**Protocolo de seguridad**

Objetivo

Establecer lineamientos claros para la recolección, uso, almacenamiento, transferencia y eliminación de la información y datos obtenidos de nuestros clientes, asegurando su confidencialidad, integridad y disponibilidad durante y después de la relación contractual.

Alcance

* Todo el personal de la empresa consultora (consultores, analistas, administrativos, proveedores externos autorizados).
* Toda la información proporcionada por el cliente o generada en el marco de un proyecto.
* Archivos electrónicos, documentos físicos, bases de datos, reportes, modelos analíticos y cualquier material derivado, datos personales, datos sensibles, información confidencial y propiedad intelectual del cliente y la consultora.

## Marco Legal

El protocolo se sustenta en:

* Contratos de prestación de servicios y cláusulas de confidencialidad.
* Buenas prácticas en seguridad de la información.

## Principios Rectores

El manejo de datos deberá regirse por los siguientes principios:

* **Licitud, consentimiento e información**: Ningún dato se obtiene sin

autorización expresa.

* **Finalidad**: Los datos solo se usan para los fines establecidos con el cliente.
* **Calidad**: Los datos deben ser exactos, completos y actualizados.
* **Proporcionalidad**: No se recaban datos innecesarios.
* **Responsabilidad**: Cada colaborador debe cumplir este protocolo y podrá ser

sancionado en caso contrario.

* **Confidencialidad**: La información del cliente no podrá ser divulgada sin

autorización expresa.

* **Integridad**: La información debe mantenerse completa, sin alteraciones no

autorizadas.

* **Disponibilidad**: Los datos deben estar accesibles solo para las personas

autorizadas.

## Clasificación de la Información

* **Información pública**: Información accesible libremente (ej. páginas web

oficiales del cliente).

* **Confidencial**: Información no pública entregada por el cliente para el

desarrollo de proyectos.

* **Reservada**: Información estratégica, financiera, operativa o técnica cuya

divulgación afectaría gravemente al cliente.

## Lineamientos de Manejo

### *a) Recolección*

* La información solo se recaba a través de canales oficiales designados por el cliente.
* Toda solicitud de información debe ser validada por el **responsable del proyecto**.

### *b) Uso y tratamiento*

* La información será usada exclusivamente para los fines estipulados en el contrato.
* Está prohibido utilizar la información para fines propios, académicos o comerciales ajenos al proyecto sin previa autorización del cliente.

### *c) Almacenamiento*

* Los archivos digitales deberán almacenarse en servidores seguros, con acceso restringido mediante usuarios y contraseñas.
* La documentación física deberá resguardarse bajo llave y acceso limitado.

### *d) Transferencia de información*

* Solo se permitirá la transferencia a terceros con autorización expresa del cliente.
* Bases de datos y reportes deben estar cifrados cuando se transmitan.
* En caso de requerir proveedores externos estos deberán firmar un **acuerdo de confidencialidad**.

### *e) Conservación y eliminación*

* La información se conservará únicamente durante la vigencia del contrato.
* Al concluir el proyecto, la empresa consultora deberá entregar los archivos finales al cliente y eliminar toda copia residual en sus sistemas, dejando constancia de ello por medio del acta de entrega-recepción y la constancia de eliminación.

## Seguridad de la Información

* Uso obligatorio de contraseñas seguras y autenticación de dos factores en sistemas críticos.
* Prohibido el uso de dispositivos personales para almacenar información del cliente sin autorización expresa.
* Realización periódica de respaldos en medios seguros y encriptados.
* Monitoreo de accesos a la información confidencial.

## 

## Capacitación y Concientización

* Todo el personal recibirá capacitación en materia de manejo de información confidencial y seguridad digital.
* Firma obligatoria de **acuerdo de confidencialidad** por parte de todo colaborador antes de tener acceso a datos del cliente.

## Sanciones Internas

* Falta leve: Amonestación escrita.
* Falta grave: Suspensión o terminación de la relación laboral/contractual.
* Daños a terceros: Responsabilidad civil y penal conforme a la ley mexicana.

## Responsable de Cumplimiento

Se designará un **Responsable de Seguridad de la Información** que supervisará la aplicación de este protocolo, coordinará auditorías internas y será punto de contacto con los clientes en temas de protección de la información.