1. Objetivo y Alcance

1.1 Objetivo

Definir lineamientos generales que garanticen la integridad, disponibilidad y confidencialidad de la información institucional reconocida como uno de los activos fundamentales de la concesión para el cumplimiento por parte de terceros.

1.2 Alcance

Esta política aplica para todos los proveedores o terceros de la concesión Ventanilla Única de servicios -VUS, seguridad, sin importar el tipo devinculación, y para cualquier entidad o persona externa que haga uso de la información, recursos tecnológicos e instalaciones físicas de la concesión.

2. Política Para Proveedores o Terceros

Se tienen en cuenta los acuerdos de nivel de servicio, cumplimiento, confidencialidad y demás directrices que se establezcan en el proceso de contratación. Ningún colaborador de la ventanilla única de servicios- VUS puede autorizar el ingreso a los sistemas de información puestos a su custodia o de propiedad de este, sin la suscripción del acuerdo de confidencialidad del tercero.

En esta política se establecen los lineamientos de seguridad informática para entidades externas que hagan uso de cuentas para ingresar a los sistemas de información de la ventanilla única de servicios - VUS, contemplando los siguientes controles establecidos por la norma NTC ISO 27001:2013:

Anexo A.9. Control de Acceso

- A.9.1.2. Acceso a redes y a servicios en red.
- A.9.2. Gestión de Acceso de Usuarios.
- A.9.3. Responsabilidades de los usuarios.
- A.9.4. Control de Acceso a Sistemas y Aplicaciones.

2.1 Cuentas de Acceso

- Cada cuenta de usuario normal tiene los privilegios de acceso debidamente autorizados para desempeñar las labores propias al cargo.
- La entidad externa debe reportar a la Dirección de Tecnología de la ventanilla única de servicios VUS, las novedades para crear, deshabilitar, modificar y eliminar cuentas de usuario de manera temporal o definitiva, según sea el caso.
- La Dirección de Tecnología, se encargará de asignar las cuentas para todos los colaboradores con los perfiles correspondientes a cada sistema de información.
- El uso de cuentas de usuario para ingresar a los sistemas de información de la ventanilla única de servicios- VUS son de uso personal e intransferible.
- La administración de las cuentas y su uso se realizan de manera independiente para mantener la trazabilidad de las transacciones realizadas en cada cuenta, adicional para hacer uso de las buenas prácticas; evitando la suplantación de identidad, entre otros.
- Todas las contraseñas de los sistemas de información deberán cambiarse con una periodicidad mensual cuando menos.
- Es responsabilidad de los usuarios del sistema de información realizar el cambio de contraseña en el primer ingreso.
- Luego de tres intentos fallidos de autenticación la cuenta de usuario se bloquea.
- Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.
- Cumplir con los términos y condiciones de uso establecidos en este documento.

2.2 Gestión de Credenciales Tipo ROOT

- La gestión de credenciales tipo root estará bajo la custodia de Seguridad de la Información, siendo la única área que podrá crear, modificar, suspender o eliminar dicho tipo de credencial.
- Todas las credenciales tipo root deben ser entregadas para su adecuada gestión al área de Seguridad de la Información.
- Todas las credenciales tipo root solo podrán ser entregadas a los gestores de plataforma por el Oficial de Seguridad de la Información.
- Las credenciales tipo root serán cambiadas en todos los activos de información con una periodicidad sugerida de cada tres (3) meses.
- Ningún gestor de plataforma o usuario debe tener credenciales tipo root en su poder o privilegios asociados a este que le permita ejecutar actividades de administración de forma no controlada.

2.3 Asignación de Contraseñas

- La longitud de la contraseña debe ser mínimo de ocho (8) caracteres.
- Los caracteres deben ser alfanuméricos y especiales.
- No debe contener caracteres repetidos continuos.
- La repetición de la contraseña solo se puede realizar cada cinco (5) cambios.
- Al tratar de ingresar al sistema en más de tres (3) intentos fallidos, el usuario quedará bloqueado y deberá reportarlo con el administrador del sistema.
- El cambio de contraseña se debe realizar cada treinta (30) días.
- La contraseña no debe contener el nombre o apellido del colaborador.
- Los administradores deben programar el sistema de aplicaciones, para que cuando ingrese un usuario por primera vez, a cualquier tipo de aplicación con las que actualmente se cuenta, el sistema solicite el cambio, el cual debe realizarse antes de realizar cualquier actividad en el sistema.
- Todos los usuarios son responsables del manejo de las contraseñas, por lo tanto, queda prohibido dejarlas escritas sobre el escritorio, en notas (post-it) o en cualquier otro lugar.
- Los usuarios son responsables de todas las actividades realizadas con sus claves, son personalese intransferibles. Los usuarios no deben permitir que otros realicen ninguna actividad con sus claves y no está permitido que los usuarios realicen cualquier actividad con claves de otros usuarios.

2.4 Nombrado de Cuentas de Usuario

El nombrado de las cuentas de usuario para los sistemas de información de la ventanilla única de servicios- VUS a los cuales tienenacceso entidades externas, son identificados con un nombre de cuenta estipulado por la ventanilla única de servicios- VUS. Este nombre de cuenta es el número de identificación de la persona que se autenticará en dichos sistemas de información, en algunas plataformas se establece el primer nombre, seguido de un punto y el primer apellido.

2.5 Equipos de Computo

- Los proveedores o terceros son los únicos responsables de sus equipos de cómputo y del respectivo licenciamiento de software, por ende, asumirán las implicaciones legales que se presenten.
- Los proveedores o terceros pueden tener acceso a la red de datos de la ventanilla única de servicios- VUS siempre y cuando asílo disponga la ventanilla única de servicios- VUS y cumpla con las medidas de seguridad mínimas (licenciamiento, antivirus y actualizaciones del sistema operativo).

La ventanilla única de servicios- VUS se reserva el derecho de monitorear las actividades y conexiones de los proveedores o terceros.

2.6 Canales de Comunicación

Los canales de comunicación que se establezcan entre la ventanilla única de servicios- VUS y los proveedores o terceros, deberán cumplir con protocolos seguros que garanticen la integridad, disponibilidad y confidencialidad de la información.

2.7 Seguridad Física

- Los proveedores o terceros que requieran ingresar a las instalaciones de la ventanilla única de servicios- VUS, se deben identificar y registrar en la recepción para su posterior autorización de ingreso.
- Todo proveedor o tercero que preste servicios en la ventanilla única de servicios- VUS, debe portar el carné de visitante y de la entidad que representa, con excepción de aquellos autorizados directamente por la Gerencia General. Adicionalmente, debe permanecer en las áreas físicas que la ventanilla única de servicios- VUS asigne para la ejecución de su labor.
- En el Centro de Gestión Documental Automotor se restringen los siguientes elementos: armas de fuego o armas blancas, teléfonos celulares personales, radios con sistema de grabación y almacenamiento de datos, cámaras fotográficas y de video, computadores portátiles ajenos a la Concesión, tabletas electrónicas, dispositivos de almacenamiento masivo, bolsos, maletas, maletines, billeteras, calzado tipo bota, documentos personales, cigarrillos, fósforos y encendedores, líquidos inflamables, libros y revistas de catálogo, chaquetas o buzos con capucha, fajas, bodi reductor y demás elementos que la Jefatura de Seguridad considere que pueden generar riesgo o vulnerabilidad para los intereses y la información de la Concesión ventanilla única de servicios- VUS.
- El personal de proveedores y terceros debe ser recibido y estar acompañado permanentemente por el colaborador responsable desde el ingreso hasta su salida.
- Ningún proveedor o tercero puede ingresar sin ser registrado.

2.8 Incidentes

Todos los proveedores y terceros deben informar los incidentes de seguridad física y de la información tan pronto se haya identificado su ocurrencia. Este reporte se realiza al correo electrónico *soporte.tecnologia@simbogota.com.co* y Comunicaciones@circulemosdigital.com.co.

Control de Cambios

Versión	Descripción del Cambio	Editó:	Revisó:	Aprobó:
2				
1				