POLÍTICA DE ACCESO Y CONTROL DE USUARIOS

MODELO DE ARQUITECTURA EMPRESARIAL (MAE)

CORPORACION PARA EL DESARROLLO SOSTENIBLE DEL NORTE Y EL ORIENTE AMAZÓNICO -CDA-

Inírida– Guainía
2026

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

TABLA DE CONTENIDO

Contenido

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

INTRODUCCION.

El presente documento establece las políticas y normas para garantizar un adecuado control de acceso a los sistemas de información de la Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA).

Para la Entidad es prioritario definir los perfiles de acceso a información sensible, limitando el uso de aplicaciones tecnológicas únicamente a funcionarios y personal (tanto interno como externo) cuyas responsabilidades y funciones requieran dicho acceso, dado el carácter confidencial o sensible de la información. En este sentido, se hace necesario implementar mecanismos de control y restricción de acceso a toda la información, independientemente de su soporte (físico o digital), garantizando así los principios de confidencialidad, integridad y disponibilidad de los datos."

OBJETIVOS.

GENERAL.

Garantizar la seguridad de la información, en procesamiento de datos, redes, recursos tecnológicos y sistemas de información de la Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA), implementando mecanismos de control de acceso lógico y físico que prevengan accesos no autorizados.

OBJETIVOS ESPECIFICOS

a) Normalización de accesos

Establecer y regular las políticas generales de control de acceso a los servicios informáticos, fortaleciendo la seguridad de la información corporativa mediante protocolos estandarizados.

b) Gestión de perfiles de usuario

Definir perfiles de acceso estandarizados para cada categoría de estaciones de trabajo, garantizando la asignación adecuada de privilegios según funciones y responsabilidades.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

c) Control de niveles de acceso

Implementar un esquema de seguridad por capas que asegure los niveles apropiados de acceso a la información institucional, preservando los principios de confidencialidad, integridad y disponibilidad en todos los sistemas y usuarios.

d) Control de accesos no autorizados

Establecer mecanismos de seguridad para prevenir accesos no autorizados a sistemas de información, bases de datos y servicios institucionales, mediante la implementación de controles técnicos y administrativos.

e) Gestión de identidad y accesos

Implementar protocolos robustos de autenticación y autorización para garantizar que solo usuarios debidamente validados puedan acceder a los recursos informáticos, según sus perfiles y necesidades operativas.

f) Monitoreo de actividades

Mantener registros sistemáticos y realizar revisiones periódicas de eventos y actividades críticas ejecutadas por usuarios en los sistemas de información, para detectar y responder oportunamente a incidentes de seguridad.

g) Concientización en seguridad

Promover entre los usuarios la adopción de prácticas seguras en el manejo de credenciales, equipos informáticos y datos corporativos, destacando su responsabilidad individual en la protección de los activos digitales.

h) Seguridad en entornos móviles

Garantizar la protección de la información institucional en escenarios de movilidad y teletrabajo, mediante la implementación de controles específicos para dispositivos remotos y conexiones externas.

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: www.cda.gov.co e-mail: cda@cda.gov.co

ALCANCE Y AMBITO DE APLICACIÓN

El presente documento aplica a:

1. **Todos los usuarios con acceso autorizado**, incluyendo:
    - Colaboradores de planta
    - Contratistas
    - Terceros debidamente autorizados
2. **Sobre todos los recursos tecnológicos de la Corporación CDA**:
    - Sistemas de información
    - Bases de datos
    - Documentación institucional
    - Programas y aplicaciones
    - Servicios de información
3. **Independientemente de:**
    - El nivel jerárquico
    - El tipo de vinculación
    - Las funciones específicas que desempeñen

NORMATIVIDAD VIGENTE

1. **Ley 1581 de 2012 (Protección de Datos Personales)**

- *Artículo 17*: Obliga a implementar medidas de seguridad para proteger bases de datos con información personal.
- *Decreto 1377 de 2013*: Establece estándares técnicos para el tratamiento seguro de datos.

2. **Decreto 1078 de 2015 (Decreto Único Sectorial TIC)**

- *Artículo 2.2.2.1.3.2*: Requiere controles de autenticación y autorización para sistemas que manejen información pública.
- *Artículo 2.2.2.1.5*: Exige registros de acceso (logs) para sistemas de información estatales.

3. **Resolución 695 de 2022 (MinTIC)**

- Establece los requisitos mínimos de seguridad digital para entidades públicas, incluyendo:

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Gestión de identidades digitales (Capítulo IV)
- Control de accesos privilegiados (Artículo 12)
- Segregación de funciones (Artículo 14)

4. **Circular 052 de 2020 (Superintendencia de Industria y Comercio)**

- Guía para implementar controles de acceso en el tratamiento de datos personales, exigiendo:
  - Autenticación multifactorial para sistemas críticos
  - Revisión periódica de privilegios
  - Protocolos para altas/bajas de usuarios

5. **Norma Técnica Colombiana ISO/IEC 27001**

- *Control A.9.2*: Gestión de accesos de usuarios
- *Control A.9.4*: Restricción de acceso a sistemas

6. **Ley 1273 de 2009 (Delitos Informáticos)**

- *Artículo 269A*: Penaliza el acceso no autorizado a sistemas informáticos

DEFINICIONES Y TERMINOS

Activo: Cualquier cosa que tenga valor para la organización.

Activos de Información: Es todo aquello que contiene, procesa, trate y/o manipule información valiosa para la Entidad y que son necesarios para que la Entidad funcione y cumpla con los objetivos establecidos para dicho fin.

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Cámara de Representantes en un momento dado.

Acceso físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la Entidad.

Acceso lógico: En general, el acceso lógico es un acceso electrónico o digital, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información sea clasificada adecuadamente y mantenga una clasificación acorde con su nivel de confidencialidad.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: Cambio adverso en el nivel de los objetivos de la corporación CDA.

Incidente: Cualquier evento que no forma parte de una operación normal de un servicio y que causa o puede causar una interrupción o reducción de la calidad del servicio.

PRINCIPIOS DE SEGURIDAD

a) Confidencialidad: La información solo podrá ser accedida, modificada y/o eliminada por quienes estén autorizados/as para ello.

b) Disponibilidad: La información deberá estar accesible siempre que se requiera.

c) Integridad: La información deberá preservar su veracidad y fidelidad a la fuente, independientemente del lugar y de la forma de almacenamiento y transmisión.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **CONTROL DE ACCESO A SERVICIOS TECNOLOGICOS.**

1. **Disposiciones Generales**
   - **Acceso Autorizado**: El acceso a la red y servicios tecnológicos de la CDA será otorgado únicamente a usuarios autorizados, previa verificación de perfiles y roles definidos por:
     - El/la jefe/a inmediato.
     - La Unidad de Talento Humano.
     - El área de Tecnologías de la Información y Comunicación (TIC's), responsable de su implementación.
   - **Uso de la Información**: Toda información generada o almacenada en los sistemas institucionales es propiedad exclusiva de la CDA y debe utilizarse únicamente para fines laborales.
   - **Requisitos de Acceso**:
     - Contar con una relación laboral vigente con la institución.
     - En caso de terceros, presentar autorización escrita de un/a servidor/a de nivel jerárquico superior.
2. **Responsabilidades**
   - **TIC**: Gestionar, monitorear y revocar accesos según los perfiles aprobados.
   - **Jefes de áreas:** Validaran las necesidades de acceso de los usuarios.
   - **Usuarios**: Utilizar los recursos tecnológicos conforme a las normas institucionales y reportar incidentes de seguridad.
3. **Cumplimiento**
   El incumplimiento de esta política dará lugar a acciones disciplinarias y/o legales, según lo establecido en los reglamentos internos de la CDA.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **GESTION DE ACCESO.**

PROCEDIMIENTO PARA LA HABILITACIÓN DE USUARIOS EN SISTEMAS INFORMÁTICOS

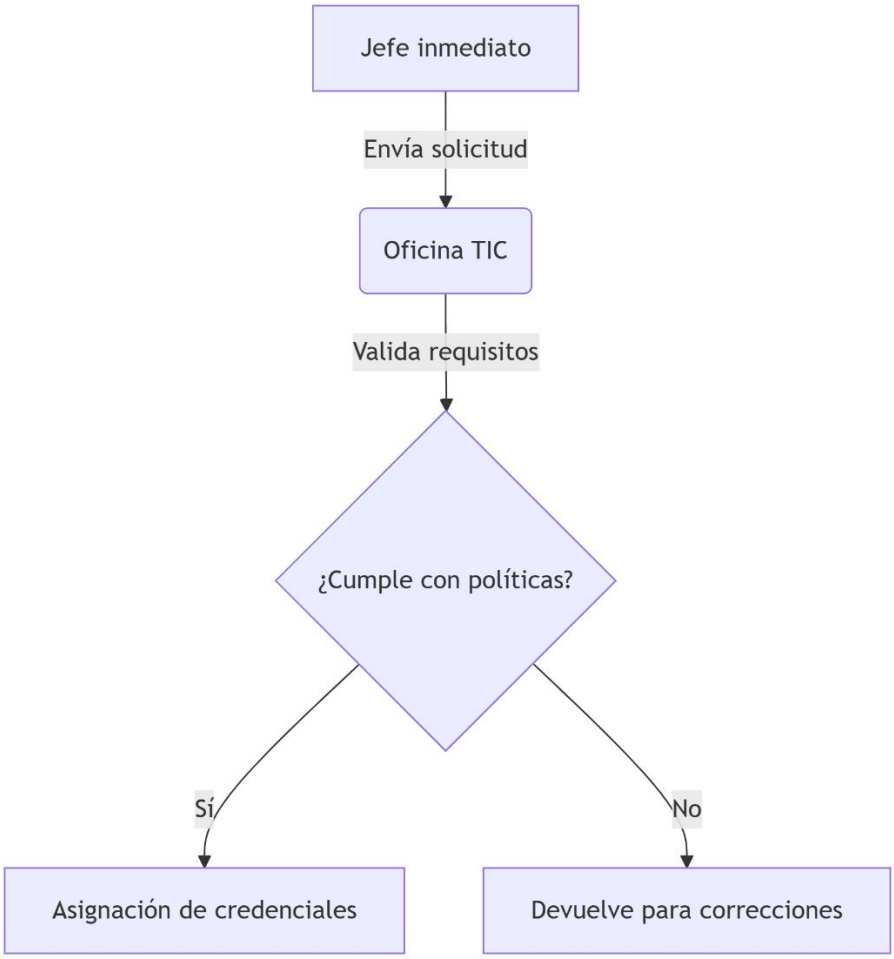
1. **Requisitos de la solicitud**
   - Todo jefe inmediato o responsable del área que requiera la habilitación de accesos tecnológicos para personal bajo su supervisión deberá remitir solicitud formal a la **Oficina de Tecnologías de la Información y Comunicaciones (TIC)** de la Corporación CDA.
2. **Información obligatoria**
   La solicitud debe contener:
   ✓ **Datos del solicitante**:
   - Nombre completo
   - Cargo/función
   - Área de adscripción
   - Nombre y firma del jefe de área

   ✓ **Detalles del acceso requerido**:
   - Sistemas informáticos involucrados (software o carpetas)
   - Nivel de privilegios (estándar, administrador)

   ✓ **Vigencia del acceso**:
   - Fecha de inicio (obligatoria)
   - Fecha de finalización (para contratistas/practicantes)
3. **Población aplicable**
   Este procedimiento cubre a:
   - Funcionarios de planta
   - Contratistas
   - Practicantes
   - Personal temporal
   - Cualquier colaborador que requiera accesos tecnológicos

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

4. **Flujo del proceso**



Notas importantes:

- Los accesos serán proporcionales a las funciones asignadas (principio de mínimo privilegio).
- Para modificaciones o revocación de accesos, seguir el mismo canal.
- Toda asignación quedara registrada y almacenada en el servidor para su trazabilidad.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

PROTOCOLO PARA CREACIÓN DE USUARIOS DE SERVICIOS TECNOLÓGICOS

1. Generación del Nombre de Usuario

- El nombre de usuario se conforma con la siguiente estructura:
  Formato estándar:
  Primer Nombre, Primer Apellido.
  Ejemplo: Maria.Gonzalez
- **Para casos de homonimia:**

- Se agregará el **segundo nombre** (ej: *Maria.Carmen.Gonzalez*)
- Si persiste la duplicidad, se incluirá la **inicial del segundo apellido** (ej: *Maria.Gonzalez.P*)
- Como último recurso, se añadirá un **número secuencial** (ej: *Maria.Gonzalez2*)

2. Creación de Credenciales

- **Contraseña inicial:**
  - Será generada automáticamente por el sistema o por el administrador de TIC, cumpliendo con: Mínimo 8 caracteres
  - Combinación de mayúsculas, minúsculas, números y símbolos
  - Caducidad a 30 días (primer uso)

- **Entrega:**
  Las credenciales se enviarán al correo institucional del usuario y a su jefe inmediato, bajo protocolo de confidencialidad.

3. Validación de Unicidad

El sistema de gestión de identidades verificará automáticamente:

- Existencia previa del usuario
- Homónimos en la base corporativa

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

ASIGNACIÓN DE PERMISOS

1. Principio de Asignación
Los permisos de acceso a sistemas y servicios tecnológicos son personales e intransferibles, y se otorgan conforme a las funciones específicas de cada colaborador dentro de la Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA).

2. Tipos de Accesos

2.1 **Servicios Básicos**
La Oficina de Tecnologías de Información y Comunicación asigna automáticamente:

- Acceso a la red corporativa
- Sistemas comunes de oficina
  A todo:
- Personal de planta
- Contratistas
- Practicantes
- Personal temporal

2.2 **Servicios Especializados**
Para accesos que requieran permisos adicionales (sistemas financieros, creación de correos institucionales, accesos a plataformas, bases de datos especializadas, etc.):

- El jefe inmediato debe presentar solicitud formal
- Debe justificar la necesidad del acceso
- Especificar el nivel de privilegios requerido
- Indicar temporalidad (si aplica)

3. Proceso de Solicitud

1. El jefe inmediato completa el formulario de solicitud de accesos especiales
2. La Oficina TIC evalúa la petición en un plazo máximo de 24 horas
3. Se notifica la aprobación o denegación con sus respectivas razones
4. En caso de aprobación, se configuran los accesos solicitados

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

4. Vigencia y Revisión

- Los accesos básicos permanecen activos durante la vigencia del contrato
- Los accesos especiales se revisan trimestralmente
- Todo acceso se revoca automáticamente al finalizar la relación contractual

5. Responsabilidades

- Los usuarios deben custodiar sus credenciales
- Está prohibido compartir accesos
- Se deben reportar anomalías inmediatamente

PERFILES DE SERVICIOS TECNOLÓGICOS.

1. **Acceso Administrador:** Este perfil permite la creación, modificación o eliminación de usuarios.
2. **Acceso estándar:** Este perfil permite acceder únicamente a los permisos asignados a su usuario y hacer uso de las funcionalidades básicas que ofrece el servicio tecnológico.

ASIGNACIÓN DE PERFILES A LOS USUARIOS DE LA CORPORACION CDA.

Se asignarán los permisos de acuerdo a los siguientes perfiles:

- **Perfil básico:** este perfil permite acceder a las aplicaciones básicas.
- **Perfil avanzado:** este perfil permite acceder a otro tipo de aplicaciones de conformidad a las autorizaciones otorgadas por el/a jefe/a inmediato/a

Todo usuario creado debe tener incluido el número de cédula y nombre en el sistema, aplicación, etc. En el caso de utilizar usuarios genéricos se debe justificar e ingresar la identificación y el nombre del usuario/a responsable.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

▪ POLÍTICA DE RESPONSABILIDADES DEL USUARIO

1. Ámbito de Aplicación

Esta política aplica a todo el personal vinculado a la CDA, incluyendo:

- Funcionarios de planta
- Contratistas
- Practicantes
- Personal temporal
- Terceros autorizados

2. Principios Generales

2.1 Todo usuario debe utilizar **exclusivamente** los recursos tecnológicos institucionales para fines laborales.
2.2 El acceso a sistemas implica la aceptación expresa de:

- Las políticas de seguridad de la información
- La confidencialidad de los datos institucionales

3. Obligaciones del Usuario

3.1 Gestión de Credenciales

- Mantener la **confidencialidad** de usuarios y contraseñas.
- **Prohibido** compartir credenciales o delegar accesos.
- Cambiar contraseñas cada **30 días** (según política de seguridad).

3.2 Uso de Equipos y Sistemas

- Solicitar soporte a **TIC** para:
    - Reemplazo de equipos
    - Reubicación física
    - Modificación de configuraciones

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Verificar que los equipos queden protegidos al ser reasignados.

3.3 Protección de Información

- Utilizar solo **aplicaciones autorizadas**.
- **Reportar inmediatamente**:
  - Pérdida o robo de dispositivos
  - Comportamiento anómalo en sistemas
  - Intentos de acceso no autorizado

4. Prohibiciones

❌ Instalar software no autorizado.
❌ Conectar dispositivos externos sin escaneo previo.
❌ Acceder a información corporativa fuera de sus funciones designadas.

5. Sanciones

El incumplimiento de estas normas dará lugar a:

- **Amonestaciones** verbales/escritas
- **Suspensión temporal** de accesos
- **Acciones disciplinarias** según el reglamento laboral
- **Denuncias penales** en casos graves

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **CONTROL DE ACCESO A REDES DE DATOS**

Para garantizar la **seguridad, confidencialidad y disponibilidad** de la red de datos institucional, se implementan los siguientes controles técnicos y administrativos:

1. Autenticación y Autorización

✅ **Autenticación fuerte:**

- **Usuario y contraseña compleja** (mínimo 8 caracteres, mayúsculas, números y símbolos).
- **Autenticación multifactorial (MFA)** con tokens, SMS o correo institucional asociado

✅ **Autorización basada en roles (Pimisys, Sila vital, Sigi, Carpetas en red, Mi doc. Millenium, token):**

Los jefes de área deben enviar una **solicitud formal** a la **Oficina de Tecnologías de la Información y Comunicaciones (TIC)**, indicando:

- **Nombre del funcionario**
- **Justificación del acceso** (según funciones)
- **Nivel de permisos requeridos** (Básico, avanzado)

Nota: (no aplica para Sigi y mi doc. Millenium) ya que en el caso del Sigi solo se les otorgará a los funcionarios el permiso de lectura y en el caso de mi doc. millenium, este solo software solo será instalado para el líder del proceso de archivo central.

Implementación

- La **Oficina TIC** validará y asignará los permisos en un plazo máximo de **24 horas hábiles**.
- Se notificará al jefe de área y al funcionario una vez configurado el acceso.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Restricciones

- **Acceso personalizado:** Cada usuario solo tendrá permisos sobre las funciones estrictamente necesarias para sus funciones.
- **No transferible:** Las credenciales y accesos son intransferibles.
- **Auditoría periódica:** La Oficina TIC revisará semestralmente los permisos asignados.

  Aplicación del **principio de mínimo privilegio**.

2-Políticas de Red

🚫 Control de dispositivos:

- Solo equipos autorizados (**por filtrado MAC**).
- **NAC (Network Access Control):** Soluciones como **MIKROTIK Reuters OS**.
- **VPN para acceso remoto:** este solo será configurado por el jefe de sistemas o quien se designe.

3. Protección contra Amenazas

🛡️ IDS/IPS (Sistemas de Detección/Prevención de Intrusos):
🔄 Actualizaciones periódicas:

- Parches de seguridad en Reuters, switches y firewalls y actualización de Windows.

4. Controles Físicos

Control de Acceso Físico

* Oficina de Sistemas

- **Acceso restringido**: Solo personal autorizado (equipo TIC, directivos o personal designados).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Mecanismos de autenticación**:
    - Tarjetas RFID o biométricos (huella/facial).
    - Registro digital o físico de entradas/salidas (nombre, hora y propósito).
- **Vigilancia**: Cámaras de seguridad 24/7 y alarmas anti intrusas.

*** Sala de Servidores**

- **Doble factor de autenticación**: RFID + PIN o biométrico.
- **Control de acompañamiento**: Personal no autorizado debe ingresar con supervisión TIC.
- **Prohibiciones**:
    - Dispositivos móviles o cámaras no autorizadas.
    - Ingreso de alimentos/bebidas.

5. Separación de redes: La unidad de Tecnologías de la información y Comunicación utilizará dispositivos de seguridad perimetral, para controlar el acceso de una red a otra y proteger la información más crítica o vulnerable, separándolos por segmentos de redes diferentes.

6. Control de conexión de las redes.

a) La capacidad de descarga de cada usuario final debe ser limitada y controlada.

b) La seguridad para las conexiones Wifi será WPA2 o superior.

c) Dentro de la red de datos institucional se restringirá el acceso a:

- Redes sociales, Facebook, YouTube, instagram, TikTok.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer o repositorios no autorizados.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Violencia contra niños, niñas y adolescentes.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

7. Control de enrutamiento de red.

El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos del Control de acceso a la red y adicionalmente se utilizarán métodos de autenticación de protocolo de enrizamiento, translación de direcciones IP y listas de control de acceso.

8. Uso de equipos de cómputo y dispositivos de almacenamiento móviles.

El uso de equipos de cómputo (laptops) institucionales y dispositivos de almacenamiento móviles, deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo
- Cifrado de la información.
- Uso de software antivirus provisto por la Oficina de Tecnología.
- Uso de software licenciado.
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.

9. Capacitación y Concientización

Entrenamiento a usuarios en:

- Phishing, contraseñas seguras y uso de redes.

10.Respuesta a Incidentes

- **Bloqueo inmediato:** de credenciales en caso de pérdida/robo.
- **Investigación forense:** ante accesos no autorizados.

11. Sanciones

- **Acceso no autorizado**: Suspensión de privilegios y acciones disciplinarias.
- **Incumplimiento de protocolos**: Amonestación escrita o terminación de contrato.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **CONTROL DE ACCESO AL SISTEMA OPERATIVO.**

1. Registro de Inicio Seguro

El acceso a los sistemas operativos corporativos estarán protegido mediante un **protocolo de inicio seguro de sesión**, que implementará las siguientes medidas:

1.1 Configuración del Inicio de Sesión

- **Ocultamiento de información**:
  - No se mostrará ninguno de los siguientes datos del sistema (correos asociados ni indicio de contraseña.)
- **Sin mensajes de ayuda**:
  - Durante el proceso de login, se evitarán mensajes que puedan revelar información sensible (ej: "indicio de contraseña").

1.2 Validación de Credenciales

- **Verificación en dos etapas**:
  1. Solo se validarán las credenciales después de ingresar *todos* los campos requeridos.
  2. Se aplicará un retardo deliberado tras cada intento fallido.
- **Máscara de contraseñas**:
  - En algunos casos las contraseñas digitadas se mostrarán como caracteres ocultos (******).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

1.3 Gestión de Intentos Fallidos

- **Bloqueo progresivo**:

Intentos Fallidos	Acción
3	Notificación al usuario
5	Bloqueo temporal (15 min)
10	Bloqueo permanente (requiere atención por parte de TIC)

- **Auditoría**:
  - Registro detallado de IP, horario y usuario en cada intento fallido.

1.4 Almacenamiento y Transmisión Segura

- **Cifrado de contraseñas**:
  - Uso de algoritmos robustos (bcrypt, PBKDF2 o Argon2).

- **Protección en tránsito**:
  - Canales encriptados (TLS 1.2+/SSL).
  - Prohibición absoluta de transmisión en texto plano.

2. Implementación Técnica

- **Sistemas Windows**:
  - Directivas de Grupo (GPO) para:
    - Ocultar información de inicio.
    - Limitar intentos fallidos (*Account Lockout Threshold*).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

3. Monitoreo y Cumplimiento

- **Herramientas**:
  - SIEM (ej: Wazuh, Splunk) para detectar ataques por fuerza bruta.
  - Scanners periódicos de vulnerabilidades (Nessus, OpenVAS).
- **Sanciones**:
  - Accesos no autorizados serán considerados **falta grave** según el Código de Conducta CDA.

- **CONTROL DE ACCESO A LAS APLICACIONES E INFORMACION.**

1. **Gestión de Accesos Basada en Roles**
   - Los privilegios de acceso a sistemas, aplicaciones o servicios se administrarán mediante roles predefinidos.
   - Estos roles y sus permisos asociados deberán documentarse en un registro centralizado, almacenado en carpetas compartidas con acceso restringido exclusivamente al personal autorizado de Tecnología.
2. **Clasificación y Protección de la Información**
   - El acceso a información física o digital se regulará conforme a su nivel de clasificación y a los protocolos de intercambio establecidos por la Corporación para el desarrollo sostenible del norte y oriente amazónico CDA.
   - La **Unidad de Tecnologías de Información y Comunicación (UTIC)** identificará los sistemas que manejen datos sensibles, los cuales deberán operar en entornos tecnológicos aislados e independientes.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- En estos casos, se garantizará un flujo seguro de información con otras fuentes de datos, evitando duplicaciones y priorizando el principio de **fuente única de verdad**.

3. **Revocación de Accesos**
   - Al desvincularse un colaborador de la Corporación CDA, la **UTIC** desactivará inmediatamente sus accesos tras recibir la notificación formal:
     - Para empleados: mediante comunicación de la oficina **de Talento Humano**.
     - Para contratistas: a solicitud del **jefe inmediato**.

- **MONITOREO DE SERVICIOS INFORMATICOS.**

La oficina de Tecnologías de Información y Comunicación (UTIC) implementará un sistema de monitoreo continuo de los servicios tecnológicos institucionales, con el objetivo de:

- Detectar y resolver oportunamente anomalías que afecten su operatividad.
- Garantizar el cumplimiento de los niveles de alta disponibilidad establecidos.

Este monitoreo abarcará:

- **Rendimiento:** Uso de recursos (CPU, memoria, ancho de banda).
- **Disponibilidad:** Tiempo de actividad y respuesta de servicios críticos.
- **Seguridad:** Alertas ante intentos de acceso no autorizado o comportamientos sospechosos.

Los incidentes identificados se escalarán siguiendo los protocolos de respuesta definidos, minimizando impactos en las operaciones institucionales.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **CASOS ESPECIALES**

En situaciones excepcionales no contempladas en esta política, la **Unidad de Tecnologías de la Información y Comunicación (UTIC)** evaluará la solicitud de excepción, considerando:

- **Pertinencia**: Justificación técnica u operativa del caso.
- **Riesgos asociados**: Impacto potencial en la seguridad, disponibilidad o integridad de los sistemas.

Procedimiento para solicitudes:

1. **Documentación**: El área solicitante deberá presentar una solicitud formal por escrito al **Oficial de Seguridad de la Información**, detallando:
    - Motivo de la excepción.
    - Plazo requerido (si aplica).
    - Medidas compensatorias propuestas para mitigar riesgos.
2. **Evaluación**: La UTIC emitirá un dictamen aprobando o denegando la solicitud, basado en el análisis de riesgos.
3. **Registro**: Todas las excepciones aprobadas se documentarán en un repositorio controlado, con seguimiento periódico para garantizar su alineación posterior con la política.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co