Seguridad Digital

La entidad ha implementado medidas de seguridad digital y de protección de la información en sus servicios web institucionales, en concordancia con las condiciones técnicas mínimas definidas en el *Anexo 3 de la Resolución MinTIC 1519 de 2020, orientadas a preservar la **confidencialidad, integridad, disponibilidad y trazabilidad de la información*.

Medidas implementadas

1. Transmisión segura de información

El portal institucional opera bajo protocolo *HTTPS* con certificado *SSL/TLS* vigente, garantizando el cifrado de la información transmitida entre el ciudadano y la plataforma institucional.

2. Protección contra automatización y abuso de formularios

Se implementó validación de seguridad mediante *reCAPTCHA* en formularios transaccionales (PQRSDF), mitigando envíos automatizados, intentos masivos de radicación y abuso del servicio digital.

3. Gestión segura de errores y excepciones

El sistema cuenta con manejo controlado de errores (419, 500 y excepciones internas), evitando exponer información sensible de infraestructura o trazas técnicas al ciudadano.

Los eventos son registrados en bitácoras internas para monitoreo y trazabilidad técnica.

4. Registro y trazabilidad de incidentes

Se mantiene registro interno de eventos del sistema mediante logs técnicos, incluyendo información de diagnóstico necesaria para seguimiento de incidentes, auditoría y mejora continua.

5. Seguridad en comunicaciones institucionales

Se fortaleció la autenticidad del correo institucional mediante implementación de políticas *SPF, DKIM y DMARC*, reduciendo riesgos de suplantación de identidad y fortaleciendo la confianza en las notificaciones electrónicas enviadas por la entidad.

6. Protección de datos personales

Los formularios institucionales incorporan autorización de tratamiento de datos personales y controles orientados al cumplimiento de la normativa de protección de datos aplicable.

7. Continuidad operativa y contingencia

Ante fallas técnicas, el sistema dispone de mecanismos de contingencia con mensajes claros al ciudadano, canales alternativos de contacto y conservación de la información diligenciada cuando aplica, garantizando continuidad en la prestación del servicio digital.

Evidencia verificable

* Navegación segura bajo HTTPS.
* Formularios con validación reCAPTCHA activa.
* Páginas controladas de error 419 / 500 implementadas.
* Registros internos de eventos en bitácoras del sistema.
* Configuración activa de SPF / DKIM / DMARC para notificaciones institucionales.
* Políticas institucionales de tratamiento de datos publicadas en el portal.

Con lo anterior, la entidad evidencia la aplicación efectiva de controles de seguridad digital y seguridad de la información en sus servicios web institucionales.