

Directrices para la aplicación de la Ley 18.331 según la familia de Normas ISO/IEC 27000

02 de Setiembre, 2010

A/P Glenda Garcés
glenda.garces@agesic.gub.uy

TEMARIO

- Introducción Ley 18.331
- Objetivo y campo de aplicación de la Directriz
- Referencias Normativas
- Términos y Definiciones
- Principios de la Ley 18.331
- Controles recomendados
- Sitos de interés

Introducción Ley 18.331

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 y su reglamentación correspondiente.

Objetivo y campo de aplicación (I)

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.

Se establece una relación directa de los principios de la Ley con los controles de la Norma UNIT-ISO/IEC 27002:2005.

Objetivo y campo de aplicación (II)

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^o 18.331 de Protección de Datos Personales y Acción de Habeas Data de 11 de Agosto de 2008 y a la reglamentación correspondiente.

Referencias Normativas (I)

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.

Referencias Normativas (II)

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.

Referencias Normativas (III)

[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 (I)

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.

Términos y Definiciones (II)

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).

Términos y Definiciones (III)

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.

Principios de la Ley 18.331

LEGALIDAD

SEGURIDAD

VERACIDAD

RESPONSABILIDAD

FINALIDAD

RESERVA

**PREVIO
CONSENTIMIENTO
INFORMADO**

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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de legalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían identificarse todos los activos y mantenerse un inventario de las bases de datos de la organización.	7.1.1 Inventario de activos

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de legalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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

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** debería establecer la clasificación, revisarla periódicamente, asegurar que esté actualizada y en el nivel apropiado.

Principio de VERACIDAD (I)

Principio de veracidad.- Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuanimes 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.

Principio de VERACIDAD (II)

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

Se recomienda:

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían identificarse, documentarse e implementarse, las buenas prácticas a seguir con el tratamiento de la información.	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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
Los cambios en los sistemas e instalaciones que procesen información deberían controlarse cuando el cambio pueda afectar los datos.	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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de veracidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Principio de FINALIDAD (I)

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.

Principio de FINALIDAD (II)

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de finalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

Nota: Ver anterior

Control Norma UNIT-ISO/IEC 27002:2005

Principio de finalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían identificarse, documentarse e implementarse las buenas prácticas a seguir con el tratamiento de la información.	7.1.3 Uso aceptable de los activos.

Nota: Ver anterior

Control Norma UNIT-ISO/IEC 27002:2005

Principio de finalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de finalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de finalidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Principio PREVIO CONSENTIMIENTO INFORMADO (I)

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.

Principio PREVIO CONSENTIMIENTO INFORMADO (II)

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.

Principio PREVIO CONSENTIMIENTO INFORMADO (III)

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.

Principio PREVIO CONSENTIMIENTO INFORMADO (IV)

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio del previo consentimiento informado	Referencia Norma UNIT-ISO/IEC 27002:2005
En caso de que el consentimiento se recabe vía electrónica, es que se debe considerar este control.	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 **SEGURIDAD** de **DATOS** (I)

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.

Principio **SEGURIDAD** de **DATOS** (II)

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

Nota: Ver anterior

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían establecerse procedimientos de rutina para implementar una política y una estrategia acordada de respaldo.	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

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
Los medios deberían controlarse y protegerse físicamente para evitar la divulgación no autorizada, modificación, borrado o destrucción de la información.	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 trasmite. 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

Nota: Ver anterior

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

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.

Control Norma UNIT-ISO/IEC 27002:2005

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 Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
Debería asegurarse el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.	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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
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.

Nota: Ver anterior

Control Norma UNIT-ISO/IEC 27002:2005

Principio de seguridad de los datos	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían ser controlados los archivos del sistema y el código original del programa.	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 (I)

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.

Principio de RESERVA (II)

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.

Principio de RESERVA (III)

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

Control Norma UNIT-ISO/IEC 27002:2005

Principio de reserva	Referencia Norma UNIT-ISO/IEC 27002:2005
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

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.

Control Norma UNIT-ISO/IEC 27002:2005

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de reserva	Referencia Norma UNIT-ISO/IEC 27002:2005
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

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.

Control Norma UNIT-ISO/IEC 27002:2005

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de reserva	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían establecerse los controles físicos contra accesos no autorizados, daños e interferencias.	9. Seguridad física y del ambiente

Nota: Ver anterior

Control Norma UNIT-ISO/IEC 27002:2005

Principio de reserva	Referencia Norma UNIT-ISO/IEC 27002:2005
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

Control Norma UNIT-ISO/IEC 27002:2005

Principio de reserva	Referencia Norma UNIT-ISO/IEC 27002:2005
Deberían establecerse procedimientos y normas para proteger la información y los medios físicos que contengan información en tránsito.	10.8 Intercambio de información

Nota: Ver anterior

Principio de RESPONSABILIDAD (I)

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

Control Norma UNIT-ISO/IEC 27002:2005

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

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.

Control Norma UNIT-ISO/IEC 27002-2005

Principio de responsabilidad	Referencia Norma UNIT-ISO/IEC 27002:2005
<p>Los roles y responsabilidades de seguridad de empleados, contratistas y de terceros deberían estar definidos y documentados.</p> <p>Los roles y responsabilidades de seguridad deberían incluir las siguientes exigencias:</p>	<p>8.1.1 Roles y responsabilidades</p>

- 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.

Control Norma UNIT-ISO/IEC 27002:2005

Principio de responsabilidad	Referencia Norma UNIT-ISO/IEC 27002:2005
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

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.

Sitios de interés

Agesic

www.agesic.gub.uy

URCDP (Unidad Reguladora y de Control
de Datos Personales)

www.datospersonales.gub.uy

Muchas gracias

normas@agesic.gub.uy

glenda.garces@agesic.gub.uy

AGESIC
Andes 1365, Piso 7
Tel: (+598 2) 901 2929
(11.100) Montevideo – URUGUAY
www.agesic.gub.uy