



## TABLA DE CONTENIDO

<b>1. OBJETIVO</b>	<b>2</b>
<b>2. ALCANCE</b>	<b>2</b>
<b>3. DEFINICIONES</b>	<b>2</b>
<b>4. DESARROLLO</b>	<b>3</b>
4.1 GESTIÓN DE PERMISOS	3
4.2 TIPOS DE PERMISOS	3
4.2.1 <i>Permisos de Usuario</i>	3
4.2.2 <i>Permisos de Grupo</i>	4
LOS PERMISOS DE GRUPO CORRESPONDEN A LOS DIFERENTES ROLES QUE PUEDEN TENER LOS USUARIOS DE MICROSOFT 365, DE ACUERDO CON LAS SIGUIENTES ACTIVIDADES:	4
4.3 PÓLITICAS DE SEGURIDAD	4
4.3.1 <i>Autenticación</i>	4
4.3.2 <i>Políticas de Contraseñas</i>	5
4.4 RESTRICCIONES	6
4.4.1 <i>Restricciones Geográficas</i>	6
4.4.2 <i>Excepciones</i>	6
4.5 SOPORTE TECNICO	7
<b>5. RELACIÓN DE FORMATOS</b>	<b>7</b>
<b>6. CONTROL DE CAMBIOS:</b>	<b>7</b>

¡Antes de imprimir este documento... piense en el medio ambiente!

	<b>PROCESO</b> <b>GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN</b>	G28.GTI	31/12/2024
	<b>GUÍA PERMISOS Y RESTRICCIONES MICROSOFT 365</b>	Versión 1	Página 2 de 7

## 1. OBJETIVO

Establecer los permisos y restricciones aplicables a los usuarios del ICBF que utilizan la suite de Microsoft 365, destacando las diferencias entre los roles y responsabilidades de usuario y las configuraciones de seguridad aplicadas para proteger la información y garantizar el cumplimiento de las políticas institucionales.

## 2. ALCANCE

Este documento aplica en todos los niveles en donde se brinden servicios del ICBF (Sede de la Dirección General, Regional y centro Zonal, CAIVAS, CESPAS, CAVIF, Unidades Locales y Unidades Móviles) que cuenten con licenciamiento para el uso de la de Microsoft 365.

## 3. DEFINICIONES

**Aplicación:** Programa informático diseñado para realizar tareas específicas para el usuario.

**Confidencialidad:** entendida como la garantía del acceso al activo de información únicamente por los usuarios autorizados.

**Correo:** método de intercambio de mensajes digitales entre personas utilizando dispositivos electrónicos.

**Disponibilidad:** entendida como la garantía del acceso al activo de información en el instante en que el usuario lo necesita.

**Directorio Activo:** Herramienta empresarial que ayuda a organizar y controlar el acceso a sus recursos de manera segura y eficiente.

**Autenticación multifactor (MFA):** Método de seguridad que requiere que una persona proporcione más de una forma de verificación para acceder a un sistema o servicio.

**Licencia E3:** suscripción empresarial que ofrece un conjunto completo de aplicaciones y servicios de productividad en la nube, junto con capacidades avanzadas de seguridad para proteger la información sensible.

**Mesa de Servicio:** Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Dirección de Información de Tecnología se informa de las necesidades que tienen los funcionarios en cuanto a los recursos informáticos a nivel nacional.

**Microsoft 365:** Conjunto de aplicaciones y servicios en la nube diseñados para mejorar la productividad y la colaboración tanto en el hogar como en el trabajo. Incluye herramientas para crear

¡Antes de imprimir este documento... piense en el medio ambiente!

	<b>PROCESO</b> <b>GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN</b>	G28.GTI	31/12/2024
	<b>GUÍA PERMISOS Y RESTRICCIONES MICROSOFT 365</b>	Versión 1	Página 3 de 7

y editar documentos, hojas de cálculo, presentaciones, y gestionar correos electrónicos y calendarios. Además, ofrece almacenamiento en la nube y aplicaciones para la comunicación y el trabajo en equipo.

**Riesgos de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias que afecta la confidencialidad, integridad o disponibilidad de la información.

**SRT:** Subdirección de Recursos Tecnológicos.

**Ticket/Número de Servicio:** Número consecutivo suministrado por una Herramienta de Gestión durante el reporte de una Solicitud de Servicio, para facilitar a través del mismo el seguimiento y control.

**Usuario:** Cualquier persona que genere, obtenga, transforme, conserve o utilice información del Instituto en medio digital, físico o a través de las redes de datos y los sistemas de información del ICBF. Son las personas que utilizan la información para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

**Rol G58:** Persona autorizada en las Regionales y dependencias de sede de la Dirección General a nivel nacional para solicitar la creación, eliminación y/o actualización de cuentas de usuarios.

## 4. DESARROLLO

### 4.1 Gestión de permisos

Conforme al proceso de Gestión de la Tecnología e información se estableció el formato de gestión de usuarios sistemas de información F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información, con el fin de que la persona autorizada con el rol (G58) realice la creación, modificación, asignación de perfil o permisos e inactivación de usuarios. Al momento de la creación del usuario, se realiza la asignación de una licencia de correo, la cual le permite acceder a las aplicaciones de Microsoft 365 desde cualquier dispositivo y conectarse desde cualquier parte de Colombia.

### 4.2 Tipos de Permisos

Los permisos asignados a este recurso se dividen en 2 tipos de usuarios:

#### 4.2.1 Permisos de Usuario

Estos permisos forman parte de las aplicaciones disponibles para los usuarios con licencias Microsoft 365 E3. Es importante recordar que cada aplicación tiene un alcance específico en cuanto a su funcionalidad. Esta licencia ofrece acceso a las siguientes herramientas:

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	G28.GTI	31/12/2024
	GUÍA PERMISOS Y RESTRICCIONES MICROSOFT 365	Versión 1	Página 4 de 7

- **Aplicaciones de Office:** Acceso a las versiones más recientes de las aplicaciones de Office (Word, Excel, PowerPoint, Outlook, OneNote, Publisher, Access, entre otros).
- **Correo electrónico y calendario:** Buzón de correo de 100 GB por usuario y calendarios compartidos.
- **Almacenamiento y uso compartido de archivos:** 1 TB de almacenamiento en OneDrive.
- **Colaboración en equipo:** Acceso a Microsoft Teams para chat, reuniones y colaboración.
- **Almacenamiento y Compartición de Archivos:** Acceso a OneDrive para almacenar, sincronizar y compartir documentos de manera segura, con 1 TB de almacenamiento por usuario.
- **Gestión de Contenidos y Colaboración:** Acceso a SharePoint para la creación de sitios de equipo, gestión de documentos y colaboración interna en proyectos.

#### 4.2.2 Permisos de Grupo

Los permisos de grupo corresponden a los diferentes roles que pueden tener los usuarios de Microsoft 365, de acuerdo con las siguientes actividades:

- **Asignación de licencias:** El administrador puede realizar la asignación de licencias, estas pueden asignarse a grupos, facilitando la gestión de permisos y accesos.
- **Colaboración y comunicación:** Grupos de Office 365 para colaboración en equipo, incluyendo correo electrónico, calendarios y archivos compartidos.
- **Gestión de dispositivos:** Administración de dispositivos móviles y políticas de seguridad para todos los miembros del grupo.
- **Listas de distribución:** Grupos de Office 365 para colaboración en equipo en la creación, actualización y modificación de listas de distribución.

### 4.3 PÓLITICAS DE SEGURIDAD

#### 4.3.1 Autenticación

La autenticación del correo electrónico Institucional está definida de acuerdo con la creación del usuario en Directorio Activo, la cual sincroniza con Microsoft. Esta autenticación puede realizarse desde cualquier dispositivo con acceso a internet, para esto, se debe tener un usuario creado y una contraseña, la cual se asigna a la persona cuando es nueva en la entidad y esta es autogestionada por el usuario.

¡Antes de imprimir este documento... piense en el medio ambiente!

	<b>PROCESO</b> <b>GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN</b>	G28.GTI	31/12/2024
	<b>GUÍA PERMISOS Y RESTRICCIONES MICROSOFT 365</b>	Versión 1	Página 5 de 7

Para el ingreso a las herramientas de 365 se requiere de forma obligatoria doble factor de autenticación (MFA), esta autenticación se configura al momento de iniciar la sesión por Microsoft 365 por primera vez, en donde le solicita 2 datos, el primero es el número de teléfono (celular) y el segundo es el correo electrónico personal, estos datos son requeridos para el envío de un código de verificación para los próximos ingresos. Estos datos también son requeridos como obligatorios para el cambio de la contraseña mediante la opción “Olvide mi contraseña”, una vez ingrese el correo institucional.

En caso de olvido, pérdida o cambio de los datos configurados para el doble factor de autenticación, se debe generar un ticket en la mesa de servicio MIS del ICBF, con el fin de que el especialista de Office 365 pueda realizar la modificación de los campos en la herramienta de gestión.

#### 4.3.2 Políticas de Contraseñas

El Instituto Colombiano de Bienestar Familiar en aras de minimizar los riesgos de seguridad de la información, establece que las contraseñas deben ser robustas, contar con los siguientes parámetros y buenas prácticas:

- **Longitud mínima:** Las contraseñas deben tener al menos 12 caracteres.
- **Complejidad:** Las contraseñas deben incluir una combinación de letras mayúsculas, letras minúsculas, números y símbolos especiales (por ejemplo, @, #, \$).
- **Información personal:** No se deben usar datos personales como nombres, fechas de nacimiento o palabras comunes.
- **Reutilización:** No se permite reutilizar ninguna de las últimas 5 contraseñas.

Así mismo, se tienen implementadas las siguientes políticas:

- **Bloqueo tras intentos fallidos:** La cuenta se bloqueará temporalmente después de 5 intentos fallidos de inicio de sesión.
- **Cambio periódico:** Las contraseñas deben cambiarse cada 30 días (obligatorio).

En caso de olvido de la contraseña de correo electrónico, pueden hacer uso del aplicativo Password Reset de Microsoft, seleccionando la opción “He olvidado mi contraseña”:

#### Escribir contraseña

Contraseña

[He olvidado mi contraseña](#)

[Iniciar sesión](#)

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN	G28.GTI	31/12/2024
	GUÍA PERMISOS Y RESTRICCIONES MICROSOFT 365	Versión 1	Página 6 de 7

Una vez seleccionen esta opción deben continuar con los pasos que allí le solicitan, escogen una de las 2 formas de verificación y el aplicativo restablecerá la contraseña del correo y usuario de red.

## 4.4 RESTRICCIONES

Las restricciones implementadas por el Instituto Colombiano de Bienestar Familiar sobre el uso de Microsoft 365, se aplican principalmente a través de la configuración de la ubicación de uso de la cuenta de usuario. Esta configuración determina la disponibilidad de los servicios y características. Por lo anterior el uso de Microsoft 365 está limitado a Nivel Nacional.

### 4.4.1 Restricciones Geográficas

Las restricciones geográficas están siendo monitoreadas por la Subdirección de Recursos Tecnológicos (SRT), la cual cuenta con una herramienta de gestión que permite visualizar e identificar los diferentes Log's, asociados a la autenticación de las cuentas de Microsoft 365, estos eventos corresponden a los siguientes registros:

- **Dirección IP:** Cada vez que inicia sesión en la cuenta de Microsoft 365, se registra la dirección IP desde la que se conecta. Si esta dirección IP es diferente a la que con normalidad hace uso, especialmente si proviene de otro país, se genera una alerta.
- **Ubicación Geográfica:** La dirección IP se puede geolocalizar para determinar la ubicación aproximada. Si la ubicación detectada es inusual o distante de los accesos habituales, se considera una actividad sospechosa y no permitirá el ingreso.
- **Dispositivo y Navegador:** Microsoft también monitorea el dispositivo y el navegador que se utiliza para acceder a la cuenta. Si inicia sesión desde un dispositivo o navegador nuevo, esto puede desencadenar una alerta de seguridad.
- **Patrones de Uso:** Microsoft analiza tus patrones de uso habituales, como las horas del día en que suele conectarse. Un acceso fuera de estos patrones puede ser considerado sospechoso.

### 4.4.2 Excepciones

Para el permiso o acceso del correo institucional o la suite de Microsoft 365 en otro país, se debe enviar a través de un ticket *dirigido a la mesa informática de soluciones MIS*. Por parte del jefe inmediato o supervisor del contrato justificando el motivo por el cual el colaborador debe desplazarse a otro país y a su vez diligenciar y adjuntar el formato *F1.P2.GTI Formato de Solicitud de Servicios de Tecnología*.

El envío de la información debe contemplar el tiempo en que el usuario va a hacer uso de los aplicativos, así mismo que NO se garantiza el permiso, toda vez que se debe evaluar por parte del equipo de Ciberseguridad y Seguridad de la información, con el fin de garantizar la Confidencialidad, Integridad y Disponibilidad de la información.

¡Antes de imprimir este documento... piense en el medio ambiente!

	<b>PROCESO</b> <b>GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN</b>	G28.GTI	31/12/2024
	<b>GUÍA PERMISOS Y RESTRICCIONES MICROSOFT 365</b>	Versión 1	Página 7 de 7

#### 4.5 SOPORTE TECNICO

En caso de requerir soporte técnico, problemas o dudas, se tienen los siguientes canales de atención:

**Correo electrónico** – MIS@icbf.gov.co

**Telefónicamente** Extensión 8080

**En Bogotá:** 4322541

**Línea Nacional:** 018000423732

**Chat** - <http://mis.icbf.gov.co/>

Redes sociales (sólo aplica en el nivel Directivo)

Módulo de autoservicio a través de la Intranet del ICBF

#### 5. RELACIÓN DE FORMATOS

Código	Nombre del Formato
F8.P2.GTI	Formato de gestión de usuarios sistemas de información
F1.P2.GTI	Formato de solicitud de servicios de tecnología

#### 6. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
N/A	N/A	N/A

¡Antes de imprimir este documento... piense en el medio ambiente!