Política para la Retención y destrucción de Información

(55) 6844 7757
contacto@integrarse.com.mx
www.integrarse.com.mx

Índice

Índice 2
Objetivo 1
1. Principios Generales 1
2. Clasificación de la Información 1
3. Retención de Información: 1
4. Almacenamiento de la Información: 2
5. Acceso y Uso de la Información: 2
6. Destrucción de Información: 2
7. Ciberseguridad: 3
8. Cumplimiento Legal y Normativo: 4
9. Responsabilidades: 4
10. Evaluación y Auditoría: 4
11. Sanciones por Incumplimiento: 5

Objetivo

Establecer las directrices y procedimientos necesarios para la correcta retención, almacenamiento y destrucción de la información de clientes, garantizando su confidencialidad, integridad y disponibilidad, así como cumplir con las leyes y regulaciones aplicables en materia de protección de datos personales.

1. Principios Generales

- IntegraRSE se compromete a manejar la información de los clientes de acuerdo con principios de privacidad y seguridad, garantizando que los datos sean protegidos durante todo su ciclo de vida, desde la recolección hasta la destrucción.
- Todos los empleados y colaboradores que tengan acceso a información confidencial de clientes deberán cumplir con esta política y recibir formación sobre el manejo adecuado de la información.

2. Clasificación de la Información

- **Información Confidencial:** Toda la información que se recoja de los clientes y que esté sujeta a regulaciones de privacidad, como datos personales, financieros, comerciales, entre otros.
- **Información No Confidencial:** Datos que no están sujetos a regulaciones de privacidad estrictas, como aquellos utilizados para fines operacionales generales que no contienen datos sensibles así como la información que sea de acceso público.

3. Retención de Información:

- **Períodos de retención:**
    - IntegraRSE retendrá la información de los clientes solo durante el tiempo necesario para cumplir con los fines para los cuales se recopiló la información. El período de retención variará según el tipo de información y las leyes locales de protección de datos.
    - Plazos de retención:
        - Información financiera: 5 años según legislación tributaria.
        - Datos de contacto y preferencias de clientes: 2 años después de la última interacción.

(55) 6844 7757
contacto@integrarse.com.mx
www.integrarse.com.mx

- Contratos y acuerdos: 10 años o según lo estipulado en la legislación vigente.
- Documentación y material de trabajo generado para el cliente en el periodo del contrato: 2 años después de la última interacción.

- **Revisión periódica:** Cada cierto tiempo, se realizará una revisión de la información almacenada para determinar si continúa siendo necesaria o si debe ser destruida según los plazos establecidos.

4. Almacenamiento de la Información:

- **Medidas de seguridad:**

Toda la información de clientes será ser almacenada de forma segura, tanto en formato físico como electrónico.

  - **Formato físico:** Los documentos que contienen información confidencial se almacenarán en archivos protegidos con acceso restringido y medidas de seguridad adecuadas (cajas cerradas, archivos protegidos por contraseña, etc.).
  - **Formato electrónico:** Los datos electrónicos serán almacenados en sistemas de gestión de información con acceso controlado. Esto incluirá el uso de contraseñas, cifrado de datos y firewalls para proteger los sistemas contra accesos no autorizados.

- **Backup de información:** IntegraRSE realizará copias de seguridad periódicas de la información relevante para garantizar su integridad y disponibilidad en caso de fallos técnicos, asegurando que estas copias estén igualmente protegidas.

5. Acceso y Uso de la Información:

- El acceso a la información de los clientes debe estar restringido a los empleados que necesiten la información para cumplir con sus responsabilidades laborales.
- Los empleados deben ser capacitados sobre el uso adecuado de la información, las consecuencias de su mal uso y la importancia de proteger la privacidad de los datos de los clientes.

6. Destrucción de Información:

- **Proceso de destrucción:**

(55) 6844 7757
contacto@integrarse.com.mx
www.integrarse.com.mx

Cuando la información de los clientes haya alcanzado el final de su período de retención y no sea más necesaria, debe ser destruida de manera segura.

- **Destrucción de documentos físicos:** Los documentos que contengan información confidencial deben ser destruidos mediante trituración o cualquier otro método que asegure que los datos no puedan ser recuperados.
- **Destrucción de información electrónica:** Los archivos electrónicos que contienen información confidencial serán eliminados de los sistemas de manera permanente, utilizando herramientas de borrado seguro que aseguren que los datos no puedan ser recuperados mediante técnicas de recuperación de datos.

- **Registro de destrucción:** IntegraRSE llevará un registro de las destrucciones realizadas, incluyendo la fecha, el tipo de información destruida, y la persona responsable de la destrucción.

7. Ciberseguridad:

Con el fin de asegurar la protección integral de la información durante todo su ciclo de vida, la empresa establece lineamientos específicos de ciberseguridad enfocados en la prevención de riesgos, el uso responsable de herramientas digitales y la protección ante amenazas externas.

- **Prevención de accesos no autorizados:** Se deberán implementar medidas de control como autenticación multifactor, administración segura de contraseñas y bloqueo automático de dispositivos, especialmente al manejar información sensible o confidencial.
- **Gestión segura de la información en entornos digitales:** Toda la información deberá almacenarse y gestionarse exclusivamente en plataformas digitales autorizadas por la empresa, evitando duplicidades innecesarias o almacenamiento en medios no controlados.
- **Protección ante amenazas cibernéticas:** El personal deberá estar atento a riesgos como phishing, enlaces maliciosos o descargas no seguras, evitando compartir información sensible a través de canales no verificados.
- **Seguridad en trabajo remoto:** Dado el modelo de trabajo remoto, se deberá asegurar que las conexiones a redes públicas o privadas se realicen mediante mecanismos seguros (VPN cuando aplique) y que los dispositivos cuenten con actualizaciones de seguridad vigentes.
- **Respaldo y continuidad operativa:** Se promoverá el respaldo periódico de la información crítica en sistemas seguros para evitar pérdidas derivadas de incidentes cibernéticos o fallas técnicas.

(55) 6844 7757
contacto@integrarse.com.mx
www.integrarse.com.mx

- **Gestión de incidentes de seguridad:** Cualquier evento que comprometa o pueda comprometer la seguridad de la información deberá reportarse de manera inmediata a la persona o área responsable, para su atención oportuna y mitigación de riesgos.
- **Cultura y capacitación en ciberseguridad:** La empresa fomentará la sensibilización continua del equipo en prácticas seguras de manejo de información digital, entendiendo la ciberseguridad como una responsabilidad compartida.

8. Cumplimiento Legal y Normativo:

- IntegraRSE se compromete a cumplir con todas las leyes, regulaciones y normativas aplicables en materia de protección de datos personales y privacidad (como la Ley General de Protección de Datos Personales en Posesión de los Particulares, GDPR, CCPA, etc.).
- En caso de que se requiera por ley la conservación de datos más allá del período estándar de retención, la empresa cumplirá con las regulaciones pertinentes, y procederá a proteger dichos datos de acuerdo con las normativas de seguridad vigentes.

9. Responsabilidades:

- **Responsable de la Seguridad de la Información:** El responsable de la seguridad de la información será el Director Administrativo, quien se encargará de supervisar la implementación de esta política, así como de coordinar las medidas de protección, retención y destrucción de los datos de clientes.
- **Empleados:** Todos los empleados que manejen datos de clientes tienen la responsabilidad de cumplir con esta política y con las medidas de seguridad relacionadas. Cualquier violación a la política deberá ser reportada inmediatamente.

10. Evaluación y Auditoría:

- **Evaluación continua:** IntegraRSE llevará a cabo auditorías anuales y evaluaciones de seguridad periódicas para asegurar que los procesos de retención, almacenamiento y destrucción de información de clientes sean efectivos y cumplan con los estándares de seguridad y privacidad requeridos.
- **Mejoras continuas:** Con base en los resultados de las auditorías y evaluaciones, se tomarán medidas para mejorar y actualizar los procedimientos de manejo de la información según sea necesario.

(55) 6844 7757
contacto@integrarse.com.mx
www.integrarse.com.mx

11. Sanciones por Incumplimiento:

- El incumplimiento de esta política podrá conllevar sanciones disciplinarias, que van desde advertencias hasta acciones legales en caso de que se haya causado un daño significativo a la privacidad de los clientes o se haya violado alguna ley de protección de datos.

Fecha de Aprobación: [27/02/2025]

Revisión: Anual o según cambios en la legislación.

(55) 6844 7757
contacto@integrarse.com.mx
www.integrarse.com.mx