POLÍTICA DE GESTIÓN DE IDENTIDADES Y CONTROL DE USUARIOS

1. OBJETIVO

Establecer los lineamientos para la administración, control, monitoreo y revocación de identidades digitales y accesos a los sistemas de información, redes, aplicaciones y recursos tecnológicos de **GLOBAL DE SEGURIDAD ZOMAC LTDA**., garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

2. ALCANCE

Aplica a:

- Funcionarios administrativos, operativos y directivos.
- Contratistas y terceros.
- Proveedores con acceso a infraestructura tecnológica.
- Cualquier usuario que interactúe con activos de información de la organización.

3. MARCO NORMATIVO

La presente política se fundamenta en:

- Ley 1581 de 2012
- Decreto 1377 de 2013
- Ley 1273 de 2009
- Lineamientos de la Superintendencia de Vigilancia y Seguridad Privada
- Buenas prácticas de ISO 27001
- Lineamientos operacionales de ISO 18788

4. PRINCIPIOS RECTORES

La gestión de identidades se regirá bajo los siguientes principios:

- Privilegio mínimo
- Necesidad de conocer
- Segregación de funciones
- Responsabilidad individual
- Trazabilidad y auditoría
- Protección de datos personales

5. RESPONSABILIDADES

5.1 Gerencia

- Aprobar la presente política.
- Garantizar los recursos para su implementación.

5.2 Líderes de Área

- Autorizar formalmente solicitudes de creación, modificación o eliminación de accesos.
- Validar periódicamente los permisos asignados.

5.3 Proceso de Sistemas

- Administrar identidades y credenciales.
- Implementar controles técnicos de autenticación.

- Mantener registros de auditoría.
- Ejecutar revisiones semestrales de accesos.
- Garantizar la revocación inmediata ante retiro o cambio de rol.

5.4 Usuarios

- Custodiar sus credenciales.
- Reportar incidentes o accesos sospechosos.
- Cumplir los lineamientos establecidos.

6. LINEAMIENTOS GENERALES

6.1 Creación de Usuarios

- Todo usuario debe contar con identificación única e intransferible.
- La creación requiere autorización escrita del líder de área.
- No se permitirán cuentas genéricas salvo justificación técnica documentada.

6.2 Administración de Contraseñas

Las credenciales deberán cumplir:

- Mínimo **12 caracteres**.
- Combinación de letras mayúsculas, minúsculas, números y caracteres especiales o uso de frases de paso.
- Prohibición de reutilizar las últimas cinco (5) contraseñas.
- Cambio obligatorio únicamente en caso de:
  - Sospecha de compromiso.
  - Incidente de seguridad.
  - Acceso privilegiado crítico.
- Almacenamiento cifrado.
- No visualización en texto claro.

6.3 Autenticación Multifactor (MFA)

Será obligatorio para:

- Accesos remotos.
- Correo corporativo.
- Aplicaciones críticas o financieras.
- Accesos administrativos.

6.4 Bloqueo por Intentos Fallidos

- Bloqueo automático tras 3 intentos fallidos.
- Tiempo de bloqueo definido por análisis de riesgo (mínimo 30 minutos o desbloqueo por administrador).

6.5 Sesiones Inactivas

- Cierre automático de sesión tras máximo 10 minutos de inactividad en aplicaciones críticas.
- Bloqueo manual obligatorio del equipo al abandonar el puesto de trabajo.

6.6 Control de Acceso a la Red

- Segmentación mediante VLAN.

- Red de invitados aislada.
- Uso obligatorio de VPN corporativa para conexiones externas.
- Deshabilitación de puertos y servicios innecesarios.
- Monitoreo continuo mediante herramientas de seguridad.

6.7 Control de Acceso a Terceros

- Firma previa de acuerdo de confidencialidad.
- Accesos limitados en tiempo y alcance.
- Monitoreo de actividades.
- Revocación automática al finalizar contrato.

6.8 Gestión de Cambios de Rol y Retiro

- Revisión inmediata de accesos ante cambio de cargo.
- Revocación total el mismo día de terminación laboral.
- Checklist de desvinculación coordinado con Gestión Humana.

6.9 Registro y Trazabilidad

- Conservación de logs mínimo por un (1) año.
- Protección contra alteración o eliminación.
- Revisión periódica documentada.

6.10 Protección de Datos Personales

La gestión de identidades deberá garantizar la protección de datos personales conforme a la Ley 1581 de 2012.

Todo incidente que comprometa datos personales deberá ser reportado al Oficial de Protección de Datos y gestionado conforme al procedimiento de incidentes de seguridad.

7. GESTIÓN DE INCIDENTES

Cualquier evento relacionado con:

- Acceso no autorizado.
- Uso indebido de credenciales.
- Suplantación.
- Filtración de información.

Deberá ser reportado inmediatamente al área de Sistemas y a la Gerencia para su evaluación, contención y documentación.

8. VERIFICACIÓN Y AUDITORÍA

- Revisión semestral de perfiles de acceso.
- Auditoría anual documentada.
- Indicadores de cumplimiento.

- Acciones correctivas cuando aplique.

9. CLÁUSULA DE CUMPLIMIENTO

El incumplimiento de la presente política podrá generar:

- Medidas disciplinarias internas.
- Terminación contractual.
- Acciones legales conforme a la Ley 1273 de 2009.

JOHN FABIO PEÑA BERMEO
REPRESENTANTE LEGAL
Fecha: 04/03/2026

1 Control de cambios

VERSIÓN	PÁGINA	DESCRIPCIÓN DEL CAMBIO	FECHA
1	Todas	Creación del documento	04/03/2024
2	Todas	Revisión y Actualización	04/03/2025
3	Todas	Revisión y Actualización	04/03/2026
Elaboró: Responsable del SIG		**Revisó y aprobó:** Gerente General	