

## ANEXO 2

### SEGURIDAD DE DATOS

#### Seguridad de datos clasificación

Las aplicaciones utilizadas para la Administración Pública Provincial y la información que manejan, especialmente los datos de carácter personal, deben protegerse contra la pérdida de autenticidad, confidencialidad, integridad y disponibilidad.

Al objeto de conseguir la protección adecuada, es necesario implantar un conjunto proporcionado de medidas de seguridad, tanto técnicas como organizativas, que permitan la creación de un entorno seguro para los datos, la información, las aplicaciones y los sistemas que sustentan a todos ellos. Estas medidas organizativas y técnicas permitirán, en líneas generales, lo siguiente:

1. Identificar, autenticar y, en su caso, autorizar el acceso a los sistemas de información.
2. Identificar fidedignamente a remitente y destinatario de las comunicaciones electrónicas.
3. Controlar el acceso para restringir la utilización y el acceso a datos e informaciones a las personas autorizadas y proteger los procesos informáticos frente a manipulaciones no autorizadas.
4. Mantener la integridad de la información y elementos del sistema, para prevenir alteraciones o pérdidas de los datos e informaciones. Garantizar la disponibilidad de la información y de las aplicaciones.
5. Prevenir la interceptación, alteración y acceso no autorizado a la información.
6. Gestionar las incidencias de seguridad.
7. Auditar y controlar la seguridad.

Las acciones de seguridad a seguir son las establecidas en los estándares internacionales definidas en la ISO/IRAM 17799 (Act. ISO/IEC 27000).

A continuación se define el cuadro de clasificación del nivel de riesgo de datos *(teniendo en cuenta el nivel del dato de acuerdo a la Protección de Datos Personales*

‘Ley de Protección de Datos Personales Nro 25.326’) en virtud de su exposición a la pérdida de Autenticidad, Confidencialidad e Integridad.

Tipos de datos	Sensibilidad	Autenticación	Confidencialidad	Integridad
Según función / Datos de carácter NO personal	Básico	Baja	Libre	Baja
Según función / Datos de carácter personal; ficheros que deben reunir las medidas de seguridad calificadas de nivel básico: Todos los ficheros que contengan datos de carácter personal.	Medio Atenuado	Normal	Restringida	Normal
Según función / Datos de carácter personal; ficheros que deben reunir las medidas de seguridad calificadas de nivel medio: Comisión de infracciones administrativas o penales. Hacienda Pública. Servicios financieros. Datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.	Medio	Alta	Protegida	Alta
Según función / Datos de carácter personal; ficheros que deben reunir las medidas de seguridad calificadas de nivel alto: Datos de ideología, religión, creencias, origen racial, salud o vida sexual. Datos recabados para fines policiales sin consentimiento de las personas afectadas.	Alto (Sensible)	Crítica	Confidencial	Crítica

Detalle de cada una de las Columnas y su clasificación:

Columna	Clasificación
Autenticación	La autenticación, mediante la firma electrónica, se refiere a la capacidad de verificar que un usuario que accede a un sistema o aplicación; o que un usuario que ha generado un documento o

Columna	Clasificación
	información es quien dice ser. La identificación de los usuarios y la verificación de la autenticidad de la misma es un requisito previo a la autorización del acceso a los recursos del sistema.
Niveles de Seguridad de la autenticación:	<p>Su escala de cuatro niveles está ligada a la menor o mayor necesidad de formalización, de autorización y de responsabilidad probatoria en el conocimiento o la comunicación de los activos:</p> <ul style="list-style-type: none"> <li>• Baja, si no se requiere conocer autor ni responsable, datos de carácter no personal.</li> <li>• Normal, si se requiere conocer autor para por ejemplo evitar el repudio de origen, datos a los que se aplican las medidas denominadas de nivel básico.</li> <li>• Alta, si se requiere además evitar el repudio en destino, datos a los que se aplican las medidas denominadas de nivel medio.</li> <li>• Crítica, si se requiere la certificación de autor y de contenido, datos a los que se aplican las medidas denominadas de nivel alto.</li> </ul>
Confidencialidad	Es la condición que asegura que la información no puede estar disponible o ser descubierta por o para personas, entidades o procesos. La confidencialidad se relaciona con la intimidad cuando se refiere a personas físicas. También se define como la “Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados. (ISO 7498-2)” o como la “Prevención de la revelación no autorizada de información. (ITSEC)’ y finalmente la ISO/IRAM 17799 (Act. ISO/IEC 27000). La define como la “Garantía que acceden a la información sólo aquellas personas autorizadas a hacerlo”.
Niveles de seguridad de la confidencialidad:	<p>Su escala usa los siguientes cuatro niveles:</p> <ul style="list-style-type: none"> <li>• Libre, sin restricciones en su difusión / datos de carácter NO personal.</li> <li>• Restringida, con restricciones normales / datos a los que se</li> </ul>

Columna	Clasificación
	<p>aplican las medidas denominadas de nivel básico.</p> <ul style="list-style-type: none"> <li>• Protegida, con restricciones altas / datos a los que se aplican las medidas denominadas de nivel medio.</li> <li>• Confidencial, no difundible por su carácter crítico / datos a los que se aplican las medidas denominadas de nivel alto.</li> </ul>
Integridad:	<p>Es la “Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. La integridad está ligada a la fiabilidad funcional del sistema de información, a su eficacia para cumplir las funciones del sistema” o se puede definir como el “Mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento (ISO/IRAM 17799)” o la “Prevención de la modificación no autorizada de información. (ITSEC)” o también como la “Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado. (ISO 7498-2)”.</p>
Niveles de seguridad de la Integridad:	<p>Su escala usa cuatro niveles referibles a la facilidad mayor o menor de reobtener el activo con calidad suficiente, o sea completo y no corrompido para el uso que se desea darle:</p> <ul style="list-style-type: none"> <li>• Baja, si se puede reemplazar fácilmente con un activo de igual calidad datos de carácter no personal.</li> <li>• Normal, si se puede reemplazar con un activo de calidad semejante con una molestia razonable, datos a los que se aplican las medidas denominadas de nivel básico.</li> <li>• Alta, si la calidad necesaria es reconstruible difícil y costosamente, datos a los que se aplican las medidas denominadas de nivel medio.</li> <li>• Crítica, si no puede volver a obtenerse una calidad semejante, datos a los que se aplican las medidas denominadas de nivel alto.</li> </ul>