar las bases legales de la colaboración con las organizaciones externas (nacionales o internacionales) en el caso de un incidente transfronterizo;

e) procedimientos para asegurar que todas las personas informan rápidamente, en el marco de la política de privacidad interna (es decir, empleados, contratados, etc.), de cualquier incidente relativo a la privacidad a los responsables de la seguridad de la información y a la persona responsable de la protección de la PII (llamado algunas veces CPO (Director responsable de la privacidad)) de acuerdo con la dirección de la organización de gestión de los incidentes;

f) una evaluación de consecuencias del incidente (tareas) para determinar la naturaleza y la extensión de los daños potenciales o reales producidos a las personas afectadas (es decir, vergüenza, molestia o injusticia) o a la organización afectada;

g) un proceso para la identificación y adopción de las medidas necesarias para mitigar los daños identificados en el punto anterior y reducir las posibilidades de su repetición;

h) procedimientos para determinar si es necesario notificar a las personas afectadas y a otras entidades concretas (por ejemplo, el regulador), los tiempos y la forma de la notificación y, cuando sea necesario, la propia notificación.

Las organizaciones pueden elegir integrar sus planes de respuesta a los incidentes relativos a la privacidad con sus planes de respuesta a incidentes de seguridad o mantenerlos separados. Un incidente relativo a la seguridad de la información debe iniciar una revisión, por parte del responsable del controlador de PII, para determinar si se ha producido fallo en la seguridad de los datos que implique la PII, como parte del procedimiento de gestión de incidentes de seguridad.

Un evento de seguridad de la información puede no provocar el inicio de una evaluación de este tipo. Un evento de seguridad de la información puede incluir, sin limitaciones, envíos de ping y otros ataques mediante mensajes de difusión sobre los cortafuegos o los servidores de borde, exploraciones de puerto, intentos fallidos de inicio de sesión, ataques de denegación de servicio y rastreo de paquetes. Un evento de seguridad de la información no necesariamente pone en peligro real o potencial las PII, o los equipos e instalaciones que procesan PII.

16.1.3 Notificación de los eventos de seguridad de la información

Se aplican el control 16.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Cuando se pone en peligro la PII, no es posible proteger los derechos y los intereses de los titulares de la PII sin adoptar medidas inmediatas.

Algunas jurisdicciones pueden imponer requisitos específicos (es decir, en la legislación o las reglamentaciones) relativos a la comunicación y/o notificación de los incidentes de seguridad que impliquen PII (por ejemplo, procesamiento no autorizado, fallo de seguridad, etc.). Cuando ocurre un incidente de seguridad que implica PII, es necesario comunicar lo más rápidamente posible los detalles del incidente, incluidas las medidas propuestas por las organizaciones (la divulgación de las cuales puede estar sujeta a restricciones), a las autoridades relevantes: autoridades de protección de los datos, agencias encargadas de hacer cumplir la ley y personas afectadas por el incidente.

Las organizaciones deben proporcionar a los titulares de la PII afectados el acceso a unas medidas correctoras eficaces y adecuadas como la corrección o el borrado de información incorrecta, en el caso de que ocurra una violación de la privacidad.

16.1.4 Notificación de las debilidades de seguridad

Se aplican el control 16.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

16.1.5 Evaluación de los eventos de seguridad de la información y toma de decisiones correspondientes

Se aplican el control 16.1.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

16.1.6 Respuesta a los incidentes de seguridad de la información

Se aplican el control 16.1.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

16.1.7 Enseñanzas de los incidentes de seguridad

Se aplican el control 16.1.6, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

16.1.8 Recopilación de pruebas

Se aplican el control 16.1.7, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

17 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

17.1 Continuidad de la seguridad de la información

17.1.1 Introducción

Se aplica el objetivo especificado en 17.1 de ISO/CEI 27002:2013.

17.1.2 Planificación de la continuidad de la seguridad de la información

Se aplican el control 17.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

17.1.3 Implementación de la continuidad de la seguridad de la información

Se aplican el control 17.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

17.1.4 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Se aplican el control 17.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

17.2 Redundancias

17.2.1 Introducción

Se aplica el objetivo especificado en 17.2 de ISO/CEI 27002:2013.

17.2.2 Disponibilidad de los medios de procesamiento de la información

Se aplican el control 17.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

18 Conformidad

18.1 Conformidad con los requisitos legales y contractuales

18.1.1 Introducción

Se aplica el objetivo especificado en 18.1 de ISO/CEI 27002:2013.

18.1.2 Identificación de la legislación aplicable y de los requisitos contractuales

Se aplican el control 18.1.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Las organizaciones deben identificar las leyes y los reglamentos relativos a la protección de la PII a los que están sujetos. Si se identifican, las organizaciones deberán tomar medidas necesarias para esos requisitos. Los siguientes casos son ejemplos de esos requisitos.

a) Cuando se requiere protección adicional para ciertas categorías de PII (por ejemplo, identificador adicional, número de pasaporte o números de tarjeta de crédito), deberán utilizarse técnicas criptográficas como encriptación. Deberán tenerse en cuenta el tipo, la potencia y la calidad del algoritmo criptográfico. Los algoritmos criptográficos solo deberían seleccionarse de listas de algoritmos aprobados.

   El control de seguridad relativo a este requisito se especifica en 10.1.2.

b) Las jurisdicciones pueden imponer una frecuencia mínima de copia de seguridad de datos para información, incluido PII, así como una frecuencia mínima de revisión de procedimientos de recuperación y copia de seguridad.

   El control de seguridad relativo a este requisito se especifica en 12.3.2.

Las organizaciones deben realizar PIA e implementar los planes de tratamiento de la privacidad resultantes para asegurar que los programas y los servicios relacionados con el procesamiento de la PII cumplen los requisitos de protección de la privacidad. Puede encontrarse orientación adicional en ISO/CEI 29134.

Las organizaciones deben establecer un programa de auditoría para ayudar a verificar la conformidad del procesamiento de la PII con los requisitos relevantes de protección de la privacidad. El programa debe especificar la frecuencia de realización de estas auditorías.

Las organizaciones pueden realizar las auditorías (es decir, mediante una función interna de auditoría) o pueden realizarse mediante un tercero independiente con la cualificación adecuada.

Otra información para la protección de la PII

En muchos marcos jurídicos, el responsable del control de la PII es el responsable último de asegurar la conformidad, sin embargo todas las personas que participan en el procesamiento de la PII deben adoptar una actitud proactiva en la identificación de los requisitos relevantes de protección de la privacidad tanto legales como provenientes de otros factores.

Un mecanismo para asegurar que el procesamiento de la PII cumple y gestiona la conformidad lo proporciona el contrato entre el controlador de PII y el procesador de PII. El contrato debe asegurar una conformidad auditada por un tercero, que sea aceptado por el procesador de PII, por ejemplo, mediante la implementación de los controles relevantes de la Especificación ISO/CEI 27002 e ISO CEI 27018.

18.1.3 derechos de la propiedad intelectual

Se aplican el control 18.1.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

18.1.4 Protección de los registros

Se aplican el control 18.1.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

18.1.5 Privacidad y protección de la Información de Identificación Personal

Se aplican el control 18.1.4, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

18.1.6 Reglamentación sobre controles criptográficos

Se aplican el control 18.1.5, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

18.2 Revisión de la seguridad de la información

18.2.1 Introducción

Se aplica el objetivo especificado en 18.2 de ISO/CEI 27002:2013.

18.2.2 Revisión independiente de la seguridad de la información

Se aplican el control 18.2.1, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002. También se aplican las directrices adicionales siguientes.

Directrices de implementación para la protección de la PII

Si las auditorías por partes interesadas individuales no son factibles o pueden incrementar los riegos de seguridad, las organizaciones deben facilitar a las partes potencialmente interesadas, antes de la firma del contrato, pruebas independientes de que la implementación de la seguridad de la información es conforme con las políticas y procedimientos del controlador de la PII. Una auditoría independiente de relieve seleccionada por el controlador de PII debería normalmente ser un método suficiente para satisfacer las necesidades de las partes interesadas relativas al examen de las operaciones de procesamiento del controlador de PII, siempre y cuando se proporcione una transparencia suficiente.

18.2.3 Conformidad con las políticas y normas de seguridad

Se aplican el control 18.2.2, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

18.2.4 Examen de la conformidad técnica

Se aplican el control 18.2.3, las directrices de implementación asociadas y otras informaciones especificadas en ISO/CEI 27002.

Anexo A

Conjunto ampliado de controles para la protección de la PII

(Este anexo es parte integrante de esta Recomendación | Norma internacional.)

A.1 General

Se describen las definiciones de los nuevos objetivos, nuevos controles y nuevas directrices de implementación que forman un conjunto ampliado de controles para cumplir los requisitos específicos para la protección de la PII.

Las directrices en esta Especificación se basan en las directrices de ISO 29100:2011 y se asume la implementación previa de las directrices de la ISO 29100:2011.

La cláusula A.2 describe las políticas generales de PII mientras que las siguientes secciones reflejan los principios de privacidad descritos en la ISO/CEI 29100.

A.2 Políticas generales para la utilización y la protección de la PII

Objetivo: Proporcionar orientación y apoyo de gestión para la protección de la PII de acuerdo con los requisitos de negocio y las leyes y requisitos.

Control

Las organizaciones implicadas en el procesamiento de la PII deben establecer una política para la utilización y protección de la PII.

Directrices de implementación para la protección de la PII

Las políticas de privacidad deberían incluir declaraciones adecuadas (en políticas de privacidad independientes o como adiciones a políticas existentes) sobre el compromiso de cumplimiento de la gestión y su apoyo, con legislación aplicable sobre protección de la PII, requisitos contractuales y otras políticas internas.

Las políticas de privacidad y seguridad puede que no cubran los mismos asuntos, aunque estén relacionados. Tanto las políticas de seguridad de la información como las políticas de privacidad deberían abordar la confidencialidad, la integridad, la disponibilidad de la información y, además, las políticas de privacidad deberían abordar temas como el consentimiento y el acceso individual.

La ISO/CEI 29100 proporciona directrices para la implementación de un marco de privacidad. La política de protección de la PII debe:

- ser adecuada a los fines de la organización;
- ser transparente en lo relativo a la recopilación y procesamiento de la PII por la organización;
- ofrecer un marco para definir los objetivos para la protección de la PII;
- definir reglas para tomar decisiones en los temas de protección de la PII;
- definir criterios sobre la aceptación de riesgos a la privacidad (véase también 6.3.1 de ISO/CEI 29134);
- incluir un compromiso de cumplimiento de los requisitos de protección de la privacidad aplicables;
- incluir un compromiso de mejora continua;
- comunicarse dentro de la organización; y
- estar disponible para las partes interesadas, si procede.

A.3 Consentimiento y elección

A.3.1 Consentimiento

Objetivo: Hacer de los titulares de la PII unos participantes activos del proceso de decisión relativo al procesamiento de su PII, excepto en los casos limitados por la legislación o la reglamentación, mediante el ejercicio de un consentimiento dado de manera consciente, informada y libre.

Control

Las organizaciones deben proporcionar los medios necesarios para que los titulares de la PII puedan ejercer un consentimiento dado de manera consciente, informada y libre, excepto en los casos en los que el titular de la PII no puede libremente denegar su consentimiento o donde la ley aplicable permite específicamente el procesamiento de la PII sin el consentimiento del titular.

Directrices de implementación para la protección de la PII

La organización debe:

a) definir los medios prácticos necesarios para obtener el consentimiento de los titulares de la PII, analizar los casos en los cuales los medios prácticos elegidos ya no son operativos y definir soluciones alternativas en caso de necesidad para asegurar que se obtiene el consentimiento antes del inicio de cualquier procesamiento;

b) proporcionar los medios, donde sea factible y adecuado u obligatorio por ley, para que los titulares de la PII den su consentimiento, asegurando que se obtiene este consentimiento antes del inicio de cualquier procesamiento. El procesamiento incluye la recopilación, el almacenamiento, la modificación, la recuperación, la consulta, la divulgación, la desidentificación, el anonimato, la difusión u otras formas de divulgación, el borrado o la destrucción de la PII;

c) cuando un representante legal da el consentimiento (por ejemplo, en nombre de un menor o de una persona legalmente incapacitada), almacenar el registro del consentimiento;

d) cuando sea necesario, informar al titular de la PII de todas las partes de la PII transferidas a una tercera parte y proporcionar los medios adecuados para que los titulares de la PII puedan dar su consentimiento a esa transferencia;

e) obtener el consentimiento, cuando sea factible y apropiado u obligatorio por ley, de los titulares de la PII antes de cualquier nueva utilización o divulgación de PII recogidos previamente y asegurar que se obtiene el consentimiento antes de que se inicie cualquier procesamiento adicional;

f) asegurar que el consentimiento se obtiene de manera informada y transparente en cuanto a los fines del procesamiento y asegurar que ese consentimiento se obtiene para un fin concreto;

g) conseguir una mayor concienciación y más consentimiento, mediante información pública actualizada;

h) proporcionar un mecanismo para que los titulares de la PII puedan modificar el alcance de su consentimiento. Cualquier modificación del consentimiento debe tenerse en cuenta rápidamente y el procesamiento modificado o cesado de acuerdo con la revisión del consentimiento;

i) asegurar que el consentimiento tiene en cuenta todos los requisitos legales aplicables, incluidos, cuando sean necesarios, los requisitos sobre el consentimiento explícito relativo a la PII sensible;

j) cuando sea adecuado, permitir el consentimiento implícito, donde se informa claramente a los titulares de la PII del procesamiento y éstos no se han opuesto, pues este comportamiento puede indicar un acuerdo;

k) notificar previamente respecto de todas las operaciones de procesamiento antes de su implementación; y

l) confirmar, cuando sea necesario, la identidad del titular de la PII, o del representante legal del titular de la PII, que da el consentimiento para el procesamiento. La información solicitada para esta verificación debe ser la mínima para cumplir este fin, debe retenerse solamente lo mínimo esencial y debe eliminarse de manera segura cuando ya no se necesite.

Otra información para la protección de la PII

Las organizaciones deben obtener el consentimiento, de acuerdo con las leyes aplicables, mediante un consentimiento previo (*opt-in*) o un consentimiento implícito. El consentimiento previo requiere que el titular de la PII realice la acción concreta de permitir a las organizaciones recoger o utilizar sus PII. En el caso de consentimiento obtenido por medios electrónicos, la organización debe determinar si es adecuada la utilización de un consentimiento previo simple o es necesario el consentimiento previo doble.

Con el mecanismo de consentimiento previo, las organizaciones asumen que el titular de la PII ha consentido implícitamente al procesamiento de su PII salvo que el titular de la PII realice una acción concreta para indicar otra cosa.

El consentimiento implícito de una persona se deduce generalmente de las acciones de esta persona, de la ausencia de acciones o de las circunstancias de éstas. Un ejemplo de consentimiento implícito: un cliente proporciona la dirección de envío a una tienda en línea, y la tienda utiliza la información exclusivamente con el fin de entregar los productos que el cliente ha comprado.

Las organizaciones deberán proporcionar los medios para facilitar la obtención de un consentimiento separado de los titulares de la PII en los casos en que se recoge el número de identificación nacional (por ejemplo, número de la seguridad social, número de registro de residente, número de pasaporte).

En algunos casos, las organizaciones pueden proporcionar una selección de temas a los titulares de la PII para que éstos indiquen si quieren ser contactados en relación con cualquiera de los temas propuestos. En esta situación, las organizaciones construyen mecanismos de consentimiento para asegurar que las operaciones de la organización cumplen las preferencias de los titulares de la PII dentro de lo posible.

El consentimiento puede ser electrónico o con una copia en papel, en función de los requisitos reglamentarios aplicables y de las consideraciones prácticas.

Si la PII se transfiere a otra una organización, o desde otra organización, las organizaciones deben establecer un proceso para actualizar sus registros y copiar las actualizaciones y los cambios realizados en los consentimientos (por ejemplo, modificación o revocación) por los titulares de la PII, y asegurar que estas actualizaciones y cambios se pasan a las organizaciones a la cuales se transfiere la PII. Solamente debe recogerse de los titulares de la PII y compartirse con otras organizaciones, la mínima cantidad de información necesaria para asegurar la actualización de los registros adecuados. Las organizaciones deben revisar periódicamente sus procesos para asegurar que no se procesa PII innecesaria.

A.3.2 Elección

Objetivo: Ofrecer a los titulares de la PII, cuando sea adecuado y factible, la posibilidad de elegir no permitir el procesamiento de su PII, rechazar o cancelar el consentimiento, oponerse a un tipo de procesamiento específico y explicar al titular de la PII las implicaciones de dar o denegar el consentimiento.

Control

Las organizaciones deben proporcionar a los titulares de la PII mecanismos claros, conocidos, fácilmente entendibles, accesibles y de bajo coste para expresar su elección respecto del procesamiento de la PII, excepto en los casos en los cuales el titular de la PII no puede retirar o rechazar libremente su consentimiento o donde la legislación aplicable permite específicamente el procesamiento de la PII sin el consentimiento del titular de la PII.

Directrices de implementación para la protección de la PII

Las organizaciones deben:

a) asegurar que los titulares de la PII que eligen una opción respecto del procesamiento de su PII pueden hacerlo antes de que se inicie cualquier procesamiento;

b) no bloquear el servicio de un titular de la PII que rechaza proporcionar PII no relevante para ese servicio;

c) cuando sea preceptivo según la legislación o la reglamentación relevante, determinar los medios prácticos necesarios para permitir que los titulares de la PII ejerzan su derecho a oponerse al procesamiento de su PII. Debe ofrecerse a los titulares de la PII diferentes medios para ejercer este derecho (por ejemplo, correo postal, correo electrónico o teléfono);

d) reconocer la notificación de oposición dentro de los plazos especificados en la ley correspondiente o en la política de la organización;

e) analizar los casos en los cuales los medios elegidos ya no son operativos e identificar soluciones alternativas, en caso de necesidad, para permitir que los titulares de la PII puedan seguir ejerciendo su derecho de oposición en un tiempo adecuado;

f) asegurar que se clasifica, se etiqueta y se almacena la PII de una manera que facilite el ejercicio del derecho de oposición y asegurar que los titulares de la PII pueden ejercer este derecho en un tiempo adecuado y sin coste;

g) confirmar la identidad del titular de la PII, o del representante legal del titular de la PII, que se opone al procesamiento. La información solicitada para esta verificación debe ser la mínima necesaria para cumplir este fin, debe retenerse solamente el mínimo tiempo esencial y debe eliminarse de manera segura cuando ya no se necesite;

h) asegurar, en el caso de que se necesiten motivos legales para ejercer el derecho de oposición, que los titulares de la PII que ejercen este derecho aporten los motivos suficientes para la oposición. Cualquier rechazo de cumplir la notificación de oposición debe detallar los motivos por los cuales el controlador de PII no considera legítimos los motivos aportados;

i) asegurar que se informa a todas las organizaciones con las cuales se ha compartido la PII de cualquier oposición presentada por el titular de la PII, y que estas organizaciones cumplen cualquier oposición válida; y

j) cuando sea posible, ofrecer a los titulares de la PII la posibilidad de oponerse a unos aspectos concretos del procesamiento de la PII, y no una aceptación u oposición de la totalidad.

Otra información para la protección de la PII

En muchos casos, dependiendo de la legislación aplicable, puede no ser necesario o práctico proporcionar un mecanismo de elección en la recopilación de la información pública disponible. Por ejemplo, no es necesario proporcionar un mecanismo de elección a los titulares de la PII cuando se obtiene el nombre y la dirección de un registro público o de un periódico.

A.4 Legitimidad y especificación de los fines

A.4.1 Legitimidad de los fines

Objetivo: Asegurar que los fines del procesamiento de la PII se ajustan a las leyes aplicables y disponen de una base legal.

Control

Las organizaciones deben adoptar las medidas adecuadas para asegurar que el procesamiento de la PII cumple las leyes aplicables y dispone de una base legal.

Directrices de implementación para la protección de la PII

Las organizaciones deben:

a) determinar si los procesamientos propuestos pueden realizarse con una base legal diferente del consentimiento (es decir, aplicación de las leyes, protección pública, obligaciones legales o interés legítimo del controlador de PII);

b) determinar si el procesamiento propuesto está sujeto a una base legal (es decir, aplicación de las leyes, protección pública u obligaciones legales) que prohíbe al titular de la PII realizar una elección respecto del procesamiento de su PII;

NOTA – Si la recopilación y el procesamiento de la PII se realizan a nivel internacional, la necesidad de consentimiento y la manera de realizarlo puede variar en los diferentes marcos legales que se aplican.

c) determinar la (base) autoridad legal que permite el procesamiento de la PII de manera general o asociado a un programa o sistema de información específicos; y

d) incorporar procedimientos que aseguran que el procesamiento se realiza de acuerdo a todas las reglamentaciones aplicables y sus interpretaciones por las autoridades competentes. Debe considerarse el contexto general del procesamiento cuando se determina la legitimidad de sus fines. Deben incluirse la naturaleza de la relación entre el controlador de PII y los titulares de la PII, los desarrollos científicos y tecnológicos y los cambios en los entornos culturales y de la sociedad.

Las organizaciones deben desarrollar procedimientos para asegurar que el procesamiento de la PII no se realiza de manera que incumple o pueda incumplir las obligaciones legales, incluidas las disposiciones legales, el derecho común y los términos contractuales.

Si la organización tiene un comité de empresa o sindicatos, las leyes aplicables pueden requerir la consulta de estos órganos cuando se determina la legitimidad de un fin en el caso de empleados.

Los responsables de programa deben consultar con la persona responsable de la protección de la PII (a veces definido como CPO) o su equivalente legal sobre la capacidad legal de un programa o actividad para recoger PII. La capacidad legal de recoger PII debe quedar documentada.

A.4.2 Especificación de los fines

Objetivo: Especificar los fines para los cuales se recoge la PII antes del momento de la recopilación y limitar la utilización posterior al cumplimiento de los fines originales.

Control

Las organizaciones deben comunicar a los titulares de la PII de quien van a recoger PII los fines para los cuales se recoge y los fines para los cuales se procesará. Esta comunicación debe realizarse antes de o durante la recopilación de la PII y antes del procesamiento de la PII para cualquier fin, o fines, no comunicados anteriormente al titular de la PII.

Directrices de implementación para la protección de la PII

Las organizaciones deben comunicar los fines al titular de la PII antes de que se recoja o utilice la información por primera vez para fines nuevos, utilizar en esta especificación un lenguaje claro y adaptado a las circunstancias y proveer suficientes explicaciones sobre la necesidad de procesar información sensible.

A menudo, el lenguaje legal autoriza expresamente la recopilación y la utilización específicas de PII. Cuando este lenguaje es general, y por lo tanto sujeta a las interpretaciones, las organizaciones deben asegurar, consultando el CPO y el responsable legal, que existe una conexión clara entre la autorización general y cualquier recopilación concreta de PII.

Una vez que se han determinado los fines específicos, se den describir claramente los fines en la documentación de conformidad con los aspectos de privacidad asociada o los formularios utilizados para la recopilación de los PII. Además, para evitar la recopilación y la utilización no autorizadas de la PII las personas que tratan la PII deben recibir una formación sobre las responsabilidades de la organización en la recopilación.

Las organizaciones deben:

a) identificar la PII útil para cada proceso de negocio;

b) separar la PII útil para cada proceso de negocio de manera lógica;

c) gestionar los diferentes derechos de acceso de acuerdo con los procesos de negocio (incluidas la gestión de salarios, la gestión de las peticiones de permisos y la gestión de carrera y promociones) y establecer un entorno TI dedicado para los sistemas que procesan la información PII más sensible; y

d) confirmar regularmente que las PII están separadas de manera eficaz y que no se han añadido nuevos destinatarios o interconexiones.

A.5 Limitación de la recopilación

Objetivo: Limitar la recopilación de la PII a la que está dentro de los límites definidos por las leyes aplicables y es estrictamente necesaria para los fines especificados.

Control

Las organizaciones deben implementar las medidas adecuadas para limitar el tipo y la cantidad de datos de la recopilación a los mínimos elementos necesarios para los fines descritos en la notificación (véase A.9.1) y ubicados dentro de los límites definidos por las leyes y reglamentos aplicables.

Directrices de implementación para la protección de la PII

Las organizaciones deben:

a) limitar la recopilación de la PII a los mínimos elementos necesarios para los fines descritos en la notificación (véase A.9.1) y para la cual el titular ha dado su consentimiento;

b) no recoger PII sensible salvo cuando la recopilación de la PII está legalmente autorizada o se ha conseguido un consentimiento; y

c) limitar la cantidad de información que se recoge de un titular de la PII de manera indirecta (es decir, mediante registros de acceso web o de sistemas).

Las organizaciones deben definir los fines del procesamiento de la PII, identificar la PII necesaria para alcanzar los fines, identificar la información que no es necesario recoger y confirmar que únicamente se recoge la información necesaria.

Las organizaciones deben considerar cuidadosamente qué PII es necesario recoger para alcanzar un fin concreto antes de proceder a la recopilación. Las organizaciones no deben recoger PII de manera indiscriminada.

Las organizaciones deben revisar regularmente los fines para los cuales están recogiendo PII para asegurar que todavía son válidos. También deben revisar regularmente la PII que recogen para asegurar que sigue siendo la mínima necesaria para los fines.

Las organizaciones no deben recoger PII sensible, es decir, número de identificación nacional, salvo cuando la recopilación de esta información es legal o se ha obtenido el consentimiento explícito.

Otra información para la protección de la PII

Algunas jurisdicciones pueden definir ciertas categorías de PII (por ejemplo, origen racial, opiniones políticas, religiosas u otras creencias, datos de carácter personal sobre la salud, vida sexual o condenas, etc.) como sensible. Estas jurisdicciones pueden imponer restricciones o condiciones a la recopilación de este tipo de PII y las organizaciones deben tener en cuenta estas restricciones y condiciones cuando deciden que PII recoger.

A.6 Minimización de datos

Objetivo: Minimizar la PII procesada hasta lo estrictamente necesario para los intereses legítimos que persigue el controlador de la PII y limitar la divulgación de PII a un número mínimo de interesados en la privacidad.

Control

Las organizaciones deberían aplicar medidas adecuadas para minimizar la cantidad de PII procesada hasta lo estrictamente necesario para los intereses legítimos que persigue el controlador de la PII (por ejemplo, una organización puede tratar de aumentar o ampliar sus operaciones comerciales de tal manera que incremente de forma legítima la cantidad de PII que procesa y almacena).

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) garantizar la adopción de un principio basado en la "necesidad de saber", esto es, únicamente habría que dar acceso a la PII que es necesaria para la realización de las funciones oficiales en el marco de la finalidad legítima del procesamiento de la PII;

b) utilizar u ofrecer, en calidad de opciones por defecto, siempre que sea posible, interacciones y transacciones que no impliquen la identificación de titulares de la PII;

c) limitar la posibilidad de filtración de la PII recopilada;

d) llevar a cabo una evaluación inicial de la PII retenida por la organización y establecer y atenerse a un plan de revisión periódica para garantizar que se recopila únicamente la PII identificada en la notificación, y que la PII sigue siendo necesaria para cumplir los propósitos comerciales actuales;

e) restringir la transmisión de documentos electrónicos que contienen PII a un número mínimo de interesados que los necesiten para su trabajo;

f) determinar qué PII debería ser anónima o desidentificada teniendo en cuenta el contexto, la forma en que se almacena esa información (por ejemplo, campos de bases de datos o extractos de textos) y los riesgos identificados;

g) desidentificar los datos que lo necesitan basándose en la forma de los datos que deben desidentificarse (por ejemplo, bases de datos y registros textuales) y los riesgos identificados;

h) borrar y eliminar PII cuando haya expirado el propósito para el procesamiento PII, cuando no hay requisitos jurídicos para mantener la PII o cuando sea práctico hacerlo así; y

i) examinar si pueden utilizarse tecnologías que refuerzan la privacidad (PET), y cuáles.

El conjunto mínimo de elementos PII necesarios para respaldar los procesos comerciales de una determinada organización puede ser un subconjunto de la PII que la organización está autorizada a recopilar.

A efectos de su recopilación, la PII debería clasificarse en obligatoria y optativa. Las organizaciones deberían recopilar únicamente la PII obligatoria necesaria para la prestación de servicio y obtener el consentimiento de aceptación adecuado de los titulares de la PII cuando recopilan PII optativa. La organización no debería declinar la prestación de servicio cuando los titulares de la PII declinan facilitar PII optativa.

El CPO y el asesor jurídico deberían instar a los encargados del programa a que justifiquen el procesamiento de la PII propuesto con objeto de garantizar que se trata del mínimo necesario para que el sistema de información o la actividad cumplan el propósito jurídicamente autorizado.

NOTA 1 – La anonimización, definida en ISO/CEI 29100, es un proceso por el cual la PII está irreversiblemente alterada de tal manera que un titular de la PII ya no puede ser identificado directa o indirectamente, ni por el controlador de la PII a título individual ni en colaboración con ningún otro interesado. Ese proceso implica necesariamente una pérdida (irreversible) de información. En ciertos casos, suprimiendo simplemente parte de los datos puede alcanzarse el objetivo deseado.

NOTA 2 – Está previsto que una descripción de las técnicas de desidentificación de datos que refuerzan la privacidad, utilizada para describir y diseñar medidas de desidentificación, con arreglo a los principios de privacidad en ISO/CEI 29100 constituya el tema de una nueva Norma Internacional. Como regla general, para llegar a la conclusión de que un proceso de desidentificación cumple con la ley, la desidentificación debe llevarse a cabo mediante, por ejemplo, la supresión o la generalización de atributos, junto con medidas organizativas y técnicas sólidas.

NOTA 3 – Cuando una PII se procesa con un determinado fin, se minimiza la cantidad de PII procesada de modo que sirva sólo para el fin previsto, sin revelar excesiva información sobre el titular, por ejemplo, si se necesita la zona geográfica de un participante en una encuesta de tráfico, considerar la posibilidad de recopilar únicamente puntos de referencia cercanos y no una dirección precisa.

NOTA 4 – Habitualmente, durante el análisis de datos anónimos cuando los datos de salida constituyen un pequeño conjunto de datos, podría ser revelada la identidad de los titulares de la PII. Por tanto, una buena práctica consiste en evitar datos de salida cuando el número de registros es inferior a un umbral, por ejemplo, 10 registros. Se debe alcanzar cuidadosamente el umbral, teniendo en cuenta el patrón de distribución de datos.

Las organizaciones tendrían que reducir los riesgos para la privacidad y la seguridad reduciendo al mismo tiempo su inventario de PII, llegado el caso. Las organizaciones deberían realizar un examen inicial, y posteriores revisiones, de sus titulares de la PII para garantizar, en la medida de lo posible, que esa pila de datos sea exacta, pertinente, oportuna y completa.

Asimismo, convendría que las organizaciones redujeran el número de titulares de la PII al mínimo necesario para el rendimiento adecuado de un objetivo comercial orgánico documentado. Las organizaciones deberían elaborar y dar a conocer un calendario de revisiones periódicas de sus pilas de datos como complemento de su examen inicial.

Con la realización de evaluaciones periódicas, las organizaciones reducen el riesgo, procuran que se recopile únicamente los datos especificados en la notificación y aseguran que los datos recopilados son aún pertinentes y necesarios.

A.7 Restricciones en materia de utilización, retención y divulgación

A.7.1 Restricciones en materia de utilización, retención y divulgación

Objetivo: Limitar la utilización y divulgación de PII a fines específicos, explícitos y legítimos, y retener la PII no más de lo necesario para alcanzar los fines indicados o para cumplir las leyes aplicables.

Control

Las organizaciones deberían aplicar medidas adecuadas para limitar el procesamiento de la PII a fines legítimos y previstos, y retener la PII únicamente mientras sea necesario para alcanzar los fines indicados o para cumplir las leyes aplicables.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) limitar la utilización, retención y divulgación (incluida la transferencia) de PII hasta donde sea necesario para alcanzar fines específicos, explícitos y legítimos; y

b) configurar sus sistemas de información para registrar la fecha en que se recopila, crea o actualiza la PII y cuándo ésta será suprimida o archivada en virtud de un plan de retención de registros aprobado.

Directrices de implementación para la protección de la PII en materia de utilización

Las organizaciones deberían:

a) bloquear (esto es, archivar, proteger y exentar de un procesamiento adicional) toda PII cuando los fines indicados han expirado pero las leyes aplicables exigen la retención de esa información;

b) utilizar técnicas o métodos adecuados para garantizar una eliminación o destrucción segura de la PII (incluidos originales, copias y registros archivados);

c) utilizar únicamente la PII para los fines acordados con el titular de la PII o revelados a él, antes o en el momento de la recopilación, y obtener, si es necesario, el consentimiento antes de todo procesamiento para cualquier propósito nuevo;

d) limitar el acceso de terceros a los sistemas de la organización y a la PII a lo estrictamente necesario y que haya sido oficialmente autorizado. Si el acceso es realmente necesario para las actividades, debe llevarse a cabo el procedimiento de aprobación adecuado;

e) confirmar que en los sistemas de terceros autorizados a conectarse con los sistemas de la organización se han puesto en práctica las técnicas de seguridad apropiadas antes de otorgarles la debida autorización;

f) revisar periódicamente las técnicas de seguridad aplicadas por terceros para procurar que sigan cumpliendo los requisitos de seguridad de la organización. Si, como resultado de dicha revisión, se observa que esas técnicas son inadecuadas, habría que suspender la conexión de los sistemas de terceros hasta que demuestran que se han restaurado las técnicas de seguridad adecuadas;

g) aplicar el mecanismo de autenticación de acceso apropiado cuando se accede a la PII a través de interfaces a distancia. Se debe registrar el acceso a la PII; y

h) facilitar una notificación destinada al público para informarle de cualquier cambio en los titulares de la PII que haya tenido lugar durante el proceso de control de la seguridad.

Directrices de implementación para la protección de la PII en materia de retención

En ciertas circunstancias, una disposición jurídica puede dar lugar a una retención de la PII que excede los límites necesarios para los fines comerciales especificados.

Las organizaciones deberían:

a) retener únicamente la PII durante el periodo de tiempo autorizado para cumplir uno o más fines identificados en la notificación o exigidos por la ley y las organizaciones, y suprimirla rápidamente cuando expira el periodo de retención;

b) retener la PII, llegado el caso, más tiempo del necesario para los fines comerciales especificados e implementar medidas tales como desidentificación para proteger la PII;

c) definir periodos de retención de la PII de duración limitada y adecuada a los fines del procesamiento;

d) confirmar que el sistema de información puede detectar la expiración del periodo de retención;

e) asegurar que se implementan periodos de retención aceptados y se elimina la PII de acuerdo con los periodos de retención;

f) desarrollar una funcionalidad automatizada que suprima la PII cuando expira su periodo de retención. Esa supresión debería tener lugar inmediatamente o tan pronto como fuera posible;

g) determinar lo que convendría desidentificar en función del contexto, la forma en que se almacena la PII (incluidos campos de bases de datos o extractos de textos) y los riesgos identificados;

h) desidentificar los datos que lo necesitan basándose en la forma de los datos que deben desidentificarse (por ejemplo, bases de datos y registros textuales) y los riesgos identificados; y

i) elegir las herramientas (entre ellas, supresión parcial, segmentación, segmentación esencial e índice) para la protección de la PII si esos datos no pueden ser desidentificados.

Directrices de implementación para la protección de la PII en materia de divulgación

Las organizaciones deberían:

a) no divulgar la PII a terceros sin previo conocimiento y consentimiento del titular de los datos a menos que esa divulgación esté autorizada por la legislación correspondiente. El conocimiento y consentimiento del titular de la PII tal vez no sea necesario si esa información se divulga a terceros (por ejemplo, empleados) que tienen "necesidad de saber"; y

b) proporcionar un mecanismo de protección sólido cuando se transfiere la PII, incluida la encriptación de datos y la protección de la integridad.

La PII del empleado debería eliminarse (esto es, suprimirse o archivarse de manera segura) de conformidad con la legislación y reglamentación aplicables, y con las políticas de eliminación de la organización y, llegado el caso, el consentimiento del empleado.

A.7.2 Supresión de archivos temporales de manera segura

Objetivo: Proporcionar medidas técnicas para la supresión de archivos temporales dentro del periodo especificado.

Control

Los archivos y documentos temporales que puedan contener PII deberían suprimirse dentro del periodo especificado.

Directrices de implementación para la protección de la PII

Los sistemas de información pueden crear archivos temporales que quizá contengan PII en el curso normal de sus operaciones. Esos archivos son propios del sistema y la aplicación, pero pueden incluir sistemas de archivo con capacidad de reversión y archivos temporales asociados a la actualización de las bases de datos y el funcionamiento de otros software de aplicación. Por lo general, los archivos temporales no se necesitan una vez concluida la tarea de procesamiento de la información conexa, pero en ciertas circunstancias no se pueden suprimir de forma automática. Aunque no siempre se puede determinar durante cuánto tiempo siguen en uso, un procedimiento "recuperador de memoria" (*garbage collection*) debería identificar los archivos temporales pertinentes y determinar el tiempo transcurrido desde su última utilización.

Los sistemas de información encargados del procesamiento de la PII deberían realizar una verificación periódica que suprima los archivos temporales no utilizados a partir de una determinada edad.

A.7.3 Notificación de divulgación de PII

Objetivo: Procurar que el procesador de la PII notifique al controlador de la PII toda solicitud jurídicamente vinculante relativa a la divulgación de esa información.

Control

El contrato entre el controlador de la PII y el procesador de la PII debería exigir al procesador que notifique al controlador, en virtud de los procedimientos y periodos de tiempo acordados en el contrato, toda solicitud jurídicamente vinculante relativa a la divulgación de PII por la entidad encargada del cumplimiento de la ley u otra autoridad, a menos que dicha divulgación esté prohibida por la ley.

Directrices de implementación para la protección de la PII

Las organizaciones deberían implementar medidas (por ejemplo, obligaciones contractuales) para procurar que:

a) los procesadores de la PII consulten al controlador de la PII pertinente antes de aceptar toda solicitud jurídicamente vinculante relativa a la divulgación de PII, a menos que esté prohibida por la ley; y

b) los procesadores de la PII acepten toda solicitud aceptada por contrato relativa a la divulgación de PII, autorizada por el controlador de la PII pertinente, a menos que esté prohibida por la ley.

A.7.4 Registro de la divulgación de PII

Objetivo: Asegurar que se registra la divulgación de PII a terceros.

Control

La divulgación de PII a terceros debería ser registrada, comprendidos el tipo de PII divulgada y a quién, en qué momento y con qué fin se dio a conocer.

Directrices de implementación para la protección de la PII

La divulgación de PII puede tener lugar durante el curso de operaciones normales. Esa divulgación debería ser registrada. También debería registrarse cualquier información adicional a terceros, como la proveniente de investigaciones legítimas o auditorías externas. Los registros tendrían que incluir la fuente de la divulgación y la entidad que autoriza la divulgación.

A.7.5 Divulgación del procesamiento de la PII subcontratada

Objetivo: Asegurar que los procesadores de la PII revelan al controlador de la PII que recurren a subcontratistas.

Control

El procesador de la PII debería revelar al controlador de la PII que recurre a subcontratistas para llevar a cabo su tarea, antes de hacerlo.

Directrices de implementación para la protección de la PII

Las disposiciones para recurrir a subcontratistas con objeto de realizar el procesamiento de la PII deberían estar contempladas en el contrato entre el procesador y el controlador de la PII. En el contrato habría que especificar que los subcontratistas únicamente serán aceptados con la previa autorización del controlador de la PII. El procesador de la PII debería informar al controlador de la PII, con suficiente antelación, de cualquier cambio previsto en este sentido, de modo que el controlador esté en condiciones de oponerse a esos cambios o de poner fin al consentimiento.

La información divulgada tendría que dar cuenta del hecho de que se utiliza la subcontratación e indicar los nombres de los subcontratistas pertinentes, pero no dar detalles propios de las actividades de la empresa. La información divulgada debería incluir también los países en que los subcontratistas pueden procesar los datos y los medios por los cuales los subcontratistas están obligados a cumplir las obligaciones del procesador de la PII o a rebasarlas.

Si se evalúa que la divulgación pública de la información relativa al subcontratista aumenta el riesgo para la seguridad más allá de límites aceptables, dicha divulgación debería llevarse a cabo con arreglo a un acuerdo de confidencialidad y/o la solicitud del controlador de la PII. El controlador de la PII debería estar al corriente de la disponibilidad de la información sobre los subcontratistas utilizados.

A.8 Exactitud y calidad

Objetivo: Procurar que la PII procesada sea exacta, completa, actualizada, adecuada y pertinente a los efectos de su utilización.

Control

Las organizaciones deberían aplicar medidas adecuadas para procurar que la PII recopilada de un titular, directa o indirectamente, tenga la calidad adecuada.

Directrices de implementación para la protección de la PII

Por calidad de los datos se entiende lograr que la PII que se está procesando tenga la exactitud adecuada, sea completa, esté actualizada y sea pertinente a los efectos de su utilización.

Las organizaciones deberían:

a) establecer procedimientos de recopilación de la PII que contribuyan a asegurar la exactitud y la calidad de los datos;

b) recopilar la PII de tal forma que se detecte toda modificación una vez que se ha extraído de la fuente autorizada;

c) confirmar en la mayor medida posible, al recopilar o crear la PII, la exactitud, la pertinencia, la puntualidad y la exhaustividad de la PII;

d) garantizar la fiabilidad de la PII recopilada de una fuente distinta a la de su titular antes de que sea procesada;

e) verificar, con medios adecuados, la validez y precisión de las solicitudes de corrección formuladas por el titular de la PII antes de introducir cambios en esa información, llegado el caso;

f) comprobar periódicamente, y corregirla si procede, toda PII inexacta o desactualizada utilizada por sus programas o sistemas; y

g) formular directrices que aseguren y maximicen la exactitud, exhaustividad, conveniencia y pertinencia de la información divulgada. Convendría que las organizaciones adoptaran medidas razonables para confirmar la exactitud de la PII como, por ejemplo, la edición y validación de direcciones, pues son recopiladas o introducidas en los sistemas de información que utilizan interfaces de programación de aplicaciones (API) para la verificación automatizada de direcciones.

Ante el carácter suficientemente confidencial de la PII (por ejemplo, cuando se utiliza para la confirmación anual de los ingresos de un contribuyente para un beneficio recurrente), las organizaciones deberían incorporar mecanismos en los sistemas de información y elaborar los procedimientos correspondientes para indicar la frecuencia con que se actualizará esa información, y por qué medios.

Para reducir al mínimo la posibilidad de inexactitud de los datos, en la medida de lo posible, el titular de la PII tendría que introducirla directamente en los sistemas de información sin necesidad de que otra persona transcriba los datos. Si esa transcripción es inevitable, las organizaciones deberían considerar la posibilidad de permitir que el titular valide la PII transcrita. Esto contribuye a corregir errores antes de que se cometan daños a raíz del procesamiento de una PII inexacta.

Otras informaciones relativas a la protección de la PII

Los tipos de medidas adoptadas para proteger la calidad de los datos pueden fundarse en la naturaleza y el contexto de la PII, la forma en que se va a utilizar y cómo fue obtenida. Sería conveniente que las medidas adoptadas para validar la exactitud de cualquier PII confidencial fueran más amplias que las aplicadas para validar una PII menos confidencial. Pueden ser necesarias otras medidas para validar la PII que se obtiene de fuentes distintas a las de los titulares de la PII o de sus representantes autorizados.

A.9 Apertura, transparencia y notificación

A.9.1 Notificación de privacidad

Objetivo: Procurar que las notificaciones de privacidad contengan el nivel adecuado de detalles, estén redactadas en un lenguaje sencillo y sean de fácil acceso.

Control

Las organizaciones deberían aplicar medidas adecuadas para facilitar a los titulares de la PII las convenientes notificaciones sobre los fines del procesamiento de esa información.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) facilitar notificaciones eficaces a los titulares de la PII relativas a:
   1) las actividades que realizan y que afectan la privacidad, incluidas, aunque no de forma exhaustiva, la recopilación, la utilización, el intercambio, las técnicas de seguridad y la eliminación segura de la PII;
   2) la autoridad para recopilar la PII;
   3) las opciones, si las hubiere, que podrían tener los titulares de la PII con respecto a cómo la organización utiliza esa información y las consecuencias de ejercer o no esas opciones; y
   4) la posibilidad de oponerse al procesamiento de la información;
b) proporcionar mecanismos de notificación y consentimiento adaptados para atender a las necesidades operativas;
c) revisar sus notificaciones para que reflejen los cambios introducidos en la práctica o política que afecta la PII o los cambios realizados en las actividades que realizan y afectan la privacidad, antes de llevar a cabo esos cambios o tan pronto como sea posible después de los mismos;
d) garantizar que la notificación esté completa y sea apropiada para el destinatario teniendo en cuenta la naturaleza de la PII, los medios prácticos elegidos para facilitar la notificación y el carácter del vínculo entre el controlador y el titular de la PII;
e) presentar la información de forma clara para que pueda ser entendida por una persona no habituada a las tecnologías de la información, a Internet o a la jerga jurídica;
f) asegurarse de que la notificación se facilita antes o en el momento de la recopilación PII;
g) asegurar que la PII no puede ser recopilada sin que se haya facilitado la notificación;
h) determinar otras soluciones en el caso de que los medios prácticos ya no sean operativos;
i) ofrecer, de ser posible, un medio que permita mostrar que se ha facilitado la notificación;
j) si se facilita una notificación de privacidad por medios físicos, colocar esa información con una indicación que los titulares de la PII deberían visualizar o exigir que una notificación o un documento sean firmados o rubricados; y
k) definir una política para el suministro de etiquetas e indicaciones necesarias para informar a los titulares de la PII la utilización de la tecnología pertinente (esto es, sistemas de circuito cerrado de televisión (CCTV), Wi-Fi e identificación por radiofrecuencia (RFID)).

En la medida de lo posible, la notificación tendría que ser claramente visible en el lugar correspondiente (por ejemplo, en el sitio web de la organización o en una ubicación física), sin que el titular de la PII tenga que solicitarla expresamente.

A.9.2 Apertura y transparencia

Objetivo: Facilitar a los titulares de la PII una información clara y de fácil acceso sobre las políticas, los procedimientos y las prácticas del controlador de la PII con respecto al procesamiento de esa información.

Control

Las organizaciones deberían aplicar medidas adecuadas para facilitar a los titulares de la PII la conveniente información sobre sus políticas, procedimientos y prácticas de procesamiento de la PII.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) facilitar a los titulares de la PII una información clara y de fácil acceso sobre las políticas, los procedimientos y las prácticas del controlador de la PII con respecto al procesamiento de esa información;

b) revelar las opciones y medios que ofrece el controlador de la PII a los titulares de esa información con la finalidad de limitar el procesamiento de su información y para acceder a ella, corregirla y suprimirla.

Asimismo, las organizaciones deberían:

a) describir la PII que recopilan y una o más finalidades de esa recopilación;

b) indicar cómo utilizan la PII a nivel interno;

c) indicar si comparten la PII con entidades externas, las categorías de esas entidades y la finalidad de ese uso común;

d) indicar si los titulares de la PII pueden consentir utilizaciones específicas o la divulgación de dicha información y la forma de ejercer ese consentimiento;

e) precisar durante cuánto tiempo se retendrá la PII;

f) indicar si venden o transfieren datos para el procesamiento a través de organizaciones de análisis de datos y los detalles aplicables a los riesgos para la PII;

g) indicar cómo los titulares de la PII pueden tener acceso a esa información para modificarla o corregirla, llegado el caso;

h) facilitar información adecuada sobre las modalidades de protección de la PII;

i) asegurar que el titular de la PII tenga acceso a la información sobre sus actividades en materia de privacidad y pueda ponerse en contacto con su CPO;

j) facilitar, cuando se solicite, información relativa a la violación de la privacidad que ha ocasionado o puede ocasionar una violación de la privacidad de los solicitantes de PII, junto con todas las medidas asociadas que el solicitante podría adoptar para atenuar los riesgos adicionales causados por ese delito.

Las organizaciones deberían utilizar también diferentes mecanismos para informar al público acerca de las prácticas de privacidad que aplican, incluidos, pero sin limitarse a ellos, informes PIA, informes sobre privacidad, páginas web de acceso público, distribución de correos electrónicos, blogs y publicaciones periódicas (por ejemplo, boletines trimestrales). Las organizaciones también deberían utilizar direcciones de correo electrónico o líneas telefónicas que permitan al público formular comentarios y/o preguntas directas a las oficinas de privacidad con respecto a las prácticas en la materia.

A.10 Participación y acceso del titular de la PII

A.10.1 Acceso del titular de la PII

Objetivo: Ofrecer a los titulares de la PII la posibilidad de tener acceso a su información y revisarla, así como de controlar su exactitud y exhaustividad.

Control

Las organizaciones deberían aplicar medidas adecuadas para ofrecer a los titulares de la PII la posibilidad de tener acceso a su información, y de obtener la rectificación o supresión de esa PII.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) determinar los medios prácticos que se pondrán en marcha para permitir a los titulares de la PII ejercer su derecho de acceso (cuando así lo permita la legislación aplicable). Las personas deberían estar en condiciones de ejercer ese derecho en el momento oportuno y de forma comprensible para el titular, similar a los medios utilizados para recopilar la PII original (por ejemplo, por correo postal y/o correo electrónico);

b) analizar los casos en que los medios prácticos elegidos ya no son operativos e identificar soluciones alternativas, si es necesario;

c) permitir a los titulares de la PII tener acceso a la información que posee la organización, con el fin de evaluar su exactitud y solicitar la rectificación, llegado el caso;

d) responder, en la medida de lo posible, en forma equivalente a la utilizada para presentar la solicitud (por ejemplo, si la solicitud se envió por correo postal, la respuesta también se enviará por correo postal);

e) publicar las normas y disposiciones reglamentarias que indican de qué forma los titulares de la PII pueden solicitar el acceso a los registros mantenidos en su sistema;

f) permitir a los titulares de la PII que pongan en duda la exactitud y exhaustividad de la PII directa o indirectamente, y que la modifiquen, la corrijan o la supriman, según proceda y sea posible en el contexto específico;

g) establecer procedimientos que permitan a los titulares de la PII ejercer esos derechos de forma simple, rápida y eficaz, y que no suponga demoras (por ejemplo, las respuestas se proporcionarán con arreglo a la legislación o disposiciones reglamentarias aplicables o como se estipula en la política de la organización) ni costes indebidos;

h) establecer un proceso para informar a los titulares de la PII que presentan solicitudes la situación de su solicitud y la tramitación necesaria (por correo postal o correo electrónico, indicándose la recepción de la solicitud y la fecha prevista en la que recibirán una respuesta). En el caso de archivos almacenados, puede haber cierto margen con respecto a la fecha de respuesta si el controlador de la PII informa al titular de la PII que presenta la solicitud del calendario para la tramitación de la solicitud y si ha previsto un plazo razonable para dar una respuesta;

i) garantizar, en la medida en que lo permita la ley, el ejercicio permanente del derecho de acceso;

j) garantizar que únicamente tiene acceso a la PII la persona a la que se refiere esa información o un agente autorizado de esa persona. Por ello, se puede exigir la identificación y autenticación de manera satisfactoria a las personas que solicitan el acceso a la información. Los requisitos de esa identificación y autenticación pueden ser definidos en la legislación o las disposiciones reglamentarias aplicables;

k) determinar la forma conveniente de identificación y autenticación, si se exigen ambos requisitos a los solicitantes, al menos que la legislación o las disposiciones reglamentarias indiquen otra cosa. Las organizaciones deberían solicitar sólo la información mínima necesaria para asegurar la identificación correcta. Habría que proteger adecuadamente esa información y conservarla sólo mientras fuera necesario;

l) procurar que la PII se envíe únicamente al titular que corresponda de forma segura;

m) procurar que se proporcione a los titulares de la PII toda la información que soliciten y, al mismo tiempo, se siga protegiendo la PII de otros titulares;

n) comunicar en notificaciones de privacidad si tienen la intención de imponer tasas de acceso, según lo permita la ley en algunas jurisdicciones; y

o) solicitar a los procesadores de la PII que ayuden al controlador de la PII a facilitar al titular de esa información el ejercicio de los derechos de acceso a sus datos, así como de su rectificación o supresión.

El derecho de acceso ofrece a los titulares de la PII la posibilidad de revisar la información que figura en los sistemas de registro de la organización. Supone el acceso inmediato, simplificado y poco oneroso a los datos. Los procesos de la organización que permiten el acceso a los registros pueden variar en función de los recursos, los requisitos legales u otros factores.

A.10.2 Rectificación y participación

Objetivo: Facilitar la modificación, corrección o eliminación de datos a los procesadores de la PII y a terceros cuyos datos personales han sido divulgados.

Control

A menos que esté prohibido por la legislación o las disposiciones reglamentarias pertinentes, las organizaciones deberían aplicar medidas adecuadas para facilitar a los titulares de la PII la posibilidad de corregir, modificar o eliminar los datos personales que mantienen las organizaciones. Las organizaciones también deberían establecer un mecanismo mediante el cual todas las correcciones, modificaciones o supresiones se notifiquen a los procesadores de la PII y, en la medida de lo posible, a terceros cuyos datos personales han sido divulgados.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) garantizar que el titular siempre pueda ejercer el derecho de corregir;

b) analizar los casos en que los medios prácticos elegidos ya no son operativos e identificar soluciones alternativas, si es necesario;

c) garantizar, en la medida que lo permitan la legislación o las disposiciones reglamentarias pertinentes, que los titulares de la PII puedan ejercer su derecho de corregir;

d) garantizar la exactitud de las correcciones solicitadas;

e) procurar que los titulares de la PII que presentan solicitudes reciban una confirmación;

f) garantizar que los terceros a quienes se les ha podido enviar la PII estén informados de las correcciones realizadas; y

g) permitir a los titulares de la PII únicamente el acceso a los datos que necesitan corregir, modificar o eliminar.

A.10.3 Gestión de las reclamaciones

Objetivo: Establecer un tratamiento eficaz de tratamiento de las reclamaciones y rectificar los procedimientos que deben ser utilizados por los titulares de la PII.

Control

Las organizaciones deberían aplicar medidas adecuadas para el tratamiento eficaz de las reclamaciones recibidas de los titulares de la PII.

Directrices de implementación para la protección de la PII

Las organizaciones deberían poner en práctica un proceso de gestión de las reclamaciones y mantener un punto de contacto que reciba las reclamaciones, inquietudes o preguntas de los titulares de la PII sobre las prácticas de privacidad de la organización, y responda a ellas.

Las organizaciones deberían facilitar mecanismos de reclamación, de acceso inmediato y fácil utilización para los titulares de la PII, que contemplen toda la información necesaria para una presentación de reclamaciones eficaz (incluidos los datos de contacto del CPO u otros funcionarios designados para atender las reclamaciones).

Los procesos de la organización en materia de gestión de las reclamaciones deberían incluir mecanismos de seguimiento para asegurar que todas las reclamaciones recibidas se examinan y tramitan puntualmente. La gestión de las reclamaciones debería contemplar además medidas correctivas desencadenadas a partir de la reclamación.

Otras informaciones relativas a la protección de la PII

Las reclamaciones, inquietudes o preguntas de los titulares de la PII pueden constituir una fuente valiosa de aportaciones externas que, en última instancia, mejoran los modelos operativos, la utilización de la tecnología, las prácticas de procesamiento de datos, la privacidad y las técnicas de seguridad.

A.11 Rendición de cuentas

A.11.1 Gobernanza

Objetivo: Establecer una gobernanza eficaz del procesamiento de la PII.

Control

Las organizaciones deberían aplicar medidas adecuadas para establecer una gobernanza eficaz con respecto al procesamiento de la PII.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) nombrar un responsable encargado de elaborar, implementar y mantener un programa de gobernanza y privacidad en toda la organización con objeto de garantizar que los programas y sistemas de información cumplan con el conjunto de leyes y disposiciones reglamentarias aplicables al procesamiento de la PII. La persona nombrada podría ser designada como CPO. Otra opción sería que un miembro de la junta de directores asumiera las responsabilidades, con apoyo de un miembro del personal especializado subcontratado;

b) asegurarse de que la persona nombrada tenga la experiencia necesaria para supervisar el procesamiento de la PII;

c) procurar que la persona nombrada participe en todas las cuestiones relativas a la protección de la PII e informe directa y puntualmente a la alta dirección;

d) facilitar a la persona nombrada el personal, las instalaciones, los equipos y otros recursos necesarios para el desempeño de sus tareas;

e) establecer un proceso para seguir de cerca los cambios introducidos en leyes y políticas en materia de privacidad que incidan en el programa de protección de la PII;

f) elaborar, difundir y poner en práctica políticas y procedimientos operativos de protección de la PII que rijan los controles de protección y seguridad de esos datos personales en programas, sistemas de información o tecnologías que guardan relación con la PII;

g) actualizar periódicamente los planes, las políticas y los procedimientos de protección de la PII; y

h) supervisar periódicamente el desempeño de la organización en materia de protección de la PII. Sería conveniente que un representante de la alta dirección o un miembro de la junta de directores se ocupara de ello dando visibilidad a aspectos tales como las mediciones cuantitativas, los riesgos y las infracciones. Aunque esa supervisión podría llevarse a cabo según las necesidades, también debería ser periódica y no esperar que se presente un factor desencadenante.

A.11.2 Evaluación de la incidencia en la privacidad

Objetivo: Establecer un proceso de evaluación de la incidencia en la privacidad y llevar a cabo dicha evaluación cuando sea necesario.

Control

Cuando se ocupan del procesamiento de la PII, las organizaciones deberían establecer los procesos necesarios para llevar a cabo una PIA.

Directrices de implementación para la protección de la PII

Por lo general, la evaluación del riesgo para la privacidad es realizada por una organización que asume seriamente su responsabilidad y trata a los titulares de la PII de forma adecuada. En algunas jurisdicciones, se debe efectuar una PIA para cumplir la legislación y las disposiciones reglamentarias. La Norma Internacional ISO/CEI 29134 puede servir de orientación para este tipo de PIA.

Al llevar a cabo la evaluación del riesgo para la privacidad, las organizaciones deberían tener en cuenta los activos, las amenazas, las vulnerabilidades y las técnicas de seguridad (existentes y propuestos). Las organizaciones deberían dejar constancia de:

a) los resultados de una PIA, incluida, aunque no se limita a ello, la PII en procesamiento;

b) los riesgos para la privacidad identificados; y

c) las medidas de atenuación propuestas.

A.11.3 Requisitos para contratistas y procesadores de la PII en materia de privacidad

Objetivo: Garantizar, a través de medios contractuales o de otro tipo, como políticas internas obligatorias, que terceros receptores ofrezcan como mínimo niveles de protección de la PII equivalentes.

Control

Las organizaciones deberían aplicar medidas adecuadas para garantizar que los contratistas y procesadores de la PII implementen niveles adecuados de protección de la PII.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) dejar constancia en el acuerdo de nivel de servicio los requisitos en materia de protección de la PII que deben cumplir los procesadores de la PII;

b) supervisar y verificar la aplicación de dichos requisitos por los contratistas;

c) establecer las funciones y responsabilidades en materia de protección de la PII para contratistas y procesadores de la PII;

d) determinar por contrato el tema y el plazo del servicio que debe prestarse, el alcance, la forma y la finalidad del procesamiento de la PII que realiza el procesador, así como los tipos de PII procesada;

e) especificar las condiciones bajo las cuales un procesador de la PII debe devolver o eliminar de forma segura la PII cuando se completa el servicio, se concluye todo acuerdo constitutivo o lo solicite el controlador de la PII;

f) incluir una cláusula de confidencialidad vinculante para el proveedor y cualquiera de sus empleados que pueda tener acceso a la PII;

g) garantizar que el proveedor de servicio no comunica la PII a terceros, ni siquiera con fines de preservación, a menos que se disponga expresamente en el contrato;

h) aclarar las responsabilidades del proveedor de servicio para notificar al controlador de la PII en caso de cualquier violación de los datos que afecte a la PII;

i) determinar por contrato que el proveedor de servicio debería notificar al controlador de la PII todo cambio importante en relación con el servicio, como la implementación de funciones adicionales; y

j) documentar y comunicar, llegado el caso, todas las políticas, los procedimientos y las prácticas que guardan relación con la PII.

Las organizaciones deberían consultar con un asesor jurídico, el CPO y los funcionarios encargados de la contratación, las leyes, directivas, políticas o disposiciones reglamentarias que puedan afectar a la ejecución de este control.

NOTA – Se aplican también las directrices de implementación adicionales de 15.1.2.

Otras informaciones relativas a la protección de la PII

Entre los contratistas y procesadores de la PII pueden mencionarse, aunque no de forma exhaustiva, oficinas de servicio, proveedores de información, procesadores de la información y otras organizaciones encargadas del desarrollo de sistemas de información, servicios de tecnología de la información y otras aplicaciones externalizadas.

A.11.4 Supervisión y verificación de la privacidad

Objetivo: Supervisar y verificar los controles de protección de la PII y la eficacia de la política interna de protección de la PII.

Control

Las organizaciones deberían aplicar medidas adecuadas para supervisar y verificar periódicamente los controles de la privacidad y la eficacia de la política interna en materia de privacidad.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) supervisar y verificar periódicamente las operaciones de procesamiento de la PII, especialmente las que se ocupan de la PII confidencial, para garantizar que se ajustan a las leyes, disposiciones reglamentarias y condiciones contractuales;

b) supervisar y verificar periódicamente los controles y las políticas de protección de la PII para garantizar que se ajustan a las leyes, disposiciones reglamentarias y condiciones contractuales;

c) procurar que la verificación sea realizada por partes cualificadas e independientes (internas o externas a la organización); y

d) si la verificación se lleva a cabo utilizando recursos internos, una parte externa realizará periódicamente la verificación con objeto de efectuar una evaluación independiente.

A.11.5 Concienciación y formación en materia de protección de la PII

Objetivo: Impartir cursos de formación y capacitación adecuados sobre la protección de la PII para el personal del controlador de PII que tendrá acceso a la PII.

Control

Las organizaciones deberían aplicar medidas adecuadas para impartir cursos de formación adecuados para el personal del controlador de PII.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) implantar y mantener una estrategia global de formación y concienciación destinada a velar por que su personal comprenda sus responsabilidades y los procedimientos en relación con la protección de la PII;

b) crear mecanismos para mantener actualizado al personal encargado de la protección de la PII en relación con la evolución del entorno regulador, contractual y tecnológico, que podría incidir en el cumplimiento de la privacidad por las propias organizaciones;

c) gestionar cursos de formación en materia de protección de la PII básicos y basados en roles de forma periódica (por ejemplo, anualmente) o según las necesidades (por ejemplo, tras un incidente). Esta medida es especialmente importante en el caso de las actividades que únicamente procesan PII con poca frecuencia; y

d) asegurarse de que su personal certifica (manual o electrónicamente) la aceptación de sus responsabilidades de protección de la PII periódicamente.

A.11.6 Informes de protección de la PII

Objetivo: Elaborar, divulgar y actualizar informes de protección de la PII.

Control

Las organizaciones deberían elaborar, divulgar, según proceda, y actualizar informes (por ejemplo, sobre fallos, investigaciones, auditorias, etc.) para los altos directivos y demás miembros del personal encargados de supervisar la protección de la PII, con el fin de mostrar que se rinden cuentas en relación con los mandatos legales y reglamentarios legales previstos en el programa de protección de la PII.

Directrices de implementación para la protección de la PII

Mediante la presentación de informes externos e internos sobre la protección de la PII, las organizaciones deberían promover la rendición de cuentas y la transparencia en sus operaciones de protección de la PII. Estos informes también permiten a las organizaciones determinar los progresos realizados en el cumplimiento de los requisitos de protección de la PII y en los controles para la protección de la PII, comparar el desempeño en toda la organización, identificar vulnerabilidades y lagunas en la política y su aplicación, e identificar modelos de éxito.

A.12 Seguridad de la información

Objetivo: Velar por la debida protección de la PII según los resultados de una evaluación de riesgos.

Control

La PII al cuidado y custodia de la organización debería protegerse mediante controles adecuados según los resultados de una evaluación de los riesgos de amenaza o PIA.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) proteger la PII mediante controles adecuados a escala operacional, funcional y estratégica para asegurar la integridad, la confidencialidad y la disponibilidad de la PII, y protegerla contra riesgos como el acceso no autorizado, la destrucción, el uso, la modificación, la divulgación o la pérdida durante todo su ciclo de vida;

b) escoger los procesadores de PII y los contratos adecuados que ofrezcan garantías suficientes con respecto a los controles organizativos, físicos y técnicos para el procesamiento de la PII y para garantizar el cumplimiento de esos controles;

c) basar los controles de seguridad en requisitos legales aplicables, normas de seguridad, los resultados de las evaluaciones sistemáticas de los riesgos para la seguridad descritos en la norma ISO 31000, y los resultados del análisis de la relación costo/beneficio;

d) limitar el acceso a la PII a aquellas personas que lo necesitan para desempeñar sus funciones, y limitar el acceso únicamente a la PII que necesitan para realizar su labor;

e) poner fin a los riesgos y a las vulnerabilidades hallados gracias a las evaluaciones del riesgo para la privacidad y los procesos de auditoría; y

f) someter los controles a exámenes y revaluaciones periódicos en un proceso continuo de gestión de los riesgos para la seguridad.

Determinadas leyes sobre privacidad de los datos obligan en ocasiones a cumplir ciertos requisitos de seguridad, en cuyo caso dichos requisitos deberían comunicarse a la función de seguridad de los datos para su cumplimiento.

A.13 Cumplimiento de la privacidad

A.13.1 Cumplimiento

Objetivo: Evitar infracciones de la política jurídica, normativa, reglamentaria, de la privacidad o el incumplimiento de obligaciones contractuales relacionadas con la privacidad o con cualquier requisito en la materia.

Control

Las organizaciones deberían aplicar medidas adecuadas para asegurarse de que el procesamiento de la PII responde a los requisitos de cumplimiento.

Directrices de implementación para la protección de la PII

Las organizaciones deberían:

a) elaborar un informe anual con información detallada sobre los riesgos existentes, en el que se indique el grado de cumplimiento y se incluya un resumen de las medidas pendientes; y

b) seguir procesos bien definidos de respuesta ante fallos que podrían, en el marco de algunas jurisdicciones, incluir el requisito de informar a los titulares de la PII y otras autoridades (por ejemplo, organismos de protección de datos).

A.13.2 Restricciones en la transferencia de datos transfronteriza en determinadas jurisdicciones

Objetivo: Proteger la PII cuando se transfiere a nivel mundial.

Control

Las organizaciones deberían aplicar medidas adecuadas para asegurarse de que las transferencias transfronterizas de PII se ajustan a los requisitos de cumplimiento pertinentes.

Directrices de implementación para la protección de la PII

Cuando es necesario transferir PII a un país distinto del territorio donde se establece la PII, la reglamentación de la privacidad de los datos de determinadas jurisdicciones puede imponer que se tomen medidas, que suelen ser alguna de las siguientes:

a) notificar a la autoridad encargada de la protección de datos;

b) obtener la aprobación de la autoridad encargada de la protección de datos, en particular si los datos son sensibles;

c) actuar con la debida diligencia para velar por que la PII transferida entre fronteras esté protegida de manera equivalente a la protección requerida en el país de origen; y

d) aplicar instrumentos específicos de transferencia de datos como cláusulas contractuales normalizadas o normas corporativas vinculantes.

Las organizaciones deberían aplicar medidas adecuadas para comprobar si se aplican restricciones específicas a cualquier transferencia prevista y si se respetan antes de efectuarla.

Bibliografía

– BSI 10012, Specification for a personal information management system.

– Comisión Europea, Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), 2011.

– ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

– ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*.

– ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*.

– ISO/IEC 27009, *Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements*.

– ISO/IEC 27018, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.

– ISO/IEC 29134, *Information technology – Security techniques – Guidelines for privacy impact assessment*.

– IEC *Electropedia*. Available (viewed 2017-07-06) at: http://www.electropedia.org/

– ISO *Online* browsing *platform*. Available (viewed 2017-07-06) at: http://www.iso.org/obp

– ITU *Terms and definitions*. Available (viewed 2017-07-07) at: http://www.itu.int/ITU-R/go/terminology-database

– KCS, *Personal information management system*, diciembre de 2011.

– NIST Special Publication 800-53 Appendix J, *Security and privacy controls for federal information systems and organizations*, julio de 2011.

– NIST Special Publication 800-122, *Guide to protecting the confidentiality of personally identifiable information (PII)*, abril de 2010.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017