ESMERALDAS
¡La Bella!

Políticas de Seguridad y Protección de Datos Personales del GADMCE

Contenido

Políticas de Seguridad y Protección de Datos Personales del GADMCE

1. Objetivo

Establecer las directrices y procedimientos para garantizar la seguridad, privacidad y protección de los datos personales tratados por el Municipio de Esmeraldas, en cumplimiento de la Ley Orgánica de Protección de Datos Personales y su Reglamento.

2. Alcance

Estas políticas aplican a todas las áreas, procesos y personal del Municipio de Esmeraldas que traten datos personales, incluyendo responsables, encargados y terceros vinculados.

3. Principios Rectores

1. **Legalidad:** El tratamiento de datos personales se realizará conforme a las disposiciones legales aplicables.
2. **Transparencia:** Garantizar que los ciudadanos estén informados sobre el uso de sus datos personales.
3. **Minimización de Datos:** Recopilar solo los datos estrictamente necesarios para los fines específicos del tratamiento.
4. **Seguridad:** Proteger los datos personales mediante medidas técnicas y organizativas adecuadas.
5. **Confidencialidad:** Asegurar que los datos sean tratados de manera confidencial y solo por personal autorizado.

4. Responsabilidades

4.1. Delegado de Protección de Datos (DPD)

En cumplimiento del Art. 48 del Reglamento, el Municipio designará un delegado de Protección de Datos, quien tendrá las siguientes funciones principales (Art. 49):

- Asesorar al personal sobre las obligaciones legales en materia de protección de datos.
- Supervisar el cumplimiento normativo y la implementación de medidas de seguridad.
- Analizar riesgos asociados al tratamiento de datos personales.
- Actuar como punto de contacto con la Autoridad de Protección de Datos Personales.
- Realizar evaluaciones de impacto sobre la privacidad.

4.2. Responsable del Tratamiento

- Garantizar que los datos sean tratados conforme a la ley.
- Aplicar medidas para proteger los derechos de los titulares de los datos personales.

4.3. Encargado del Tratamiento

- Cumplir con las instrucciones del responsable del tratamiento.
- Implementar medidas técnicas y organizativas para proteger los datos.

5. Derechos de los Titulares de Datos

El Municipio garantizará el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y demás derechos establecidos en la ley. Los ciudadanos podrán:

- Acceder a sus datos personales.
- Solicitar la rectificación de datos incorrectos.
- Solicitar la cancelación o eliminación de datos innecesarios o excesivos.
- Oponerse al tratamiento de sus datos en determinadas circunstancias.

6. Medidas de Seguridad

6.1. Medidas Técnicas

6.1.1. Seguridad en la Autenticación

- Implementación de bcrypt-nodejs para el hash seguro de contraseñas.
- Longitud mínima de contraseñas: 8 caracteres.
- Requisitos de complejidad: mayúsculas, minúsculas, números y caracteres especiales.
- Bloqueo temporal de cuentas después de múltiples intentos fallidos.

6.1.2. Arquitectura de Seguridad

Frontend (Angular 18+)

- Implementación de PrimeNG para componentes seguros y validados.
- Interceptores HTTP para manejo de tokens JWT.
- Guards para protección de rutas.
- Manejo seguro de estados y sesiones.
- Implementación de Socket.IO para actualizaciones en tiempo real

Backend (Node.js + Express)

- Arquitectura RESTful con endpoints seguros
- Validación de JWT en cada petición
- Implementación de middleware de seguridad
- Conexión segura con MongoDB
- Socket.IO para notificaciones de cambios de permisos en tiempo real

Comunicación Frontend-Backend

- Uso exclusivo de HTTPS/TLS para todas las comunicaciones

- Implementación de JWT para autenticación stateless
- Websockets seguros para actualizaciones en tiempo real
- Control de acceso basado en roles (RBAC) sincronizado

6.1.3. Seguridad en las Comunicaciones.

- Encriptación de datos en tránsito mediante TLS 1.3
- Validación de certificados SSL/TLS
- Implementación de cabeceras de seguridad HTTP
- Configuración segura de CORS

6.1.4. Protección de Datos y Gestión de Ambientes

Gestión de Ambientes

- Configuración de ambientes mediante variables globales:

typescript

```
export const GLOBAL = {
  // Ambiente de Producción
  production: {
        url: 'https://geoapi.esmeraldas.gob.ec/new/',

  },
  // Ambiente de Desarrollo/Pruebas
  development: {
        url: 'http://127.0.0.1:4201/api/',
  },
};
```

Control de Versiones

- Gestión de código fuente a través de GitHub

Protección de Datos

- Encriptación de datos sensibles en la base de datos
- Respaldos periódicos encriptados
- Monitoreo continuo de actividades sospechosas
- Logs separados por ambiente

6.1.5. Gestión de Respaldos y Recuperación

Sistema Automatizado de Respaldos

- Respaldos diarios programados mediante node-cron
- Ejecución automática a las 12:00 PM
- Nomenclatura estandarizada: backup-YYYY-MM-DD-HH-MM-SS.gz
- Verificación de duplicados antes de la generación

Almacenamiento Redundante

- Almacenamiento primario: Servidor local
- Almacenamiento en la nube: Google Drive
  - Autenticación mediante cuenta de servicio
  - Gestión automatizada de permisos
- Respaldo adicional en máquina personal autorizada
  - Transferencia segura mediante SSH/SCP
  - Verificación de integridad post-transferencia

6.2. Organizativas:

- Capacitación periódica del personal en materia de protección de datos.
- Políticas claras de clasificación y manejo de información.
- Designación de responsables para la gestión de incidentes de seguridad.

7. Gestión de Riesgos

El Municipio realizará evaluaciones periódicas de riesgos y análisis de impacto para identificar y mitigar posibles vulnerabilidades en el tratamiento de datos personales.

8. Procedimiento para Incidentes de Seguridad

En caso de un incidente que comprometa la seguridad de los datos personales:

1. Notificación inmediata al delegado de Protección de Datos delegadodeprotecciondedatos@esmeraldas.gob.ec
2. Contención del incidente y evaluación del impacto.
3. Informe a la Autoridad de Protección de Datos Personales según lo dispuesto en la normativa vigente.
4. Implementación de medidas correctivas para prevenir futuros incidentes.

Al ingresar los datos requeridos por el sistema, el usuario otorga su consentimiento para que el GADMCE utilice los mismos para efectos de contacto, localización, notificaciones y respuestas solicitadas por el usuario.

Responsabilidad

El GADMCE solamente será responsable del tratamiento y uso de los datos personales que recabe en forma directa a través de los servicios en línea.

El GADMCE no se hace responsable por la veracidad o exactitud de la información contenida en los enlaces a otros sitios web o que haya sido entregada por terceros.

El uso de este portal o de cualquiera de sus componentes o servicios, implica la aceptación expresa de la presente política de privacidad.

18. Acceso de terceros a información confidencial

El acceso de información a terceros se realizará solo con fines específicos, siendo solicitado formalmente y debidamente aprobado por la máxima autoridad de la Institución y/o su delegado.

Se prohíbe replicar, copiar y/o divulgar ***información confidencial***.

Los contratistas, proveedores y/o terceros a quienes se otorgue acceso a la ***información confidencial,*** deberán suscribir el respectivo acuerdo de confidencialidad y, en consecuencia, estarán sujetos a la presente política.

19. Envió de información a terceros

Previo al envío de cualquier tipo de información institucional, ésta deberá contar con la aprobación del director del área respectiva.

Se prohíbe el envío de ***información confidencial*** a terceros.

El incumplimiento de la presente política será sujeto a las sanciones administrativas que

se estimen pertinentes.

20. Información disponible al público.

Establecer procedimientos para que la información sensible sea protegida durante la recolección, procesamiento y almacenamiento.

21. Uso de firma electrónica

La utilización de firma electrónica en cualquiera de sus formas (token, archivo y contraseña, etc.) es de absoluta responsabilidad del usuario propietario de la misma.
Quien adultere o modifique el contenido de un documento previamente suscrito electrónicamente, será sancionado sin perjuicio de las acciones legales que la institución pueda llevar a cabo.

22. Uso del correo electrónico institucional

El correo electrónico institucional es de uso exclusivo para actividades laborales de los funcionarios y/o personal operativo en el ejercicio de sus funciones quienes, a su vez, son absolutos responsables y custodios de los buzones asignados.

No se utilizará el correo electrónico institucional con fines de envío publicitario, difusión de cadenas y/o cualquier actividad no relacionada a las actividades de trabajo.
No se utilizará la cuenta de correo electrónico institucional para suscribirse a servicios ajenos a las actividades institucionales.

23. Seguridad en el uso del correo electrónico

Se consideran confiables aquellos correos electrónicos que tengan el formato (también llamado “dominio”): xxxxx@esmeraldas.gob.ec. Visualmente se puede comprobar el dominio de origen dando clic en el mismo.
No abrir adjuntos en correos electrónicos de remitentes desconocidos, o en su defecto consultar a quien se dice destinatario si envió un adjunto determinado.
Se solicita no abrir el correo personal con los recursos institucionales; en casos de urgencia personal, asegurarse de no dejar archivos descargados en la computadora institucional.

24. Uso de los sistemas de información

El acceso a los aplicativos, servicios y sistemas de la información serán solicitadas por el director de la unidad requirente; la DTI definirá el perfil del funcionario de conformidad a los privilegios requeridos por la Dirección solicitante.

Las credenciales (usuario y contraseña) para el acceso a los sistemas informáticos, aplicativos, bases de datos, reportes, sitio web, correo institucional y computador son de uso estrictamente personal, con fines laborales y son de exclusiva responsabilidad del funcionario a quien le son otorgadas.

Las contraseñas son de absoluta responsabilidad de quienes les fueron asignadas oportunamente, por lo tanto, no dejar las contraseñas expuestas al público, y menos compartirlas con terceros.

Los usuarios no deben dejar abiertas las sesiones mientras el equipo no esté siendo atendido.

9. Sanciones

El incumplimiento de estas políticas será considerado una falta grave y estará sujeto a medidas disciplinarias, de acuerdo con las normativas internas y la legislación aplicable.

10. Vigencia

Estas políticas entrarán en vigor desde su aprobación y deberán revisarse anualmente o cuando se produzcan cambios normativos significativos.

10.1. Procedimiento Operativo

10.1.1. Recepción del Reclamo o Solicitud

Canales habilitados:

- Presenciales: Oficinas de Atención al Ciudadano.
- Digitales: Correo electrónico, sitio web oficial o la aplicación móvil ‘Esmeraldas La Bella’.

- Telefónicos: Línea de atención ciudadana.

Registro:

- Asignar un número de caso único al reclamo o solicitud.
- Incluir los siguientes datos:
  - Nombre completo y contacto del ciudadano.
  - Descripción clara y detallada del reclamo o solicitud.
  - Documentos o pruebas adjuntas (si aplica).

Confirmación:

- Entregar un comprobante de recepción al ciudadano, con el número de caso y plazo estimado de respuesta.

10.1.2. Clasificación y Priorización

Clasificación:

- Reclamos generales: Problemas menores o de resolución administrativa.
- Reclamos críticos: Aquellos que afectan derechos fundamentales o servicios esenciales.
- Solicitudes de información: Requerimientos de datos específicos sobre servicios municipales.

Priorización:

- Los reclamos críticos deben ser atendidos en un plazo máximo de 5 días hábiles.
- Los reclamos generales y solicitudes, dentro de 10 días hábiles.

10.1.3. Análisis y Resolución

Derivación:

- Remitir el caso al área correspondiente en las primeras 24 horas posteriores a la recepción.

Investigación:

- Analizar el reclamo o solicitud, verificando los hechos y recopilando información relevante.

Resolución:

- Proponer una solución o respuesta adecuada conforme a la normativa vigente y los procedimientos internos.

Revisión:

- Verificar que la respuesta sea clara, precisa y fundamentada.

10.1.4. Comunicación de la Respuesta

Medios:

- Notificar al ciudadano a través del medio elegido al presentar su reclamo.

Contenido de la respuesta:

- Resumen del reclamo o solicitud.
- Explicación de las acciones tomadas o solución propuesta.
- Información de contacto para aclaraciones o seguimiento.

Plazos:

- Garantizar que la respuesta se emita dentro del plazo establecido según la clasificación del caso.

11. Anexo Técnico: Implementación de Seguridad A1. Gestión de Contraseñas

javascript

```javascript
// Ejemplo de implementación de hash de contraseñas
const bcrypt = require('bcrypt-nodejs');

const hashPassword = (password) => {
    return bcrypt.hashSync(password, bcrypt.genSaltSync(10));
};

const comparePassword = (password, hash) => {
    return bcrypt.compareSync(password, hash);
};
```

12. A2. Configuración de Seguridad Frontend (Angular)

typescript

```typescript
// Interceptor para JWT
@Injectable()
export class JwtInterceptor implements HttpInterceptor {
    constructor(private authService: AuthService) {}

    intercept(request: HttpRequest<any>, next: HttpHandler): Observable<HttpEvent<any>> {
        const token = this.authService.getToken();
        if (token) {
            request = request.clone({
                setHeaders: {
                    Authorization: `Bearer ${token}`
                }
            });
        }
        return next.handle(request);
    }
}
```

```
// Guard para protección de rutas
@Injectable({
  providedIn: 'root'
})
export class AuthGuard implements CanActivate {
  constructor(
    private router: Router,
    private authService: AuthService
  ) {}

  canActivate(route: ActivatedRouteSnapshot): boolean {
    const requiredRoles = route.data['roles'];
    if (!this.authService.isAuthenticated() ||
        !this.authService.hasRequiredRoles(requiredRoles)) {
        this.router.navigate(['/login']);
        return false;
    }
    return true;
  }
}
```

13. A3. Gestión de Control de Versiones y Ambientes

A3.1 Políticas de GitHub

- Uso obligatorio de autenticación de dos factores (2FA)
- Configuración de .gitignore para excluir:

```
# Archivos de configuración sensibles
.env
.env.*
database/credentials.json

# Dependencias
node_modules/
dist/
```

```
# Logs y archivos temporales
*.log
npm-debug.log*
yarn-debug.log*
yarn-error.log*

# Archivos
uploads/

# Archivos del Sistema
swaggerRoutes/labellaModule/


# Archivos de respaldo
Database/backups/
```

A3.2 Gestión de Permisos en Tiempo Real

javascript

```javascript
// Configuración de Socket.IO para actualización de permisos
const io = require('socket.io')(server, {
    cors: {
        origin: process.env.FRONTEND_URL,
        methods: ["GET", "POST"],
        credentials: true
    }
});

// Manejo de actualizaciones de permisos
io.on('connection', (socket) => {
    socket.on('permissionUpdate', (data) => {
        // Notificar a usuarios específicos sobre cambios en permisos
        io.to(data.userId).emit('updateUserPermissions',  data.newPermissions);
    });
});
```

Controles	Nombres/Cargo	Firma
Aprobado:	Abg. Vicko Villacís Tenorio Mgtr. **Alcalde del Cantón Esmeraldas**	Firmado electrónicamente por: VICKO ALFREDO VILLACIS TENORIO Validar únicamente con FirmaEC
Revisado:	Tnlgo. Henri Daniel Rodriguez Portes **Director de tecnologías**	Firmado electrónicamente por: DANIEL HENRI RODRIGUEZ PORTES Validar únicamente con FirmaEC
Elaborado:	Ing. Juan Carlos Zalazar **Analista 1 de Sistemas**	Firmado electrónicamente por: JUAN CARLOS SALAZAR FARIAS Validar únicamente con FirmaEC