

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Nuestro compromiso

En **DLF International Movers** reconocemos que la información es uno de los activos más valiosos de nuestra organización. Por ello, trabajamos para proteger la información, los datos personales y los sistemas tecnológicos que respaldan nuestros servicios, garantizando una gestión segura, responsable y alineada con las mejores prácticas de seguridad y ciberseguridad.

La protección de la información forma parte de nuestro compromiso con la calidad, la continuidad del negocio, la privacidad de nuestros clientes y la confianza de todas las partes interesadas.

1. Protección de la información

Trabajamos para garantizar la confidencialidad, integridad y disponibilidad de la información, aplicando medidas adecuadas para prevenir accesos no autorizados, pérdidas, alteraciones o usos indebidos.

Nuestra gestión de la información busca proteger tanto los datos empresariales como la información confiada por clientes, empleados, proveedores y colaboradores.

2. Protección de datos y privacidad

Tratamos los datos personales de forma responsable y conforme a la normativa aplicable en materia de protección de datos y privacidad.

Aplicamos medidas organizativas y técnicas destinadas a proteger la confidencialidad de la información y garantizar un tratamiento seguro de los datos personales.

3. Gestión segura de sistemas y accesos

Promovemos una gestión controlada y segura de los sistemas, plataformas y herramientas utilizadas en nuestras actividades.

Para ello, aplicamos mecanismos de control de accesos, asignación de permisos según funciones y protección de las credenciales de usuario, con el fin de reducir riesgos y proteger los recursos tecnológicos de la organización.

4. Uso responsable de la tecnología

Fomentamos el uso profesional, ético y responsable de los sistemas de información y de las herramientas digitales utilizadas por la organización.



Todos los usuarios deben contribuir a proteger la información y actuar con diligencia frente a posibles amenazas, como correos fraudulentos, intentos de phishing o actividades sospechosas

5. Ciberseguridad y prevención de amenazas

Trabajamos para prevenir, detectar y mitigar riesgos tecnológicos que puedan afectar a nuestros sistemas, operaciones o datos.

Para ello, mantenemos medidas de protección adecuadas, impulsamos buenas prácticas de seguridad digital y revisamos periódicamente nuestros controles para adaptarnos a la evolución de las amenazas.

6. Gestión de incidentes de seguridad

Promovemos la identificación y comunicación temprana de incidentes o vulnerabilidades que puedan afectar a la información o a los sistemas tecnológicos.

La notificación y gestión adecuada de incidentes nos permite minimizar impactos, adoptar medidas correctivas oportunas y fortalecer continuamente nuestros mecanismos de protección.

7. Formación y concienciación

Consideramos que la seguridad también depende de las personas.

Por ello, promovemos acciones de formación y sensibilización para reforzar el conocimiento de nuestros equipos sobre protección de datos, ciberseguridad y buenas prácticas digitales.

8. Continuidad y resiliencia

Trabajamos para garantizar la disponibilidad de la información y la continuidad de los servicios mediante medidas de protección, recuperación y gestión de riesgos adecuadas.

Nuestro objetivo es fortalecer la resiliencia de la organización frente a posibles incidentes tecnológicos o ciberataques.

9. Cumplimiento y mejora continua

Revisamos periódicamente nuestras medidas de seguridad para adaptarlas a los cambios tecnológicos, regulatorios y organizativos.

La mejora continua constituye un principio esencial para mantener un entorno digital seguro, confiable y alineado con las necesidades de nuestros clientes y de la organización.

10. Nuestro objetivo

Mantener una cultura de seguridad de la información y ciberseguridad que proteja los datos, garantice la continuidad de los servicios y refuerce la confianza de clientes, empleados, proveedores y demás grupos de interés

