INFORME TECNICO A LA PLATAFORMA ICP DE LA OFICINA PRESIDENCIAL DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN, (OPTIC) 2020

Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital

Departamento de Firma Digital

6 de agosto del 2020

Equipo de Auditores

Ing. José Raúl Madera Oropeza
Lic. Richard Nixon Sarmiento Rosario

Introducción

Según el Artículo 56 de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digital, el INDOTEL podrá realizar auditorías ordinarias anuales para asegurar el correcto funcionamiento y la eficiente prestación del servicio de Certificación Digital a las Entidades de Certificación (CA) del país. En este caso, procedemos a la auditoria anual correspondiente al 2019 de la Oficina Presidencial de Tecnología de la Información y Comunicación, (OPTIC) autorizada a operar como Entidad de Certificación (CA), mediante la Resolución del Consejo Directivo No. 024-18 de fecha 6 de junio de 2018.

Base de los resultados

Los criterios de auditoria se basan en la Norma Complementaria Por La Que Se Establece La Equivalencia Regulatoria Del Sistema Dominicano De Infraestructuras De Clave Publicas Y De Confianza Con Los Marcos Regulatorios Internacionales De Servicios De Confianza, la norma ETSI EN 319 401 V2.2.1 Sobre Requisitos Generales de Políticas para Proveedores de Servicios de Confianza y la Norma ETSI EN 319 411-2 son los requisitos de políticas y seguridad para los proveedores de servicios de confianza que emiten certificados, ETSI EN 319 412-1,2,3 y 5), Sobre Perfiles de los Certificados entre los que figuran: emitidos a personas naturales, a personas jurídicas o legal y los Certificados para el control de calidad, Las recomendaciones de la norma técnica ETSI EN 319 401 y ETSI EN 319 411-1, Tienen como objetivo cumplir con los requisitos generales de la comunidad internacional con la finalidad de proporcional confianza en las transacciones electrónicas.

Alcance

Se verificaron los procesos de:

- Conexión segura de la Entidad de Certificación;
- Segregación de funciones administrativas en la plataforma de la Entidad de Certificación;
- Segmentación de logs, evidencias y registros de acciones;
- Procedimientos para el manejo de datos personales del suscriptor;
- Confidencialidad por parte del personal registrador;
- Procedimientos de acreditación de identidad del suscriptor, vía física y remota.; y

Procesos de registros y gestión del ciclo de vida de los distintos tipos de Certificados Digitales de la Entidad de Certificación de la Oficina Presidencial de Tecnología de la Información y Comunicación, OPTIC

Plan de Auditoria

Fecha/Hora	Auditor	Área/Función/Proceso/Actividad	Auditado	Entorno
6/8/20 10:00am 10:30am	José Raúl Madera Richard Sarmiento	Reunión Apertura	Encargados de áreas	Remoto
6/8/20 10:30am 11:30am	Richard Sarmiento	Análisis Información Documentada	Encargado Proyecto	Remoto
6/8/20 1:00pm 1:30pm	Richard Sarmiento	Análisis de vulnerabilidad al portal donde se alojan los distintos formularios de RA	Encargado de seguridad	Remoto
6/8/20 1:30pm 2:00pm	José Raúl Madera	Conocimiento de esquema operativo y de seguridad lógica	Encargado de seguridad	
6/8/20 2:00pm 3:00pm	Richard Sarmiento	Verificación de proceso de la generación de los Certificados Digitales.	Gerente de Cuentas Corporativas	Remoto
6/8/20 3:30pm 4:30pm	José Raúl Madera Richard Sarmiento	Reunión Cierre Auditoria (vía Videoconferencia)	Gerente General	Remoto

Participantes Reunión de Apertura

Ing. Charlis Polanco.
Licda. Estefany Genao.
Señor. George Bueno.
Ing. José Raúl Madera.
Lic. Richard Sarmiento.

Lista de Personal Entrevistado

Ing. Charlis Polanco.
Licda. Estefany Genao.
Señor. George Bueno.

Participantes Reunión de Cierre

Ing. Charlis Polanco.
Licda. Estefany Genao.
Señor. George Bueno.
Ing. José Raúl Madera.
Lic. Richard Sarmiento.

Resumen de la auditoría

En fecha 6 de agosto del 2020, por vías telemáticas se dio inicio a las acciones correspondientes al Plan de auditoria programado, con el objetivo de verificar todo el cumplimiento requerido por la normativa. Se inició el proceso de verificación documental sobre Manual de Procedimiento, Planes de Contingencia, Continuidad de Negocio, Cese de Actividades, contratos con terceros sobre Infraestructuras como servicios y servicios de colocación, además de las Políticas de Seguridad y Protección de Datos. Se procedió a analizar dicha información documentada con respecto a los criterios exigidos en las Normas

El sistema analizado corresponde a la aplicación web utilizada para realizar el registro, la identificación del suscriptor y la gestión de los Certificados Digitales, El sistema analizado corresponde al propio módulo operativo de registro, emisión y gestión de los Certificados Digitales, el cual pertenece a la Entidad de Certificación de la Oficina Presidencial de Tecnología de la Información y Comunicación. Dicho módulo trabaja en un ambiente web y funciona como ventanilla de trabajo entre la Unidad de Registro y la Entidad de Certificación.
La herramienta que se utiliza en la actualidad es proporcionada por la CA, viafirma Fortress, esta unidad se utiliza para custodiar las claves privadas de los suscriptores.

En adición, se ejecutó la herramienta **OWASP ZAP**, al portal web de la RA, para el análisis de vulnerabilidades web al módulo de registro, la misma evidenció la existencia de una (X) alerta de medio impacto, cinco (X) alertas de bajo impacto y dos (X) alertas informativas, las últimas dos alertas no se detallan en este informe por el hecho de esta no representan un peligro a dicho modulo, los demás hallazgos se detallan de la siguiente manera:

Resumen de alertas:

Cabe destacar que dentro de las alertas encontradas durante el análisis cuatro (4) de ellas se replican, dentro del rango de las alertas medias y alertas bajas y por ellos solo se registraran en este informe seis (6), las mismas se detallan más adelante.

Las alertas de medio impacto:

Es una alerta media que consiste en el ID de sesión en reescritura de URL y se utiliza para rastrear la identificación de la sesión del usuario. Esto quiere decir que la información del usuario puede ser divulgada a través del encabezado de referencia del sitio cruzado. También el ID del usuario podría ser almacenado en el historial del navegador o en los registro del servidor.
Alerta media: Se encontró un hipervínculo que apuntan a otro nombre de host. A medida que se utiliza la

reescritura de URL del ID de la sesión, puede divulgarse en el encabezado de referencia a hosts externos.
Alerta media: el encabezado X-frame-options no se encuentra establecido en la respuesta HTTP para proteger ante ataques "ClickJacking" (es una técnica maliciosa para engañar a usuario de internet con la finalidad de revelar información confidencial o de tomar control de su ordenador).
Alerta baja: la protección del buscador web XSS no está disponible o habilitada por la configuración de la cabecera de respuesta de HTTP X-XSS-Protection" en el servidor web.
Alerta baja: el cache-control y encabezado HTTP Pragma no sea establecido apropiadamente o falta determinarlo al navegador y a los servidores proxy que se encuentran conectados a dicho contenido.
La protección del buscador web XSS no está disponible o esta deshabilitada por la configuración de la cabecera de respuesta de HTTP "X-XSS-Protection" en el servidor web.

Recomendaciones

En cuanto a las alertas descubiertas por la herramienta OWASPZAP para análisis de vulnerabilidades web; se remiten las siguientes consideraciones:

1. Alerta media, para el contenido seguro, coloque el ID de sesión en una cookie y para estar más seguro considere usar una combinación de cookies y reescritura de URL.
2. Alerta media, esto podría ser un riesgo si el ID de sesión es sensible y el hipervínculo se refiere a un host externo o de un tercero. Para el contenido seguro coloque el ID de sesión en la cookies de sesión segura.
3. Alerta media, Los navegadores de web más modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
4. Alerta baja, Asegúrese que el filtro XSS del navegador web este habilitado, estableciendo el encabezado de respuesta HTTP X-XSS-Protection en '1'.
   Nota: El encabezado de respuesta HTTP X-XSS-Protection le permite al servidor web habilitar o deshabilitar el mecanismo de protección del navegador web XSS.
5. Alerta baja, Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
6. Alerta baja, Asegúrese que el filtro XSS del navegador web está habilitado, estableciendo el encabezado de respuesta HTTP X-XSS-Protection en '1'.

Resumen

Luego de agotar todos los procesos existentes, con la excepción de las situaciones encontradas indicadas en el cuadro anterior, se evidenció que la Oficina Presidencial de Tecnología de la Información y Comunicación, (OPTIC), ha cumplido de manera satisfactoria con los demás requerimientos que esta verificación exige, incluyendo el resultado satisfactorio del primer control de vulnerabilidades ejecutado para el 2020, demostrando que la mayoría de sus procedimientos están siendo llevados de forma correcta y de acuerdo a lo establecido en la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firma Digital,

su Reglamento de Aplicación y Normas Complementarias.