Cartilla

Guía para el uso aceptable de los activos de información

Proceso Información, Innovación y Tecnología
Subproceso Seguridad de la información
Versión 1
CT-IIT-0138
Año 2024

El contenido de este documento corresponde a Información Pública

TABLA DE CONTENIDO

INTRODUCCIÓN

Este documento establece el uso adecuado de los activos de información de la entidad por parte de todos los colaboradores y proveedores que creen, actualicen, tengan acceso, utilicen, almacenen transfieran o eliminen activos de información de la entidad.

A continuación, se indica cómo se deben usar los activos de acuerdo con el ciclo de vida de la información:

A. CREACIÓN

1. Al crear entornos de trabajo colaborativos [1]se debe compartir únicamente con el personal que corresponda.
2. El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
3. Se debe definir el tipo de acceso (lectura, escritura, modificación y borrado) y los roles estrictamente necesarios sobre la carpeta compartida.

B. ACTUALIZACIÓN

1. Los propietarios deben realizar actualización del inventario de activos de información de la **DIAN,** de acuerdo con lo establecido en la normatividad y definiciones adoptadas por la entidad.
2. Mantener el tipo de acceso (lectura, escritura, modificación y borrado) y los roles estrictamente necesarios sobre la (s) carpeta (s) compartida (s) cuando estas sean actualizadas o los usuarios cambien de funciones.
3. Cuando se retire un colaborador de la entidad, su usuario se desactiva y por lo tanto ya no tiene acceso a los aplicativos y recursos compartidos.

C. ACCESO

1. Los colaboradores directos y/o terceros de la entidad solo deben tener acceso a los aplicativos asignados para el cumplimiento de sus funciones.
2. Los colaboradores deberán utilizar únicamente los aplicativos, equipos de cómputo y equipos móviles autorizados por la Dirección de Gestión de Innovación y Tecnología, en

[1] Permite que se pueda compartir la información a través de almacenamiento en la nube (OneDrive) e incluye la aplicación Teams de mensajería instantánea, llamadas y videollamadas, pensadas para el trabajo colaborativo ya sea que se realice de forma remota o presencial.

caso de que utilicen equipos personales deben usar controles de acceso adicionales como VPN.
3. Está prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por la **DIAN** a través de la política de navegación.
4. Todo colaborador de la **DIAN** es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
5. Los colaboradores y terceras partes que estén dentro del dominio deben abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material ya sea vía web o medios magnéticos.
6. No se debe permitir el acceso a carpetas compartidas a colaboradores o terceras partes que no cuenten con antivirus corporativo actualizado, en caso de utilizar equipos personales estos también deben contar con antivirus actualizado.

D. USO

1. Sólo está permitido el uso de software licenciado por la **DIAN** y/o aquel que sin requerir licenciamiento este permitido por la entidad.
2. Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas y/o de procedencia desconocida.
3. Los colaboradores no podrán efectuar ninguna de las siguientes acciones sin previa autorización de la Dirección de Gestión de Innovación y Tecnología:
    a. Usar licencias no autorizadas por la Dirección de Gestión de Innovación y Tecnología a través de la Subdirección de Soluciones y Desarrollos.
    b. Modificar, revisar, transformar o adaptar cualquier software propiedad de la **DIAN**.
    c. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la **DIAN**.
4. Los colaboradores deberán hacer uso responsable de la información que puedan obtener de los aplicativos de la entidad y de los recursos compartidos, de acuerdo con las funciones asignadas.
5. La Dirección de Gestión de Innovación y Tecnología es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
6. El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización, por lo tanto, deben ser utilizados por los colaboradores o terceras partes únicamente para realizar las funciones establecidas en su labor dentro de la **DIAN**.
7. La información de la **DIAN no** podrá ser llevada a tecnologías de computación en la nube si no está previamente autorizado por la Dirección de Gestión de Innovación y Tecnología.
8. Los colaboradores se comprometen a hacer uso adecuado de los dispositivos móviles institucionales (celulares o computadores portátiles) para el acceso a los servicios institucionales de movilidad proporcionados por la Dirección de Gestión de Innovación y Tecnología (ejemplo la suite de Office 365).
9. El proveedor o la tercera parte contratados por la entidad, tendrán responsabilidad tanto civil como penal en lo relacionado al uso aceptable de los activos de la **DIAN**.

E. ALMACENAMIENTO

1. Los colaboradores y/o terceros no deben guardar ningún tipo de información personal en los equipos asignados, solo se permite la información necesaria para cumplir con su labor.
2. Es responsabilidad de los colaboradores mantener copias de seguridad de la información contenida en sus estaciones de trabajo, en los repositorios definidos por la Dirección de Gestión de Innovación y Tecnología (SharePoint, OneDrive o similares) y entregarlas a la **DIAN** en custodia al finalizar la vinculación con la entidad.
3. Todo archivo recibido a través de medio magnético/electrónico o descarga de Internet de red externa, deberá ser revisado para detección de virus y otros programas destructivos antes de ser utilizados para no afectar la infraestructura tecnológica de la **DIAN**.
4. Usar los mecanismos disponibles para proteger las copias temporales o permanentes de la información, ejemplo: asignación de acceso con restricciones, autenticación con contraseña o cifrado si está implementado, entre otros.
5. Almacenar la información de acuerdo con la clasificación (pública, pública clasificada o pública reservada).

F. TRANSFERENCIA

1. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.
2. La Dirección de Gestión de Innovación y Tecnología es la única dependencia autorizada para la administración del software de la entidad, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
3. Se deben firmar acuerdos de confidencialidad o compromisos de protección de los activos y su información de propiedad de terceros, incluyendo servicios de computación en la nube pública.

G. ELIMINACIÓN

1. En general, cuando un funcionario va a entregar su equipo de cómputo, debe llevar toda la información a OneDrive o SharePoint y luego eliminar documentos y/o carpetas.
2. Para la Subdirección de Soluciones y Desarrollo, los funcionarios que estén desarrollando software deberán publicar las versiones de desarrollo trabajadas en los respectivos repositorios, antes de realizar cualquier movimiento o borrado de información del equipo.
3. Los ingenieros de soporte en sitio deben aplicar el procedimiento de borrado seguro a todos los equipos de cómputo que serán entregados a otros colaboradores o se van a dar de baja.
4. La información impresa que cuente con datos públicos clasificados o reservados deben eliminarse rasgándolos con las manos o utilizando maquinas pica papeles.

No. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	18/01/2024		"Versión inicial".	Esta versión corresponde a Información Pública

Elaboró:	Tito Alejandro Menjura Murcia ***Elaboración metodológica*** *Diana Shirley Zambrano Ramírez* ***Elaboración Técnica***	Gestor II Analista IV	Coordinación de Procesos y Riesgos Operacionales Oficina de Seguridad de la Información
Revisó:	Miguel Alfonso Caucali Pinzon	Gestor II	Oficina de Seguridad de la Información
Aprobó:	Edgar Fernando Aviles Gomez	Jefe Oficina	Oficina de Seguridad de la Información