AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA DE INTERCAMBIO DE INFORMACIÓN

BOGOTÁ D.C. JUNIO DE 2020

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Agencia para la Reincorporación y la Normalización considera que la información es uno de sus principales activos intangibles indispensable en el cumplimiento de su misión y en la dirección y consecución de sus objetivos, programas, planes, proyectos y metas, por lo que se hace necesario establecer estrategias y mecanismos que nos permitan protegerla independientemente del medio en que se encuentre o la forma en que se maneje, transporte o almacene.

En el marco del Decreto 1008 de 2018 referido a la Política de Gobierno Digital se cuenta con el habilitador transversal de Seguridad y Privacidad el cual busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de la adopción del Modelo de Seguridad y Privacidad de la Información.

La seguridad de la información es una prioridad para la ARN y por tanto es responsabilidad de todos dar cumplimiento a cada una de las políticas y lineamientos.

El presente documento establece las directrices mínimas para intercambiar información relacionada con la ARN. Todas las Entidades involucradas deben proteger la información para asegurarse de cumplir con las normas y políticas establecidas y que no implique perjuicios a las partes como consecuencia del intercambio de información.

2. OBJETIVO

Proporcionar una guía a la Entidad que le permita gestionar los intercambios de información a nivel interno, con otras entidades, con proveedores o con terceros de forma adecuada, estandarizada y regulada garantizando la confidencialidad, la integridad y la disponibilidad de la información, promoviendo una cultura de seguridad entre todos los servidores públicos y colaboradores como medida preventiva para proteger la información y mitigar los riesgos en su gestión.

3. ALCANCE

El presente documento aplica para intercambios de información internos y externos que gestione la ARN.

4. DEFINICIONES

ACTA DE INTENCIÓN: es un tipo de acuerdo que contiene compromisos que más tarde pueden formalizarse mediante la redacción de un contrato o convenio.

ANONIMIZACIÓN: Hace referencia al proceso por el cual deja de ser posible establecer, por medios razonables, el nexo entre un dato y el sujeto al que se refiere.

CIFRADO: El cifrado ayuda a proteger los datos en el dispositivo para que solo puedan acceder a ellos personas con autorización.

CONTRATO: Acuerdo, generalmente escrito, por el que dos o más partes se comprometen recíprocamente a respetar y cumplir una serie de obligaciones.

CONVENIO: Acuerdo cuya celebración se realiza entre dos entidades públicas.

CUSTODIO: Es el colaborador o dependencia de la Entidad responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido.

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables

DATO PRIVADO: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.

DATO SEMIPRIVADO: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

DATO SENSIBLE: Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos

ETIQUETADO: Se trata de una señal, marca o rótulo que se adhiere a la información para su identificación, clasificación o valoración.

FILE TRANSFER PROTOCOL (FTP): Es un protocolo para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol). desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

INFORMACIÓN PÚBLICA: Es aquella información que puede ser distribuida abiertamente al público sin que cause daño alguno a la entidad, a sus colaboradores, otras dependencias o a otras entidades.

INFORMACIÓN PÚBLICA CONFIDENCIAL O CLASIFICADA: Es aquella información que, con base en el análisis de riesgo, haya sido clasificada como confidencial por su carácter de restringido a un grupo de personas o área en particular, bajo el concepto de necesidad de conocer.

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que tiene establecido el carácter de “Dato Sensible”, pues afecta la intimidad de las personas y su uso indebido puede generar su discriminación.

INTERCAMBIO DE INFORMACIÓN: mecanismo a través del cual las instituciones y organizaciones o personas naturales comparten información.

PROPIETARIO: Es el colaborador o dependencia de la Entidad a la cual, se le ha asignado la responsabilidad formal sobre un activo de información.

PUBLICAR O DIVULGAR: Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.

USUARIO: Se refiere a los servidores públicos y colaboradores debidamente autorizados para usar equipos, sistemas o aplicativos o servicios informáticos, disponibles en la red de la ARN y a quienes se les otorga un nombre de usuario y una clave de acceso

VIRTUAL PROTOCOL NETWORK (VPN): Es una tecnología de red de computadoras que permite una extensión segura de la red de área local(LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

WEB SERVICES: Es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

5. CONTENIDO Y DESARROLLO

5.1 CLASES DE INFORMACIÓN

La ARN clasifica la información de acuerdo con lo establecido en los documentos DE-I-03 Instructivo para la actualización de activos de información y el Programa de gestión documental, los aspectos a tener en cuenta se describen a continuación.

La información que se maneja en la ARN posee diferentes niveles de criticidad en cuanto al riesgo que representa su divulgación, adulteración o indisponibilidad. Por lo que se hace necesario diferenciar y clasificar la información según el nivel de riesgo.

Para la clasificación de la información, la ARN adopta el siguiente modelo de clasificación, compuesto por los subsiguientes tres niveles o categorías, los cuales cubren las definiciones y conceptos de la legislación vigente y estándares internacionales (Ley 1581 de 2012 para Protección de Datos y demás relacionada con habeas data, Ley 1712 de 2014 de Transparencia y acceso a la información, ISO 27000-2013).

- Información pública
- Información pública reservada
- Información pública confidencial o clasificada

El propietario del activo de información debe establecer los mecanismos de protección teniendo en cuenta su disposición final definida en las Tablas de Retención Documental, las políticas de gestión documental y de seguridad de la información para garantizar el manejo y custodia adecuados para la misma.

El responsable de la información evalúa los mecanismos requeridos para garantizar su preservación, integridad, respaldo y controles de acceso apoyándose en las instrucciones brindadas en el Sistema Integrado de Conservación que comprende el Plan de Conservación documental y el Plan de Preservación Digital reglamentado mediante acuerdo 006 de 2014 y TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información.

Una de las medidas de protección básicas sugiere el etiquetado de la información en lo posible desde el mismo momento de su producción y durante su ciclo de vida, para que en los trámites requeridos se mantengan los controles del caso.

Para ello, se sugiere tomar como guía las disposiciones descritas en la siguiente tabla:

TABLA No.1 DESCRIPCIÓN DE CONTROLES SEGÚN LA CLASE DE INFORMACIÓN

Clase de información	Controles físicos y administrativos	Autorización para reproducción	Autorización para distribución	Disposición final
Información Pública	Distribución autorizada por el creador de la información.	Ilimitada.	Sin restricción.	La que indique la tabla de retención documental
Información Pública Reservada	• Utilizar pie de página con nota “Reservada”. • El autor es responsable de asegurar la confidencialidad de la información y garantizar su distribución únicamente bajo autorización y siguiendo el principio “necesidad de conocer debido a los fines de su trabajo”. Si es electrónica cifrarla cuando sea necesario.	Con autorización del autor	• Externa: Sobre sellado sin marcas. Entrega a mano y firma de planilla de acuse de recibo con niveles de seguridad apropiada a la información (sobres de única apertura, monitoreo de entrega, entre otros). • Electrónica: Uso del correo electrónico institucional con cifrado de datos o canal seguro definido entre las entidades involucradas.	Para datos electrónicos. se deben seguir las disposiciones del Programa de Gestión Documental – PGD, para la disposición de los documentos electrónicos en cuanto a la conservación total, selección y eliminación; actividades asociadas a la Tabla de Retención Documental – TRD. Los documentos y expedientes electrónicos sin valores secundarios y que hayan cumplido su tiempo de retención documental conforme a lo establecido en las tablas de retención documental, deberán eliminarse mediante procedimientos de borrado permanente y seguro.
Información Pública Confidencial o Clasificada	• Utilizar pie de página con nota “Confidencial o Clasificada”. • El autor es responsable de asegurar la confidencialidad de la	Con autorización del autor	• Externa: Sobre sellado sin marcas. Entrega a mano o por correo certificado	Para datos electrónicos. Los documentos y expedientes electrónicos sin valores secundarios y que hayan cumplido su

Clase de información	Controles físicos y administrativos	Autorización para reproducción	Autorización para distribución	Disposición final
	información y garantizar su distribución únicamente bajo autorización y siguiendo el principio "necesidad de conocer debido a los fines de su trabajo". • El custodio de la información es responsable de almacenar la información apropiadamente y controlar su circulación solo para uso interno. Debe solicitar autorización para su distribución a los entes de control, al autor o a una autoridad superior para su distribución inclusive dentro de la organización.		• Electrónica: Uso del correo electrónico institucional con cifrado de datos o canal seguro definido entre las entidades involucradas.	tiempo de retención documental conforme a lo establecido en las tablas de retención documental, deberán eliminarse mediante procedimientos de borrado permanente y seguro de medios electrónicos. Para Datos electrónicos: Borrado para CD, DVD y discos duros usar los procedimientos de borrado permanente y seguro.

5.2 MEDIDAS DE PROTECCIÓN PARA LAS CLASES DE INFORMACIÓN

Entre las medidas de protección de la información que se adoptan en la ARN según las necesidades se incluyen las siguientes:

- **Autenticación**: Para proteger la confidencialidad de la información se requiere autenticar las personas en los sistemas de información que tendrán acceso a la información. El mecanismo más simple es usar una palabra clave comunicada a los involucrados.

- **Acceso basado en roles:** Otorgar acceso de acuerdo con las responsabilidades o funciones que debe cumplir el colaborador. Es decir, otorgar acceso a los datos únicamente si es indispensable para el desarrollo de sus actividades.

- **Cifrado de datos**: El cifrado de datos consiste en transformar la información de modo que no pueda ser visualizada o no pueda ser comprensible, si es accedida por un usuario no autorizado.

- **Controles administrativos:** Se distinguen entre otros los siguientes: procedimientos, segregación de funciones, gestión de control de cambios, rotación de funciones, entrenamiento cruzado (un funcionario entrena a otro para que lo supla en ausencias provisionales), que permiten establecer mecanismos para proteger la confidencialidad y la integridad de los datos.

- **Controles de tecnología:** Se cuenta con antivirus, redundancia en aplicaciones y separación de redes de datos entre otros que facilitan la protección de los datos.

- **Aseguramiento:** La Oficina de Tecnologías de la Información valida que los sistemas estén efectivamente protegidos a través del cumplimiento de las políticas de seguridad configuradas en la infraestructura, auditoría de sistemas, pruebas de intrusión, evaluación del desempeño de sistemas de información, supervisión administrativa y supervisión del acceso a los datos.

6. TIPOS Y LINEAMIENTOS DE INTERCAMBIOS DE INFORMACIÓN

La ARN a definido un modelo básico de gestión de los intercambios de información, así como los tipos y lineamientos a tener en cuenta en los diferentes intercambios, que se describen a continuación:

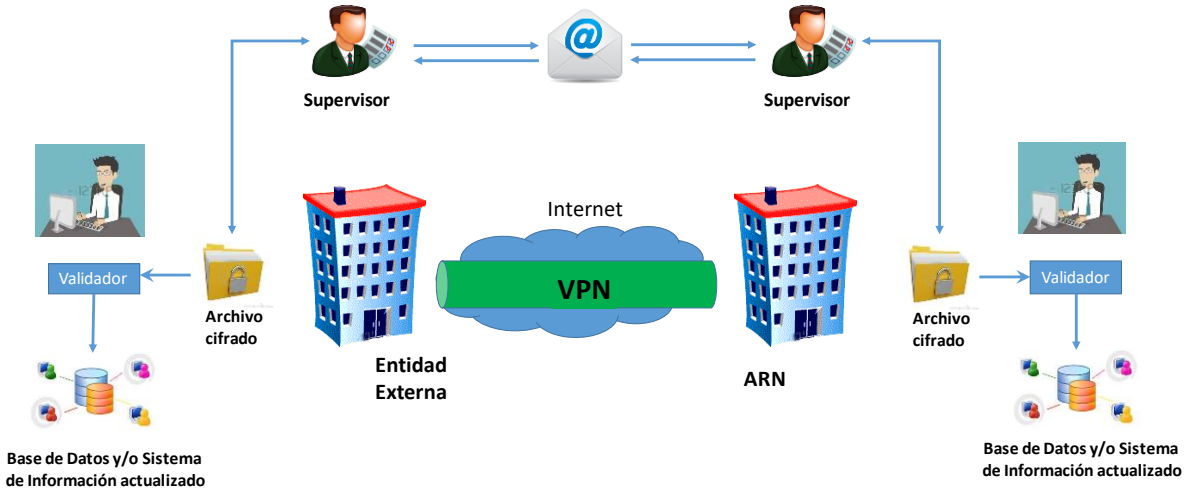
- Modelo tecnológico para intercambio de información entre entidades y proveedores
- Intercambio interno digital
- Intercambio externo digital

Toda solicitud relacionada con el servicio de intercambio de información que requiera el soporte técnico de la Oficina de Tecnologías de la Información debe ser canalizada a la Mesa de Servicios por los supervisores de convenios y/o profesionales responsables de intercambios a través del BX: 443 0020 Ext: 10999, o al correo soporte@reincorporacion.gov.co

6.1 MODELO TECNOLÓGICO PARA INTERCAMBIO DE INFORMACIÓN ENTRE ENTIDADES Y PROVEEDORES

La Oficina de Tecnologías de la Información propone el siguiente modelo para intercambio de información que incluye la participación de los Supervisores de los contratos o convenios, en concordancia con lo dispuesto en el documento BS-M-01 Manual de Contratación y Supervisión e Interventoría.

FIGURA1. MODELO TECNOLÓGICO DE INTERCAMBIO DE INFORMACIÓN



6.2 INTERCAMBIO INTERNO DIGITAL

Para el intercambio interno digital se indican las siguientes disposiciones:

- Para el intercambio entre colaboradores hacer uso únicamente de los siguientes medios: carpeta compartida, correo electrónico institucional o herramienta de comunicaciones institucional.

- La información pública confidencial o reservada transmitida debe contar con la leyenda en marca de agua “Confidencial”.

- Cuando la información a intercambiar se encuentre almacenada en carpeta compartida, los responsables de las carpetas deben establecer los roles y privilegios de acceso a dicha información (lectura y escritura) para garantizar la integridad de la información e identificar que el contenido es de carácter confidencial.

- Garantizar el obligatorio cumplimiento del numeral 3.9 Política de Intercambio de Información descrita en el documento TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información.

6.3 INTERCAMBIO EXTERNO DIGITAL

6.3.1 PARA ENTIDADES Y PROVEEDORES

- Los intercambios de información deben estar regulados a través de un contrato, convenio o acta de intención, con un documento complementario denominado anexo técnico el cual será generado con el acompañamiento de la Oficina de Tecnologías de la Información quien apoya las acciones relacionadas con la definición de los mecanismos a utilizar para asegurar los principios de seguridad de la información relacionados con Confidencialidad, Integridad y Disponibilidad, asimismo especificar el flujo de la información, aprobaciones y autenticación detallada para la transferencia de información. El mejor escenario para establecer un intercambio es aquel donde exista la mínima intervención humana en el proceso y que en la medida de lo posible sea automatizado.

- Si la información a intercambiar contiene datos sensibles se debe asegurar los siguientes aspectos:

    - Anonimización de la información
    - Tiempo del uso de la información
    - Responsables de los intercambios
    - Mecanismos para evitar la interceptación, copiado, modificación y/o destrucción de la información.
    - Cumplimiento de Ley 1581 de 2012 que constituye el marco general de la protección de los datos personales y demás reglamentación relacionada con habeas data.
    - Cumplimiento de Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública.
    - Correcta Custodia o eliminación de la información histórica teniendo en cuenta el Plan de preservación digital y el Programa de gestión documental.

- Todo archivo que contenga datos sensibles relacionado con la población objeto de atención debe ser anonimizado (según la naturaleza de la solicitud) y cifrado.

- La Subdirección de Seguimiento es la encargada de realizar el proceso de anonimización de la información a través de los protocolos internos establecidos, asimismo, se encarga de orientar y brindar las pautas necesarias para la entrega o intercambio de información sujeto a las políticas de datos personales.

- El cifrado de la información se debe realizar mediante el uso de herramientas de cifrado, compresión, codificación etc., tales como 7Zip, PGP, entre otros, siguiendo los documentos que se encuentran en documentos complementarios del SIGER llamados: Instructivo Cifrado Documentos - 7Zip y/o Instructivo Cifrado Documentos- PGP de cada herramienta dependiendo del modelo tecnológico acordado entre las entidades.

- En caso de NO poder adoptar el modelo de intercambio de información a través del uso de VPN y/o FTPS, dicho intercambio debe ser realizado a través de correo electrónico institucional, los archivos deben ser cifrados con las herramientas definidas por la OTI.

- La información sensible transmitida debe contar con la leyenda en marca de agua “Confidencial”.

- Para los supervisores de convenios o contratos se indican las siguientes disposiciones:

    - Garantizar el obligatorio cumplimiento de la Política de Intercambio de Información descrita en el documento TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información, en concordancia con lo dispuesto en el documento BS-M-01 Manual de Contratación y Supervisión e Interventoría.
    - Los convenios, contratos o actas de intención deben incluir un numeral que especifiquen la obligatoriedad de cumplir con la *Guía para la implementación del principio de responsabilidad demostrada* (Accountability) emitida por la Superintendencia de Industria y Comercio dirigida a todas las organizaciones que deben cumplir con el régimen general de protección de datos personales.
    - Definir las personas autorizadas para los intercambios.

- La transferencia de información digital es liderada por las dependencias encargadas de la gestión o supervisión de los intercambios de información con el acompañamiento técnico de la Oficina de Tecnologías de la Información. La transmisión de datos está limitada a lo descrito en la Ley 1581 de 2012 artículo 26 y el Decreto 1377 de 2013 artículos 24 y 25, donde se prohíbe la

transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Este listado de países es definido por la Superintendencia de Industria y Comercio, en la cual, la ARN o su encargado de tratamiento, debe garantizar intercambio y resguardo de la información.

6.3.2 PARA PETICIONES DE INTERÉS GENERAL Y PARTICULAR

- Si la información intercambiada es utilizada para la generación de algún tipo de estudio se deben respetar los derechos de autor teniendo en cuenta las disposiciones descritas en AJ-P-12 Procedimiento para el registro de propiedad intelectual y todas las disposiciones descritas en DE-G-02 Guía para presentar solicitudes de apoyo a proyectos de investigación, DE-G-04 Guía para evaluar propuestas de investigación de personas externas a la entidad.

- Para las Peticiones, Quejas, Reclamos, Sugerencias y Denuncias de la ciudadanía se deben seguir todas las disposiciones descritas en AC-M-01 Manual del Sistema de PQRS'D.

- Todo archivo que contenga datos sensibles relacionados con la población objeto de atención debe ser anonimizado (según la naturaleza de la solicitud) y además cifrado.

- La protección de la información a nivel de confidencialidad debe realizarse mediante el uso de herramientas de cifrado o compresión, tales como 7Zip, PGP entre otros, siguiendo los documentos Instructivo Cifrado Documentos - 7Zip y/o Instructivo Cifrado Documentos- PGP de cada herramienta dependiendo del modelo tecnológico acordado entre las entidades.

7. ENTREGA Y RECEPCIÓN DE INFORMACIÓN A TRAVÉS DE MEDIOS EXTRAÍBLES

Las siguientes disposiciones son definidas como casos especiales en los cuales no se pueda realizar el intercambio en línea mediante VPN, cuando se reciba o se entregue información a través de (Dispositivos USB, Discos Duros portables, CD, DVD, Blu-ray, etc.)

- El uso de dispositivos removibles es un requerimiento que debe ser evaluado por el Oficial de Seguridad de la Información de la ARN y así mismo será autorizado de acuerdo con lo dispuesto en la Circular 018 de 2018 y según el

formato TI-F-01 Solicitud de usuario y/o recursos tecnológicos a través de la mesa de servicios.

- Todo el manejo que se haga de los datos sobre medios removibles debe mantener el tratamiento de acuerdo con la clase de información. Antes de copiar un archivo hacia un medio removible debe verificarse su clasificación con base en los criterios de Confidencialidad, Integridad y Disponibilidad, según estos criterios se procederá con los controles que se describen a continuación:

    - Confidencialidad: Si el archivo pertenece a la clasificación “Información Pública Reservada” o “Información Pública Clasificada” se deben usar las herramientas de cifrado o compresión, tales como 7Zip, PGP, entre otros, siguiendo los documentos Instructivo Cifrado Documentos - 7Zip y/o Instructivo Cifrado Documentos- PGP de cada herramienta dependiendo del modelo tecnológico acordado entre las entidades.
    - En caso de entregar información a un encargado de tratamiento, se debe definir en los diferentes acuerdos contractuales la correcta custodia y/o eliminación parcial o total.
    - Disponibilidad: Consideraciones sobre quien recibe los datos y el formato en que debe leerlos, teniendo en cuenta que, si es cifrado, debe contar con las llaves de acceso.

8. DISPOSICIÓN FINAL DE LA INFORMACIÓN

A continuación, se indican las acciones para la disposición final de la información según su naturaleza:

- Para dispositivos USB, Discos Duros portables, CD, DVD, Blu-ray, etc., se debe seguir lo dispuesto por el Grupo de Gestión Documental según lo dispuesto en el documento GD-P-02 Procedimiento para eliminación documental en archivo central.

- Para los archivos que se intercambien a través de Correo Electrónico, Web Services y/o VPN se debe tener en cuenta lo descrito en numeral 3.9 Política de Intercambio de Información del documento TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información y las disposiciones del documento Plan de Preservación Digital.

9. REFERENCIAS

- Ley 1581 de 2012 y demás reglamentación relacionada con habeas data
- Ley 1712 de 2014
- TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
- Guía para la implementación del principio de responsabilidad demostrada (Accountability)
- Norma técnica internacional ISO 27001:2013 de Sistemas de Gestión de la Seguridad de la Información
- Instructivo_Cifrado_Documentos_7Zip
- Instructivo_Cifrado_Documentos_PGP