EDICIÓN 2 FECHA: 03 OCTUBRE 2025 RCE-21-PE01 NIVEL DE SEGURIDAD: PUBLICA	**DIRECCION Y LIDEGAZGO**	
	Política de Control de Accesos	

TABLA DE CONTENIDO

EDICIÓN 2 FECHA: 03 OCTUBRE 2025 RCE-21-PE01 NIVEL DE SEGURIDAD: PUBLICA	**DIRECCION Y LIDEGAZGO** **Política de Control de Accesos**	

1. POLITICA DE CONTROL DE ACCESOS

Establecer lineamientos para la gestión y control de accesos a los sistemas, instalaciones y recursos de información de Conexiones Empresariales S.A.S., garantizando la confidencialidad, integridad y disponibilidad de los datos, en cumplimiento con la norma ISO/IEC 27001:2022.

2. ALCANCE

Esta política aplica a todos los colaboradores, terceros y proveedores que requieran acceso a los sistemas de información, bases de datos, infraestructura tecnológica y espacios físicos de Conexiones Empresariales S.A.S., con especial atención en el proceso de facturación física y electrónica.

3. PRINCIPIOS Y COMPROMISOS

3.1. Principios de Seguridad

Confidencialidad: Solo el personal autorizado podrá acceder a la información según su rol.

Integridad: Se implementarán controles para prevenir accesos indebidos o modificaciones no autorizadas.

Disponibilidad: Se garantizará que los usuarios autorizados puedan acceder a la información cuando lo requieran.

3.2. Control de Acceso a Sistemas de Información

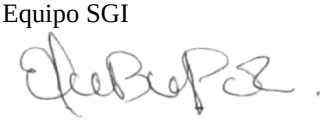
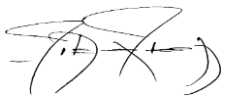
Todo usuario debe contar con credenciales únicas e intransferibles, deben cumplir con las siguientes condiciones: al menos 8 a 10 caracteres, Que estén compuestas por letras mayúsculas y minúsculas, números y caracteres especiales, Que no sean patrones sencillos, como repetir una letra en mayúscula seguida.

Se aplicará el principio de "privilegios mínimos", otorgando acceso solo a la información y sistemas necesarios.

La autenticación multifactor (MFA) será obligatoria para accesos críticos.

Los accesos se registrarán y auditarán periódicamente para identificar posibles vulneraciones.

Se implementará un proceso de revisión y revocación de accesos en caso de cambios de rol o desvinculaciones.

REALIZO:	REVISO:	APROBO:
Equipo SGI  Coordinador SGI	LAIDY SEGURA  Director Nacional de operaciones	Luis Alejandro Rodríguez Ariza  Gerente General

3.3. Control de Acceso a Infraestructura Física y digital

- Se regulará el acceso a las instalaciones según el rol del colaborador o proveedor.
- Se restringe el total acceso a personal que no esté autorizado por el comité de seguridad en la información a nivel nacional incluso entregar información de manera verbal.
- Se mantendrán registros de acceso a instalaciones críticas como servidores y salas de datos.
- Se aplicarán controles de video vigilancia y monitoreo en tiempo real.
- Control de Accesos con AWS IAM y Firewalls
- Rotación periódica de claves PEM y eliminación de claves de usuarios inactivos.

3.4. Control de Acceso en Facturación Física y Electrónica

- Solo el personal autorizado podrá generar, modificar y validar documentos de facturación.
- Se implementará cifrado en la transmisión y almacenamiento de facturas electrónicas.
- Los accesos serán auditados para prevenir alteraciones no autorizadas.
- Se utilizará autenticación multifactorial para la aprobación de facturas.
- Se verificará periódicamente la integridad de la información de facturación.
- Conexión a los Servidores EC2 mediante SSH y Certificados PEM
- Cada usuario autorizado tiene una clave privada (.pem) asignada para conectarse a instancias EC2 específicas.
- Se requiere autenticación por clave SSH, sin permitir accesos con usuario/contraseña.
- Solo permiten tráfico SSH desde direcciones IP autorizadas.
- Se aplican reglas específicas para restringir accesos según necesidades

3.5 procedimiento para eliminación de Usuarios:

- Solicitud de Eliminación de Usuario
- El gerente o supervisor del área, en conjunto con el departamento de recursos humanos (si corresponde), debe solicitar la eliminación del usuario.
- La solicitud debe realizarse por escrito o a través de un sistema de gestión de acceso, indicando la razón de la eliminación (desvinculación laboral, cambio de rol, etc.).
- Se debe verificar que la solicitud es legítima y que se cumple con los procedimientos internos establecidos.
- Acción Inicial: Antes de eliminar la cuenta, desactívala temporalmente para evitar que el usuario siga teniendo acceso.

- Sistema de Gestión de Identidad: Utiliza una herramienta centralizada (como un sistema de gestión de identidades) para desactivar las cuentas del usuario en todos los sistemas y plataformas donde tiene acceso (correo electrónico, aplicaciones internas, VPN, etc.).
- Revisión de Permisos: Revisa los permisos y accesos que el usuario tenía para evitar la pérdida de datos o el acceso a información sensible.
- Revocación de Accesos de sistemas informáticos y aplicaciones.
- Cuentas de correo electrónico y aplicaciones de mensajería instantánea.
- Accesos a bases de datos y plataformas de almacenamiento de archivos.
- Retiro de permisos en Dispositivos de hardware asignados (portátiles, teléfonos móviles, USB, etc.).
- Tarjetas de acceso o llaves de seguridad.
- Eliminación de Datos Asociados como son: Archivos de trabajo y documentos relacionados con proyectos o clientes, Correos electrónicos y correspondencia, Historial de actividad (accesos a aplicaciones y sistemas)
- Recuperación de Activos Físicos pertenecientes a la empresa (laptop, teléfono, tarjeta de identificación, equipo de trabajo, etc.), estos deben ser devueltos y revisados por el área Infraestructura.
- Notificación de Eliminación a las partes correspondientes sobre la eliminación de la cuenta, como los supervisores, otras áreas, clientes y realiza la actualización en las plataformas de recursos humanos si es necesario.

3.6 seguridad de los servicios en la red, incluyen firewalls, sistemas de detección de intrusos (IDS), encriptación de datos en tránsito, y políticas de acceso basadas en roles, entre otros. Estos controles están continuamente monitoreados y actualizados para proteger nuestra infraestructura frente a amenazas:

- Segmentación y Control de Tráfico de Red Amazon VPC (Virtual Private Cloud) para aislar entornos de producción, pruebas y desarrollo.
- Uso de Security Groups y Network ACLs para controlar accesos y limitar tráfico no autorizado. Bloqueo de acceso público a instancias y bases de datos críticas, solo accesibles por VPN o redes internas. Gestion de listas blancas para garantizar tráfico de ingreso y salida únicamente a IPs autorizadas.
- Cifrado de Comunicación y Seguridad de Tráfico TLS 1.2+/SSL obligatorio en todas las conexiones de red y APIs expuestas. Uso de AWS Certificate Manager (ACM) para gestionar certificados SSL. Cifrado de datos en tránsito con AWS PrivateLink y VPN segura.

- Monitoreo y Detección de Amenazas AWS CloudTrail para auditoría de accesos y cambios en configuraciones de red.
- Segmentación y Control de Tráfico de Red, Amazon VPC (Virtual Private Cloud) para aislar entornos de producción, pruebas y desarrollo.
- Uso de Security Groups y Network ACLs para controlar accesos y limitar tráfico no autorizado.
- Bloqueo de acceso público a instancias y bases de datos críticas, solo accesibles por VPN o redes internas. Gestion de listas blancas para garantizar tráfico de ingreso y salida únicamente a IPs autorizadas.
- Cifrado de Comunicación y Seguridad de Tráfico TLS 1.2+/SSL obligatorio en todas las conexiones de red y APIs expuestas. Uso de AWS Certificate Manager (ACM) para gestionar certificados SSL.
- Cifrado de datos en tránsito con AWS PrivateLink y VPN segura.
- Monitoreo y Detección de Amenazas
- AWS CloudTrail para auditoría de accesos y cambios en configuraciones de red.

4. RESPONSABILIDADES

a. Coordinador de SGI (sistema de Gestión Integral): Implementar y monitorear los controles de acceso.
b. Official de Seguridad de la Information: Supervisor el cumplimiento de la política.
c. Usuarios Finales: Cumplir con las normas de seguridad establecidas.
Proveedores y Terceros: Cumplir con los requisitos de seguridad definidos en contratos.

5. INCUMPLIMIENTO

El incumplimiento de esta política podrá resultar en acciones disciplinarias, hasta la terminación del contrato, según la gravedad del caso y la legislación vigente.

6. DISPONIBILIDAD Y COMUNICACIÓN

a) Esta política se encuentra disponible como información documentada en el sistema de gestión de documentos de la organización.
b) Se comunicará a todos los colaboradores y partes interesadas relevantes mediante capacitaciones, boletines y reuniones periódicas.
c) Será revisada y actualizada anualmente o cuando se requiera por cambios normativos o tecnológicos.