BUENAS PRÁCTICAS EN MATERIA DE CONFIDENCIALIDAD

Contenido

Introducción

El presente documento establece las “Buenas Prácticas en Materia de Confidencialidad” aplicable a los documentos, información y datos de la Administración Pública Nacional obrante en los sistemas de Gestión Documental Electrónica – GDE, sus módulos y sistemas informáticos vinculados. Describe los principios, métodos y procedimientos para proteger la confidencialidad y privacidad de los documentos que integran los sistemas informáticos de Gestión Documental Electrónica – GDE, Trámites a Distancia (TAD), Compras Electrónicas, Compr.ar, Contrat.ar, Infraestructura de Firma Digital, Interoper.ar, PAEC, Firm.ar, RCE, RPI, y los que se implementen en el futuro, en cualquiera de sus modalidades de implementación.

Sujetos alcanzados

Toda persona que trabaje con relación a los documentos electrónicos de los mencionados sistemas informáticos tiene el deber de respetar la confidencialidad y la integridad de cualquier documento, información o dato al

que tenga acceso, y es personalmente responsable de proteger y salvaguardar estos recursos en cumplimiento de la presente política.

Los recursos de documentación e información de la APN pueden clasificarse en: documentos oficiales, documentos reservados y documentos secretos. Las presentes "Buenas Prácticas en Materia de Confidencialidad" determina el tratamiento que debe darse a cada uno de ellos a los fines de proteger su confidencialidad. Adicionalmente a esta política, los sistemas y servicios informáticos podrán requerir medidas de protección de seguridad informática que no son parte de esta política.

Las entidades y jurisdicciones que utilizan los sistemas de gestión documental electrónica – GDE deberán aplicar esta política y asegurar el cumplimiento de los controles.

Estas Buenas Prácticas de confidencialidad se aplican tanto a los usuarios de los sistemas de gestión documental electrónica – GDE, como a los proveedores contratados para su desarrollo, incluyendo a los terceros que en función de los contratos deben tener acceso a los sistemas.

Principios de confidencialidad

Estas "Buenas Prácticas en Materia de Confidencialidad" se enmarcan en la normativa vigente respecto del tratamiento de los documentos, información y datos en la República Argentina:

- Ley N° 24.766 de confidencialidad de la información
- Ley N° 25.326 modificatorias y complementarias
- Ley N° 19.549 procedimientos administrativos

El tratamiento de los documentos, información y datos de la APN se ajustará a los siguientes principios:

Principio 1

Toda documentación y datos que la APN necesite recolectar, conservar, procesar, generar o compartir para prestar servicios y gestionar la actividad administrativa tiene un valor intrínseco y requiere de un adecuado grado de protección.

Las clasificaciones de seguridad de los documentos, información o datos indican el grado de sensibilidad que poseen en relación al impacto que pudiere generar su compromiso, pérdida o mal uso. Hay tres niveles de clasificación:

1.- Documentos oficiales públicos: la mayor parte de los documentos, información y datos generados y procesados en la APN. Tienen un bajo nivel de riesgo ante pérdida, robo o publicidad.

2.- Documentos oficiales reservados: documentos que en virtud de alguna norma de carácter superior, y debido a su alto nivel de sensibilidad, se encuentran amparados bajo normas de confidencialidad, y su divulgación está prohibida.

3.- Documentos oficiales secretos: documentos que por su altísimo valor estratégico pueda poner en riesgo la seguridad de la nación, cuyo conocimiento se encuentra restringido por leyes de defensa nacional.

Todos los documentos, información y datos deben ser gestionados con cuidado para cumplir la normativa y reducir el riesgo de su compromiso, pérdida o acceso no autorizado. Esto no se aplica a la información oficial de rutina publicada en los sitios de acceso público.

Principio 2

Toda persona que trabaje con documentos oficiales obrantes en los sistemas informáticos de Gestión Documental Electrónica – GDE, sus módulos y sistemas informáticos vinculados (incluyendo personal de planta, contratados, proveedores, personal de los proveedores, y cualquier tercer usuario de los sistemas) tiene el deber de confidencialidad y es responsable de proteger y salvaguardar todo documento, información o dato a los que tiene acceso, y será advertido al respecto.

El compromiso, pérdida o mal uso accidental o deliberado de la documentación, información o dato puede generar un daño y constituir una falta administrativa, civil o penal. Las personas son individualmente responsables por la protección de los documentos, información o datos a su cargo, y deben ser capacitados acerca de los métodos de seguridad y protección relativos a su rol, incluyendo las potenciales sanciones (administrativas, civiles o penales) derivadas de conductas inapropiadas.

Principio 3

El acceso a documentos con información sensible solamente debe ser autorizado en base a una necesidad genuina y con un adecuado procedimiento de control.

La información necesita ser confiable y estar disponible para las personas correctas en el momento oportuno. Una falla en la entrega de información puede acarrear severas consecuencias (por ejemplo en el caso de historias clínicas o casos judiciales). Deben considerarse tanto la normativa de acceso a la información, como la de protección de datos personales y confidencialidad de la información.

Principio 4

La protección de la confidencialidad de la documentación, información y datos debe alcanzar tanto al manejo interno dentro del sistema informático GDE como al intercambio con terceros usuarios de otros sistemas, incluyendo intercambios internacionales.

Las presentes “Buenas Prácticas en Materia de Confidencialidad” serán de aplicación tanto a la documentación, información o datos obrantes en los sistemas de Gestión Documental Electrónica – GDE y demás sistemas informáticos mencionados, administrados por la APN, como a su intercambio

con otros sistemas, otras jurisdicciones subnacionales e incluso, internacionales.

Compromiso de confidencialidad

A los fines de implementar las presentes “Buenas Prácticas en Materia de Confidencialidad”, los sujetos alcanzados deberán firmar un compromiso expresando que se encuentran advertidos de sus obligaciones, del carácter confidencial que posee la documentación, información y datos a los cuales tendrá acceso, obrantes en los sistemas informáticos, y de las consecuencias administrativas, civiles y penales que su incumplimiento podrá generar.

Se adjuntan los siguientes documentos modelo a ser firmados por los sujetos alcanzados:

Anexo I: “Modelo de compromiso de confidencialidad para usuarios GDE”

Anexo II: “Modelo de compromiso de confidencialidad del proveedor y de sus dependientes”.

Anexo III: “Modelo de compromiso de confidencialidad de usuarios GDE modalidad cloud”.

Anexo IV: “Modelo de Compromiso de Confidencialidad para usuarios de tableau del sistema GDE”

Anexo V: “Términos y condiciones de uso del sistema de Gestión Documental Electrónica – GDE”.