República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Anexo

Número: IF-2024-57335981-APN-DNCIB#JGM

CIUDAD DE BUENOS AIRES
Viernes 31 de Mayo de 2024

Referencia: Anexo - Lineamientos para el uso de herramientas digitales

---

ANEXO

LINEAMIENTOS PARA EL USO DE HERRAMIENTAS DIGITALES

1. **INTRODUCCIÓN**

Los organismos del Sector Público Nacional son algunos de los principales receptores y productores de información de nuestro país. La información puede ser hoy en día objeto de una amplia gama de peligros, amenazas y usos indebidos e ilícitos, debiéndose, por lo tanto, extremar las medidas tendientes a la preservación de su confidencialidad, integridad y disponibilidad.

La presente Resolución, tiene por objeto proteger los derechos y libertades individuales de las personas al tiempo de contribuir a la efectiva prestación continua e ininterrumpida de los diversos servicios ofrecidos por las diferentes entidades y jurisdicciones y, al mismo tiempo, propender a su correcta y mejor gestión interna. En un contexto de transversalidad, en el uso de las tecnologías para la vida social, económica, política y cultural de las personas, la seguridad de la información cumple un rol fundamental.

Consiguientemente, todos los agentes públicos, cualquiera sea el nivel jerárquico y la modalidad de contratación, tienen la obligación de dar tratamiento y hacer un uso responsable, seguro y cuidado de los datos que utilizan en sus labores habituales, adoptando todas las medidas a su alcance para protegerlos.

Por su parte, los responsables de los activos de la información deben atender y diligenciar los recursos necesarios para asegurar el cumplimiento de los objetivos relativos a la ciberseguridad en el ámbito de su jurisdicción. Los datos gestionados en los organismos deben ser protegidos tanto dentro como fuera del ámbito institucional, con independencia del formato y del soporte en el que estén contenidos y si los mismos están siendo objeto de tratamiento electrónico, se encuentran almacenados o están siendo transmitidos. Es por ello, que corresponde a cada organismo determinar sus políticas, normas específicas, procedimientos y guías que, sobre la base de los siguientes lineamientos, sean aplicables a los procesos específicos que desarrollen. Va de suyo, las pautas de tratamiento deben surgir a partir de un análisis de los riesgos para los procesos que lleven adelante.

2. **PRINCIPIOS**

Se entenderán como principio de seguridad de la información, la preservación de confidencialidad, integridad y disponibilidad de la información y de los activos de información del Sector Público Nacional utilizados en su gestión.

3. **ALCANCE**

Los lineamientos establecidos en el presente Anexo se extienden para todos los organismos del Sector Público Nacional alcanzados por la Decisión Administrativa N° 641/2021 y para todos los agentes y funcionarios que en ellos se desempeñen, quienes, con independencia de su nivel jerárquico, deberán conocerlas, entenderlas y cumplirlas, en la medida que les corresponda según su función.

4. **LINEAMIENTOS**

i. CORREO ELECTRÓNICO, TRABAJO COLABORATIVO EN LÍNEA, MENSAJERÍA INSTANTÁNEA Y ALMACENAMIENTO.

Se recomienda cursara través de las herramientas propias del Estado y/o aquellas que hubieran sido contratadas como servicio a terceros de manera oficial por el área pertinente de cada jurisdicción y notificadas a todo el personal, toda vez que se involucre información producida, comunicada, gestionada o almacenada por el Estado:

a. Las comunicaciones a través de correo electrónico.
b. La creación y/o edición de documentos en forma colaborativa.
c. El intercambio de mensajería instantánea
d. El almacenamiento de datos, perfiles, configuraciones, archivos que se encuentren adjuntos en los correos electrónicos, documentos creados colaborativamente y/o incluidos en servicios de mensajería

ii. CONEXIÓN A RED PARA EQUIPOS INVITADOS.

En los casos en que se requiera conectar equipos personales (notebooks, tabletas, etc.) en forma directa a la LAN de un edificio público, se recomienda crear canales seguros tales como VLAN especiales dedicadas a la conexión de equipos invitados con acceso limitado. En los casos en los que la infraestructura lo permita, se podrá configurar un portal cautivo que solicite el registro de los datos personales previo al acceso a la VLAN de invitados.

iii. CONEXIÓN A RED PARA EQUIPOS AUTORIZADOS

El acceso completo a la VLAN por parte de personal autorizado con equipo propio, se recomienda concederlo sólo a aquellos equipos que cumplan con requisitos mínimos de seguridad siendo estos definidos por cada organismo, considerando la versión vigente de los Estándares Tecnológicos de la Administración Pública y la DA 641/2021 o modificatorias y complementarias.

iv. ACCESO REMOTO.

Para el acceso a sistemas internos del organismo en forma remota, se recomienda implementar una solución VPN (red privada virtual) y la correspondiente instalación del cliente VPN en el equipo invitado.

v. CONTROL DE USUARIOS Y PRIVILEGIOS.

Las gestiones de altas y bajas de cuentas de usuario y privilegios se recomienda realizarlas de manera adecuada y oportuna, en coordinación con todas las áreas involucradas, incluyendo las direcciones de recursos humanos. Asimismo, se recomienda realizar en todo momento un seguimiento detallado sobre las cuentas con privilegios especiales, y revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento. También se

recomienda evitar el uso de cuentas genéricas de usuario tales como “soporte”, “administrador”, etc. de modo que el responsable de la configuración, acceso o perfil esté debidamente identificado.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.05.31 16:52:01 -03:00

Federico Sebastián PIERRI
Director Nacional
Dirección Nacional de Ciberseguridad
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.05.31 16:52:01 -03:00