PROCEDIMIENTOS DE AUTENTICACIÓN Y CONTROL DE ACCESO
Página de Subastas – Comercializadora Nave Ltda.

1. OBJETIVO
Garantizar que el acceso a la plataforma de subastas se realice exclusivamente por usuarios autorizados, mediante mecanismos de autenticación robustos y controles de acceso basados en roles y atributos operativos.

2. AUTENTICACIÓN DE USUARIOS

2.1. Registro inicial
- Todos los usuarios deben crear una cuenta ingresando:
- Nombre completo o razón social.
- Número de identificación (Cédula/NIT).
- Correo electrónico institucional.
- Contraseña segura (mínimo 8 caracteres, alfanumérica y con símbolos).

2.2. Verificación
- Envío de correo de validación para activar cuenta.
- Validación de documentos habilitantes si participan en subastas vinculadas a entidades públicas.

2.3. Autenticación de acceso
- **Autenticación multifactor (MFA)**: Contraseña + código enviado a correo o teléfono.
- **Certificados electrónicos**: Se habilita uso de firma digital Cl@ve u otro certificado válido cuando aplica.
- **Bloqueo por intentos fallidos**: 5 intentos erróneos activan verificación manual.

3. CONTROL DE ACCESO

3.1. Roles definidos
- **Administrador General**: Gestión de usuarios, eventos y ajustes del sistema.
- **Proveedor Participante**: Consulta de subastas habilitadas y envío de ofertas.
- **Entidad Contratante**: Visualización de participantes y control de adjudicación.
- **Auditor**: Acceso solo a reportes y trazabilidad operativa.

3.2. Segmentación por operación

Los usuarios solo podrán acceder a:

- Subastas habilitadas para su rol
- Lotes asignados según precalificación
- Documentos públicos o privados según permisos.

3.3. Gestión de privilegios

- Los privilegios se asignan por contrato o autorización del área jurídica.
- Toda modificación requiere validación y registro por el administrador.

4. SEGURIDAD DEL SISTEMA

- **Cifrado SSL/TLS** para toda la navegación.
- **Control de versiones** en documentos y cambios operativos.
- **Bitácora de auditoría**: Registro de accesos, movimientos y acciones críticas.
- **Protección contra bots y accesos automatizados.**
- **Política de contraseñas**: Renovación cada 90 días.

5. MONITOREO Y AUDITORÍA

- Informes mensuales de accesos sospechosos o bloqueos.
- Evaluaciones semestrales del sistema de autenticación.
- Pruebas de penetración anuales por terceros especializados.