exmagon
transporte y logística

Política de la Seguridad de la Información

1. Objetivo

Establecer los lineamientos para proteger la información de la Exmagon, C.A. para asegurar la continuidad de las operaciones, y reducir los riesgos asociados al uso de dispositivos móviles, laptops y la operación de transporte de carga.

2. Alcance

- Todo el personal administrativo (aprox. 10 personas).
- Choferes locales que realizan operaciones de transporte de carga.
- Contratistas que tengan acceso a información de la empresa.
- Equipos y activos tecnológicos: laptops, teléfonos corporativos, radios, sistemas de rastreo GPS y aplicaciones utilizadas para la gestión operativa**.**
- Información no digital pero sensitiva, tales como contratos, facturas y otros documentos impresos físicamente**.**

3. Principios de Seguridad de la Información

- **Confidencialidad:** La información solo será accesible por personal autorizado.
- **Integridad:** La información debe ser precisa, completa y estar protegida contra modificaciones no autorizadas.
- **Disponibilidad:** La información y los sistemas deben estar disponibles cuando se necesiten para las operaciones.
- **Principio de Escritorio Limpio y Pantalla Limpia (Clean Desk & Clean Screen):**
    - Todo empleado debe mantener su espacio de trabajo libre de documentos visibles, credenciales, notas con contraseñas o información sensible.
    - Las pantallas deben bloquearse al alejarse del puesto de trabajo.
    - Documentos físicos deben guardarse en archivadores o gavetas cerradas

4. Gestión de Activos

- Toda laptop debe estar inventariada y asignada a un responsable.
- Los dispositivos utilizados por los choferes (ej. celulares, tablets de ruta) deben ser registrados.
- La información operativa (manifiestos, órdenes de entrega, guías de entrega es información sensitiva.

5. Control de Accesos

exmagon
transporte y logística

- Cada empleado un equipo laptop o pc que tenga tendrá un *usuario personal* y *contraseña fuerte.
- Las contraseñas deben cambiarse cada 90 días.
- Prohibido compartir credenciales.
- Acceso a información sensible se otorga bajo el principio de *necesidad-de-saber*.

6. Seguridad de Laptops

- Laptops deben contar con:
- Antivirus actualizado.
- Encriptación de disco duro.
- Bloqueo automático a los 5 minutos de inactividad.
- Prohibido instalar software sin autorización.
- Las laptops deben transportarse en mochilas apropiadas y no dejarse en vehículos sin supervisión.

7. Seguridad Operativa (Choferes)

- Documentos impresos (manifiestos, cartas de porte, guías) deben mantenerse protegidos dentro del vehículo.
- Prohibido divulgar información sobre rutas, cargas o clientes.
- Uso adecuado de dispositivos GPS o aplicaciones proporcionadas.
- Cualquier pérdida de documentos o dispositivos debe reportarse inmediatamente.

8. Uso Aceptable de los Sistemas

- Los equipos corporativos son para uso laboral.
- Prohibido acceder a sitios web maliciosos, descargar contenido pirata o abrir correos sospechosos.
- Prohibido conectar USB personales sin autorización.

9. Copias de Seguridad

- Los respaldos deben almacenarse en ubicación segura (nube o servidor externo).

Aprobado por la Gerencia General el 1 de enero de 2026.

Versión 1.0. Ámbito de aplicación: Operaciones Logísticas, Transporte y Sedes Administrativas.

exmagon
transporte y logística

10. Protección de Datos del Cliente

- Toda información de carga, rutas, tarifas y clientes es confidencial.
- No debe compartirse fuera de la empresa sin autorización escrita del gerente general.

11. Seguridad Física

- Acceso al área administrativa solo para personal autorizado.
- Los vehículos deben mantenerse cerrados cuando el chofer no esté presente.
- Llaves, guías y documentos deben mantenerse bajo control.

12. Gestión de Incidentes

Todo empleado debe reportar inmediatamente:

- Pérdida o robo de laptop, celular o documentos.
- Sospechas de intento de hackeo o phishing.
- Accidentes que comprometan carga o información.

La administración deberá documentar y analizar cada incidente.

13. Formación y Concienciación

Todo el personal recibirá capacitación anual en:

- Buenas prácticas de seguridad digital.
- Prevención de fraude y phishing.
- Manejo seguro de información operativa.

14. Cumplimiento

El incumplimiento de esta política puede resultar en:

- **Acciones disciplinarias internas.**
- **Medidas contractuales con proveedores.**
- **Denuncias legales en caso de negligencia grave**

Aprobado por la Gerencia General el 1 de enero de 2026.

Versión 1.0. Ámbito de aplicación: Operaciones Logísticas, Transporte y Sedes Administrativas.