



MANUAL DE GESTIÓN DE USUARIOS

CODIGO: AGRI-SI-MN-005

VERSION: 02

FECHA: 13/12/2021

RESPONSABLE: SISTEMAS



Manual de Gestión de Usuarios

Canal Capital

Bogotá D.C., 2021

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto es copia No Controlada. La versión vigente reposará en la carpeta del Sistema Integrado de Gestión en la intranet. Verificar su vigencia en el listado maestro de documentos.



MANUAL DE GESTIÓN DE USUARIOS

CODIGO: AGRI-SI-MN-005

VERSION: 02

FECHA: 13/12/2021

RESPONSABLE: SISTEMAS



Tabla de contenido

1	Introducción.....	3
2	Objetivo.....	3
3	Responsabilidades	3
4	Reglas Generales para la Gestión de Usuarios	3
4.1	Normas para la Gestión de Usuarios	4
4.1.1	Gestión de acceso privilegiado	4
4.1.2	Gestión de autenticación secreta de usuarios	4
4.1.3	Revisión de accesos de usuario.....	4
4.1.4	Uso de información de autenticación	4
4.1.5	Restricción de acceso.....	5
4.1.6	Gestión de contraseñas.....	5
4.1.7	Uso de programas utilitarios	5
4.1.8	Acceso a códigos fuente de software.....	5
5	Procedimiento General	6

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto es copia No Controlada. La versión vigente reposará en la carpeta del Sistema Integrado de Gestión en la intranet. Verificar su vigencia en el listado maestro de documentos.



1 Introducción

El uso de diferentes sistemas de control, de información y aplicaciones facilita la proliferación de diversas identidades digitales para clientes, empleados y socios de negocio, lo que hace evidente la existencia de diferentes repositorios y estándares que dan como resultado inconsistencia de datos y las apariciones de brechas de seguridad.¹

La gestión de usuarios y los controles de acceso son medidas que permiten gestionar las identidades y el control de acceso a los recursos tecnológicos con el fin de mitigar riesgos.

2 Objetivo

Establecer los parámetros de Seguridad de la Información que deben ser aplicadas a la gestión de acceso de usuarios y responsabilidades de usuarios de Canal Capital

3 Responsabilidades

Profesional Universitario de Sistemas: Planea, coordina, administra y genera procesos de la Seguridad de la Información de Canal Capital

Oficial de Seguridad de la Información: Asegura el cumplimiento de la Política General de Seguridad de la Información y el Manual de Políticas Complementarias de Seguridad de la Información.

Ingenieros de Soporte: Garantiza el cumplimiento del presente Manual de Gestión de Usuarios.

Usuarios de Canal Capital: Cumple con la Política General de Seguridad de la Información y el Manual de Políticas Complementarias de Seguridad de la Información.

4 Reglas Generales para la Gestión de Usuarios

El Área de Sistemas de Canal Capital tiene como compromiso implementar mecanismos y controles que permitan llevar una adecuada administración de los usuarios de la entidad.

- Proteger los datos de usuarios como los datos asociados con los recursos tecnológicos de Canal Capital.
- Control de acceso basado en roles.
- Regulación con la protección de los datos de usuario.

¹ <http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf>

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto es copia No Controlada. La versión vigente reposará en la carpeta del Sistema Integrado de Gestión en la intranet. Verificar su vigencia en el listado maestro de documentos.

- Administrar delegada de usuarios, recursos y políticas para el acceso a las aplicaciones.

4.1 Normas para la Gestión de Usuarios

4.1.1 Gestión de acceso privilegiado

- Infraestructura (dominio, correo, recursos compartidos en red, impresión): La solicitud de creación y acceso de usuarios se realiza a través del formato solicitud de servicios TIC que se encuentra alojado en la Intranet de la entidad - [AGRI-SI-FT-029 SOLICITUD DE SERVICIOS TIC](#), esta debe ser diligenciada y aprobada por el supervisor de contrato o jefe directo del área solicitante.

4.1.2 Gestión de autenticación secreta de usuarios

En la creación de usuario en el directorio activo y cuenta de correo electrónico debe tener en cuenta los siguientes factores:

- Se debe realizar la entrega al usuario de su cuenta de dominio y correo de forma confidencial y privada.
- Al iniciar sesión por primera vez con el usuario de dominio y correo electrónico se debe solicitar el cambio de las claves de acceso.
- Por política GPO del directorio activo se debe solicitar el cambio de clave a los usuarios cada 45 días.
- Se debe aplicar la autenticación de doble factor en el ingreso al correo electrónico.

Para la gestión de usuarios en las aplicaciones, los dueños del proceso son quienes deciden qué tipo de acceso a la información y sobre qué módulos de software acceden.

4.1.3 Revisión de accesos de usuario

En el Área de Sistemas de la entidad se debe depurar periódicamente (1 vez por semestre) los usuarios activos en el directorio activo y plataforma de correo electrónico el cual es comparado con un listado de colaboradores activos generado por el Área de Recursos Humanos.

4.1.4 Uso de información de autenticación

Por ningún motivo los usuarios de Canal Capital pueden ni deben compartir información de sus credenciales y claves de acceso a los sistemas de información, correo electrónico y directorio activo, en caso de ser necesario debe existir autorización escrita por parte del supervisor de contrato o jefe directo.

4.1.5 Restricción de acceso

La asignación de permisos de usuario se realiza por medio de la solicitud de servicios TIC, cualquier otro requerimiento debe ser tramitado por la mesa de ayuda o por correo electrónico directamente por el supervisor de contrato o jefe directo.

4.1.6 Gestión de contraseñas

- La contraseña inicial emitida a un nuevo usuario debe ser válida únicamente para el primer inicio de sesión.
- Mantener mecanismos y controles que obliguen al usuario a cambiar sus contraseñas de accesos a red como mínimo cada 45 días.
- Limitar el número de intentos de inicio de sesión a tres (3); después del tercer intento fallido la cuenta involucrada debe ser bloqueada.
- Las contraseñas deben ser alfanuméricas y contener caracteres especiales.

4.1.7 Uso de programas utilitarios

Se establece un CheckList de software básico instalado en los equipos de cómputo de la entidad, cualquier otro software utilitario que requiera ser instalado debe ser analizado primero por el Área de Sistemas esto con el fin de evitar poner en riesgo la Seguridad de la Información o el uso indebido de software.

4.1.8 Acceso a códigos fuente de software

Directrices dictadas por los desarrolladores externos y/o empresas que tengan relaciones comerciales con la entidad.

5 Procedimiento General

Líder de Proceso	Actividad	Aspectos Relevantes
Recursos Humanos, Supervisor de Contrato, Área de Sistemas	Reporte de novedades	La creación de usuarios, modificación de permisos, actualización de accesos y eliminación de estos (contratistas y personal de planta), deben ser informados al área de sistemas por parte del supervisor de contrato o jefe directo y el área de recursos humanos.
Área de Sistemas	Creación de Usuarios	Una vez diligenciada la AGRI-SI-FT-029 SOLICITUD DE SERVICIOS TIC , por parte del supervisor de contrato o jefe directo, el área de sistemas procede con la gestión y asignación del usuario. <ul style="list-style-type: none"> • Usuario de directorio activo • Cuenta de correo electrónico • Asignación de equipo de cómputo • Acceso a los recursos de red necesarios
Recursos Humanos, Supervisor de Contrato, Área de Sistemas	Asignación de Usuarios (Área de Sistemas)	Realizar la entrega de los usuarios y elementos asignados, dando a conocer el AGRI-SI-MN-002 MANUAL DE USO DE RECURSOS TECNOLÓGICOS y firmando el AGRI-SI-FT-019 ACTA DE ENTREGA SERVICIOS TIC
Recursos Humanos, Supervisor de Contrato, Área de Sistemas	Desactivar cuentas de Usuario (Área de Sistemas)	Al ser entregado al área de sistemas el formato AGTH-FT-003 PAZ Y SALVO que se debe diligenciar al terminar el contrato o desvinculación del colaborador de la entidad se deben desactivar los privilegios de acceso del usuario. Por los siguientes motivos también se deben desactivar las cuentas de usuario. <ul style="list-style-type: none"> • Vacaciones • Incapacidad • Licencias

Líder de Proceso	Actividad	Aspectos Relevantes
Recursos Humanos, Supervisor de Contrato, Área de Sistemas	Activar cuentas de Usuario (Área de Sistemas)	<p>Por solicitud escrita vía correo electrónico de parte del Supervisor de Contrato, Jefe Directo o Área de Recursos Humanos dirigida al Profesional Universitario de Sistemas o los correos soporte@canalcapital.gov.co mesadeayuda@canalcapital.gov.co se debe solicitar la activación de las cuentas y privilegios de usuarios que se encuentren suspendidos teniendo en cuenta los siguientes motivos:</p> <ul style="list-style-type: none"> • Reintegro • Consulta • Nueva asignación
Recursos Humanos, Supervisor de Contrato, Área de Sistemas	Retirar y eliminar Usuarios (Área de Sistemas)	Se debe dar un tiempo mínimo de 1 mes para realizar el borrado de los usuarios y permisos, previa realización de BackUp al equipo de cómputo asignado y cuenta de correo.