GOB-PT-006 Política de Control de Accesos e Identidades V4

TABLA DE CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. DIRECTRICES DE LA POLITICA DE CONTROL DE ACCESO E IDENTIDADES 3
3.1. DIRECTRICES GENERALES 4
3.2. RESPONSABILIDADES DE LOS USUARIOS 5
4. CONTROLES DE SEGURIDAD EN LA GESTIÓN DE ACCESOS E IDENTIDADES 6
5. DOCUMENTOS ASOCIADOS 10
6. CONTROL DE CAMBIOS 10

ÍNDICE DE TABLAS

Tabla 1. Control de cambios 10

1. OBJETIVO

Establecer las directrices y controles para gestionar, controlar y regular los accesos a los datos, la información, las aplicaciones, las plataformas y software utilizados por la **Concesión RUNT 2.0 SAS** para toda su operación y que se encuentran alojados en las áreas de procesamiento, redes y comunicaciones, para que se encuentren debidamente protegidos contra accesos tanto físicos y/o lógicos no autorizados.

2. ALCANCE

El alcance de la presente política abarca los controles pertinentes al aseguramiento de la gestión de acceso a los diferentes activos de información entre los cuales se encuentran: áreas de procesamiento, redes y comunicaciones, recursos de plataforma tecnológica, los sistemas de información, las aplicaciones, las plataformas, el software y bases de datos de la **Concesión RUNT 2.0**; teniendo como referencia los controles y buenas prácticas de la ISO IEC 27001:2022 en específico al control 5.15 control de accesos. La presente política está definida para dar cumplimiento normativo (ISO 27001), contractual (Contrato 604 de 2022 MT) y legal según la normatividad vigente.

3. DIRECTRICES DE LA POLITICA DE CONTROL DE ACCESO E IDENTIDADES

Con la finalidad de preservar la Confidencialidad, Integridad y Disponibilidad de los datos e información que se generan, modifican, custodian y almacenan en los activos de información y que son accedidos y/o se encuentran a cargo de los empleados, contratistas y/o terceros acordes con su cargo y/o responsabilidades que desempeña en la **Concesión RUNT 2.0.** se establecen controles que permiten regular el acceso a las respectivas redes, datos e información, sistemas de información, aplicaciones, bases de datos, infraestructura tecnológica, así como la implementación de perímetros de seguridad física y lógica para la protección de las instalaciones, especialmente aquellas clasificadas como áreas seguras, tales como los centros de procesamiento de información, áreas de almacenamiento de información física y lógica, cuartos de suministro de energía eléctrica, aire acondicionado, entre otros sitios.

La **Concesión RUNT 2.0.** realizará de manera periódica una revisión sobre el control de acceso a través de la validación y verificación de solicitudes sobre creaciones/cancelaciones/inactivaciones de usuarios que sean informadas por la oficinas responsables de la contratación de personal directo y por contratistas acorde con la vinculación o desvinculación del personal a la **Concesión RUNT 2.0**, lo cual permitirá tener en cuenta al interior de las bases de datos que soportan los sistemas de información los aspectos lógicos como físicos que permitan garantizar la trazabilidad de las acciones realizadas, identificando, entre otros, datos relevantes tales como: quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados, entre otros.

Una vez se aprueben los respectivos accesos a los datos e información, redes, comunicaciones, sistemas de información, aplicaciones, bases de datos, infraestructura tecnológica y sitios de almacenamiento físicos y lógicos a los empleados y/o contratistas, éstos deben abstenerse de realizar modificaciones sobre la información sin la debida autorización, o acciones que vulneren los controles de seguridad establecidos por la **Concesión RUNT 2.0.**; así mismo, deben guardar confidencialidad de la información a la cual tienen acceso e informar a la Oficina de Desarrollo y Tecnología acerca de las debilidades y/o eventos/incidentes de seguridad que se identifiquen.

3.1. DIRECTRICES GENERALES

1. Se debe establecer controles para que sólo los empleados y/o contratistas responsables de su actualización puedan acceder a su modificación y conocimiento, incorporando los nuevos datos que se produzcan.

2. El acceso a los datos e información como a las aplicaciones y sistemas de información debe estar restringido conforme a los roles y responsabilidades asignados en la Concesión RUNT 2.0. a cada uno de los empleados y/o contratistas.

3. Como responsables de los datos e información las partes interesadas como empleados y/o contratistas debe administrar y hacer cumplir los controles de seguridad digital, seguridad y privacidad de la información establecidos en el presente documento, con el fin de evitar accesos no autorizados, impresiones documentales no autorizadas, pérdidas y/o utilización indebida de los datos e información almacenados en los activos de información.

4. Los empleados y/o contratistas de la Concesión RUNT 2.0. son responsables de velar y garantizar la Confidencialidad, Integridad y Disponibilidad de los datos e información, los activos de información, los sistemas de información, aplicaciones, infraestructura tecnológica, sitios de almacenamiento y responsabilidades encomendadas.

5. Los responsables de las áreas restringidas y los encargados del manejo y custodia de los activos de información deben realizar al menos una revisión anual (o cuando sea requerido) sobre los derechos de acceso de los usuarios autorizados, con el fin de mantener un control eficaz de acceso a los datos e información y a los servicios de información que ofrecen los sistemas de información, las aplicaciones las plataformas, el software y/o bases de datos.

6. Es responsabilidad de cada una de las Gerencias de la Concesión RUNT 2.0. realizar la respectiva solicitud sobre la creación de un recurso compartido (carpeta de almacenamiento onpremise o en la nube) y con ella la solicitud de acceso con los diferentes permisos (lectura, escritura o control total).

7. La responsabilidad de la Gerencia de Infraestructura de TI se basa en el establecimiento y aplicación de parámetros de seguridad y privacidad de la información para el uso de los recursos de red compartidos en la Concesión RUNT 2.0.

8. La responsabilidad de la Gerencia de Desarrollo de Software es garantizar que los sistemas de información/aplicativos que gestionan las solicitudes de trámites virtuales, deben encontrarse configurados de manera tal que sólo generen los documentos en el formato establecido para envío por el canal de comunicación establecido y contar con los respectivos registros (logs) que permitan realizar los seguimientos que se consideren necesarios por los Entes de Control o el Cliente Ministerio de Transporte.

9. La responsabilidad de la Gerencia de Infraestructura de TI es garantizar las herramientas para la impresión documental a los empleados y contratistas autorizados para ello, a través de la protección de los documentos y dependiendo el perfil autorizado para su consulta, modificación, eliminación y/o impresión.

10. Para las oficinas físicas que cuentan con sistemas de información y aplicaciones, son los

responsables de su respectiva administración funcional, por lo tanto, también de mantener y garantizar el control de acceso de usuarios sobre estos sistemas de información, aplicaciones y sus respectivas bases de datos.

11. Es responsabilidad de la Gerencia de Infraestructura de TI y Seguridad Física la definición de los controles biométricos, así como los respectivos accesos a espacios de uso restringido y verificar los permisos a través de las respectivas tarjetas de proximidad y garantizar el almacenamiento del registro a cada una de las áreas de la Concesión RUNT 2.0. en donde se evidencie quien ingresa con fecha y hora a los recintos de ésta.

12. En el caso de accesos a los sistemas de información y/o aplicaciones, debe almacenar el registro del último acceso con fecha y hora recién realice la solicitud de ingreso el usuario a los sistemas de información y/o aplicaciones y garantizar el almacenamiento en los respectivos logs de seguimiento para validaciones en caso de ser necesarios a futuro.

13. Se debe garantizar la seguridad sobre los respectivos almacenamientos o bóvedas en donde se almacenan los datos e información que se gestionan, modifican, crean y custodian en la Concesión RUNT 2.0.

14. Se debe garantizar el debido registro a través de logs para realizar seguimiento a las transacciones realizadas en la plataforma de la Concesión RUNT 2.0. así como el almacenamiento y gestión de usuarios, actividades que realizó cada uno en las mencionadas plataformas.

15. La Gerencia de Desarrollo de Software debe cerrar la sesión de los sistemas de información por inactividad mayor o igual a 5 minutos, esto con el fin de salvaguardar la Confidencialidad e Integridad de los datos e información que se gestiona, administra, modifica y custodia en la Concesión RUNT 2.0.

16. La Gerencia de Infraestructura de TI, garantiza a través de los administradores de servidores y sistemas de información el cambio de contraseña luego de ser instalado un sistema operativo y/o sistema de información en la Concesión RUNT 2.0.

3.2. RESPONSABILIDADES DE LOS USUARIOS

1. Todos los empleados y contratistas cuentan con la asignación de un usuario y contraseña único, personal e intransferible y asumen la responsabilidad de los eventos e incidentes que puedan ocurrir bajo su autenticación sobre los activos de información a los cuales acceden, gestionan, administran, modifican y procesan dentro del desarrollo de las funciones y responsabilidades designadas.

2. Todos los empleados y contratistas deben dar un adecuado uso a los activos de información y éstos deben ser únicamente utilizados para el desarrollo de funciones y responsabilidades designadas.

3. Los empleados y contratistas no están autorizados para divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar tanto el(os) usuario(s) y la(s) contraseña(s) de acceso asignada(s) para el acceso a los sistemas de información, aplicaciones, bases de datos, plataforma tecnológica, correo electrónico, dispositivos electrónicos, equipos de cómputo y similares.

4. Los empleados y contratistas que cuentan con usuarios de acceso a los sistemas de información/aplicativos misionales, de apoyo y estratégicos deben cumplir con la salvaguarda de la información que remiten a los centros de impresión (impresoras conectadas en red) y solamente enviar los documentos necesarios físicos de acuerdo con el(los) trámite(s) que se realicen en los puntos de atención de manera presencial.

5. Todos los empleados y/o contratistas que requieran tener acceso a los sistemas de información, aplicaciones y bases de datos de la Concesión RUNT 2.0. deben estar debida y previamente autorizados por el jefe directo y debe acceder a lo mencionado haciendo uso de un usuario y contraseña, la cual debe cumplir con las mejores prácticas para la construcción de contraseñas.

4. CONTROLES DE SEGURIDAD EN LA GESTIÓN DE ACCESOS E IDENTIDADES

1. La información y sus activos asociados, sistemas de información y las aplicaciones, las plataformas y el software de la concesión RUNT 2.0 deben tener asignados responsables frente a sus gestiones de accesos y aseguramiento de la información; para ello se debe tener en cuenta:

   a) Establecer una matriz de responsabilidades y roles de acceso para las distintas aplicaciones de la entidad, segregando responsabilidades de los distintos usuarios bajo perfiles. Esta actividad debe ser realizada en conjunto con los responsables y administradores de las aplicaciones; también se deben identificar los responsables de las aplicaciones y demás componentes tecnológicos de información, así como quien o quienes autorizan, responsable(s) de la administración, tiempo de depuración de usuarios planeado para cada aplicación, criticidad y factores adicionales de autenticación.

   b) La concesión RUNT dispone de un proceso de solicitudes de acceso, bajo este se establecen los flujos de aprobación requeridos para los accesos a los sistemas lógicos de información teniendo como base la "Matriz de responsabilidades y roles de acceso", de igual forma se debe identificar la criticidad de la aplicación y establecer los niveles de autenticación adicionales frente a roles privilegiados.

   c) Las legislaciones, los reglamentos y las obligaciones contractuales con respecto a las limitaciones de acceso a datos y servicios por parte de sus colaboradores (internos, externo y proveedores).

   d) Todos los procesos de solicitudes para ingreso de aplicaciones de tipo privilegiados, identidades y mínimos necesarios deben ser gestionados bajo el proceso de gestión de acceso.

2. El proceso encargado de gestionar las solicitudes de acceso con niveles privilegiados, tendrán en cuenta para el desarrollo de estas asignaciones las siguientes recomendaciones:

   a) Los roles y permisos de accesos privilegiados deben ser identificados bajo la "matriz de responsabilidades y roles de acceso" para las aplicaciones, sistemas de información, sistemas operativos, Sistemas de Gestión de bases de datos y otros que requieran este nivel de privilegios. Los usuarios que requieran estos roles deben ser identificados bajo las plataformas como grupos de dominio de AD, grupos de trabajo, estructuras de nombres

especificas u otros distintivos frente a usuarios normales según las directrices establecidas por la Concesión RUNT 2.0.

b) Los permisos de acceso con nivel privilegiado se asignan según la necesidad y con base en el requisito mínimo de cada usuario para el desarrollo de sus funciones, por ello los procesos de autorización deben ser evaluados en el comité de seguridad y privacidad de la información, contemplando los riesgos y justificaciones de los mismos frente a las vulnerabilidades que se puedan presentar.

c) Los procesos de autorización de niveles de acceso privilegiados deben disponer de un flujo de aprobación teniendo en cuenta la criticidad de los datos e información del activo asociado frente a los riesgos de seguridad. Este tipo de aprobaciones deben contar con el visto bueno de los representantes del Comité de seguridad y privacidad de la información.

d) Los procesos de autorización de accesos privilegiados establecidos por la Concesión RUNT 2.0 deben tener en cuenta:

   I. Las cuentas privilegiadas podrán ser asignadas con un tiempo de expiración para el acceso no superior a 1 día y limitado al tiempo requerido para el desarrollo de la actividad programada.

   II. Informar a los usuarios de estas cuentas, la estructura, sus derechos, responsabilidades, alcances y los posibles distintivos de sesión (Interfaz de usuarios para este nivel de acceso o uso de identidades).

   III. Contar con un proceso de autenticación más estricto frente al acceso de cuentas normales, estos contaran con:

      - Métodos de autenticación como lo son SSO (Single Sign on), protocolos SAML y WS-FEDERATION, OPEN ID CONNECT (OIDC), AD/LDAP entre otros.
      - Factores de autenticación como podría ser el caso de los PINES, Dispositivos fuera de banda, Dispositivo OTP factor único y Dispositivos OTP multifactor.
      - Códigos de validación frente a posibles bots (Captcha).

e) Al menos una vez al mes o según la entidad lo requiera, se deben verificar los deberes, roles, responsabilidades y competencias del personal que dispongan de estas cuentas de nivel privilegiado validando si aún son requeridas.

f) En la configuración de los sistemas de información, sistemas operativos, bases de datos, se deshabilitan y restringen las cuentas de administración genéricas como root, administrator, administrador y otras de privilegios elevados.

g) Desde el SOC se deben programar monitoreos constantes para las actividades realizadas con los accesos privilegiados.

h) No se deben compartir o vincular identidades con accesos privilegiados a múltiples personas, estas deben ser asignadas de manera individual, se recomienda su agrupación por medio de grupos "administradores" del AD de la entidad.

i) Las identidades con derechos de acceso privilegiados solo podrán ser usadas para realizar tareas administrativas, esto debe ser informado a los usuarios y se deberá realizar una bitácora por parte de estos detallando las actividades realizadas durante la vigencia.

3. Las responsabilidades y roles de accesos deben ser establecidos bajo la segregación de funciones establecidos al interior de la Concesión RUNT 2.0.

4. El contexto para la gestión de identidades de la Concesión RUNT 2.0 debe tener en cuenta:

   a) La asignación de identidades de acceso es única por persona, por ello y con fin de individualizar responsabilidades, se dispondrá de una identidad vinculada a una sola persona.

   b) En caso de requerirse identidades compartidas, solo serán permitidas con fines comerciales y operativas y están sujetas a aprobación y documentación especifica que la soporte. Así como un responsable frente a las responsabilidades que conllevan su uso.

   c) Toda identidad no asignada a entidades no relacionadas personas, deben estas sujetas a su aprobación, estas identidades deben estar bajo monitoreo constante.

   d) Todas las identidades asignadas deben contar con su vigencia respectiva, así como por parte de la entidad un proceso de depuración para cuentas activas sin uso.

   e) La operación TI debe mantener registros de los eventos más significativos relacionados con el uso y la gestión de identidades de los usuarios y de la información de autenticación, estos eventos deben ser establecidos en conjunto con los lineamientos de seguridad de la información y clasificación de la información de la entidad.

   f) Todas las identidades proporcionadas o emitidas por terceros deben garantizar el nivel de confianza requerido por la entidad, para ello, los riesgos asociados de estas identidades deben ser identificados, debe ser puestos en conocimiento y deben ser tratados adecuadamente en la gestión de riesgos de seguridad de la información.

5. Los procesos realizados con las cuentas asignadas deben genera registros que se almacenaran, protegerán y analizaran frente a actividades, excepciones, fallas y otros eventos relevantes.

6. Se debe establecer un proceso de asignación y gestión para las asignación y gestión de la autenticación por parte de los usuarios de la concesión RUNT 2.0, este proceso debe tener en cuenta los siguientes puntos:

   a) Todas las contraseñas, códigos y pines generados automáticamente durante los procesos de creación de cuentas de acceso deben ser de alta complejidad y únicos para cada persona. Una vez el usuario ingrese por primera vez, se le debe solicitar el cambio inmediato de contraseña. Como buena práctica para la creación de contraseñas, cada sistema de información, aplicación debe parametrizarlas de la siguiente manera:

      I. Al menos 1 carácter especial.
      II. Al menos 1 carácter en Mayúscula.
      III. Al menos 1 carácter numérico.
      IV. Debe contener una longitud mínima de 10 Caracteres.
      V. No utilizar contraseñas de fácil identificación, ejemplo años de nacimiento, nombres de hijos.
      VI. La contraseña no pude ser el mismo usuario.
      VII. No se deben permitir información clara de los usuarios relacionadas con los atributos del usuario.

   b) Las validaciones previas al cambio de la información de autenticación deben tener en cuenta procedimientos para verificar la identidad de un usuario, estos deben ser realizados bajo

preguntas de tipo personal, respuestas a preguntas parametrizadas. Como un ejemplo se podrían contemplar:

I. Fecha de nacimiento.
II. Nombre de padres.
III. Nombre de mascotas
IV. Nombre de hijos.

c) Una vez sean aprobados los procesos de asignación de las cuentas de acceso y estas se encuentren registradas, se reportarán al usuario bajo medios oficiales de la concesión RUNT 2.0 como correo corporativo, intranet. Estos medios deben estar cifrados (Sin texto claro)) y/o ser procesos validados por ingresos autenticados. Se debe contar con evidencia del acuse de recibido de la contraseña.

d) La información de autenticación de los dispositivos adquiridos por la Concesión RUNT 2.0 deben ser cambiada una vez sean instalados sus sistemas o softwares.

e) Los registros de eventos significativos de asignación y gestión de autenticación de la información deben estar evidenciados y asegurados manteniendo su confidencialidad, esto puede ser realizado por medio de bóvedas de contraseñas permitidas por el responsable del área de seguridad de la información de la entidad.

7. Los usuarios de la Concesión RUNT que tengan acceso o utilicen información de auténtica deben ser puestos en conocimiento de las siguientes directrices:

a) La información de autenticación secreta, como la contraseña, así como las utilizadas en el contexto de las identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales se comparten únicamente con personas autorizadas (admin de BD, Aplicaciones, dispositivos de red y otros).

b) La información de autenticación afectada o comprometida debe cambiada por el responsable de manera inmediata.

c) Las contraseñas generadas por los usuarios deben tener en cuenta dentro de las buenas prácticas las siguientes pautas:

I. las contraseñas no se basan en nada que otra persona pueda adivinar u obtener fácilmente utilizando información relacionada con la persona (por ejemplo, nombres, números de teléfono y fechas de nacimiento);
II. las contraseñas no se basan en palabras del diccionario o combinaciones de las mismas;
III. use frases de contraseña fáciles de recordar e intente incluir caracteres alfanuméricos y especiales;
IV. las contraseñas tienen una longitud mínima.

d) Las contraseñas deben ser diferentes en cada servicio y sistema al que se requiera el acceso.

e) La concesión RUNT 2.0 debe establecer estas responsabilidades bajo los términos y condiciones de empleo del personal interno y externo de la entidad.

8. Los sistemas de administración de la concesión RUNT 2.0 cumplen los siguientes requisitos:

a) Permitir a los usuarios el cambio de sus contraseñas validando su seguridad mediante la presentación de errores en pantalla que orienten a las buenas prácticas.

b) aplicación de reglas para la construcción de contraseñas seguras.

c) Obligar a los usuarios al cambio de contraseña en su primer inicio de sesión.

d) Hacer cumplir cambios de contraseñas según la necesidad de la entidad en casos como incidentes de seguridad, cambio de contraseñas conocidas para identidades que permanecen activas (por ejemplo. Identidades compartidas).

e) Evita la reutilización de contraseñas.

f) Evita el uso de contraseñas de uso común y nombres de usuarios comprometidos bajo las reglas de construcción de contraseñas seguras.

g) Presentación de ingreso de contraseñas ocultando los caracteres.

h) Almacenando y transmitiendo contraseñas en forma protegida usando funciones de resumen (hashing) para las contraseñas.

5. DOCUMENTOS ASOCIADOS

Anexo 1 Política de Control de Accesos – Estrategia de implementación

6. CONTROL DE CAMBIOS

Control de cambios					
Versión	**Elaboró**	**Revisó**	**Aprobó**	**Fecha**	**Descripción**
1	IT Managers	Jefe de seguridad de información	Líder dominio de seguridad	14/03/2023	Versión inicial
2	Jefe de seguridad de información	Jefe de seguridad de información	Líder dominio de seguridad	30/06/2023	Observaciones RUNT2-DA-M03-F01- GOB-PT-006 Política de Control de Accesos e Identidades V1_V14.06
3	Jefe de seguridad de información	Jefe de seguridad de información	Líder dominio de seguridad	10/10/2023	Precisiones menores sobre el objetivo y el alcance del procedimiento para hacer más claro el cumplimiento contractual
4	Analista de seguridad de la información	Jefe de seguridad de información	Jefe de seguridad de información	19/04/2024	Se ajusta clasificación de la información.

Tabla 1. Control de cambios