code100

SERVICIOS DE CERTIFICACIÓN DIGITAL

Aspectos Relevantes Auditoria Externa

Diciembre 2017.

Ver 1.0

At: Pablo Casal

Introducción:

El presente documento tiene por objeto resumir los Aspectos más relevantes de las tareas realizadas en la Auditoria Externa en el periodo de Diciembre del 2017.

I. *MARCO INTRODUCTORIO*

La Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE) dependiente del Ministerio de Industria y Comercio (MIC) se constituye en la Autoridad Certificadora Raíz en el marco de la infraestructura de Claves Publicas de la República del Paraguay, creada por la Ley de Firma Digital N° 4017/2010. Entre sus atribuciones como Autoridad de Aplicación establece aprobar el sistema de auditoria al que deben someterse los Prestadores de Servicios de Certificación (PSC).

En cumplimiento a lo dispuesto en el párrafo anterior el MIC requiere que sean publicados los aspectos más relevantes resultantes de la auditoria externa en el repositorio público del PSC CODE100 S. A.

II. *OBJETIVO*

La presente auditoria en conformidad a las resoluciones Ministeriales N° 1584, 1105/2015 ,501/2016 y 1430/2017 tuvo como objetivo principal determinar el efectivo cumplimiento de las normas vigentes impartidas por el MIC y lo establecido en los documentos elaborados por la firma CODE100 y que fueran utilizados como base para la presente auditoria, analizando su infraestructura tecnológica y la legalidad de los documentos que la sustentan.

III. ALCANCE

La presente Auditoria ha sido realizada durante los días 01 de Diciembre al 28 de Diciembre del 2017, abarco la revisión de la funcionalidad y de los controles implementados en el sitio principal de la AC CODE100 , en su servicio de publicación del sitio de contingencia , de sus políticas, procedimientos.

IV. EQUIPO DE TRABAJO

Estuvieron presente y participaron l equipo de trabajo conformado por Code100 fueron:

- **Pablo Casal** (Gerente de Sistemas)
- **Ignacio Balzaretti**(Técnico Especialista)
- **Eduardo Silnik** (Técnico Especialista)

V. ACTIVIDADES REALIZADAS

El equipo auditor concurrió a la empresa CODE100 a fin de proceder con la auditoria, donde se llevaron a cabo diversas pruebas y entrevistas con el personal designado por Code100, realizando la revisión de la documentación presentada por la empresa como así también la inspección de la infraestructura de sus Data Centers, se solicitaron evidencias que respalden sus procedimientos.

- Se analizaron los documentos presentados por el auditado.
- Se efectuaron tareas de relevamiento que incluyeron entrevistas con el personal de Code100 afectado al área de Firma Digital.
- Seguridad Física de la AC.
- Seguridad Física del Sitio de Contingencia.
- Revisión de Registros de Auditoria.
- Configuración de los Firewalls.
- Plan de Contingencia.
- Protección de Recursos Sensibles.
- Plan de Seguridad.

VI. OBSERVACIONES DETECTADAS Y REOMENDACIONES

Observación 1: Se observa que el punto 7.1.5 Restricciones de nombre de la CP Tipo F1 y de la CP tipo F2 de CODE 100 S. A. no está alineado a lo establecido en la resolución 1400/2016 anexo II en el párrafo 2 que indica que los nombres deberán ser escritos en mayúsculas. Ya que en las CP de CODE100 establecen que los nombres se escriben en mayúsculas y sin tildes, únicamente se acepta el carácter "Ñ" como un caso especial para los nombres de personas físicas y jurídicas. Esto podría ocasionar errores en el perfil de los certificados emitidos. De los certificados revisados se visualizaron certificados con nombre del suscriptor que contenía diéresis o acento sin embargo el documento cédula de identidad no permite acentos.

Observación 2: Entre los certificados emitidos se observó que hubo un caso en que hubo 2 certificados válidos para un mismo suscriptor. El error fue subsanado revocando el certificado minutos después de haberse emitido el segundo certificado.

Observación 3: Se observó que existen certificados emitidos a personas jurídicas cuya representación legal está dada por más de una persona física sin embargo el acuerdo de suscriptores está firmado por uno solo de ellos.

Observación 4: Se observa que el punto 4.9.7 Frecuencia de emisión de la CRL de la CP Tipo F1 y de la CP tipo F2 de CODE 100 S. A. no está alineado a lo establecido en la resolución 1400/2016 anexo I en cuanto al apartado que indica que la CRL debe actualizarse y publicarse inmediatamente cuando surja una revocación con una frecuencia de emisión máxima permitida de 12 (doce) horas para la CRL referente a los usuarios finales. Se verificó que la CRL es generada cada 1 hora por el sistema pero con una validez de 24 horas.

Observación 5: Se verificó que NO son publicadas por el PSC en su servicio de repositorio la resolución del MIC N° 1431/13.

Observación 6: No se entregó información respaldaría que evidencie los controles y las eventuales restricciones para el acceso, lectura y escritura de las informaciones publicadas por el PSC.

Observación 7: No se entregó información respaldaría que indique en los archivos de auditoria evidencia de operaciones de escritura del repositorio de CODE 100 S.A.

Observación 8: No se evidencia una relación entre la Evaluación de Riesgo y el Plan de Continuidad de Negocio y el Plan de Recuperación de Desastre.

Observación 9: No se evidencia un procedimiento de verificación, revisión y evaluación periódica la continuidad de la seguridad de la información.

Observación 10: Se observa que el punto 6.6.4 Controles en la Generación de CRL de la CPS v2 de CODE 100 S. A. no está alineado a lo establecido en la resolución 1400/2016 anexo I en lo que refiere a que la CPS no establece que antes de su publicación, todas las CRL generadas por el PSC, debe ser comprobada la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de CRL, la fecha / hora de emisión y otra informaciones relevantes. Tampoco se entregó un procedimiento de control de generación de CRL.

Observación 11: En el Data Center principal como la contingencia no se evidencio un sistema de protección contra rayos.

Observación 12: El resguardo de las cintas del sistema de video de vigilancia no cumple con en el periodo de un año, siendo el periodo de 6 meses en el Data Center Principal y de 3 meses en el Data Center de Contingencia.

Observación 13: No se evidencio que las cintas de videos son testeadas por lo menos cada 3 meses y de manera aleatoria.

Observación 14: No se evidencia que los mecanismos y procedimientos de emergencias no son verificados semestralmente.

Observación 15: En el Data Center de Principal como en el Contingencia no existen registros que los cables son inspeccionado mínimo cada 6 meses.

Observación 16: No Disponen de un procedimiento formal para la eliminación de dispositivos electrónicos medios de almacenamientos pero no se registraron eventos.

Observación 17: Se recomienda adoptar los procedimientos para generar copias de seguridad de los registros de auditoría como establece la Resolución 1400/2016 anexo 1 en el ítem 5.4.5.

Observación 18: No se verifica la existencia de un procedimiento de protección de archivos.

Observación 19: No se describen detalladamente los procedimientos para la obtención y verificación de las informaciones de archivo como se establece en la Resolución 1400/2016 anexo 1 en el ítem 5.5.7.

Observación 20: No se describen los procedimientos para el suministro de un nuevo certificado, antes de la expiración de certificado a pedido del titular del certificado.

Observación 21: Se observa que el punto 3 IDENTIFICACIÓN Y AUTENTICACIÓN de la CPS v2 de CODE 100 S. A. no se encuentra alineado a lo establecido en la resolución 1400/2016 anexo I en lo que se refiere la obligación de la CPS de describir en detalle, los requisitos y procedimientos utilizados por las RA vinculadas al PSC responsable de llevar a cabo los procesos que se citan en el punto 3 de la resolución 1400/2016 anexo I.

Observación 22: Se observa que el punto 5.2.1 Roles de Confianza de la CPS v2, CP F1 V1 Y CP V2 de CODE 100 S. A. no está alineado a lo establecido en la resolución 1400/2016 anexo I y anexo II en lo que se refiere cuando el empleado es desvinculado del PSC sus permisos son revocados inmediatamente?, no se encuentra mencionada en la CPS, adicionalmente no se encontró información respaldatoria que avale dicha acción.

Observación 23: Se verifica que en el Documento Gestión de Recursos Humanos versión 1.1.1, no se contempla en el apartado Reclutamiento y Selección, la verificación y confirmación de empleos anteriores así como tampoco las referencias profesionales de los candidatos.

Observación 24: En cuanto a los requerimientos de capacitación, no se encontraron evidencias de capacitación acerca de Principios y Mecanismos de Seguridad del PSC y de las RA vinculadas; así como tampoco acerca de los Procedimientos de Recuperación de Desastres y Continuidad del Negocio.

Observación 25: En cuanto a las sanciones por acciones no autorizadas se verifica que en el documento Reglamento Interno versión 1.0 no se hace distinción de sanciones para cada rol.

Observación 26: Se verifica que no se cuenta con procedimiento detallado acerca de las acciones a seguir para implementar sanciones y principalmente los tipos de sanciones que pueden aplicarse como establece las directivas del MIC.

Observación 27: La documentación proporcionada o compartida con todo el personal no se encuentra actualizada y/o revisada recientemente. Ej. El PCN y el PS.

VII. CONCLUSIONES

De la evaluación realizada de los requerimientos establecidos y de la documentación presentada por la empresa se concluye que el PSC CODE100 cumple con los requerimientos principales establecido en la norma para operar de forma adecuada como Prestador de Servicios de Certificación Las observaciones pendientes de cumplimiento requiere de una pronta subsanación a fin de brindar un óptimo servicio de Certificación digital para firmas Digitales.

MATIAS
GRESEONOMCE
DNI 33597232