



## 1. OBJETIVO

Establecer directrices que permitan controlar el acceso a los medios de procesamiento de información del Instituto Para la Economía Social – IPES, para proteger los activos de información sensible y activos de infraestructura tecnológica contra daño, acceso no autorizado e interferencia.

## 2. ALCANCE

El presente procedimiento aplica para todos los medios de procesamiento de información y las áreas donde se encuentran alojados los activos de infraestructura tecnológica que soportan la operación informática del Instituto para la economía Social – IPES.

Aplicable a todos los funcionarios, contratistas y terceros que requieran acceder a los activos de información institucional, medios de procesamiento de información y las áreas donde se encuentran alojados.

## 3. RESPONSABLES

La Subdirección de Diseño y Análisis Estratégico es responsable de designar a las personas encargadas de hacer cumplir los lineamientos, otorgar permisos de acceso a los medios de procesamiento de información de acuerdo a las directrices y lineamientos dispuestos por la entidad relacionados con la seguridad y privacidad de la información.

### 3.1 Administradores de la plataforma tecnológica (medios de procesamiento de información) de la entidad:

- Definir controles de seguridad física para los medios de procesamiento de información de la entidad.
- Definir niveles de seguridad asociados a cada rol y cargo del área, así como los controles adecuados de cada nivel.
- Habilitar los permisos de acceso a los usuarios (funcionarios, contratistas, terceros), establecido desde las diferentes dependencias, de acuerdo al perfil y rol designado.

Elaboró: Yamel Orlando Martínez John Jair Garzón Delgado Cristhian Andrés Ríos Alayon	Revisó: Clarisa Díaz García	Aprobó: Clarisa Díaz García
CPS 720/2018 Profesional Universitario SDAE Profesional Especializado 222-19 SDAE Sistemas	Subdirectora de Diseño y Análisis Estratégico	Subdirectora de Diseño y Análisis Estratégico



- Generar el listado de usuarios autorizados y mantenerlo actualizado con tareas predefinidas y acceso a los diferentes medios de procesamiento de información.
- Autorizar el traslado de equipos de computación. (Se hace con formato de traslado de elementos de almacén).

### 3.2 Usuarios de los medios de procesamiento de información - Deberes:

- Los usuarios que tienen acceso a los medios de procesamiento de información deben aceptar las condiciones de confidencialidad, restricción y de uso adecuado de los activos de infraestructura tecnológica y de información, así como cumplir y respetar estrictamente los lineamientos y directrices establecidas en los manuales, políticas y estándares de seguridad y privacidad de la información.
- Proteger y dar buen uso a los medios de procesamiento de información bajo su responsabilidad.
- Evitar fugas de información del instituto que se encuentre almacenada en los medios de procesamiento que tenga a su cargo.
- No acceder sin previa autorización a áreas restringidas o de acceso limitado.
- No mover ni reubicar equipos sin previa autorización.
- Está prohibido alterar o eliminar configuraciones predeterminadas por el administrador.
- Es responsable de la información almacenada en los equipos asignados a su cargo, deberá mantener la privacidad, integridad y respaldo de la misma.

### 3.3 Director/a y Subdirectores/as, Jefes de Oficina Asesora – Deberes:

Es responsabilidad de la Dirección General y de las Subdirecciones técnicas o administrativas (SAF, SDAE), Asesoría de Control Interno:

- Aprobar los permisos de acceso y solicitar al área de sistemas los permisos de acceso a los medios de procesamiento de la información.
- Informar oportunamente al SDAE y a los Administradores de la plataforma tecnológica sobre las modificaciones o denegación en los permisos de acceso a los sistemas de información, conforme las novedades de cambio de funciones, obligaciones, o desvinculación respecto a funcionarios, contratistas y terceros que tienen a su cargo a través de los medios institucionales vigentes.



#### 4. DEFINICIONES

- a) **Medios de procesamiento de información:** Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.<sup>1</sup>
- b) **Tercera parte:** Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.<sup>1</sup>
- c) **Áreas Seguras:** Los sitios físicos en los cuales se encuentran los servicios de procesamiento de información sensible o crítica.
- d) **Derechos de accesos:** Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, rol o responsabilidades, para acceder a un determinado recurso.
- e) **Restringir el acceso:** Delimitar el acceso a determinados recursos de los funcionarios y terceros.
- f) **Activos de información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
- g) **Administradores de TI:** Personal que hace parte del proceso de gestión de seguridad de la información y recursos tecnológicos, responsables de administrar los activos de infraestructura tecnológica del IPES.

#### 5. CONDICIONES GENERALES

- En los casos en que sean representantes de terceros los que requieran acceso, se debe efectuar, asegurando que dicho personal cuente con las competencias requeridas y bajo la estricta supervisión del área a donde llega la persona autorizada por el tercero.
- El control de acceso a los medios de procesamiento de información se realizará a través de roles que administren los privilegios de los usuarios dentro de dichos medios de procesamiento.
- Cuando un funcionario o contratista termina su relación laboral con la entidad, sus permisos de acceso a los diferentes medios de procesamiento de información deben inactivarse, por tal razón es necesario que el área de talento humano mantenga actualizada periódicamente la información referente a novedades de funcionarios, igualmente el área de jurídica debe reportar novedades relacionadas con contratistas.

<sup>1</sup> TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. NTC-ISO/IEC 27002



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
DESARROLLO ECONÓMICO  
Instituto para la Economía Social

## PROCEDIMIENTO

### OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN

Código: PR-133

Versión: 02

Fecha 18/12/2018

- El acceso a oficinas o áreas de trabajo que contengan medios de procesamiento de información con alto nivel de sensibilidad, debe estar físicamente restringidos.
- Asegurar el cumplimiento de los requisitos normativos, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
- Ningún usuario final, deberá tener privilegios de usuario administrador.
- Se debe evitar el ingreso físico de terceros a las áreas operativas donde se encuentren instaladas las aplicaciones y/o los programas fuente.

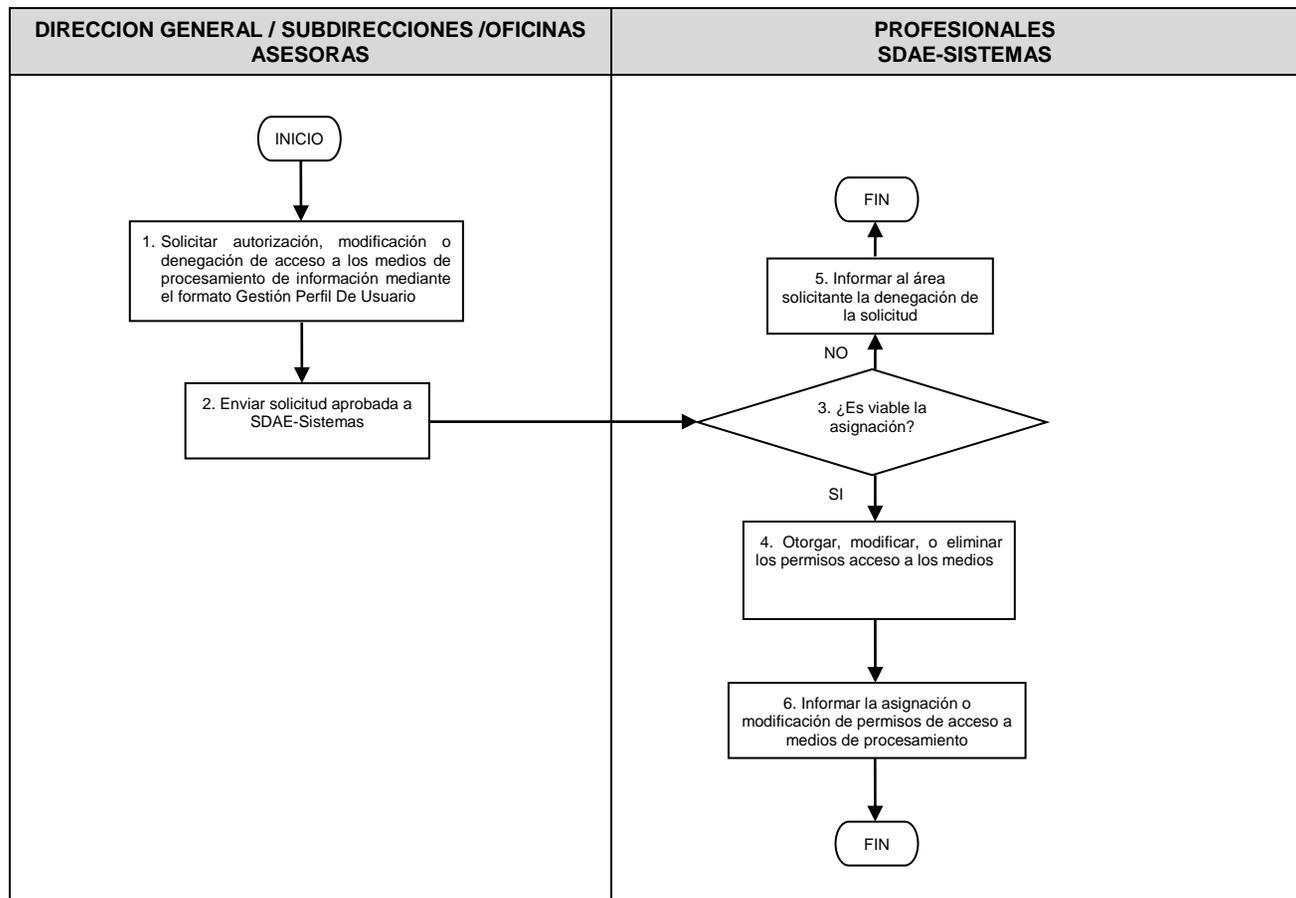
Elaboró: John Jair Garzón –  
Profesional universitario  
Yamel Orlando Martinez  
Balaguera – CPS 60-2018

Revisó: Clarisa Díaz García –  
Subdirectora de Diseño y Análisis  
Estratégico

Aprobó: Clarisa Díaz García –  
Subdirectora de Diseño y Análisis  
Estratégico



## 6. DESCRIPCIÓN DEL PROCEDIMIENTO





PROCEDIMIENTO

OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN

Código: PR-133

Versión: 02

Fecha 18/12/2018

6.1 TABLA EXPLICATIVA DEL PROCEDIMIENTO

No.	Nombre de la actividad	Descripción de la Actividad	Responsable	Punto de control	Registro	Tiempo (Hora o fracción de hora)
1	Solicitar acceso a los medios	Se solicita que se habiliten/modifiquen/denieguen a los usuarios bajo su responsabilidad, permisos de acceso al medio de procesamiento de información llámese Servidores de aplicaciones: de correo, de impresión, aplicaciones web, Servidores de Almacenamientos, Computadores personales, Discos duros externos, entre otros	Director/a, Subdirectores/as, Jefe de Oficina Asesora		FO-325 - GESTION PERFIL DE USUARIO	
2	Enviar solicitud aprobada a SDAE-Sistemas.	Se entrega solicitud aprobada en la SDAE-Sistemas	Dirección General, Subdirecciones, Oficina asesora		FO-325 - GESTION PERFIL DE USUARIO	
3.	¿Es viable la Asignación?	Se valida la viabilidad de otorgar permisos de acceso a medios de procesamiento de información. SI: pasa a la actividad No. 4 NO: pasa a la actividad No. 5	Oficial de Seguridad de la Información, Administradores de TI		FO-325 - GESTION PERFIL DE USUARIO	
4	Otorgar, modificar, o eliminar los permisos de acceso a los medios.	Se otorga, modifica o eliminan los permisos de acceso previamente autorizados con el rol y privilegios definidos, así mismo se activa el proceso de monitoreo de medios de procesamiento para hacerle seguimiento al acceso creado.	Administradores de TI		FO-325 - GESTION PERFIL DE USUARIO.	
5	Informar la asignación, modificación de permisos de acceso a los medios	Se informa al usuario solicitante la autorización/modificación/eliminación de acceso a medios de procesamiento de información.	Administradores de TI			
6	Informar al área solicitante la denegación de la solicitud	Se informa al área solicitante que permisos NO fueron otorgados.	Oficial de Seguridad de la Información, Administradores de TI		FO-325 - GESTION PERFIL DE USUARIO	



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
DESARROLLO ECONÓMICO  
Instituto para la Economía Social

## PROCEDIMIENTO

### OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN

Código: PR-133

Versión: 02

Fecha 18/12/2018

No.	Nombre de la actividad	Descripción de la Actividad	Responsable	Punto de control	Registro	Tiempo (Hora o fracción de hora)
	Fin					

	<b>PROCEDIMIENTO</b>	
	<b>OTORGAR ACCESO A LOS MEDIOS DE PROCESAMIENTO DE INFORMACIÓN</b>	Código: PR-133
		Fecha 18/12/2018

## 7. DOCUMENTOS ASOCIADOS

MS-013 MANUAL SUBSISTEMA GESTION SEGURIDAD INFORMACION

PO-013 PROCESO GESTIÓN SEGURIDAD INFORMACIÓN Y REC ECNOLÓGICOS

FO-325 - GESTION PERFIL DE USUARIO

## 8. MARCO NORMATIVO

TECNOLOGÍA DE LA INFORMACIÓN.TÉCNICAS DE SEGURIDAD. SISTEMAS GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS NTC-ISO/IEC 27001

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. NTC-ISO/IEC 27002

NORMA TECNICA DISTRITAL DEL SISTEMA INTEGRADO DE GESTION PARA LAS ENTIDADES Y ORGANISMOS DISTRITALES NTD SIG 001:2011

Decreto 1499 de 2017 *“Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015*

## 9. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
4	18/12/2018	Objetivo Alcance Responsables Definiciones Condiciones Generales Marco Normativo Se ajusta el formato	Se realizaron cambios en diferentes numerales, ajustando el procedimiento a los accesos físicos a los medios de procesamiento de información.