RESUMEN EJECUTIVO

Entidad: Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación

Referencia: Auditoría a la Confidencialidad, Integridad, Disponibilidad y Confiabilidad del Mecanismo de Autenticación de la Plataforma de Ciudadanía Digital

Informe Nº: K3/IP37/A24-Q1

Objetivo: Expresar una opinión independiente respecto a la Confidencialidad, Integridad, Disponibilidad y Confiabilidad del Mecanismo de Autenticación de la Plataforma de Ciudadanía Digital.

Objeto: El Mecanismo de Autenticación de la Plataforma de Ciudadanía Digital (versión 2), implementado por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC)

Periodo auditado: La información remitida hasta el 27 de diciembre de 2024.

Resultados: Como resultado de la auditoría se emiten tres (3) recomendaciones para superar los hallazgos identificados.

a. El método implementado en el Mecanismo de Autenticación para la verificación de la identidad del ciudadano digital.

El principal hallazgo identificado al respecto, es el siguiente:

- El método de autenticación empleado no evita la posibilidad de suplantación de identidad del ciudadano en las Gestiones Digitales que así lo requieran.

En el informe consta de una (1) recomendación orientada a fortalecer el método implementado en el Mecanismo de Autenticación para la verificación de la identidad del ciudadano digital.

R1. Implementar los ajustes necesarios en el diseño conceptual y desarrollo del Mecanismo de Autenticación, a fin de alinearse a los principios, lineamientos y marcos normativos aplicables, para:

- Garantizar la aplicación del principio de Autenticidad establecido en los "*Lineamientos y Estándares Técnicos de Ciudadanía Digital y Notificación Electrónica (versión 4.1)"*, mediante la adopción de un esquema de autenticación multifactor alineado con la legislación y normativa vigente.

- Implementar un esquema de niveles diferenciados de seguridad de autenticación, que permita asignar un nivel de autenticación específico a cada tipo de gestión

digital, en función de sus requisitos técnicos, legales y jurídicos. Esto incluye, entre otros, aquellos trámites que involucren actos con implicaciones legales o de disposición de derechos.

Conclusión: El Mecanismos de Autenticación implementado en la Plataforma de Ciudadanía Digital (v.2), basado en el esquema de un solo nivel máximo de autenticación basado en dos Factores (2FA), no garantiza el principio de Autenticidad, lo cual implica una debilidad en la seguridad de la información de la Plataforma de Ciudadanía Digital, cuyas consecuencias repercuten negativamente en los principios de Integridad y Confidencialidad. La ausencia de diferentes niveles de seguridad de autenticación, tal como recomienda el estándar NIST SP 800-63B, limita la capacidad del sistema para proteger adecuadamente los datos sensibles o confidenciales y garantizar que todas las acciones sean atribuibles con certeza al ciudadano correcto, al no evitar la posibilidad de suplantación de identidad en Gestiones Digitales con requisitos e implicaciones legales específicos. Así también, este esquema denota la falta de flexibilidad en situaciones donde este método puede ser insuficiente para Sistemas Clientes con requisitos e implicaciones legales críticas o excesivos para otros de menor riesgo.

b. La Disponibilidad del Mecanismo de Autenticación en función de la infraestructura tecnológica y controles definidos.

El principal hallazgo identificado al respecto es el siguiente:

- Existen deficiencias en los controles para la continuidad del servicio de autenticación en la plataforma de Ciudadanía Digital, comprometiendo su Disponibilidad.

En el informe constan dos (2) recomendaciones orientadas a fortalecer la Disponibilidad del Mecanismo de Autenticación en función de la infraestructura tecnológica y controles definidos.

R2. Realizar las acciones necesarias para asegurar la actualización y aprobación del Plan de Contingencias de acuerdo a *los "Lineamientos para la elaboración e Implementación de Planes de Contingencia Tecnológica en entidades del sector público",* especialmente en lo relacionado con:

- Identificar Procesos Críticos.
- Analizar Riesgos e Impactos.
- Establecer Protocolo de Comunicación.
- Realizar Pruebas y Revisiones del Plan.
- Definir Roles y Responsabilidades.
- Definir Tiempos de Restauración y Periodos de Pérdida de Datos.
- Definir Cronograma de Pruebas y Revisiones del Plan.

R3. Tomar las acciones necesarias para que su documento *"Políticas y Procedimientos de Copias de Respaldo de la AGETIC"* se encuentre en el marco de las Normas Básicas del Sistema de Organización Administrativa e implementar que la copia de respaldo sea almacenada en un lugar remoto o externo, según su propia Política y Procedimiento.

Conclusión: El plan de contingencia actual de AGETIC presenta deficiencias, como la falta de identificación de procesos críticos, análisis de riesgos, pruebas y protocolos de comunicación claros. Además, la ausencia de copias de seguridad remotas y la inactividad del centro de datos alterno aumentan la vulnerabilidad ante fallos catastróficos, lo que puede comprometer la Disponibilidad de los servicios, afectando la experiencia de los usuarios y la confianza en la Plataforma de Ciudadanía Digital.

Conclusión General:

La evaluación efectuada al Mecanismo de Autenticación de la Plataforma de Ciudadanía Digital (v.2) permitió identificar insuficiencias en la parte de la seguridad, que comprometen su Confiabilidad y la percepción de seguridad en sus operaciones.

El sistema actual utiliza únicamente autenticación de dos factores (2FA) sin una diferenciación según el nivel de riesgo de las transacciones. Esta práctica no está de acuerdo con las recomendaciones del estándar NIST SP 800-63B, lo que genera amenazas que afectan a los principios de Autenticidad, Integridad y Confidencialidad. Esta limitación incrementa la exposición a posibles ataques de suplantación de identidad en Gestiones Digitales con requisitos legales específicos y carece de flexibilidad para adaptarse a las diversas necesidades de los Sistemas Clientes.

Por otra parte, las deficiencias identificadas en el plan de contingencia agravan las vulnerabilidades de la plataforma, incluyendo la ausencia de análisis de riesgos adecuado, falta de copias de seguridad remotas e inactividad del centro de datos alterno, constituyen una riesgo a la Disponibilidad de los servicios, lo que podría resultar en interrupciones prolongadas que impacten negativamente en la confianza en la Plataforma de Ciudadanía Digital y los servicios que esta presta a la ciudadanía.

En conjunto, estos hallazgos destacan la necesidad de adoptar medidas correctivas en los aspectos técnicos y operativos, con el propósito de fortalecer la Confiabilidad, Integridad, Disponibilidad y Continuidad de los servicios ofrecidos por la Plataforma de Ciudadanía Digital, en especifico el Mecanismo de Autenticación.

--0--