



STRT
20255360000084
Información Pública

CIRCULAR N. 8 DE 2025

FECHA: Bogotá D.C., Marzo 28 de 2025

PARA: **Dirección General, Dirección Técnica de Proyectos, Dirección Técnica de Predios, Dirección Técnica de Construcciones, Dirección Técnica de Administración de Infraestructura, Dirección Técnica de Procesos Selectivos, Dirección Técnica de Gestión Judicial, Dirección Técnica de Gestión Contractual, Dirección Técnica Administrativa y Financiera, Dirección Técnica de Apoyo a la Valorización, Dirección Técnica de Inteligencia de Negocio e Innovación, Dirección Técnica de Conservación de la Infraestructura, Oficina Asesora de Planeación, Oficina de Control Interno, Oficina Asesora de Comunicaciones, Oficina de Relacionamiento y Servicio a la Ciudadanía, Oficina de Coordinación Interinstitucional, Oficina de Gestión Ambiental, Oficina de Control Disciplinario Interno, Subdirección General de Desarrollo Urbano, Subdirección General de Infraestructura, Subdirección General Jurídica, Subdirección General de Gestión Corporativa, Subdirección Técnica de Ejecución del Subsistema Vial, Subdirección Técnica de Ejecución del Subsistema de Transporte, Subdirección Técnica de Recursos Humanos, Subdirección Técnica de Recursos Físicos, Subdirección Técnica de Recursos Tecnológicos, Subdirección Técnica de Presupuesto y Contabilidad, Subdirección Técnica Jurídica y de Ejecuciones Fiscales, Subdirección Técnica de Operaciones, Subdirección Técnica de Tesorería y Recaudo, Subdirección Técnica de Estructuración de Proyectos, Subdirección Técnica de Seguimiento a Estudios y Diseños, Subdirección Técnica de Conservación del Subsistema Vial, Subdirección Técnica de Conservación del Subsistema de Transporte**

DE: Subdirectora General de Gestión Corporativa



STRT
20255360000084
Información Pública

REFERENCIA: Recomendaciones de seguridad para la Gente IDU

Como parte del fortalecimiento del Subsistema de Gestión de Seguridad y Privacidad de la Información y en pro del cumplimiento de los lineamientos internos sobre la protección de la información institucional, buenas prácticas y el aumento en los ataques cibernéticos contra las entidades públicas colombianas de forma preventiva se invita a todos los colaboradores a seguir las siguientes recomendaciones:

1. Contraseñas fuertes y únicas

- Utilice contraseñas complejas que incluyan una combinación de letras, números y caracteres especiales (aAbBcC012\$%*+).
- Evite utilizar información fácil de adivinar, como fechas de cumpleaños o frases comunes (Colombia, IDU, meses, nombres de mascotas, etc.).
- Cambie constantemente las contraseñas y evite usar la misma en diferentes servicios o aplicaciones.

2. Active el Múltiple factor de Autenticación (MFA):

Siempre que sea posible, active la autenticación de dos factores en todas las cuentas para aumentar la seguridad. Esto suele implicar la recepción de un código en su teléfono o correo electrónico que debe introducir junto con su contraseña.

3. Mantenga actualizado el software

- Actualice regularmente en todos los dispositivos el sistema operativo, aplicaciones y software antimalware o antivirus.
- Las actualizaciones suelen contener parches para vulnerabilidades de seguridad descubiertas por los desarrolladores.

4. Tenga cuidado con el correo electrónico y los enlaces

- Verifique el origen de los correos electrónicos antes de hacer clic en enlaces o descargar archivos adjuntos.



STRT
20255360000084
Información Pública

- Desconfíe de los correos electrónicos inesperados, especialmente los que solicitan información personal o una acción urgente.
- En caso de recibir correos sospechosos puede reportarlos a Helpdesk IDU helpdesk@idu.gov.co o seguridad de la información seguridaddigital@idu.gov.co para su respectivo análisis previo.

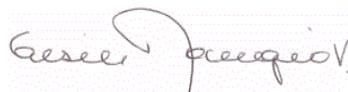
5. Navegación segura

- Compruebe las URL de los sitios web antes de introducir información personal.
- Verifique que la página WEB tenga HTTPS en la URL y un icono de candado que indique una conexión segura, de lo contrario, absténgase de usarla y enviar información.

Al seguir estas recomendaciones se reducen las brechas de seguridad y los ciberdelincuentes no tendrán accesos a los datos personales o información institucional de forma fácil. En caso de requerir asistencia o tener preguntas favor contactar al equipo de la STRT o a través del correo seguridaddigital@idu.gov.co.

La *Gente IDU* tiene responsabilidad en el cuidado y custodia de la información como parte fundamental del cumplimiento de la misionalidad y del fortalecimiento del Sistema de Gestión de Seguridad y Privacidad de la información – SGSPI del IDU.

Cordialmente,



GISELE MANRIQUE VACA

Subdirectora General de Gestión Corporativa

Firma mecánica generada el 28-03-2025 04:47:38 PM autorizada mediante Resolución No. 400 de marzo 11 de 2021

Aprobó: JOSE ALFREDO RUIZ PERALTA-Subdirección Técnica de Recursos Tecnológicos
Elaboró: DANIELA ALEXANDRA OSPINA FORERO-Subdirección Técnica de Recursos Tecnológicos