

Sistema de Gestión de Seguridad de la Información

# Directrices para la aplicación de la Ley Nº 18.331 según la familia de Normas ISO/IEC 27000

## BUENAS PRÁCTICAS

Versión V1.0 - 2010



Este documento ha sido elaborado por AGESIC (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento así como hacer obras derivadas, siempre y cuando tengan en cuenta citar la obra de forma específica y no utilizar esta obra para fines comerciales. Toda obra derivada de ésta deberá ser generada con estas mismas condiciones.

Nota de derechos de copia:

La reproducción parcial de la Norma UNIT-ISO/IEC 27002:2005 incluida en este documento fue autorizada por el Instituto Uruguayo de Normas Técnicas (UNIT). Para acceder a la versión completa consultar a UNIT (Web: <http://www.unit.org.uy>; E-mail: [unit-iso@unit.org.uy](mailto:unit-iso@unit.org.uy)).

## Resumen Ejecutivo

El régimen de Protección de Datos Personales fue establecido en Uruguay por la Ley N° 18.331 de Protección de Datos Personales y Acción de “Habeas Data” de 11 de Agosto de 2008.

Con el objeto de facilitar a los directores de organizaciones públicas y privadas el cumplimiento de la Ley y su correspondiente reglamentación, es que AGESIC elabora y pone a disposición esta guía con el propósito de facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos personales.

Debe entenderse, en cualquier caso, que siempre habrá que atenerse a lo dispuesto por la Ley y la reglamentación vigente.

La conectividad de hoy obliga a las organizaciones y empresas a trascender la infraestructura tecnológica para evaluar la importancia de la gestión de la seguridad, el perfil de quien la desempeña, además del alcance e impacto de las funciones adquiridas.

Con esta directriz se pretende, en base a lo dispuesto por la Ley, acercar a nuestras organizaciones buenas prácticas aceptadas internacionalmente en materia de seguridad de la información. Es así que se establece una relación directa de los principios desarrollados en la Ley con los controles de la Norma UNIT-ISO/IEC 27002:2005.

La Norma UNIT-ISO/IEC 27002:2005 forma parte de un modelo de gestión de la seguridad de la información, ampliamente difundido. En este modelo se establece un marco de políticas, procedimientos, guías y recursos basados en un enfoque hacia los riesgos del negocio; cuyo fin es establecer, implementar, operar, revisar y mejorar la seguridad de la información.

La gestión de la seguridad de la información implica:

- Desarrollo de una política de seguridad de la información.
- Identificación de funciones y responsabilidades dentro de la organización.
- Análisis y gestión de riesgos.

- Selección e implantación de controles.
- Concientización en materia de seguridad.
- Seguimiento, que incluye: mantenimiento, auditoría, verificación y revisión.
- Gestión de incidentes.
- Gestión de la continuidad del negocio.

En esta guía se ha realizado una selección discreta de los controles de la Norma UNIT-ISO/IEC 27002:2005 bajo el criterio de alineación a la Ley N° 18.331.

A continuación se presentan los principios de la Ley y un resumen de los controles seleccionados, los cuales se detallan más adelante en el capítulo 7.

Al principio de **legalidad** se asocian controles del dominio de gestión de activos de la Norma de referencia. En particular se recomienda mantener un inventario de las bases de datos que contengan datos de carácter personal y clasificar estas bases de acuerdo a su valor, requisitos legales, sensibilidad y criticidad para la organización.

En cuanto al principio de **veracidad**, que establece que los datos personales recogidos a efectos de su tratamiento deberán ser veraces, adecuados, ecuanimes y no excesivos, se han asociado controles relacionados con la seguridad en los acuerdos con terceros y aquellos controles que apuntan a mantener la integridad de los datos personales recogidos. Estos controles abarcan aspectos administrativos y técnicos. Dentro de los controles administrativos se encuentran: definir procedimientos para el manejo de la información y establecer políticas de intercambio de la misma. Mientras que los controles técnicos, recomendados bajo el principio de veracidad abarcan, entre otros, la protección contra código malicioso, controles de red y controles que aseguren el correcto procesamiento de los datos personales dentro de los sistemas de información.

El principio de **finalidad** de la Ley vela para que los datos no sean utilizados con finalidades distintas o incompatibles respecto de aquellas que motivaron su obtención, y para que los mismos sean eliminados cuando hayan dejado de ser necesarios. Se busca recomendar un conjunto de controles que aseguren la utilización, intercambio y disposición de los datos de forma segura. Por esto último, los controles recomendados abarcan los requisitos de seguridad en contratos con terceros involucradas en el procesamiento, comunicación y

gestión de los datos; así como los aspectos de seguridad a considerar en la utilización y disposición de los datos en la interna de la organización.

Para el caso del principio del **previo consentimiento informado** sólo se ha recomendado (en caso de que la organización recoja el consentimiento del titular de los datos vía electrónica), la protección de la información implicada en la transacción.

El principio de **seguridad de los datos** es quizás el que tiene la relación más directa con la Norma UNIT-ISO/IEC 27002:2005, por lo cual la selección de controles es más amplia que en el resto de los principios. Atendiendo el alcance de la Ley y el objeto de esta guía, se recomienda una serie de controles que implican a las áreas relacionadas con la organización de la seguridad, la seguridad física, la seguridad operativa, el control de acceso y la seguridad en la adquisición; así como el desarrollo y mantenimiento de sistemas de información.

Con relación al principio de **reserva**, que obliga a utilizar los datos en forma reservada exclusivamente para las operaciones habituales y prohíbe la difusión de los mismos a terceros, se han recomendado los controles que principalmente cubren la propiedad de confidencialidad de la información. Los controles seleccionados buscan proteger la información de amenazas internas, a través del establecimiento de acuerdos de confidencialidad, requisitos de seguridad en los términos de empleo; así como a través de controles físicos sobre las instalaciones de procesamiento de la información y sobre los medios que la soportan. Asimismo buscan proteger contra amenazas externas a través de requisitos de seguridad en los acuerdos con terceros, controles de seguridad física y procedimientos para proteger la información en tránsito.

Las recomendaciones de controles se cierran con aquellos asociados al principio de **responsabilidad**. Los mismos cubren la asignación de funciones y responsabilidades en materia de seguridad y la segregación de tareas como mecanismo para reducir las oportunidades de modificación no autorizada, no intencional o el mal uso de la información.

## Introducción

### Seguridad de la Información



La información es un activo de la organización que, como otros activos importantes, tiene valor y necesita de una adecuada protección.

La información puede estar contenida en diversos soportes, tales como papel, electrónico, filmada o en conversaciones grabadas.

La seguridad de la información es la protección de la misma contra un gran número de amenazas que atentan contra la continuidad de los servicios de la organización.

La seguridad de la información se consigue implantando controles adecuados como políticas, procesos, procedimientos, estructuras organizativas y aplicaciones, entre otros. [1]

### Participantes

Este documento fue elaborado por AGESIC con la participación de UNIT. En la discusión del mismo participaron, además, el Consejo Asesor de Seguridad Informática de AGESIC y el Comité Técnico de Seguridad de la Información de UNIT.

## Objeto y campo de aplicación

El objeto de este documento es recomendar a las organizaciones un conjunto mínimo de directrices en lo que refiere a la seguridad de la información. Promueve poder dar cumplimiento a la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data de 11 de Agosto de 2008 y a la reglamentación correspondiente.

El presente documento será de aplicación a las bases de datos que contienen datos de carácter personal, e incluyen sistemas de información, soportes y equipamiento utilizado para el tratamiento de los mismos que deban ser protegidos de acuerdo a la normativa vigente.

Está dirigido a la dirección de las organizaciones y a todo el personal vinculado a la gestión de la seguridad de la información, ya sea de la misma organización o parte externa que apoya esta actividad.

## Referencias normativas

Las siguientes referencias son indispensables para la aplicación de esta directriz. Para las referencias fechadas sólo se aplica la edición citada y para las no fechadas, se aplica la última edición del documento referenciado (incluida cualquier corrección).

- Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data.
- UNIT-ISO/IEC 27001:2005, Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información – Requisitos.
- UNIT-ISO/IEC 27002:2005, Tecnología de la Información – Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
- UNIT-ISO/IEC 27005:2008, Tecnología de la Información – Técnicas de Seguridad – Gestión de Riesgos de la Seguridad de la Información.

## Términos y definiciones

A los efectos de este documento se aplican los siguientes términos y definiciones.

### **Base de datos**

Designan, indistintamente, al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, (electrónico o no) cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

**Nota:** la definición de base de datos de la Ley N° 18.331 no corresponde con el uso habitual en el ámbito de TI. Una base de datos, desde el enfoque de la Ley, puede estar constituida por una agrupación de información o bases de datos de TI.

### **Comunicación de datos**

Toda revelación de datos realizada a una persona distinta del titular de los datos.

### **Consentimiento del titular**

Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consiente el tratamiento de datos personales que le concierne.

### **Dato personal**

Información de cualquier tipo referida a personas físicas o jurídicas, determinadas o determinables.

### **Dato sensible**

Datos personales que revelen origen racial y étnico; preferencias políticas, convicciones religiosas o morales; afiliación sindical e informaciones referentes a la salud o a la vida sexual.

### **Destinatario**

Persona física o jurídica; pública o privada; que recibiere comunicación de datos, se trate o no de un tercero.

### **Disociación de datos**

Todo tratamiento de datos personales de manera que la información obtenida, no pueda vincularse a persona determinada o determinable.

### **Encargado del tratamiento**

Persona física o jurídica; pública o privada; que sola o en conjunto con otros, trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

**Nota:** se puede relacionar el *encargado del tratamiento* con cualquier individuo que acceda o manipule la información (ej.: Jefe de Marketing, usuario operativo, administrativo).

### **Fuentes accesibles al público**

Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

### **Tercero**

La persona física o jurídica; pública o privada; distinta del titular del dato, del responsable de la base de datos o tratamiento; del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

### **Responsable de la base de datos o del tratamiento**

Persona física o jurídica; pública o privada; propietaria de la base de datos o que decide sobre la finalidad, contenido y uso del tratamiento.

**Nota:** este rol se asocia con la máxima autoridad dentro de la organización. Excluye al administrador de las bases de datos, que si bien posee facultades para dirigir, organizar y ordenar; no decide sobre la finalidad, uso y contenido del tratamiento

### **Titular de los datos**

Persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la Ley N° 18.331.

### **Tratamiento de datos**

Operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permiten el procesamiento de datos personales; así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

### **Usuario de datos**

Toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

## Estructura de esta directriz

Esta directriz contiene siete capítulos, de los cuales dos conforman el cuerpo del documento. En el capítulo seis se señalan una serie de recomendaciones adoptadas en base a buenas prácticas internacionales en materia de seguridad de la información. Ésta constituye un elemento precedente a la gestión en sí de la seguridad de la información de los datos de carácter personal. Cierra la directriz el capítulo siete, el cual replica los siguientes principios de la Ley N° 18.331:

- A) Legalidad.
- B) Veracidad.
- C) Finalidad.
- D) Previo consentimiento informado.
- E) Seguridad de datos.
- F) Reserva.
- G) Responsabilidad.

Para cada uno de estos principios se establece una relación con los dominios, objetivos de control o controles de la Norma UNIT-ISO/IEC 27002:2005. En la relación se redefine el control o el objetivo de control en base a lo establecido en la Ley, se señala la referencia a la Norma y se indica si la aplicación de dicho control u objetivo de control, se presenta como un mínimo recomendado o si su implantación es deseable. Por “mínimo recomendado” se entiende aquellos controles u objetivos de control que deberían implementarse para alinearse a lo establecido en la normativa. Por cada relación establecida se genera una recomendación para la implantación, que adapta o complementa aquello establecido en la Norma UNIT-ISO/IEC 27002:2005.

## Buenas prácticas en seguridad de la información



Las organizaciones, independientemente de su área de actividad y su tamaño, recopilan, procesan, almacenan y transmiten grandes cantidades de información. La misma en muchos casos es un importante activo para el logro de los objetivos de la organización. Esta información es objeto de amenazas de distinta índole y se asocian a ella vulnerabilidades inherentes a su uso y a su naturaleza. Así, la pérdida de disponibilidad, confidencialidad e integridad (entre otras propiedades) de la información, puede significar un impacto negativo para la organización. En consecuencia, es necesaria una adecuada protección de la información. Este requisito se conoce como seguridad de la información. [1]

### Gestión de riesgos de seguridad de la información

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad de la información. Los resultados de esta evaluación ayudarán a orientar y a determinar las adecuadas acciones y prioridades para gestionar los riesgos de seguridad de la información; así como la implementación de los controles seleccionados para proteger contra dichos riesgos.

La evaluación del riesgo debería repetirse periódicamente para tratar cualquier cambio que pudiera influenciar los resultados de ésta [1].

El proceso de gestión del riesgo de la seguridad de la información se compone de los siguientes procesos y actividades:

Procesos	Actividades
Planificación	<ul style="list-style-type: none"> <li>- Identificación del contexto de la organización.</li> <li>- Evaluación del riesgo.</li> <li>- Planificación del tratamiento del riesgo.</li> <li>- Aceptación del riesgo.</li> </ul>

Procesos	Actividades
Hacer	- Implementación del plan de tratamiento del riesgo.
Verificar	- Seguimiento y revisión continua de los riesgos.
Actuar	- Mantenimiento y mejora del proceso de gestión del riesgo de la seguridad de la información.

Para el proceso de gestión del riesgo se recomienda seguir las directrices de la Norma UNIT-ISO/IEC 27005:2008

**Nota:** al momento de publicarse este documento, AGESIC está elaborando un modelo para la gestión de riesgo, propuesto inicialmente para organismos públicos.

## Punto de partida

A fin de implementar la seguridad de la información en la organización, se recomienda partir de una cantidad básica y esencial de controles, tales como:

1. Documentar la política de seguridad de la información.
2. Asignar las responsabilidades de seguridad.
3. Concientizar y formar en seguridad de la información.
4. Garantizar el correcto procesamiento de las aplicaciones.
5. Gestionar las vulnerabilidades técnicas.
6. Gestionar la continuidad del negocio.
7. Gestionar los incidentes de seguridad de la información.

Si bien estos controles se consideran un buen punto de partida, no sustituye a la selección de controles basada en la evaluación de riesgo.[1]

## Política de seguridad de la información

Las organizaciones deberían contar con un documento formalmente aprobado por la dirección, publicado y comunicado, que contenga su política de seguridad de la información.

Esta política debería contemplar al menos los siguientes puntos:

- Compromiso de la dirección en la identificación y protección de los activos de la organización.
- Objetivo y alcance de la seguridad de la información en la organización.
- Responsabilidades en cuanto a la seguridad de la información.
- Evaluación y gestión del riesgo.
- Concientización y formación en seguridad de la información.
- Cumplimiento de requisitos legales, regulatorios y contractuales.
- Gestión de incidentes de seguridad.
- Gestión de la continuidad del negocio.
- Consecuencias de las violaciones a la política de seguridad de la información.

**Nota:** al momento de publicarse este documento, AGESIC está elaborando un modelo de política de seguridad de la información, propuesta inicialmente para organismos públicos.

## Responsabilidades de seguridad de la información

Se deberían establecer formalmente las responsabilidades relacionadas con la seguridad de la información en la organización. En consecuencia, surge la necesidad de que la seguridad de la información se incluya en las responsabilidades del personal laboral al mismo nivel que el desempeño de las funciones que, en su momento, crearon la necesidad del puesto de trabajo. En

caso contrario, las políticas, normas y procedimientos de seguridad, corren peligro de no ser utilizados de forma adecuada.

La seguridad de la información cobra un papel fundamental en las organizaciones. Tal seguridad va mucho más allá de los riesgos inherentes a la vulnerabilidad y al buen funcionamiento de la infraestructura tecnológica. Debería tratarse de un asunto prioritario para la dirección de la organización, en el sentido de evaluar el papel que desempeña el responsable de esa seguridad, su perfil profesional, la posición jerárquica que ocupa dentro de la empresa, además del alcance y la responsabilidad legal de sus funciones.

## Concientización y formación

La concientización es un elemento esencial para una seguridad efectiva. El personal de la organización generalmente es considerado como uno de los eslabones más débiles en la cadena de seguridad. Con el fin de asegurar la existencia de un nivel adecuado de concientización y formación en seguridad de la información, es importante establecer y mantener un plan efectivo. El propósito de este plan es explicar a los diversos actores:

- Los objetivos, estrategias y políticas de seguridad.
- La necesidad de seguridad, sus funciones y las responsabilidades asociadas.

Además, el plan debería estar diseñado para motivar a los diversos actores, y para asegurar la aceptación de sus responsabilidades en materia de seguridad.

Un plan de concientización y formación en seguridad debería implantarse a todos los niveles de la organización. Será necesario desarrollar y repartir material de concientización al personal de las diferentes partes de la organización, con diferentes funciones y responsabilidades. Un plan integral de concientización y formación en seguridad se desarrolla y estructura en diferentes etapas. Cada etapa se construye a partir de la previa, empieza por el concepto de seguridad, hasta llegar a cuestiones relativas a las responsabilidades en la implantación, implementación continua y seguimiento.

El plan de concientización y formación en seguridad de la organización incluye una gran variedad de actividades. Una de ellas es el desarrollo y la distribución de material de concientización en seguridad (afiches, boletines, folletos o

informes). El objeto de este material es aumentar la concientización general de los diversos actores implicados en la actividad de la organización. Otra actividad es la realización de cursos en temas de seguridad según la definición de roles de la organización, considerando las necesidades de seguridad. Finalmente, pueden ser necesarios cursos específicos que proporcionen formación a nivel profesional en temas de seguridad.

En algunos casos es muy efectivo incorporar mensajes de seguridad dentro de otros planes de formación. Este enfoque debería considerarse junto (o como una alternativa) con planes de concientización y formación en seguridad. [2]

## Procesamiento adecuado de aplicaciones

Deberían incluirse controles de validación de datos de entrada, salida y del tratamiento interno de la información, en las aplicaciones de la organización.

## Gestión de las vulnerabilidades técnicas

Debería establecerse un procedimiento formal y documentado para gestionar y controlar las vulnerabilidades técnicas que pudieran suponer un riesgo, como por ejemplo, la actualización de seguridad de los sistemas operativos.

Por lo que se recomienda básicamente dos cosas:

- 1.- Contar con un buen inventario de activos de información, identificando para cada uno si se trata de elementos tecnológicos, su sistema operativo y aplicaciones instaladas.
- 2.- Disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas.

Para este segundo aspecto, es recomendable contar con buenas fuentes de información que actualicen al responsable de seguridad sobre las vulnerabilidades actuales. De este modo se podrá valorar si tienen un potencial impacto a fin de tomar medidas al respecto.

En líneas generales, la gestión de vulnerabilidades enfocada desde las buenas prácticas consiste en obtener información a tiempo sobre las vulnerabilidades técnicas, evaluar la exposición de la organización ante dichas problemáticas y

definir las acciones apropiadas, con el fin de mitigar y solucionar las deficiencias técnicas. Para un adecuado gobierno de la Tecnología de la Información, no debería bastar con esperar a que los fabricantes nos propongan los parches. Habría que contar con metodologías de previsión de los incidentes documentados. Este pequeño valor añadido es el que convierte a la gestión de parches tradicional en una gestión de vulnerabilidades proactiva, acorde a las necesidades de gestión de riesgo que se recomienda a las organizaciones.

## Gestión de la continuidad del negocio

Se debería contar con un proceso formal y documentado para garantizar la continuidad del negocio de la organización, donde la capacidad de continuar la actividad sea primordial para la organización en sí, así como para sus clientes y partes interesadas.

La gestión de la continuidad del negocio es un proceso de gestión que identifica los impactos de incidentes potenciales que amenazan a una organización. Proporciona un marco para desarrollar una respuesta eficaz y una capacidad de recuperación de los servicios que brinda la organización, en donde se protegen sus intereses y su imagen.

La responsabilidad del desarrollo de la gestión de la continuidad del negocio recae en la dirección de la organización, quien deberá tener en cuenta su cometido.

## Gestión de incidentes de seguridad de la información

Deberían establecerse procedimientos formales y documentados, de reporte y tratamiento de incidentes de seguridad de la información.

La gestión de incidentes de seguridad de la información consiste en la asignación, oportuna, de los recursos necesarios y su uso adecuado. Su fin es prevenir, detectar y corregir incidentes que afecten la seguridad de la información.

Nota: por mayor información sobre este punto consultar la documentación del CERTuy (Centro Nacional de Respuesta a Incidentes en Seguridad Informática) en el sitio [www.certuy.uy](http://www.certuy.uy)

## Principios generales de la Ley N° 18.331

**Valor y fuerza.-** La actuación de los responsables de las bases de datos, tanto pública como privada y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales:

- A) Legalidad.
- B) Veracidad.
- C) Finalidad.
- D) Previo consentimiento informado.
- E) Seguridad de datos.
- F) Reserva.
- G) Responsabilidad.

### Principio de legalidad

**Principio de legalidad.-** La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia.

Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

Principio de legalidad	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
Deberían identificarse todos los activos y mantenerse un inventario de las bases de datos de la organización.	7.1.1 Inventario de activos	MR
Las bases de datos deberían clasificarse de acuerdo a su valor, requisitos legales, sensibilidad y criticidad para la organización.	7.2 Clasificación de la información	MR

## Recomendaciones para la implantación

### Inventario de bases de datos

*Referencia UNIT-ISO/IEC 27002:2005 - 7.1.1 Inventario de activos.*

El inventario de bases de datos debería incluir en forma mínima los siguientes elementos:

- a) Tipo de base de datos (electrónica, papel, u otro tipo).
- b) Localización.
- c) Información de respaldo.
- d) Responsable de la base de datos o del tratamiento (funcional).
- e) Encargado del tratamiento de la base de datos (operativo).
- f) Responsable técnico.
- g) Valoración del negocio (alta, media, baja).
- h) Clasificación.
- i) Identificación.

j) Finalidad.

k) Tiempo de preservación.

## Clasificación de bases de datos

*Referencia UNIT-ISO/IEC 27002:2005 - 7.2 Clasificación de la información.*

Las bases de datos deberían clasificarse en forma mínima en “*básicas*” o “*sensibles*”, según el tipo de datos que contengan. Entendiéndose como “básicos” aquellos datos de carácter personal “no sensibles”.

El **responsable de la base de datos o del tratamiento** (4.11) debería establecer la clasificación, revisarla periódicamente, asegurar que esté actualizada y en el nivel apropiado.

**Nota:** al momento de publicarse este documento, AGESIC está elaborando, en forma normativa, pautas para la clasificación de la información, propuesta inicialmente para organismos públicos.

## Principio de veracidad

**Principio de veracidad.**- Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, equánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley.

Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario.

Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

**Nota:** se parte de la base que los datos son inicialmente veraces, por ende se asocian los controles relacionados con integridad al principio de veracidad de la Ley.

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
Los datos personales que sean procesados por terceros e involucren acceso, procesamiento, comunicación y gestión de los mismos, deberían cumplir con todos los requisitos de seguridad.	6.2.3 Tener en cuenta la seguridad en los acuerdos con terceros.	MR
Deberían identificarse, documentarse e implementarse, las buenas prácticas a seguir con el tratamiento de la información.	7.1.3 Uso aceptable de los activos.	MR
Debería protegerse la integridad de los datos y del software que los procesa.	10.4 Protección contra código malicioso y código móvil.	D
Las redes deberían controlarse para mantener la seguridad de los sistemas y la información que circula a través de ellos, así como para mantener la disponibilidad de los servicios soportados por éstas.	10.6.1.c) Controles de red.	MR
La gestión de medios removibles debería estar regulada por controles y procedimientos que garanticen la seguridad de los datos contenidos en éstos.	10.7.1 Gestión de los medios removibles.	D
Deberían definirse procedimientos formales para la utilización y almacenamiento de la información a fin de protegerla contra el mal uso.	10.7.3 d) Procedimientos para el manejo de la información.	MR
Los cambios en los sistemas e instalaciones	10.1.2 Gestión de Cambios.	MR

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
que procesen información deberían controlarse cuando el cambio pueda afectar los datos.		
El intercambio o procesamiento de información con terceros debería estar regulado por políticas, procedimientos y controles.	10.8.1 Políticas y procedimientos de intercambio de información.	MR
En las aplicaciones de la organización deberían incluirse controles que aseguren el correcto tratamiento de la información, sobre todo aquellas aplicaciones que tienen impacto sobre la información de tipo “sensible”.	12.2 Procesamiento correcto en las aplicaciones.	MR
Se debería contar con una política sobre el empleo de controles criptográficos, así como para la gestión de sus claves.	12.3 Controles criptográficos.	D

## Recomendaciones para la implantación

### Seguridad en los acuerdos con terceros

*Referencia UNIT-ISO/IEC 27002:2005 - 6.2.3 Tener en cuenta la seguridad en los acuerdos con terceros.*

Los acuerdos con terceros que involucren acceso, proceso, comunicación de la información o de las instalaciones de procesamiento de la organización deberían cumplir con los requisitos de seguridad de la organización expresados en la política de seguridad de la información y procedimientos relacionados, así como en la aplicación de ciertos controles.

Se recomienda considerar la implantación, al menos de los siguientes controles, en los acuerdos con terceros:

- Establecer una política de seguridad de la información.

- Asegurar la protección física y lógica de los activos de información.
- Concientizar y formar a los usuarios.
- Establecer acuerdos de confidencialidad con el personal.
- Asignar claramente las responsabilidades.
- Establecer procedimientos para la gestión de cambios.
- Establecer políticas y procedimientos para el control de acceso.
- Gestionar los incidentes de seguridad de la información.
- Gestionar los problemas.
- Establecer acuerdos de nivel de servicio.
- Establecer contratos con detalle de servicios y responsabilidades.
- Realizar auditorías por terceros.
- Gestionar la continuidad del servicio.
- Brindar protección de la propiedad intelectual.

## **Uso aceptable de los activos de información**

*Referencia UNIT-ISO/IEC 27002:2005 - 7.1.3 Uso aceptable de los activos.*

La dirección de la organización debería definir reglas para el uso aceptable de los activos de información e instalaciones de procesamiento de la información.

Todos los empleados y terceros deberían conocer y cumplir estas reglas.

## **Protección contra código malicioso y código móvil**

*Referencia UNIT-ISO/IEC 27002:2005 - 10.4 Protección contra código malicioso y código móvil.*

Con el objetivo de proteger los datos y los sistemas que procesan código malicioso (virus informáticos, gusanos de la red, caballos de Troya) y código móvil, se detallan a continuación algunos controles recomendados para su implementación:

- Instalar y actualizar de forma regular el antivirus.
- No permitir la utilización ni instalación de software no autorizado.
- Concientizar y formar a los usuarios en buenas prácticas de seguridad de la información.
- Mantenerse informado sobre nuevo código malicioso.
- Permitir la utilización de código móvil bajo las condiciones de la política de seguridad definida.

## Controles de la red

*Referencia UNIT-ISO/IEC 27002:2005 - 10.6.1.c) Controles de red.*

Los administradores de redes deberían implementar controles para preservar la seguridad de los sistemas y de los datos que circulen por la misma.

Se recomienda considerar la implantación, como mínimo, de los siguientes controles:

- Designar responsables por la administración de la red.
- Mantener registros de las acciones de seguridad.
- Controlar los registros de las acciones de seguridad.

## Gestión de los medios removibles

*Referencia UNIT-ISO/IEC 27002:2005 - 10.7.1 Gestión de los medios removibles.*

La organización debería implementar procedimientos para la gestión de los medios removibles (discos, cintas, CD, DVD y medios impresos). Deberían considerarse controles tales como:

- Borrar o destruir el medio cuando no se necesiten más.
- Autorizar y registrar el movimiento de los medios para tener trazabilidad.
- Almacenar en un lugar seguro los medios, teniendo además en cuenta las especificaciones del fabricante.

- Verificar la disponibilidad de la información de acuerdo con la vida útil del medio removible que la almacena.
- Registrar los medios removibles así como sus características (tipo, lugar de guarda, contenido, entre otros datos).
- Utilizar medios removibles sólo si la organización lo necesita.

## Procedimientos para el manejo de la información

*Referencia UNIT-ISO/IEC 27002:2005 - 10.7.3 d) Procedimientos para el manejo de la información.*

La organización debería definir procedimientos que regulen la utilización y almacenamiento de la información con el fin de asegurar que los datos de entrada estén completos, que el procesamiento se complete adecuadamente, y que se valide su salida.

## Gestión de cambios

*Referencia UNIT-ISO/IEC 27002:2005 - 10.1.2 Gestión de Cambios.*

La organización debería controlar los cambios en los sistemas e instalaciones de procesamiento de información (equipamiento, software o procedimientos), a través de procedimientos formales que contemplen las siguientes actividades: registrar los cambios, planificar y probar los cambios, evaluar el impacto potencial del cambio, aprobar formalmente los cambios, comunicar el cambio a todas las personas involucradas y establecer procedimiento de vuelta atrás del cambio.

## Intercambio de información

*Referencia UNIT-ISO/IEC 27002:2005 - 10.8.1 Políticas y procedimientos de intercambio de información.*

El intercambio de información y software entre organizaciones deberían basarse en políticas y procedimientos de intercambio de información.

Se recomienda establecer políticas y procedimientos para:

- Intercambiar información.

- Establecer la seguridad de la red.
- Prevenir, detectar y corregir software malicioso.
- Establecer responsabilidades de todas las partes.
- Establecer separación de tareas.
- Utilización del correo electrónico.
- Comportamiento correcto de los usuarios.

## Procesamiento correcto de las aplicaciones

*Referencia UNIT-ISO/IEC 27002:2005 -12.2 Procesamiento correcto en las aplicaciones.*

Las aplicaciones que procesan o tienen impacto sobre información sensible requieren de controles especiales. Estos controles deberían ser seleccionados sobre los requisitos de seguridad de la organización y la evaluación del riesgo.

Con el objetivo de prevenir errores, pérdida, modificación no autorizada o mal uso de información en las aplicaciones se detallan, a continuación, algunos controles recomendados para su implementación:

- Validar los datos de entrada.
- Controlar el procesamiento interno de las aplicaciones.
- Establecer los requisitos para la integridad del mensaje.
- Validar los datos de salida.

**Nota:** se entiende por mensaje la información de carácter personal comunicada a través de aplicaciones, en el contexto de la Ley y según el alcance del control 12.2.3 de la Norma de referencia.

## Integridad del mensaje

*Referencia UNIT-ISO/IEC 27002:2005 - 12.2.3 Integridad del mensaje.*

**Nota:** De acuerdo con la nota indicada en “Procesamiento correcto de aplicaciones” en el contexto de la Ley y según el alcance del control 12.2.3 de la Norma de referencia.

Se recomienda utilizar técnicas de criptografía como control de la integridad del mensaje, en especial para el proceso de la información de tipo “sensible”.

## Controles criptográficos

*Referencia UNIT-ISO/IEC 27002:2005 -12.3 Controles criptográficos.*

Se debería contar con una política sobre el empleo de controles criptográficos, así como para la gestión de sus claves.

Se recomienda implantar los siguientes controles estableciendo:

- La política y procedimientos sobre el empleo de controles criptográficos.
- La política y procedimientos para la gestión de claves.

## Principio de finalidad

**Principio de finalidad.**- Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o pertinencia.

Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

Principio de finalidad	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
Los datos personales que sean procesados por terceros e involucren acceso, procesamiento, comunicación y gestión de los mismos, deberían cumplir con todos los requisitos de seguridad.	6.2.3 Tener en cuenta la seguridad en los acuerdos con terceros.	MR
Deberían identificarse, documentarse e implementarse las buenas prácticas a seguir con el tratamiento de la información.	7.1.3 Uso aceptable de los activos.	MR
Los datos deberían ser eliminados en forma segura, cuando hayan dejado de ser necesarios, a través de procedimientos formales.	10.7.2 Eliminación de los medios.	MR
En caso de que la organización realice intercambio de datos y software con otras organizaciones, el mismo debería realizarse a través de procedimientos formales, a fin de proteger la información de intercambio.	10.8 Intercambio de información.	MR
Si la organización cuenta con un área de desarrollo de software, los datos de prueba deberían ser seleccionados en forma cuidadosa, protegidos y utilizados en forma controlada.	12.4.2 Protección de datos de prueba del sistema.	MR

## Recomendaciones para la implantación

### Seguridad en los acuerdos con terceros

*Referencia UNIT-ISO/IEC 27002:2005 - 6.2.3 Tener en cuenta la seguridad en los acuerdos con terceros.*

Ver el punto Principio de veracidad “Seguridad en los acuerdos con terceros” del presente documento.

### Uso aceptable de los activos de información

*Referencia UNIT-ISO/IEC 27002:2005 - 7.1.3 Uso aceptable de los activos.*

Ver el punto **Principio de veracidad** “Uso aceptable de los activos de información” del presente documento.

### Eliminación de la información

*Referencia UNIT-ISO/IEC 27002:2005 - 10.7.2 Eliminación de los medios.*

Deberían eliminarse los datos en forma segura cuando no se necesiten más. Los medios de información que contengan información de tipo “sensible”, deberían eliminarse ya sea borrándola, triturándola o incinerándola, según el medio en que se encuentren los datos.

La organización debería contar con procedimientos formales para la eliminación segura de la información con el fin de evitar el uso indebido dentro o fuera de la misma.

### Intercambio de información

*Referencia UNIT-ISO/IEC 27002:2005 - 10.8 Intercambio de información.*

Ver el punto Principio de veracidad. “Intercambio de información” del presente documento.

En caso de que la organización realice intercambio de datos y/o software con otras organizaciones, éste debería realizarse a través de procedimientos formales a fin de proteger la información de intercambio.

Se recomienda implantar los siguientes controles:

- Establecer políticas y procedimientos de intercambio de información.
- Formalizar acuerdos de intercambio.
- Proteger los medios físicos en tránsito que contengan información de la organización.
- Proteger la información contenida en la mensajería electrónica
- Proteger la información asociada a los sistemas que comparten información de la organización con partes externas.

## **Protección de los datos de prueba**

*Referencia UNIT-ISO/IEC 27002:2005 - 12.4.2 Protección de datos de prueba del sistema.*

Si la organización cuenta con un área de desarrollo de software, los datos de prueba deberían ser seleccionados en forma cuidadosa, protegidos y en forma controlada.

Para realizar pruebas debería evitarse utilizar datos extraídos del ambiente de producción que contengan información de carácter personal y/o sensible.

Como excepción, los datos de producción podrán ser utilizados para pruebas, siempre y cuando se realice una disociación de los datos de carácter personal y/o sensible.

Se recomienda la utilización de los siguientes controles cuando los datos de producción sean utilizados para hacer pruebas:

- a) Los controles de acceso que se aplican a sistemas en producción, deberían aplicarse también a los sistemas de prueba de aplicaciones.
- b) Debería autorizarse formalmente la copia de datos de producción a ambiente de prueba.
- c) Debería borrarse la información de prueba inmediatamente después de que se haya utilizado.

d) Debería registrarse formalmente la copia y el empleo de información de producción en pruebas con el fin de contar con pistas de auditoría. [UNIT-ISO/IEC 27002:2005].

## Principio del previo consentimiento informado

**Principio del previo consentimiento informado.**- El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 12 de la presente ley.

No será necesario el previo consentimiento cuando:

- A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.
- B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
- C) Se trate de listados cuyos datos se limiten (en el caso de personas físicas) a nombres y apellidos; documento de identidad, nacionalidad, domicilio y fecha de nacimiento. Tampoco en el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.
- D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.
- E) Se realice por personas físicas o jurídicas; privadas o públicas; para su uso exclusivo personal o doméstico.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

Principio del previo consentimiento informado	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
En caso de que el consentimiento se recabe vía electrónica, es que se debe considerar este control.	10.9 Servicios de comercio electrónico.	MR

## Recomendaciones para la implantación

### Consentimiento vía electrónica

*Referencia UNIT-ISO/IEC 27002:2005 -10.9 Servicios de comercio electrónico.*

Cuando el consentimiento se recabe vía electrónica sobre redes públicas, la información del mismo debería ser protegida ante actividades fraudulentas, divulgación o modificación no autorizada.

### Principio de seguridad de los datos

**Principio de seguridad de los datos.-** El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
Debería utilizarse un sistema de clasificación de la información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas especiales de manejo.	7.2 Clasificación de la información.	MR
A fin de evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización; deberían definirse áreas seguras, resguardadas por un perímetro de seguridad, con barreras de seguridad y controles de acceso apropiados.	9.1 Áreas seguras	MR
Es necesaria la protección del equipamiento para reducir el riesgo de accesos no autorizados a la información y para evitar pérdidas o daños. Debería considerarse también la ubicación y la disposición del equipamiento.	9.2 Seguridad del equipamiento	MR
La organización debería verificar la implementación de acuerdos, supervisar el cumplimiento de los mismos y gestionar los cambios para asegurar que los servicios entregados cumplen los requisitos acordados con la tercera parte.	10.2 Gestión de la entrega del servicio por terceros.	MR
Debería protegerse la integridad del software y de la información de la introducción de código malicioso.	10.4 Protección contra código malicioso y código móvil.	MR
Deberían establecerse procedimientos de rutina para implementar una política y una estrategia acordada de respaldo.	10.5 Respaldo.	MR
Los medios deberían controlarse y protegerse físicamente para evitar la divulgación no autorizada,	10.7 Manejo de los medios.	MR

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
modificación, borrado o destrucción de la información.		
El intercambio de información y software entre organizaciones debería estar basado en una política de intercambio formal, llevarse a cabo según los acuerdos de intercambio, y debería cumplir, además, con cualquier legislación relevante.	10.8 Intercambio de información.	MR
Deberían considerarse las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea.	10.9 Servicios de comercio electrónico.	MR
Debería asegurarse el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.	11. Control de acceso.	MR
Deberían establecerse los controles para prevenir errores, pérdida, modificación no autorizada o mal uso de información en aplicaciones.	12.2 Procesamiento correcto en las aplicaciones.	MR
Deberían ser controlados los archivos del sistema y el código original del programa.	12.4 Seguridad de los archivos del sistema.	MR

## Recomendaciones para la implantación

### Clasificación de la información

*Referencia UNIT-ISO/IEC 27002:2005 - 7.2 Clasificación de la información.*

Ver el punto Principio de legalidad “Clasificación de bases de datos” del presente documento.

## Áreas Seguras

*Referencia UNIT-ISO/IEC 27002:2005 - 9.1 Áreas Seguras.*

La protección física puede ser alcanzada creando una o más barreras físicas alrededor de las premisas de la organización y de las instalaciones de procesamiento de la información.

Los controles de seguridad física incluyen la fortaleza de las paredes internas del edificio, cerraduras de puertas y vigilantes.

Se recomienda implantar los siguientes controles:

- Establecer perímetros de seguridad física.
- Controlar el acceso físico para garantizar el acceso sólo al personal autorizado.
- Asegurar oficinas, despachos e instalaciones.
- Proteger contra amenazas externas y del ambiente (incendio, inundación, terremoto, explosión, disturbios civiles, y otras formas de desastre natural o artificial).
- Establecer protección física y de carácter organizativo (directrices) para el trabajo en las áreas seguras.
- Proteger las áreas de acceso público, de entrega y de carga o aislamiento de las instalaciones de procesamiento de la información.

## Seguridad del equipamiento

*Referencia UNIT-ISO/IEC 27002:2005 - 9.2 Seguridad del equipamiento.*

Respecto al equipamiento, se deberían implementar controles para minimizar los riesgos de robo, fuego, explosión, humo, polvo, vibración, efectos químicos e inundación. Además, se debería definir una política que prohíba comer o beber en la proximidad del centro de procesamiento de datos.

La seguridad del equipamiento implica considerar condiciones ambientales como temperatura, inundación y falta de fluido eléctrico. Los cables de

suministro de datos y electricidad deben ser protegidos para que no puedan ser interceptados o dañados.

Se recomienda particular atención sobre el equipamiento sacado fuera de las instalaciones de la organización ante riesgos de daño, robo o escucha.

## **Gestión de la entrega del servicio por terceros**

*Referencia UNIT-ISO/IEC 27002:2005 - 10.2 Gestión de la entrega del servicio por terceros.*

Las organizaciones que deleguen servicios con terceros deberían garantizar que están siendo contemplados los requisitos de seguridad en los acuerdos con estos. Dichos servicios deberían ser objeto de revisiones periódicas. En caso de contratación externa, es necesario que la organización sepa que la máxima responsabilidad por la información procesada por una parte contratada externamente, sigue siendo de la organización.

## **Protección contra código malicioso y código móvil**

*Referencia UNIT-ISO/IEC 27002:2005 - 10.4 Protección contra código malicioso y código móvil.*

La protección contra el código malicioso debería basarse en la combinación de controles tecnológicos (software antivirus) con medidas no técnicas (educación, concientización y formación).

## **Respaldo**

*Referencia UNIT-ISO/IEC 27002:2005 - 10.5 Respaldo.*

A la hora de definir una estrategia de respaldo y recuperación, se recomienda establecer el tipo de almacenamiento, soporte a utilizar, aplicación de respaldo, frecuencia de copia y prueba de soportes.

Se recomienda, al menos, cifrar las copias de seguridad y archivos que contengan datos sensibles (ver el punto Principio de veracidad “Procesamiento correcto de las aplicaciones” del documento de referencia).

## Manejo de los medios

*Referencia UNIT-ISO/IEC 27002:2005 - 10.7 Manejo de los medios*

Deberían establecerse los procedimientos operativos adecuados para la gestión de los medios. Entendiéndose por medio, el soporte en el cual la información se almacena o transmite. A la hora de gestionar los medios se recomienda considerar:

- Su manejo.
- Su eliminación.

Se recomienda cifrar, al menos, todos los datos sensibles antes de ser transportados.

## Intercambio de información

*Referencia UNIT-ISO/IEC 27002:2005 - 10.8 Intercambio de información.*

Ver el punto Principio de veracidad “Intercambio de información” de este documento.

## Servicios de comercio electrónico

*Referencia UNIT-ISO/IEC 27002:2005 - 10.9 Servicios de comercio electrónico.*

Se recomienda en todo momento trabajar estrechamente con las unidades de negocio para desarrollar un servicio de comercio electrónico seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de comercio electrónico.

Las consideraciones de seguridad para transacciones en línea deberían incluir lo siguiente:

- a) El empleo de firmas electrónicas por cada una de las partes implicadas en la transacción.
- b) Todos los aspectos de la transacción deberían asegurar que:
  - 1) Las cartas credenciales de usuario de todas las partes son válidas y verificadas.

- 2) La transacción permanece confidencial.
  - 3) La privacidad asociada con todas las partes implicadas es conservada.
- c) El canal de comunicación entre todas las partes implicadas es cifrada.
- d) El protocolo utilizado para comunicarse entre todas las partes implicadas es seguro.
- e) El almacenamiento de los detalles de transacción es localizado fuera de cualquier ambiente público accesible, por ejemplo, en una plataforma de almacenamiento que exista en la Intranet de la organización, y no conservado y expuesto en un medio de almacenamiento directamente accesible desde Internet.
- f) Cuando se emplea una autoridad confiable (por ejemplo para propósitos de emitir y mantener firmas electrónicas y/o certificados electrónicos) la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado / firma.

## **Control de acceso**

*Referencia UNIT-ISO/IEC 27002:2005 - 11 Control de acceso.*

Los propietarios de activos de información que son responsables ante la dirección de la protección de sus activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso. Estas reglas deberían estar formalmente establecidas y documentadas. Ellas deberían ser objeto de revisiones periódicas y la dirección de la organización debería conocer los resultados de estas revisiones.

La responsabilidad de los usuarios es esencial en materia de control de acceso, por esto se recomienda asegurar que se establezcan las responsabilidades de seguridad y que sean entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo. Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Se recomienda comunicar regularmente a los empleados los perfiles de sus puestos, para recordarles sus responsabilidades y recoger cualquier cambio.

Debería controlarse el acceso a los servicios en red, tanto internos como externos. Se recomienda mantener el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN).

## Procesamiento correcto en las aplicaciones

*Referencia UNIT-ISO/IEC 27002:2005 -12.2 Procesamiento correcto en las aplicaciones.*

Ver el punto Principio de veracidad “Procesamiento correcto de las aplicaciones” del presente documento.

## Seguridad de los archivos del sistema

*Referencia UNIT-ISO/IEC 27002:2005 - 12.4 Seguridad de los archivos del sistema.*

Se recomienda restringir la instalación de software no autorizado y la desinstalación de aplicaciones.

En caso de que la organización utilice datos de prueba, estos deberían ser seleccionados cuidadosamente, protegidos y controlados (ver el punto “Protección de los datos de prueba” del documento de referencia).

## Principio de reserva

**Principio de reserva.-** Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, quedando prohibida toda difusión de la misma a terceros.

Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

Principio de reserva	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
Deberían identificarse y revisarse con regularidad los requisitos para los acuerdos de confidencialidad o de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	6.1.5 Acuerdos de confidencialidad	MR
Los términos y condiciones de empleo deberían enunciar que todos los empleados, contratistas y usuarios de terceros a los cuales se les de acceso a información personal, deban firmar un acuerdo de confidencialidad o de no-divulgación previo al otorgamiento del acceso a las instalaciones de procesamiento de información.	8.1.3 Términos y condiciones de empleo	MR
Deberían establecerse los controles físicos contra accesos no autorizados, daños e interferencias.	9 Seguridad física y del ambiente	MR
Los medios deberían controlarse y protegerse físicamente a fin de evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades del negocio.	10.7 Manejo de los medios	MR
Deberían establecerse procedimientos y normas para proteger la información y los medios físicos que contengan información en tránsito.	10.8 Intercambio de información	MR

## Recomendaciones para la implantación

### Acuerdos de confidencialidad

*Referencia UNIT-ISO/IEC 27002:2005 - 6.1.5 Acuerdos de confidencialidad.*

Los acuerdos de confidencialidad y no-divulgación deberían considerar los siguientes elementos:

- a) Una definición de la información a ser protegida (por ejemplo, información sensible).
- b) Duración prevista del acuerdo, incluyendo los casos en que sea necesario mantener la confidencialidad indefinidamente.
- c) Acciones requeridas cuando termina un acuerdo.
- d) Responsabilidades y acciones de los signatarios para evitar la divulgación no autorizada de la información (“necesidad de saber”).
- e) Propiedad de la información, secretos comerciales y propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial.
- f) El uso permitido de la información confidencial y los derechos del signatario para utilizar información.
- g) El derecho de auditar y de supervisar actividades que involucran información confidencial.
- h) Procesos para la notificación y reporte de divulgación no autorizada o brechas de la información confidencial.
- i) Términos vinculados a la destrucción o devolución de información cuando cesa un acuerdo.
- j) Acciones previstas a tomar en caso de ruptura del acuerdo.

## **Tener en cuenta la seguridad en los acuerdos con terceros**

*Referencia UNIT-ISO/IEC 27002:2005 - 6.2.3 Tener en cuenta la seguridad en los acuerdos con terceros.*

Ver el punto Principio de veracidad “Seguridad en los acuerdos con terceros” del presente documento.

## **Términos y condiciones de empleo**

*Referencia UNIT-ISO/IEC 27002:2005 - 8.1.3 Términos y condiciones de empleo.*

Los términos y condiciones de empleo deberían reflejar la política de seguridad de la organización además de aclarar y enunciar:

- a) Que todos los empleados, contratistas y usuarios de terceros a los cuales se le de acceso a información sensible deberían firmar un acuerdo de confidencialidad o de no-divulgación, con previo otorgamiento de acceso a las instalaciones de procesamiento de información.
- b) Las responsabilidades y derechos legales de empleados, contratistas y todo otro usuario, como por ejemplo las relativas a derechos de copia o legislación de protección de datos.
- c) Responsabilidades para la clasificación de información y gestión de activos de la organización asociados a sistemas y servicios de información manejados por el empleado, el contratista o el usuario de terceros.
- d) Responsabilidades del empleado, contratista o usuario de terceros por el manejo de información recibida de otras organizaciones o partes externas.
- e) Responsabilidades de la organización por el manejo de información personal, incluyendo información personal creada como resultado o durante el contrato laboral con la organización.
- f) Responsabilidades que se extiendan fuera de las instalaciones de la organización y del horario normal de trabajo, por ejemplo, en el caso de trabajo en el domicilio.

g) Acciones a ser tomadas si el empleado, contratista o usuario de terceros, desatiende los requisitos de seguridad de la organización.

## Seguridad física y del ambiente

*Referencia UNIT-ISO/IEC 27002:2005 - 9 Seguridad física y del ambiente.*

Ver los puntos Principio de seguridad de los datos “Áreas Seguras” y “Seguridad del equipamiento” del presente documento.

## Manejo de los medios

*Referencia UNIT-ISO/IEC 27002:2005 - 10.7 Manejo de los medios*

Ver el punto Principio de seguridad de los datos “Manejo de los medios” del presente documento.

## Intercambio de información

*Referencia UNIT-ISO/IEC 27002:2005 - 10.8 Intercambio de información.*

Ver el punto Principio de seguridad de los datos “Intercambio de información” del presente documento.

## Principio de responsabilidad

**Principio de responsabilidad.**- El responsable de la base de datos es responsable de la violación de las disposiciones de la presente ley.

## Referencias a la Norma UNIT-ISO/IEC 27002:2005

Principio de responsabilidad	Referencia Norma UNIT-ISO/IEC 27002:2005	Mínimo recomendado / Deseable
La asignación de funciones y responsabilidades específicas son una parte integral en el marco de seguridad de los	7.1 Responsabilidad sobre los activos	MR

<b>Principio de responsabilidad</b>	<b>Referencia Norma</b> <b>UNIT-ISO/IEC 27002:2005</b>	<b>Mínimo recomendado / Deseable</b>
datos.		
Los roles y responsabilidades de seguridad de empleados, contratistas y de terceros deberían estar definidos y documentados.	8.1.1 Roles y responsabilidades	MR

Principio de responsabilidad	Referencia Norma <b>UNIT-ISO/IEC 27002:2005</b>	<b>Mínimo recomendado / Deseable</b>
Deberían segregarse las tareas y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	10.1.3 Segregación de tareas	MR

## Recomendaciones para la implantación

### Responsabilidad sobre los activos

*Referencia UNIT-ISO/IEC 27002:2005 - 7.1 Responsabilidad sobre los activos*

Según el punto Principio de legalidad “Inventario de bases de datos” del presente documento. Se recomienda identificar responsables y encargados de las bases de datos, quienes deberían ser asignados formalmente por la organización.

El responsable de la base de datos o la persona asignada debería definir y revisar, en forma periódica, el acceso apropiado a los datos por parte de las personas y sistemas que correspondan. La responsabilidad puede ser asignada a:

- a) Un proceso de negocio.
- b) Un conjunto definido de actividades.
- c) Una aplicación determinada.
- d) Un conjunto definido de datos.

## **Roles y responsabilidades**

*Referencia UNIT-ISO/IEC 27002:2005 - 8.1.1 Roles y responsabilidades.*

Los roles y responsabilidades de seguridad deberían incluir las siguientes exigencias:

- a) Implementar y actuar de acuerdo con las políticas de seguridad de la información de la organización.
- b) Proteger los activos de accesos no autorizados, divulgación, modificación, destrucción o interferencia.
- c) Ejecutar procesos o actividades particulares de seguridad.
- d) Asegurar que la responsabilidad sea asignada al individuo por acciones tomadas.
- e) Reportar eventos de seguridad, eventos potenciales u otros riesgos de seguridad para la organización.

## **Segregación de tareas**

*Referencia UNIT-ISO/IEC 27002:2005 - 10.1.3 Segregación de tareas.*

A fin de evitar violaciones a la normativa, los responsables deberían garantizar que se verifica que ninguna persona tiene acceso, capacidad de modificar o utilizar información sin autorización o detección.

Las organizaciones pequeñas pueden considerar que este control es difícil de lograr; en estos casos se recomienda considerar otros controles como el monitoreo de las actividades y los registros de auditoría.

## Seguimiento y mejora



Se recomienda que las organizaciones emprendan revisiones regulares de los controles de seguridad implantados. Como herramientas de revisión se recomienda utilizar auditorías de seguridad, revisión de incidentes y retroalimentación de todas las partes interesadas. Las mejoras identificadas durante la revisión deberían ser implementadas.

## Referencias

- [1] UNIT-ISO/IEC 27002:2005 - TECNOLOGIA DE LA INFORMACION. CODIGO DE BUENAS PRÁCTICAS PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION.
- [2] UNE 71501-1:2001 IN - TECNOLOGÍA DE LA INFORMACIÓN (TI) - GUÍA PARA LA GESTIÓN DE LA SEGURIDAD DE TI. PARTE 1: CONCEPTOS Y MODELOS PARA LA SEGURIDAD DE TI.

## Tabla de contenido

Resumen Ejecutivo .....	3
Introducción .....	6
Seguridad de la Información .....	6
Participantes .....	6
Objeto y campo de aplicación .....	7
Referencias normativas.....	8
Términos y definiciones .....	9
Estructura de esta directriz.....	12
Buenas prácticas en seguridad de la información .....	13
Gestión de riesgos de seguridad de la información .....	13
Punto de partida.....	14
Política de seguridad de la información.....	15
Responsabilidades de seguridad de la información.....	15
Concientización y formación.....	16
Procesamiento adecuado de aplicaciones .....	17
Gestión de las vulnerabilidades técnicas.....	17
Gestión de la continuidad del negocio .....	18
Gestión de incidentes de seguridad de la información .....	18
Principios generales de la Ley N° 18.331 .....	19
Principio de legalidad .....	19
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	20
Recomendaciones para la implantación.....	20
Principio de veracidad .....	21
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	22
Recomendaciones para la implantación.....	23
Principio de finalidad.....	28
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	29
Recomendaciones para la implantación.....	30
Ver el punto Principio de veracidad “Seguridad en los acuerdos con terceros” del presente documento. ....	30
Principio del previo consentimiento informado .....	32
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	33
Recomendaciones para la implantación.....	33
Principio de seguridad de los datos .....	33
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	34

Recomendaciones para la implantación.....	35
Ver el punto Principio de legalidad “Clasificación de bases de datos” del presente documento.....	35
Principio de reserva .....	40
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	41
Recomendaciones para la implantación.....	42
Principio de responsabilidad .....	44
Referencias a la Norma UNIT-ISO/IEC 27002:2005 .....	44
Recomendaciones para la implantación.....	46
Seguimiento y mejora.....	48
Referencias.....	48
Tabla de contenido.....	49