1. Objetivo

Otorgar el derecho a recursos informáticos: sistemas de información, herramientas informáticas de colaboración y otros recursos informáticos integrados al directorio activo institucional a usuarios autorizados, mientras se previene el acceso de usuarios no autorizados.

- Objetivo Procesal: asegurar que el Catálogo de Usuarios sea apropiado para los servicios ofrecidos a los clientes y prevenir una acumulación indeseada de derechos de acceso.

- Objetivo Procesal: procesar pedidos para agregar, cambiar o revocar derechos de acceso, y asegurar que sólo los usuarios autorizados tengan derecho a usar determinados servicios.

2. Alcance

Aplica únicamente para empleados, proveedores individuales de servicios del Intecap, así como participantes de la formación y empleados de organizaciones consumidoras de los servicios de la Institución, que utilizarán sistemas de información y herramientas informáticas de colaboración.

3. Responsabilidad

Todas las jefaturas de Unidades Operativas y Administrativas que soliciten accesos, creación y/o suspensión de usuarios. El personal del Departamento de Informática involucrado en el procedimiento.

4. Definiciones

4.1 Derechos de Acceso

Es un conjunto de datos que establece o define a qué servicios tiene acceso un usuario. Esta definición se logra asignándole a cada usuario, identificado mediante una Identidad de Usuario, uno o más Roles de Usuario.

4.2 Solicitud de Derechos de Acceso

Es un pedido para conceder, cambiar o revocar el derecho a usar un servicio particular o para acceder ciertos activos.

4.3 Registro de Identidad de Usuario

Es un conjunto de datos que detallan la identidad de un usuario o de un individuo. Se usa para concederle derechos a ese usuario o persona.

4.4 Solicitud de Identidad de Usuario

Es un pedido para crear, modificar o eliminar una Identidad de Usuario.

4.5 Gestor de Acceso

Concede el derecho a usar un servicio a usuarios autorizados, mientras previene el acceso de usuarios no autorizados. El Gestor de Acceso ejecuta políticas definidas por personal de Gestión de la Seguridad de TI.

4.6 Sistema de Control

Es el sistema de información para control de incidencias y requerimientos de cambios de las diferentes áreas del Departamento de Informática.

4.7 Sistema de Información

(SI) es un conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información para apoyar la toma de decisiones. Además, apoyan la coordinación, control, análisis y visualización de una organización.

4.8 Herramienta de Colaboración

Herramienta de gestión interna organizacional que permite el trabajo, la colaboración y la comunicación por medios digitales entre los miembros de la comunidad. Intecap utiliza Microsoft365.

4.9 Usuario

Se refiere al usuario final (personal del Intecap, instructores y consultores) de un servicio de TI.

5. Políticas

El uso de este procedimiento está definido por las siguientes políticas.

5.1 De Gestión de Identidad

Rol	Sistemas de Información	Herramienta de Colaboración
Directores de Junta Directiva	▪ Alta: todos pueden tener usuario. ▪ Baja: cuando concluye el plazo de su nombramiento.	▪ Alta: todos pueden tener usuario. ▪ Baja: cuando concluye el plazo de su nombramiento.
Empleados	▪ Alta: todos pueden tener usuario. ▪ Baja: cuando termina la relación laboral.	▪ Alta: todos pueden tener usuario. ▪ Baja: cuando termina la relación laboral.
Proveedores individuales de servicios	▪ Alta: todos pueden tener usuario. ▪ Baja: cuando la relación termina por contratación como proveedor o por inconvenientes que definan la no contratación.	▪ Alta: todos pueden tener usuario. ▪ Baja: cuando la relación termina por contratación como proveedor o por inconvenientes que definan la no contratación. El usuario puede estar activo, aunque no tenga contrato vigente, considerando que el correo electrónico funciona como medio de comunicación.
Participantes	▪ Alta: cuando se auto registra en el portal de participantes. ▪ Baja: los usuarios de participantes no se dan de baja, pueden ser	▪ Alta: cuando se auto registra en el portal de participantes. ▪ Baja: los usuarios de participantes no se dan de baja, pueden ser

	suspendidos cuando la relación con Intecap termina en malos términos.	suspendidos cuando la relación con Intecap termina en malos términos.
Empleados de Organizaciones clientes	▪ Alta: cuando se auto registra en el portal de empresas. ▪ Baja: los usuarios de empleados de organizaciones clientes no se dan de baja, pueden ser suspendidos cuando la relación con Intecap termina en malos términos.	▪ No se asigna usuario.

Nota: únicamente las personas catalogadas dentro de los roles indicados pueden tener usuario para los recursos informáticos indicados en el alcance.

5.2 De Acceso de Usuarios

La habilitación e inhabilitación de funciones debe ser solicitado por el jefe inmediato superior o el jefe de la División o Departamento a la que pertenece. La responsabilidad de la solicitud de habilitación de funciones es del jefe que la solicita.

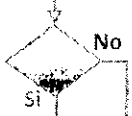
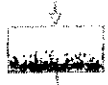
Para participantes o empleados de organizaciones consumidores o potenciales consumidores de los servicios del Intecap se asignan permisos estándar en las plataformas respectivas (portal de participantes y portal de empresas). Por tanto, no requieren habilitación o inhabilitación personalizada de funciones.

Rol	Sistemas de Información	Herramienta de Colaboración
Directores de Junta Directiva	▪ Acceso a las funciones de los sistemas de información para Directores.	▪ Acceso a gestión de su información personal. ▪ Acceso a las herramientas.
Empleados	▪ Acceso a gestión de su información personal como empleado. ▪ Acceso a las funciones de los sistemas de información según las atribuciones del puesto.	▪ Acceso a gestión de su información personal como empleado. ▪ Acceso a las herramientas y accesos como empleado.
Proveedores individuales de servicios	▪ Acceso a gestión de su información personal como proveedor. ▪ Acceso a las funciones de los sistemas de información según las atribuciones objeto de la contratación.	▪ Acceso a gestión de su información personal como proveedor. ▪ Acceso a las herramientas y accesos como proveedor.
Participantes	▪ Acceso a gestión de su información personal como participante de eventos de formación y capacitación en el **portal de participantes**.	▪ Acceso a gestión de su información personal como participante. ▪ Acceso a las herramientas y accesos como participante.
Empleados de Organizaciones clientes	▪ Acceso a gestión de su información organizacional como organización	▪ No tienen acceso.

	cliente de servicios en el **portal de empresas**.	

6. Descripción del proceso

6.1 Habilitación de permisos de usuarios para sistemas de información

Actividad	Diagrama	Responsable	Documento Consultado	Documento Generado	Descripción
					
1. Solicitar habilitación de permisos		JUO/JUA		1	La jefatura de la Unidad requirente envía un correo electrónico a la jefatura del Departamento de Informática con copia al asistente administrativo, solicitando la habilitación de permisos para el usuario correspondiente.
2. Validar datos		AAIT/JIT	1		El asistente administrativo por medio del Sistema de Administración de Usuarios, valida los puestos de la jefatura de la Unidad requirente y del nuevo usuario, así como la existencia de las funcionalidades, permisos solicitados y la posibilidad de habilitarlos.
3. Habilitar permisos		AAIT/JIT	1		El asistente administrativo por medio del Sistema de Administración de Usuarios, habilita los sistemas de información y los permisos solicitados para el usuario correspondiente.
4. Enviar notificación		AAIT/JIT		2	El asistente administrativo envía un correo electrónico a la jefatura de la Unidad requirente con copia a la jefatura del Departamento de Informática, notificando la atención realizada para la habilitación de permisos del usuario correspondiente.
5. Registrar la habilitación de permisos		AAIT/JIT	1,2	3	El asistente administrativo registra en el Sistema de Requerimientos IT, la atención realizada con copia digital de los correos electrónicos asociados con la solicitud.
					

Referencias del diagrama

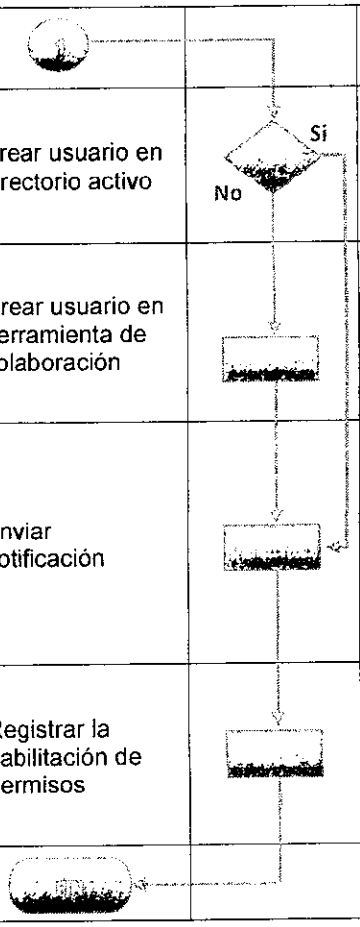
No.	Código	Nombre del Documento
1	N/A	Solicitud de habilitación de permiso
2	N/A	Notificación de habilitación de permiso
3	N/A	Registro de habilitación de permisos

Abreviaturas del diagrama

No.	Abreviatura	Definición
1	JUO	Jefe de Unidad Operativa
2	JUA	Jefe de Unidad Administrativa
3	JIT	Jefe del Departamento de Informática
4	AAIT	Asistente Administrativo del Departamento de Informática

6.2 Creación de usuarios

Actividad	Diagrama	Responsable	Documento Consultado	Documento Generado	Descripción
INICIO					
1. Solicitar creación de usuario		JUO/JUA		1	La jefatura de la Unidad requirente envía un correo electrónico a la jefatura del Departamento de Informática con copia al asistente administrativo, solicitando la creación de usuario para el personal correspondiente.
2. Validar datos		AAIT/JIT	1		El asistente administrativo por medio del Sistema de Administración de Usuarios, valida los puestos de la jefatura de la Unidad requirente y del nuevo usuario.
3. Crear usuario		AAIT/JIT	1		El asistente administrativo crea el usuario solicitado en el Sistema de Administración de Usuarios.
1					

					
4. Crear usuario en directorio activo		AUDA/JIT		2	Si el usuario tendrá acceso a los Sistemas de Información, el administrador crea el usuario solicitado en el Directorio Activo.
5. Crear usuario en herramienta de colaboración		AUDA/JIT			Si el usuario utilizará únicamente las herramientas de colaboración (Microsoft365), el administrador crea el usuario solicitado en Herramienta de Colaboración.
6. Enviar notificación		AAIT/JIT		3	El asistente administrativo envía un correo electrónico a la jefatura de la Unidad requirente con copia a la jefatura del Departamento de Informática, notificando la creación del usuario solicitado, así como la contraseña temporal.
7. Registrar la habilitación de permisos		AAIT/JIT	1,3	4	El asistente administrativo registra en el Sistema de Requerimientos IT, la atención realizada con copia digital de los correos electrónicos asociados con la solicitud.

Referencias del diagrama

No.	Código	Nombre del Documento
1	N/A	Solicitud de creación de usuario
2	N/A	Directorio activo
3	N/A	Notificación de creación de usuario
4	N/A	Registro de habilitación de permisos

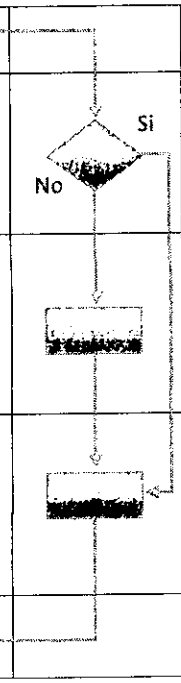
Abreviaturas del diagrama

No.	Abreviatura	Definición
1	JUO	Jefe de Unidad Operativa

2	JUA	Jefe de Unidad Administrativa
3	JIT	Jefe del Departamento de Informática
4	AUDA	Administrador de usuarios en Directorio Activo
5	AAIT	Asistente Administrativo del Departamento de Informática

6.3 Suspensión de usuarios

Actividad	Diagrama	Responsable	Documento Consultado	Documento Generado	Descripción
INICIO					
1. Solicitar suspensión de usuario		JUO/JUA/DH		1	La jefatura de la Unidad requirente o personal designado de la División de Recursos Humanos, envía un correo electrónico a la jefatura del Departamento de Informática con copia al asistente administrativo, solicitando la suspensión del usuario correspondiente.
2. Validar datos		AAIT/JIT	1		El asistente administrativo por medio del Sistema de Administración de Usuarios, valida los puestos de la jefatura de la Unidad requirente y del usuario.
3. Suspender usuario		AAIT/JIT			El asistente administrativo por medio del Sistema de Administración de Usuarios, suspende los sistemas de información y los permisos del usuario correspondiente.
4. Enviar notificación		AAIT/JIT		2	El asistente administrativo envía un correo electrónico al administrador de usuarios en Directorio Activo con copia a la jefatura del Departamento de Informática, notificando suspensión del usuario correspondiente.
1					

					
5. Suspender usuario en directorio activo		AUDA/JIT		3	Si el usuario cuenta con acceso a los Sistemas de Información, el administrador suspende el usuario solicitado en el Directorio Activo.
6. Suspender usuario en herramienta de colaboración		AUDA/JIT			Si el usuario utiliza únicamente las herramientas de colaboración, el administrador suspende el usuario solicitado en Herramienta de Colaboración.
7. Registrar la suspensión de usuario		AAIT/JIT	1,2	4	El asistente administrativo registra en el Sistema de Requerimientos IT, la atención realizada con copia digital de los correos electrónicos asociados con la solicitud.

Referencias del diagrama

No.	Código	Nombre del Documento
1	N/A	Solicitud de suspensión de usuario
2	N/A	Notificación de suspensión de usuario
3	N/A	Directorio Activo
4	N/A	Registro de suspensión de usuario

Abreviaturas del diagrama

No.	Abreviatura	Definición
1	JUO	Jefe de Unidad Operativa
2	JUA	Jefe de Unidad Administrativa
3	DH	División de Recursos Humanos
4	JIT	Jefe del Departamento de Informática

5	AUDA	Administrador de usuarios en Directorio Activo
6	AAIT	Asistente Administrativo del Departamento de Informática

7. Responsabilidad de los Usuarios

Toda persona que tenga una cuenta para acceder a los sistemas de información y/o a la herramienta de colaboración institucionales es responsable de:

1. Los usuarios o cuentas de usuario asignada en los sistemas de información y las herramientas de colaboración.
2. El resguardo de las contraseñas de acceso de los usuarios o cuentas de usuarios institucionales.
3. Las transacciones u operaciones realizadas en los sistemas de información y/o con las herramientas de colaboración.
4. El resguardo de los datos obtenidos por consultas o impresión de reportes en los sistemas de información; evitando compartir información obtenida de los sistemas de información, o por medio de las herramientas de colaboración, con personas no relacionadas o ajenas a la Institución.
5. Los accesos otorgados a funcionalidades de los sistemas de información y herramientas de colaboración, debiendo contar con los accesos necesarios según su rol.
6. Si tiene un puesto de jefatura, en nombre del puesto que ocupa, es responsable de los accesos otorgados a sus subalternos,
7. Reportar, si hubiere, inconsistencias de funcionamiento de los sistemas de información o de la información que generan.
8. Usar correctamente los sistemas de información y las herramientas de colaboración, es decir, utilizar las funcionalidades según el objetivo con el que fueron creadas y con la intención correcta; evitando retorcer o forzar las funcionalidades, sobrepasando o contradiciendo su alcance, con la intención incorrecta.
9. Conocer el funcionamiento correcto de los sistemas de información y las herramientas de colaboración.
10. Capacitarse y solicitar la inducción o asesoramiento para mejorar la comprensión de los sistemas de información y las herramientas de colaboración.
11. Utilizar los sistemas de información vigentes y autorizados para realizar los procedimientos administrativos y operativos.
12. Utilizar las herramientas de colaboración vigentes y autorizadas institucionalmente.
13. El prestigio y valoración de los sistemas de información y las herramientas de colaboración como no de los principales recursos institucionales, evitando emitir comentarios negativos o adversos, promoviendo la mejora continua de estas herramientas tecnológicas.
14. Las sesiones abiertas en los sistemas de información y herramientas de colaboración, evitando dejar sesiones abiertas sin uso y/o en dispositivos compartidos.
15. La calidad y cantidad de información gestionada por los sistemas de información y las herramientas de colaboración, respetando la capacidad y el alcance de estas.
16. Utilizar las herramientas de colaboración únicamente para temas relacionados con el rol dentro de la Institución, evitando utilizarlas para temas personales.
17. Utilizar los sistemas de información y herramientas de colaboración en dispositivos electrónicos seguros, preferiblemente no compartidos.

8. Anexos

No aplica.

Aprobado por	Fecha	Firma
Gerencia	02-05-2023	Antecap Gerencia