POLÍTICA DE PROTECCIÓN DE INFORMACIÓN
"Querétaro Circular"

Última actualización: 1 de junio de 2025

1. Alcance y Objetivo

La presente Política de Protección de Información describe las medidas y prácticas que Querétaro Circular implementa para garantizar la seguridad, confidencialidad e integridad de la información personal y corporativa que recaba, procesa, almacena y comparte a través de sus sistemas y plataformas digitales. Aplica a todos los datos cargados en formularios, bases de datos, correos electrónicos y cualquier otro canal oficial de Querétaro Circular.

2. Principios Rectores

1. **Legalidad:** Tratamos los datos conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento, así como a normas relacionadas de carácter local.

2. **Finalidad:** Cada dato recabado se utiliza solo para los fines previamente informados y autorizados por el titular.

3. **Consentimiento:** Solo tratamos datos personales cuando el titular ha otorgado su consentimiento expreso para las finalidades específicas.

4. **Minimización:** Recabamos únicamente la información estrictamente necesaria.

5. **Confidencialidad:** Los datos se mantienen accesibles únicamente al personal autorizado y con necesidad de conocerlos.

6. **Transparencia:** Informamos de manera clara y oportuna sobre el uso que daremos a tus datos.

7. **Seguridad:** Aplicamos controles técnicos, administrativos y físicos para proteger los datos contra amenazas y vulnerabilidades.

8. **Responsabilidad:** Comprendemos la importancia de la información y asumimos la responsabilidad de mantenerla segura.

3. Responsables del Tratamiento y Custodia

- **Responsable Técnico:** Coordinador de Sistemas y Tecnología de Querétaro Circular, quien supervisa la implementación de medidas de seguridad y responde por el mantenimiento de la infraestructura tecnológica.

- **Responsable Administrativo:** Coordinador de Finanzas y Administración, quien asegura el cumplimiento de esta política en todas las áreas y la correcta clasificación de información según niveles de confidencialidad.

- **Usuario Titular de Datos:** Toda persona física o jurídica que proporcione información personal o corporativa a través de registros, formularios, correo electrónico o cualquier medio digital a Querétaro Circular.

4. Tipos de Información Protegida

1. **Información Personal (Datos Personales):**

    - Nombre, correo electrónico, teléfono, cargo, institución y otros datos proporcionados en formularios de registro.

    - Vínculos a perfiles profesionales (LinkedIn) o documentos con información biográfica.

2. **Información Sensible:**

    - Datos personales que requieran protección adicional (tarjetas de identificación, currículums con detalles confidenciales).

    - Cualquier tipo de dato que el titular indique como “confidencial” al momento de su captura.

3. **Información Corporativa:**

- Planes de acción, proyecciones, proyectos en desarrollo, diagnósticos y reportes internos.
- Bases de datos de aliados, convenios, contratos y documentos financieros.

4. **Información Técnica y Operativa:**
   - Accesos a servidores, contraseñas y configuraciones de sistemas.
   - Fotografías y videos de reuniones internas que no sean de acceso público.

5. Medidas de Seguridad Administrativas

1. **Clasificación de información:**
   - **Pública:** Contenido accesible en el sitio web (Hoja de Ruta, noticias, recursos).
   - **Interna:** Documentos compartidos exclusivamente con personal autorizado y miembros de la Comunidad Circular.
   - **Confidencial:** Información financiera, contratos, datos personales sensibles y reportes internos críticos.
2. **Acceso restringido:**
   - Cada colaborador tiene credenciales únicas y permisos basados en su rol (principio de “privilegio mínimo”).
   - Auditoría de accesos: registros de sesión y acciones en servidores y plataformas.
3. **Política de contraseñas:**

- Contraseñas robustas (mínimo 10 caracteres, combinación de letras, números y símbolos).
- Cambio de contraseña cada 90 días y bloqueo de cuenta tras 3 intentos fallidos.

4. **Formación continua:**
   - Capacitación anual obligatoria a todo el personal sobre protección de datos, buenas prácticas y reconocimiento de phishing.
   - Manual interno de uso de sistemas y manejo de información clasificada.
5. **Confidencialidad contractual:**
   - Contratos y convenios de confidencialidad (NDA) con colaboradores, prestadores de servicios y consultores externos.
   - Cláusulas específicas en contratos de proveedores que brindan respaldo técnico o gestionan información en la nube (Wix, Mailchimp, Google Workspace).

6. Medidas de Seguridad Técnicas

1. **Infraestructura segura:**
   - Servidores y bases de datos alojados en entornos con certificación ISO/IEC 27001 (proveedores cloud con alta disponibilidad).
   - Certificado SSL (https) en todo el sitio web para encriptar tráfico y prevenir interceptación.
2. **Cifrado de datos:**
   - Datos sensibles (contraseñas, claves API) cifrados en reposo con algoritmos AES-256.

- Transmisión de datos cifrada mediante protocolos TLS 1.2 o superior.

3. **Actualizaciones y parches:**
    - Mantenimiento periódico de software y sistemas operativos en servidores.
    - Aplicación oportuna de parches de seguridad en CMS (Wix) y complementos usados.
4. **Antimalware y firewall:**
    - Instalación de soluciones antimalware en servidores de desarrollo y estaciones de trabajo críticas.
    - Configuración de firewall perimetral para limitar puertos abiertos y prevenir ataques de fuerza bruta o DDoS.
5. **Respaldo de información:**
    - Copias de seguridad automáticas diarias de bases de datos y archivos críticos en servidores externos.
    - Retención de backups por un mínimo de 30 días, con verificación de integridad semanal.

7. Medidas de Seguridad Físicas

1. **Control de acceso a oficinas o salas de almacenamiento:**
    - Uso de credenciales físicas o tarjetas de proximidad en áreas restringidas.
    - Registro de entrada y salida de personal en áreas donde se almacenan dispositivos con información confidencial.
2. **Almacenamiento seguro de dispositivos:**

- Computadoras portátiles, discos duros externos y medios extraíbles protegidos con bloqueo físico (candados o lockers).
- Prohibición de dejar dispositivos desbloqueados o sin supervisión en áreas comunes.

3. **Eliminación segura de información:**
   - Destrucción de documentos impresos en trituradoras cross-cut para información clasificada.
   - Sobrescritura o destrucción física de discos duros y memorias USB que contengan datos sensibles.

8. Conservación y Retención de Información

1. **Plazos de retención:**
   - **Datos personales de usuarios registrados:** Conservación mientras mantengan su membresía o hasta que soliciten cancelación.
   - **Backups y logs de sistema:** Conservación mínima de 30 días para backups diarios y 1 año para logs de auditoría, salvo disposiciones legales que exijan más tiempo.
   - **Documentos financieros y contratos:** Conservación por 5 años a partir de la fecha de cierre del ejercicio fiscal.
2. **Eliminación y anonimización:**
   - Al cumplir los plazos de retención, la información se elimina completamente de sistemas o se anonimiza (en el caso de datos estadísticos).
   - Procedimiento documentado para garantizar la eliminación irrecuperable de datos.

9. Notificación de Incidentes de Seguridad

1. **Detección de incidentes:**
    - Monitoreo continuo de sistemas mediante herramientas de detección de intrusiones (IDS) y sistemas de información de seguridad (SIEM).
    - Registro de eventos sospechosos o fallas críticas en logs de servidor.
2. **Protocolo de respuesta:**
    - **Paso 1:** Reporte inmediato del incidente al responsable técnico (correo seguro).
    - **Paso 2:** Clasificación del incidente (baja, media, alta) según impacto y urgencia.
    - **Paso 3:** Copias de seguridad previas al incidente, diagnóstico forense y contención (aislar sistemas comprometidos).
    - **Paso 4:** Notificación a las autoridades competentes en caso de exposición de datos personales y al titular afectado, si aplica.
    - **Paso 5:** Implementación de medidas correctivas (parches, cambio de contraseñas, auditoría adicional).
3. **Notificación a titulares:**
    - En caso de brecha de seguridad que afecte datos personales, se notificará a los titulares a través del correo registrado dentro de las 72 horas posteriores a la confirmación del incidente, indicando naturaleza, datos implicados, acciones tomadas y recomendaciones para mitigar daños.

10. Evaluación y Mejora Continua

1. **Auditorías periódicas:**

- Auditorías internas semestrales sobre cumplimiento de esta política.
- Revisiones externas anuales por un tercero especializado en seguridad de la información.

2. **Actualización de controles:**
    - Incorporación de nuevas medidas ante cambios en amenazas, tecnología o normativas.
    - Capacitación continua al personal sobre nuevas prácticas de ciberseguridad.

11. Reporte de Problemas o Consultas

Si detectas anomalías, vulnerabilidades o tienes preguntas sobre la protección de tu información, contáctanos inmediatamente a:

direccion@queretarocircular.org

Tu reporte será tratado con confidencialidad y te informaremos de las acciones implementadas.

12. Vigencia y Modificaciones

Esta Política de Protección de Información entrará en vigor en la fecha de su publicación y se revisará anualmente o cuando se modifiquen las disposiciones legales aplicables. La versión vigente se encontrará disponible en el pie de página del sitio web de Querétaro Circular

Con esta Política de Protección de Información, **Querétaro Circular** asegura el resguardo y la integridad de los datos personales y corporativos de sus usuarios y aliados, reforzando la confianza y la colaboración multisectorial en la implementación de la economía circular.