Contenido

1. NOBJETIVO

Intercambiar información con nuestros proveedores, aliados estratégicos y solicitantes de entidades públicas de manera controlada y segura, desde o hacia el ICETEX.

2. ALCANCE

Aplica para la recepción y entrega de información a terceros, que se encuentre catalogada como información pública reservada e información pública clasificada, quedando oficializado su intercambio a través del diligenciamiento del Formato de intercambio de información con terceros.

3. DEFINICIONES

Las definiciones de este documento son las pertinentes para el adecuado entendimiento del intercambio de información y por ende facilitar la ejecución de las actividades que conforman el conjunto de operaciones en los procesos involucrados.

- **Aliado estratégico**: persona natural o jurídica con la cual el Icetex tiene una motivación para fortalecer el desarrollo de su estrategia de servicio de acuerdo con la constitución y la Ley 1002 de 2005.

- **Activo:** en el ámbito de la seguridad digital, se refiere a cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del instituto y, en consecuencia, debe ser protegido (ISO/IEC 27000).

- **Archivo:** es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados y respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia.

  Anonimización: transformar los datos individuales de las unidades de observación, de tal modo que no sea posible identificar sujetos o características individuales de la fuente de información, preservando así las propiedades estadísticas en los resultados**.**

- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados (según la norma ISO/IEC 27001:2013)

- **Cifrado Fuerte / Robusto:** técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES (Circular Externa 029 de 2014 Superintendencia Financiera de Colombia).

- **Entidades Públicas:** en este documento, se refiere a las Entidades Públicas que requieren información del Instituto, fundamentados en la Ley 1581 de 2012 de Protección de datos personales que menciona "*Artículo 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.*"

- **Información Digital:** cualquier tipo de información, contenida en formatos tangibles (DVD, CD ROM, DVD y sucesores) y no tangibles (bases de datos, archivos, textos online).

- **Información Pública:** es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (Ley 1712 de 2014). Es de aclarar que ICETEX es sujeto obligado al cumplimiento de esta Ley, de igual manera las personas naturales y jurídicas, públicas o privadas, que presten función pública.

- **Información Pública Clasificada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014

- **Información Pública Reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

- **Información Original:** en el ámbito de seguridad digital, es cuando la información debe ser enviada en el formato original. Se deben definir las técnicas de criptografía y los mecanismos de protección y control para garantizar la confidencialidad de la información y el cumplimiento legal.

- **Información anonimizada:** es el dato que no permite identificar o individualizar al dueño del dato o de la información, como resultado de un proceso de tratamiento de datos ejecutado para impedir de forma irreversible la identificación del interesado, al destruir el vínculo con toda la información que

identifique al sujeto o porque la asociación para la identificación exige una gran cantidad de tiempo, esfuerzo, inversión, operación y trabajo desmedidos.

- **Intercambio de información**: proceso entre entidades en el que se comparten e intercambian información de interés común. Requiere de acuerdos entre las partes para definir la estructura de los datos que serán intercambiados, entre otros aspectos. (Definición de MinTIC).
- **Medios removibles:** cualquier componente extraíble de hardware que sea usado para el almacenamiento de información.
- **Nivel de clasificación de la Información**: es la clasificación que tiene la información, acorde con la Ley 1712 de 2012.
- **Propietario de la Información:** nombre del área, dependencia, grupo de trabajo que genera la información y/o que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, así como definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso de la entidad externa que genera la información o es dueña del activo de información.
- **Responsable por el Activo de Información:** es el cargo, designado por los propietarios, encargado de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar y proteger dichos activos a su cargo.
- **Servicio de interoperabilidad:** es el servicio que brinda las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración y la compartición de la información. con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.
- **SFTP:** SSH File Transfer Protocol, Protocolo de transferencia de archivos que utiliza SSH para asegurar los comandos y los datos que se transfieren entre el cliente y el servidor.
- **SSH:** Secure Shell, Protocolo que permite acceder a máquinas remotas a través de una red.
- **SSL:** Secure Sockets Layer, Protocolo criptográfico que proporciona comunicaciones seguras por una red.
- **TLS:** Transport Layer Security, Protocolo criptográfico que proporciona comunicaciones seguras por una red.
- **Tercero**: para el ICETEX se definen como terceros ciudadanos, entidad estatal que requiere información de la Entidad de forma esporádica, ciudadanos. proveedores, aliados estratégicos (bien sea entidad pública o privada).
- **Tratamiento de datos personales**: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

MARCO NORMATIVO

Norma	Descripción	Aplicabilidad
ISO 27001 – A.13.2	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. Se debe contar con políticas y procedimientos y controles de transferencia formales para proteger la transferencia de la información mediante el uso de todo tipo de instalaciones de comunicaciones.	Todo intercambio de información
Ley 1581 de 2012	Disposiciones para la protección de datos personales de acuerdos con los **principios** del artículo 4. Reglamenta las transferencias y transmisiones de datos personales.	Intercambio que contenga datos personales
Ley 2052 de 2020	Los sujetos obligados en los términos de la presente ley, deberán crear, diseñar o adecuar los mecanismos de intercambio de información de los sistemas y soluciones tecnológicas que soportan sus trámites, dando cumplimiento al Marco de Interoperabilidad y los lineamientos de vinculación al servicio de interoperabilidad de los servicios ciudadanos digitales según lo establecido sobre el particular por el Ministerio de Tecnologías de la Información y las Comunicaciones.	Acuerdos de interoperabilidad con entidades públicas donde la frecuencia sea mayor a una sola vez

Decreto 620 02/05/2020	Marco de interoperabilidad estructura de trabajo común donde se alinean los conceptos y criterios que guían el intercambio de información.	Acuerdos de interoperabilidad con entidades públicas donde la frecuencia sea mayor a una sola vez

4. CONDICIONES GENERALES

4.1 Intercambio de información general

- Las condiciones descritas aplican para la entrega y recepción de información.

- Para intercambio de información de datos personales es necesario:
  - o Asegurar que el titular de los datos haya dado la autorización de tratamiento de datos personales, Además, el uso que se dará en el intercambio de información debe estar definido en las finalidades en dicha autorización.
  - o Identificar el tipo de datos a intercambiar.
  - o Alcance y actividades para realizar con la información.
  - o Obligaciones en materia de seguridad y privacidad.

- Para el intercambio de información se formaliza con el "formato Intercambio de información" (F313) con terceros, el cual tiene la misma vigencia del contrato y/o acuerdo estratégico, por cuanto es necesario diligenciarse al inicio del mismo. Es responsabilidad de su diligenciamiento el Líder de Riesgo del área.

- El derecho de acceso a la información en ningún caso puede colisionar con la privacidad y confidencialidad de los datos de las personas o extralimitarse a la constitución y la ley de protección de datos personales.

- Está prohibido suministrar a terceros información que no ha sido producida por ICETEX, es la información obtenida por la Entidad mediante convenios, acuerdos de un tercero.

- El intercambio de información con aliados estratégicos cuya información sea de un Fondo de Administración, es requisito consultar al Constituyente y obtener su aprobación para entrega de información.

- Toda información pública clasificada o pública reservada a intercambiar se debe proceder de acuerdo con el "Procedimiento de Transferencia segura de información" (A7-1-20), considerando:

  ✓ Hacer uso de mecanismos de transferencia segura como cifrado, SFTP, SSL, TLS.
  ✓ Realizar cifrado de información haciendo uso de un algoritmo de cifrado robusto PGP, SSH (RSA y/o DSA).
  ✓ Entregar de forma segura la contraseña asignada al usuario utilizando el protocolo de seguridad establecido por el Instituto.
  ✓ Asegurar que las contraseñas cumplan con las políticas establecidas: considerar complejidad, longitud y tiempo de expiración de las mismas.
  ✓ Informar a los usuarios las políticas de contraseñas que deben cumplir para la información clasificada y reservada.
  ✓ Garantizar el registro de los logs de auditoría y el registro de las actividades del usuario(s) creado(s).

- El Propietario de la información o quien este designe, serán los responsables de autorizar el intercambio de información con los proveedores, aliados estratégicos y entidad pública, controlar la entrega, recibo, transporte y transferencia de la información, garantizando se establezcan las condiciones de intercambio y de protección a la información de la Entidad.

- Los documentos requeridos para intercambio de información son los siguientes, donde se define la información a intercambiar, el medio usado y las responsabilidades, así como los acuerdos de seguridad a realizar por las dos (2) partes:

Entidad	Requerimiento de la Entidad Pública	Formato de Intercambio de información - F313)	Contrato / Acuerdo	Matriz de riesgos
Entidades Públicas (No aliado estratégico)	**X**	**X**		
Proveedores		**X**	**X**	**X**
Aliado Estratégico		**X**	**X**	**X**

- La Oficina de Riesgos da asesoría en materia de riesgos de seguridad, privacidad y ciberseguridad a las áreas con el propósito que los Líderes de Proceso – Propietario de Información tomen decisiones para el intercambio de información.

- Los formatos de intercambio de información son elaborados por el tiempo que dura el contrato / acuerdo o única vez por el Líder Proceso o Propietario de información o por quien éste delegue y en caso de identificar modificaciones se hará el ajuste al respectivo formato.

4.2 Entrega de información a ciudadanos

- Está prohibido entregar información catalogada como información pública clasificada y/o pública reservada a personas naturales o jurídicas de naturaleza privada, que no cuenten con vínculos contractuales con la Entidad.

- La entrega de información a ciudadanos se hará de acuerdo con los lineamientos descritos en este procedimiento y a través del "Procedimiento de Peticiones, Quejas, Reclamos, Sugerencias, y Denuncias – PQRSD" (M5-1-18)

4.3 Entrega de información a entidades públicas (no aliado estratégico)

- La Ley 1581 de 2012 de Protección de datos personales en su artículo 10, numeral a. *"Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales"* permite la entrega de la información, no obstante, éste debe ser visto a la luz de las obligaciones que tienen los servidores públicos en materia de protección de datos de acuerdo con el artículo 34 de la Ley 734.

4.4 Recepción de información de terceros

- El Líder de Proceso es responsable de la información recibida de terceros, la cual requiere para operar sus procesos y decide sobre la misma en el ámbito de las operaciones del Instituto. Esta información debe registrarse en el Inventario y Clasificación de Activos de Información.

- El Supervisor del Contrato o responsable del aliado estratégico y el Líder del Proceso son responsables de la protección de la información desde su recepción inicial hasta su disposición final, por consiguiente, se deben implementar controles consistentes con la clasificación y acorde con las obligaciones contractuales, para lo cual se pueden apoyar con la Oficina de Riesgos y la Dirección de Tecnología.

- El intercambio de información con entidades públicas debe efectuarse bajo el marco jurídico vigente, con miras a garantizar la interoperabilidad a través de canales digitales por lo que deben considerarse a las TIC en particular para que se permita:

  - Garantizar que el intercambio de información, no solo se adecua al mundo físico, sino también al que se realiza por medios digitales.
  - Identificar los obstáculos y oportunidades normativas que habiliten el intercambio digital.
  - Identificar, determinar y evaluar el impacto del uso de la TIC en las entidades como partes interesadas de la interoperabilidad.
  - Cumplir la normatividad frente a la protección de datos personales.
  - Cumplir con la política pública de Gobierno Digital.

5. DESCRIPCIÓN

5.1. DIAGRAMA DE FLUJO

(No aplica).

5.2. ACTIVIDAES

¿Qué activada va a realizar?

- Entrega de información a entidades públicas, continúa con la actividad 5.2.1
- Intercambio de información con proveedores y aliados estratégicos, continúa con la actividad 5.2.29

Funcionario que atiende solicitud / PROCESOS ICETEX

5.2.1 Recibe solicitud por parte de Entidad Pública para entrega de información.

5.2.2 Verifica la clasificación de la información solicitada en el inventario de activos de Información que reposa en la página web de la Entidad, el cual puede ser consultado en el link de Transparencia y acceso a la información pública, sección instrumentos de Gestión de información pública, además cada área tiene su Inventario de Clasificación de Activos de Información:

¿La información se encuentra en el inventario de activos de información?
- Si la información no está clasificada en el inventario de activos de información, continúe con la actividad 5.2.3.
- Si la información se encuentra en el inventario de activos de información , continúa con la actividad 5.2.4.

5.2.3 Ingresa el activo al Inventario de Activos de Información, con el apoyo de la Oficina de Riesgos, continúa en la actividad 5.2.4.

5.2.4 Valida la viabilidad de entregar la información objeto de la petición:

- Si la solicitud de información está relacionada con información pública continúa con la actividad 5.2.5.
- Si la solicitud no cumple con las condiciones generales de este procedimiento continúa con la actividad 5.2.6.
- Si la solicitud cumple con las condiciones generales de entrega de información, continúe con la actividad 5.2.7.

5.2.5 Responde al solicitante a través de comunicación formal, la ubicación de la información en la sección de Transparencia de la página web de la Entidad, con esta actividad se da por terminado este procedimiento.

5.2.6 Informa al solicitante la justificación del rechazo de la información, con esta actividad se da por terminado este procedimiento.

5.2.7 Solicita autorización al Propietario de la Información a intercambiar los activos de información, usando como medio el correo electrónico.

5.2.8 Diligencia el "Formato de intercambio de información" (F313)- sección "Información a diligenciar por el usuario funcional".

5.2.9 Solicita autorización de intercambio al Líder del Proceso, mediante el Formato de intercambio de información.

Líder de Proceso

5.2.10 Verifica el correcto diligenciamiento del Formato de Intercambio de Información, específicamente que la información a requerir corresponda con las necesidades de la solicitud:
¿La información corresponde con las necesidades?

- Si el Formato de intercambio de información no se encuentra diligenciado correctamente, continúe con la actividad 5.2.11.
- Si el formato, continúa con la actividad 5.2.12.

5.2.11 Solicita ajustes al Formato de intercambio de información se devuelve a la actividad 5.2.8.

5.2.12 Aprueba en el Formato de Intercambio de Información mediante su firma, en la sección "Información a diligenciar por el usuario autorizador". Remite este documento y la solicitud de la entidad pública a la Oficina de Riesgos para su formalización a través de correo electrónico.

Analista de Grupo de Riesgos No Financieros / Oficina de Riesgos

5.2.13 Recibe y verifica la solicitud en los aspectos de: información requerida y su clasificación, tipo de solicitante y aprobación por el Líder de Proceso.

¿información debe ser suministrada?
- Si la información no debe ser suministrada por el tipo de solicitante o por el nivel de clasificación continúe con la actividad 5.2.14,
- Si la información debe ser suministrada, continúa con la actividad 5.2.15.

5.2.14 Rechaza la solicitud e informa a través de correo electrónico al funcionario solicitante y al líder de proceso con la justificación del rechazo. Devuelve a actividad 5.2.4

5.2.15 Diligencia el Formato de intercambio de información" (F313), sección "Información a diligenciar por Oficina de Riesgos", indicando las instrucciones para la entrega de información y las consideraciones de seguridad y privacidad.

5.2.16 Firma el Formato de intercambio de información" (F313),, sección "Información a diligenciar por la Oficina de Riesgos" y entrega atraves de correo electrónico a la Dirección de Tecnología.

Profesional (Rol Especialista de seguridad) /Dirección de Tecnología

5.2.17 Recibe la solicitud y prepara la información a entregar, ya sea información original o anonimizada.

5.2.18 Realiza el cifrado de la información y/o del medio utilizando un algoritmo de cifrado robusto (3DES y/o AES) y teniendo en cuenta en cuenta las condiciones generales para la entrega de información.

Nota: Este control se realiza con el fin de proteger la información transferida contra la interceptación, copiado, modificación, enrutamiento y destrucción.

5.2.19 Genera las llaves de cifrado de acuerdo con los parámetros definidos en la política de cifrado del Instituto.

5.2.20 Registra la información de las llaves de cifrado y las almacena en el lugar que la Dirección de Tecnología tiene destinada.

5.2.21 Distribuye la llave de cifrado a las personas autorizadas e informa su tiempo de expiración vía correo electrónico. Una vez expiren, se eliminan las llaves de cifrado. Si una de las personas autorizadas indica que necesita renovación de las llaves de cifrado, elimina las llaves actuales y vuelve a generar llaves.

5.2.22 Identifica si la información se transfiere de forma electrónica o en medio removible (CD, DVD, entre otros).

- Si la transferencia de información se requiere en un medio de almacenamiento externo, continuar en el numeral 5.2.23, de entregarse a través de correo electrónico, continuar en el numeral 5.2.24.

5.2.23 Realiza copia en un medio de almacenamiento externo y entrega al funcionario solicitante, pasa a 5.2.26.

5.2.24 Entrega la información a través de correo electrónico con los controles de cifrado, sigue con la actividad 5.2.25.

5.2.25 Diligencia el Formato de intercambio de información" (F313) en la sección "Información a diligenciar por la dirección de Tecnología" y entrega al funcionario que atiende la solicitud de entrega de información vía correo electrónico. Pasa a 5.2.26.

Funcionario que atiende solicitud

5.2.26 Emite comunicación para la Entidad Pública solicitante de la información, informando de la entrega de la misma y las condiciones de protección de la información que debe realizar, copia de la misma debe enviarse a la Oficina de Riesgos.

5.2.27 Archiva respuesta de entrega de información y registro Formato de intercambio de información" (F313) en carpeta compartida de la Oficina.

Analista de Grupo de Riesgos No Financieros- Oficina de Riesgos

5.2.28 Archiva el registro del Formato de intercambio de información" (F313), junto con el soporte de entrega de la información, en la carpeta compartida de la Oficina de Riesgos, con el fin de tener un Inventario de Información a Terceros.

INTERCAMBIO DE INFORMACIÓN CON PROVEEDORES Y ALIADOS ESTRATÉGICOS

Supervisor de contratos – PROCESOS ICETEX ACUERDOS

5.2.29 Identifica las necesidades de información para el desarrollo del contrato o acuerdo, asegurando no incluir más información de la requerida para ejecución de las actividades contractuales. Este análisis va en dos (2) vías: la entrega de información para que el proveedor / aliado estratégico la procese y la recepción de información por parte de proveedor/ aliado estratégico para complementar procesos en Icetex.

5.2.30 En caso de que los activos a intercambiar sean propiedad de otra área, solicita autorización al Propietario de la información a través de correo electrónico, de la necesidad de intercambiar la información con el proveedor / aliado estratégico, indicando los activos de información requeridos.

Nota: Es necesario contar con la autorización del Propietario de la Información.

5.2.31 Diligencia el Formato de intercambio de información" (F313), sección "Información a diligenciar por el usuario funcional", en los campos relacionados de la forma como se va realizar intercambio de información, objeto del intercambio, los activos de información a entregar, clasificación de la información a entregar, actividades a desarrollar con la información, periodicidad de la entrega de información, aprobación del líder de proceso dueño de la información para su intercambio, tipo de tratamiento (anonimizada u original) firma de este formato por el líder de proceso que aprueba el intercambio.

Nota: En caso de ser necesario, realiza reunión de socialización de las necesidades de información con las áreas requirentes, pudiendo participar: áreas usuarias, Oficina de Riesgos, Dirección de Tecnología y Proveedor / aliado estratégico.

5.2.32 Solicita autorización de intercambio al Líder del Proceso, mediante el Formato de Intercambio de Información.

Líder de Proceso

5.2.33 Verifica que la información de la solicitud corresponda con las necesidades del desarrollo del contrato:
¿ La información corresponde con las necesidades del desarrollo?
- Si la solicitud no está bien, continúe con la actividad 5.2.34.

- Si la solicitud está bien, continúe con la actividad 5.2.35.

5.2.34 Solicita ajustes al Formato de intercambio de información" (F313). Se devuelve a la actividad 5.2.31.

5.2.35 Aprueba en el Formato de intercambio de información" (F313), sección "Información a diligenciar por el usuario autorizador", la transferencia de información y lo remite a la Oficina de Riesgos para su formalización.

Analista de Riesgos No Financieros - Oficina de Riesgos

5.2.36 Verifica la solicitud en los aspectos de: información a intercambiar y su clasificación, las condiciones de entrega y de seguridad, la aprobación por el Líder de Proceso:

¿La solicitud presenta inconsistencias?
- Si la solicitud contiene debilidades o incompletitud en las condiciones de intercambio o fallas, continúe con la actividad 5.2.37,
- Si la solicitud se encuentra correcta, continúa con la actividad 5.2.38.

5.2.37 Solicita correcciones al diligenciamiento de la solicitud e informa al funcionario solicitante. se devuelve a la actividad 5.2.31.

5.2.38 Diligencia el Formato de intercambio de información" (F313) sección de "Información a diligenciar por la Oficina de Riesgos", indicando las instrucciones para la entrega de información y las consideraciones adicionales sobre seguridad, considerando la Ley 1581 de 2012 que regula el tratamiento de datos personales. En caso de ser necesario, realiza reunión de socialización de las necesidades de información con las áreas responsables.

5.2.39 Firma el Formato de intercambio de información" (F313), sección "Información a diligenciar por la Oficina de Riesgos" y entrega a la Dirección de Tecnología.

Profesional (Rol Especialista de seguridad)/ Dirección de Tecnología

5.2.40 Procede de acuerdo con el Procedimiento Transferencia segura de la información (A7-1-20).

5.2.41 Registra la actividad realizada en la sección correspondiente al responsable de implementar la solicitud en el "Formato de intercambio de información" (F313)" sección "Información a diligenciar por Dirección de Tecnología".

5.2.42 Envía al Supervisor del Contrato y a la Oficina de Riesgos a través de correo electrónico, el Formato de Intercambio de Información pasa a las actividades 5.2.43 y 5.2.45.

Supervisor del Contrato / Acuerdo estratégico

5.2.43 Emite comunicación al proveedor/aliado estratégico informando las condiciones de intercambio y de protección de la información establecidas durante la vigencia contractual.

5.2.44 Archiva el registro del Formato de intercambio de información" (F313), junto con la comunicación enviada al proveedor y acuerdo de confidencialidad (cuando aplique) en el expediente del proveedor, de acuerdo con el procedimiento de "Administración de archivos de Gestión" (A8-3-01).

Analista de Riesgos No Financieros - Oficina de Riesgos

5.2.45 Mantiene copia del registro del Formato de intercambio de información" (F313), en la carpeta compartida de la Oficina de Riesgos – Intercambio Información Terceros.

Líder de Interoperabilidad /Especialista de Seguridad / Dirección de Tecnología

5.2.46 Entrega a MinTic el Acuerdo para que continúe el proceso según la" *Guía de Lineamientos de Arquitectura – Interoperabilidad".*

6. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Determinar el tipo de información a	Revisa en el inventario de activos de información la	Diligenciamiento del Formato de intercambio	Funcionario solicitante para el intercambio de

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
intercambiar	clasificación que tiene la información a transferir	de información" (F313)	información.
Autorización de intercambio de información para el Tercero	Diligenciar el formato de intercambio de información por el Líder de Proceso.	Formato de intercambio de información" (F313)	Funcionario solicitante para el intercambio de información y Líder del Proceso.
Que la información a intercambiar cumpla con los lineamientos de transferencia al tercero.	Incorpora los controles de transferencia de la información	Formato de intercambio de información" (F313)	Analista de Riesgos – Oficina de Riesgos Profesional / Dirección de Tecnología

7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIGO
Formato de intercambio de información	F313
Instructivo formato intercambio de información	I313
Procedimiento Administración de Archivos de Gestión	A8-3-01
Procedimiento para Identificar y clasificar activos de información	E2-1-13
Procedimiento de Transferencia segura de informaciónl	A7-1-20
Guía de Lineamientos de Arquitectura – Interoperabilidad	N.A.

Modificaciones

Descripción de cambios

- Objetivo: se elimina ciudadanos y de manera no autorizada, se adiciona la palabra sociedades.
- Alcance: se elimina datos personales protegidos por la ley 1581 de 2012 y se adiciona el Formato de intercambio de información con terceros
- Definiciones se incluye las siguientes: Aliado estratégico, Tercero, Tratamiento de datos personales se elimina dato anonimizado y cambia anonimizado por anonimización
- Condiciones generales: Se incluye cuadro especificando los requerimientos para intercambio de información, se incluye el numeral 4.4. Entrega de información a terceros
- Actividades: se ajustan las actividades en general. se dividen las actividades de Entrega de información a entidades públicas e Intercambio de información con proveedores y aliados estratégicos

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2022-04-11	2	• Objetivo: se elimina ciudadanos y de manera no autorizada, se adiciona la palabra sociedades. • Alcance: se elimina datos personales protegidos por la ley 1581 de 2012 y se adiciona el Formato de intercambio de información con terceros • Definiciones se incluye las siguientes: Aliado estratégico, Tercero, Tratamiento de datos personales se elimina dato anonimizado y cambia anonimizado por anonimización • Condiciones generales: Se incluye cuadro especificando los requerimientos para intercambio de información, se incluye el numeral 4.4. Entrega de información a terceros • Actividades: se ajustan las actividades en general. se dividen las actividades de Entrega de información a entidades públicas e Intercambio de información con proveedores y aliados estratégicos
2019-06-11	1	-