# Intercambio de Información Digital con Terceros



Contenido

**1. OBJETIVO**

Intercambiar información con proveedores, aliados estratégicos, ciudadanos y/o entidades públicas de manera controlada y segura, con el fin de evitar la divulgación no autorizada de la información del ICETEX.

**2. ALCANCE**

Aplica para la recepción y entrega de información a terceros, que se encuentre clasificada como información pública reservada e información pública clasificada, datos personales protegidos por la Ley 1581 de 2012.

**3. DEFINICIONES**

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

- **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).
- **Anonimizado**: cuando se transforman los datos o información para garantizar la confidencialidad de la información, el cumplimiento legal y eliminar el riesgo de individualización del dueño del dato / de la información.
- **Archivo:** es el conjunto de documentos, sea cual fuere su fecha, forma y soporte materia, 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.
- **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).
- **Dato anonimizado:** 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.
- **Entidades Públicas:** en este documento, se refiere a las Entidades Públicas que requieren información del Instituto, fundamentados en el artículo 10 de Ley 1581 de 2012 de Protección de datos personales, y/o Entidades Públicas que intercambian información con el Instituto para la ejecución de las operaciones que el estad colombiano faculta.
- **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.
- **Intercambio de información**: distribuir información almacenada digitalmente. En este documento se interpreta como entregar o recibir información de un tercero.
- **Medios removibles:** cualquier componente extraíble de hardware que sea usado para el almacenamiento de información.
- **Propietario de la Información:** es la unidad organizacional donde se crean los activos 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.
- **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.

**4. CONDICIONES GENERALES**

**4.1 Intercambio de información**

- Las condiciones en este sub numeral aplican para la entrega y recepción de información a interesados.

  El propietario de la información y el encargado por éste son los responsables de autorizar el intercambio de información con sus proveedores, 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.
- La información perteneciente a entidades públicas que sea objeto de intercambio de forma continua debido a que se usa en el desarrollo de la operación, se debe propender por contar con un convenio interadministrativo o convenio de interoperabilidad que incorpore la clasificación de datos, alcance de uso, condiciones para disposición final de información.
- Para intercambio de información personal es necesario incluir requerimientos de la Ley 1581 y las necesidades de operar en los procesos, considerando: que el titular de los datos haya dado el consentimiento a través de las finalidades expresas en la autorización de tratamiento de datos personales, tipo de datos, alcance y actividades a realizar con la información, obligaciones en materia de seguridad y privacidad. En el mismo sentido, es deber aplicar los principios de confidencialidad, seguridad, privacidad, finalidad, acceso y circulación restringida, libertad e interpretación integral de derechos constitucionales.
- Para el intercambio de información con proveedores y aliados estratégicos, como Encargados del tratamiento de datos, debe existir previamente cláusulas de confidencialidad y/o acuerdo de confidencialidad debidamente firmado y vigente. Adicional, ICETEX en de la autorización de tratamiento de datos personales de clientes h solicitado el consentimiento para la entrega de datos personales a Encargados, quienes deben mantener la debida protección de información de acuerdo con la Ley 1581 de 2012.
- 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.
- Para intercambio de información con nuevos contratos, fondos en administración, por una vez, se debe diligenciar el formato de Intercambio de información digital con terceros" (F313), con el objetivo de definir la información a intercambiar, los medios para realizarlo y las responsabilidades, así como los acuerdos de seguridad a realizar por las dos (2) partes. Para esta definición puede apoyarse con la Oficina de Riesgos y la Dirección de Tecnología.

**4.2 Entrega de información**

- Está prohibido entregar información catalogada como información pública clasificada y pública reservada a personas naturales o jurídicas de naturaleza privada, que no cuenten con vínculos contractuales con la Entidad.
- 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 y diligenciar el formato F313 por una vez.
- Está prohibido suministrar a terceros información que no ha sido producida por ICETEX, es decir corresponde a información obtenida por la Entidad mediante convenios, acuerdos de un tercero.
- Toda la información entregada por ICETEX a través de un medio electrónico, medio magnético o de almacenamiento, se debe proteger de acuerdo con la clasificación de la información.
- Toda información clasificada o reservada a entregar debe ir cifrada y llevar el registro de entrega de la información por medio del diligenciamiento del "Formato de intercambio de información digital con terceros" (F313).
- Para la transferencia de información electrónica se debe cifrar 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 (3DES y/o AES).
  ✓ 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.
  ✓ Hacer uso del protocolo HTTPS, en caso de hacer uso de la interface Web.
  ✓ Garantizar el registro de los logs de auditoria y el registro de las actividades del usuario(s) creado(s).

**4.3 Recepción de información de terceros**

- Es responsabilidad del Líder de Proceso la información recibida de terceros que la 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 usuario responsable, supervisor de contrato 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 implementarse controles consistentes con la clasificación y vida útil de la información, acorde con las políticas de seguridad digital de la Entidad, para lo cual se pueden apoyar con la Oficina de Riesgos y la Dirección de Tecnología.
- El desarrollo de la recepción de información de terceros se encuentra en este documento en la sección de actividades para intercambio de información a proveedores y aliados.

**5. DESCRIPCIÓN**

Este procedimiento comprende las actividades para entrega y recepción de información, las mismas se encuentran agrupadas en tres bloques, correspondientes a:

- Actividades para entrega de información a ciudadanos y entidades públicas.
- Actividades para intercambio de información a proveedores y aliados.

**5.1 DIAGRAMA DE FLUJO**

(Ver anexo)

**5.2 DESCRIPCIÓN DE ACTIVIDADES**

**ACTIVIDADES PARA ENTREGA DE INFORMACIÓN A CIUDADANOS Y ENTIDADES PÚBLICAS**

| **Funcionario/Trabajador que atiende solicitud** |
|---|

5.2.1 Recibe solicitud por parte del ciudadano / entidad pública para entrega de información.

5.2.2 Verifica que la información puede ser entregada, de acuerdo con las condiciones generales de este documento, procediendo así:

- Si la información no se debe entregar, se avisa al solicitante la decisión y justificación. Finaliza el procedimiento. De lo contrario pasa al numeral 5.2.3.

5.2.3 Verifica el tipo de información solicitada y su clasificación 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:

- Si la información no está clasificada en el inventario de activos de información, continúe con la actividad 5.2.4. De lo contrario continua con la actividad 5.2.5.

5.2.4 Clasifica la información e incluye en el inventario de activos de información, con el apoyo de la Coordinación de Riesgos No Financieros, de la Oficina de Riesgos, continúa en la actividad 5.2.5.

5.2.5 Diligencia el "Formato de intercambio de información digital con terceros" (F313) considerando la ley 1581 de 2012 que regula el tratamiento de datos personales, en la sección "Información a diligenciar por el usuario funcional"

5.2.6 Solicita autorización de intercambio al líder del proceso, mediante el "Formato de intercambio de información digital con terceros" (F313).

**Líder de Proceso**

5.2.7 Realiza validación sobre la posibilidad de entregar la información objeto de la petición:

- Si la solicitud no cumple con las condiciones generales de este procedimiento o es información pública que se encuentra en la sección de Transparencia de la Página Web rechaza la solicitud y continúa con la actividad 5.2.8.
- Si la solicitud cumple con las condiciones generales de entrega de información, continúe con la actividad 5.2.9.

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

5.2.9 Verifica el correcto diligenciamiento del Formato F313, específicamente que la información a requerir corresponda con las necesidades de la solicitud:

- Si el formato F313 no se encuentra diligenciado correctamente, continúe con la actividad 5.2.10. De lo contrario, continúe con la actividad 5.2.11.

5.2.10 Solicita ajustes al "Formato de intercambio de información digital con terceros" (F313), continúe con la actividad 5.2.5.

5.2.11 Aprueba en el "Formato de Intercambio de Información digital con terceros" (F313), en la sección "Información a diligenciar por el usuario autorizador". Remite este documento y el soporte a la Coordinación de Riesgos No Financieros de la Oficina de Riesgos para su formalización.

**Coordinador de Riesgos No Financieros Oficina de Riesgos**

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

- Si la información no debe ser suministrada por el tipo de solicitante o por el nivel de clasificación continúe con la actividad 5.2.13, de lo contrario continua con la actividad 5.2.14.

5.2.13 Rechaza la solicitud e informa al funcionario solicitante y al líder de proceso con la justificación del rechazo. Con esta actividad se da por terminado este procedimiento.

5.2.14 Diligencia el "Formato de Intercambio de Información digital con terceros" (F313), indicando las instrucciones para la entrega de información.

5.2.15 Firma el "Formato de Intercambio de Información digital con terceros" F313, sección "Información a diligenciar por la Oficina de Riesgos" y entrega a la Dirección de Tecnología.

**Dirección de Tecnologia**

5.2.16 El ingeniero responsable recibe la solicitud y prepara la información a entregar.

5.2.17 El ingeniero responsable 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. Se realiza este control con el fin de proteger la información transferida contra la interceptación, copiadc modificación, enrutamiento y destrucción.

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

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

5.2.20 Distribuye la llave de cifrado a las personas autorizadas e informa su tiempo de expiración vía correo electrónico. Una vez expiren las llaves, se elimina 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.

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

- Si la transferencia de información es por medio de correo electrónico, continúe con la actividad 5.2.22, de lo contrario continúe con la actividad 5.2.23.

5.2.22 Entrega la información a través de correo electrónico al usuario solicitante, con los controles de cifrado.

5.2.23 Realiza copia en un medio de almacenamiento externo y entrega al funcionario solicitante.

5.2.24 Registra la actividad realizada en la sección "Información a diligenciar por Dirección de Tecnología" del "Formato de Intercambio de Información digital con Terceros" (F313).

5.2.25 Envía el "Formato de Intercambio de Información digital con Terceros" (F313) diligenciado a la Oficina de Riesgos. Pasa a 5.2.27.

**Funcionario/Trabajador que atiende solicitud**

5.2.26 Emite comunicación para el ciudadano / 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.

**Técnico de Administración – Oficina de Riesgos**

5.2.27 Archiva "Formato de Intercambio de Información digital con Terceros" (F313), junto con el soporte de entrega de la información, de acuerdo con el procedimiento de"Administración de archivos de Gestión" (A8-3-01) con esta actividad se da por terminadas las actividades para entrega de información a ciudadanos y entidades públicas.

**ACTIVIDADES PARA INTERCAMBIO DE INFORMACIÓN A PROVEEDORES Y ALIADOS**

**S u p e r v i s o r d e c o n t r a t o s o R e s p o n s a b l e d e l a A l i a n z a**

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

5.2.29 Realiza reunión de socialización de las necesidades de información con las áreas de Riesgos, Tecnología y Proveedor, donde se establezca:

- La información requerida en el proceso y clasificación de la misma.
- Canal de comunicación de intercambio de información.
- Controles de seguridad y responsabilidad ante un incidente de seguridad de la información.
- Periodicidad de entrega de información.

5.2.30 Diligencia el "Formato de intercambio de información digital con terceros" (F313), sección información a diligenciar por el usuario funcional relacionando las condiciones definidas en la reunión de socialización de intercambio de información.

5.2.31 Solicita autorización de intercambio al líder del proceso, mediante el "Formato de intercambio de información digital con terceros" (F313).

**Líder de Proceso**

5.2.32 Verifica que la información de la solicitud corresponda con las necesidades de la solicitud:

- Si la solicitud no está bien, continúe con la actividad 5.33.
- Si la solicitud está bien, continúe con la actividad 5.2.34.

5.2.33 Solicita ajustes al "Formato de intercambio de información digital con terceros" (F313). Continua con la actividad 5.2.5

5.2.34 Aprueba en el "Formato de Intercambio de Información digital con terceros" (F313), sección "Información a diligenciar por el usuario autorizador", la transferencia de información y lo remite, junto con el documento soporte, a la Coordinación de Riesgos No Financieros de la Oficina de Riesgos para su formalización.

**Coordinador de Riesgos No Financieros - Oficina de Riesgos**

5.2.35 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:

- Si la solicitud contiene debilidades en las condiciones de intercambio o fallas, continúe con la actividad 5.2.36, de lo contrario continúe con la actividad 5.2.37.

5.2.36 Solicita correcciones la solicitud e informa al funcionario solicitante. Pasa a actividad 5.2.28.

5.2.37 Diligencia el "Formato de Intercambio de Información digital con terceros" (F313), indicando las instrucciones para la entrega de información.

5.2.38 Firma el "Formato de Intercambio de Información digital con terceros" F313, sección "Información a diligenciar por la Oficina de Riesgos" y entrega a la Dirección de Tecnología.

**Dirección de Tecnológica**

5.2.39 El ingeniero encargado asesora al área usuaria en ICETEX en la selección de medios transporte de información y controles de seguridad para el intercambio de información.

5.2.40 Implementa controles definidas en reunión de socialización de intercambio de información.

5.2.41 Comunica a los interesados el estado de los controles implementados para el intercambio de información.

5.2.42 Registra la actividad realizada en la sección correspondiente al responsable de implementar la solicitud en el "Formato de Intercambio de Información digital con Terceros", sección "Información a diligenciar por Dirección de Tecnología"(F313).

5.2.43 Envía el "Formato de Intercambio de Información digital con Terceros" (F313) diligenciado a la Oficina de Riesgos, pasa a actividad 5.2.46.

5.2.44 Envía copia de este formato al supervisor del contrato o responsable de la alianza, pasa a la actividad 5.2.45.

**Supervisor del Contrato o responsable de la alianza**

5.2.45 Emite comunicación al proveedor o alianza, informando las condiciones de intercambio y de protección de la información establecidas durante la vigencia contractual, copia de la misma debe enviarse a la Oficina de Riesgos.

**Técnico de Administración – Oficina de Riesgos**

5.2.46 Archiva "Formato de Intercambio de Información digital con Terceros" (F313), junto con la comunicación enviada al proveedor o alianza referente a las condiciones de intercambio de información, de acuerdo con el procedimiento de"Administración de archivos de Gestión" (A8-3-01) con esta actividad se da por terminado este procedimiento.

**6. SEGUIMIENTO Y CONTROL**

| ACTIVIDAD A CONTROLAR | COMO EJERCER EL CONTROL | EVIDENCIA DEL CONTROL | RESPONSABLE |
|---|---|---|---|
| Determinar el tipo de información a intercambiar | Revisa en el inventario de activos de información la clasificación que tiene la información a transferir | Consolidado de activos de información. | Funcionario solicitante para el intercambio de información. |
| Autorización de intercambio de información para el Tercero | Diligenciar el formato de intercambio de información digital con terceros (F313) por el Líder de Proceso. | Formato de intercambio de información digital con terceros (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 el control de cifrado | Formato de intercambio de información digital con terceros (F313) | Profesional / Dirección de Tecnología |

**7. DOCUMENTOS RELACIONADOS**

| NOMBRE DEL DOCUMENTO | CODIGO |
|---|---|
| Formato de Intercambio de Información Digital con Terceros | F313 |
| Procedimiento Administración de Archivos de Gestión | A8-3-01 |
| Procedimiento para Identificar y clasificar activos de información | E2-1-13 |

**Anexos:**
E2-1-16 Intercambio de Información digital con terceros V1.pdf

**Historial de Versiones**

| Fecha Vigencia (Acto Adtvo) | Versión | Descripción de Cambios |
|---|---|---|
| 2019-06-11 | 1 | - |