DIGITO
FIRMA DIGITAL

ASPECTOS RELEVANTES DE AUDITORÍA EXTERNA - AÑO 2017

Objetivo

La presente auditoría externa regida por resolución N°1582 y sus normas reglamentarias, en conformidad a las resoluciones Ministeriales N° 1584, 1105/2015 ,501/2016 y 1430/2017, consistiendo principalmente en el estudio de los mecanismos de control que se encuentran implantados actualmente en el Cliente, determinando si los mismos son los adecuados y cumplen con los requisitos impartidos por el Ministerio de Industria y Comercio.

Tiene por objetivo principal verificar el cumplimiento de las normativas impartidas por el MIC analizando su infraestructura tecnológica, sus procesos de emisión y administración de firmas, y la legalidad de los documentos que la sustentan.

Alcance

La presente Auditoría ha sido realizada durante los días 01 de octubre al 15 de noviembre del 2017, abarco la revisión de las políticas y la infraestructura.

Equipo de Trabajo

El equipo de trabajo conformado por Digito son:

- **José Oricchio** (Director Ejecutivo, Miembro del Directorio)
- **Javier Dávalos** (Coordinador de Seguridad)
- **Pablo Aranda** (Jefe Comercial)
- **Roberto Fretes** (Oficial de Registro)
- **Luis González** (Gerente Administrativo)
- **Alejandro Cardozo** (Gerente de TI)

Actividades Realizadas

Se llevaron a cabo diversas pruebas y entrevistas con el personal designado por el cliente y se solicitaron evidencias que respalden sus procedimientos.

- Análisis de los documentos presentados por el auditado.
- Auditoría de los Data Centers principal y secundario.
- Tareas de relevamiento que incluyeron entrevistas con el personal de Digito afectado al área de Firma Digital.

Recomendaciones

- Incrementar la capacitación a los Agentes de Registros.
- Disponibilizar los materiales y procedimientos necesarios para que el Agente de Registro tenga la información necesaria para realizar sus tareas de acuerdo a lo estipulado en la norma.
- Establecer e implementar un mecanismo que permita monitorear de forma periódica el legajo del suscriptor y su alineación con su certificado digital correspondiente de forma detectar posibles errores en el menor tiempo posible.
- Establecer un procedimiento que permita garantizar que se mantenga actualizado la información del sitio web conforme a lo estipulado en el punto 2.2 de la *DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA PRÁCTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)*.
- Establecer e implementar un procedimiento que describa el detalle del sitio Web donde publicará la información, la tecnología utilizada, la disponibilidad, accesibilidad, conexión, esquemas, diagramas de funcionamiento y las medidas de seguridad implementadas para asegurar que solo personal autorizado pueda modificar el sitio a fin de proteger la integridad y disponibilidad de la información.
- Relación entre la evaluación de Riesgos y el Plan de Continuidad de Negocio y el Plan de Recuperación de Desastres.
- La implementación de un sistema de seguridad de la información SGSI coherente con su Política de Seguridad.

- Actualizar la Política de Certificación de Firma Digital Tipo F2 de la CA (PKIpy-DocSA-CPF2v1.0.0) específicamente el ítem 6.2.1 estableciendo como estándar el FIPS 140-2 nivel 2 o nivel 3 para este tipo de certificado.
- Implementar un mecanismo que permita registrar la operativa de los equipos que son sometidos a un proceso de mantenimiento o aquellos que ya no se utilizarán de forma permanente.
- Implementar una metodología formal de gerenciamiento de configuración para la instalación y el continuo mantenimiento de los niveles de configuración de seguridad.
- Implementar procedimiento formal de destrucción física de dispositivos electrónicos.
- Documentar las verificaciones de los mecanismos y procedimientos de emergencias cada 6 meses.
- Establecer e implementar un procedimiento de archivos de registros conforme a los requerimientos indicados.
- Establecer e implementar procedimiento para informar al titular sobre la aproximación de la fecha de caducidad de su certificado y prever el suministro de un nuevo certificado antes de la expiración del certificado a pedido del titular del certificado.
- Establecer un procedimiento para transferencia de guarda de los datos de registro y de archivo en caso de extinción del PSC.
- Adecuar la plataforma PKI de forma que quede registro que relacione el proceso de validación del Agente de Registro que se encuentran fuera del ambiente físico de la RA con el equipo utilizado.
- Establecer e implementar un procedimiento de acceso a datos privados que contenga las responsabilidades consignadas al personal del PSC y la forma de presentación para una autorización de liberación de información privada.
- Se empleen personal calificado para el desempeño de las funciones técnicas y profesionales que exigen los servicios de firma digital, los

mismos deben ser sometidos regularmente a capacitaciones acerca de prácticas de seguridad de acuerdo a su cargo o función.

- Establecer un documento interno relacionado a las sanciones posibles a aplicarse por acciones no autorizadas del personal con roles de confianza determinados.
- Toda documentación suministrada al personal cuente con las revisiones y actualizaciones necesarias.

Conclusiones

La ejecución de la auditoría contó en términos generales con la disponibilidad y entrega de información requerida por parte de cada responsable de las áreas de Sistemas, Recursos Humanos, Comercial, Administración, y de Seguridad.

De la evaluación realizada y de los documentos presentados por la empresa se concluye que Documenta S.A. desarrolló e instaló la plataforma necesaria y elaboró políticas, planes y procedimientos exigidos por el Ministerio de Industria y Comercio.

A partir de la auditoría realizada se concluye que Digito mantiene un nivel adecuado del servicio de certificación digital, sin embargo se resalta que se han detectado algunas no conformidades que deberán ser subsanadas para la siguiente auditoría.

Diego Altamirano

Auditor - Leader