INFORME TÉCNICO Nro. DTIC-01-0001

| | |
|---|---|
| **Asunto:** Medidas de protección de datos personales | **Fecha presentación:** 28/01/2025 |
| **Realizado por:** Ing. Bladimir Reyes, Mgs. | |
| **Lugar:** Planta Central | |

## 1. ANTECEDENTE

Mediante Registro Oficial - Quinto Suplemento Nº 459, de miércoles 26 de mayo de 2021, se publica la Ley Orgánica de datos personales, con el objetivo y finalidad de garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección.

Mediante Memorando Nro. AGR-AGROCALIDAD/DAJ-2024-001368-M, de 10 de diciembre de 2024, se solicita la elaboración de un informe comunicacional dirigido a los usuarios internos y externos de la Agencia, proporcionando información clara sobre los mecanismos de protección de datos personales implementados en los sistemas GUIA, SIFAE y SIZE.

## 2. OBJETIVO

Proporcionar información a usuarios internos y externos sobre los mecanismos de protección de datos personales implementados en los sistemas institucionales GUIA, SIFAE y SIZE.

## 3. DESARROLLO

En cumplimiento con la Ley Orgánica de Protección de Datos Personales, la Agencia ha implementado una serie de medidas de seguridad en los sistemas oficiales que manejan datos personales. Estas medidas tienen como objetivo garantizar la protección, confidencialidad y seguridad de la información de los usuarios, tanto internos como externos.

**Medidas de Seguridad Implementadas**
**Origen y Calidad de los Datos.**

La información utilizada en estos sistemas proviene de servicios proporcionados por la Dirección Nacional de Registros Públicos (DINARP), una fuente gubernamental confiable que asegura la calidad, precisión y autenticidad de los datos. Este origen garantiza que los datos personales que manejamos sean verídicos y estén actualizados, contribuyendo a la integridad del proceso.

**Prevención de Acceso No Autorizado a la Base de Datos.**

A nivel de base de datos, los sistemas cuentan con estrictos controles de acceso para prevenir cualquier intento de acceso no autorizado. Esto incluye políticas y configuraciones que limitan y controlan quién puede acceder y manipular la información almacenada.

**Encriptación de contraseñas.**

Las contraseñas de los usuarios se almacenan utilizando métodos de encriptación avanzados, imposibilitando su lectura incluso en caso de acceso no autorizado.

**Autenticación con tokens seguros.**

Tokens de inicio de sesión respaldados por llaves públicas para garantizar accesos seguros y proteger contra intentos de suplantación de identidad.

**Mecanismos de Respuesta ante Incidentes.**

La Agencia dispone de herramientas de monitores y protocolos establecidos para actuar rápidamente ante cualquier brecha de seguridad, minimizando el impacto sobre los datos personales y tomando las medidas correctivas necesarias.

Lo que permite mantener la confidencialidad, integridad y disponibilidad de los datos personales.

**A nivel de Infraestructura**

Se cuenta con seguridad perimetral, Previniendo inclusiones no autorizadas, ataques de DDoS y aplicación, así como certificados de SSL/TSL que autentifican el dominio agrocalidad.gob.ec como sitios seguros.

Acceso a servidores restringido mediante claves encriptadas, permisos y roles de usuarios restringidos.

## 4. CONCLUSIONES

- Al utilizar información proveniente de la Dirección Nacional de Registros Públicos (DINARP), se asegura la calidad, autenticidad y precisión de los datos. Esto refuerza la integridad del proceso y minimiza el riesgo de errores por datos incorrectos o desactualizados.
- Los estrictos controles de acceso a los sistemas de Agrocalidad protegen los datos personales frente a accesos indebidos, asegurando que solo el personal autorizado pueda manipular esta información.
- El uso de métodos avanzados de encriptación para el almacenamiento de contraseñas refuerza la seguridad de los datos, incluso si ocurre un acceso no autorizado.
- La implementación de tokens respaldados por llaves públicas protege los sistemas frente a intentos de suplantación de identidad y garantiza que solo usuarios autorizados tengan acceso esto permite proteger contra intentos de suplantación de identidad
- Con la incorporación de herramientas de monitoreo y protocolos de actuación rápida, la Agencia puede identificar, gestionar y mitigar los efectos de cualquier incidente de seguridad, reduciendo los riesgos asociados.

## 5. RECOMENDACIONES

- Realizar auditorías de seguridad y evaluaciones de riesgo de forma periódica para identificar posibles vulnerabilidades y asegurarse de que las medidas de seguridad estén actualizadas y efectivas.
- Capacitar en forma continua a los usuarios, tanto técnicos como no técnicos, sobre las mejores prácticas en seguridad de la información, manejo de datos personales y cómo reconocer intentos de phishing o cualquier otro tipo de ataque cibernético.
- Asegurarse de que todos los dispositivos móviles que tengan acceso a los sistemas de la agencia estén protegidos mediante cifrado, autenticación biométrica y políticas de seguridad móviles.
- Utilizar herramientas avanzadas de monitoreo y detección de amenazas mediante Inteligencia Artificial para identificar actividades sospechosas o no autorizadas en tiempo real y tomar medidas preventivas rápidamente.
- Mantener y mejorar los principios de privacidad por diseño en el desarrollo de nuevos sistemas y aplicaciones, asegurando que la protección de datos personales sea una consideración clave desde el inicio.
- Evaluar y monitorear a los proveedores y terceros que tengan acceso a los datos personales para asegurarse de que cumplan con los mismos estándares de seguridad y protección de datos que la agencia.
- Desarrollar y probar regularmente planes de continuidad del negocio para asegurarse de que la agencia pueda seguir operando en caso de interrupciones significativas.

| **Elaborador por:** | **Firma** |
|---|---|
| Ing. Bladimir Segundo Reyes Cueva, Mgs.<br>CC: 1712644770<br>Analista de Infraestructura y Soporte Técnico | Firmado electrónicamente por:<br>BLADIMIR SEGUNDO REYES CUEVA |

| **Revisado por:** | **Firma** |
|---|---|
| Ing. Patricio Roberto Sizalima Pucha Msc.<br>CC: 1713810560<br>Analista de Gestión de la Información 3 | Firmado electrónicamente por:<br>PATRICIO ROBERTO SIZALIMA PUCHA |

| **Aprobado por:** | **Firma** |
|---|---|
| Ing. Elba Elizabeth Encalada Elizalde, Mgs.<br>CC: 1104556269<br>Directora de Tecnologías de la Información y Comunicación | Firmado electrónicamente por:<br>ELBA ELIZABETH ENCALADA ELIZALDE |