INFORME SOBRE LA AUDITORIA A LA PKI DE LA ENTIDAD DE CERTIFICACION CAMARA DE COMERCIO Y PRODUCCION DE SANTO DOMINGO

2020

DIRECCIÓN DE CIBERSEGURIDAD, COMERCIO ELECTRONICO Y FIRMA DIGITAL

11/03/2020

Equipo de Auditores

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

Introducción

Según el Artículo 56 de la Ley Núm. 126-02 sobre Comercio Electrónico, Documento 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 2018 a la Cámara de Comercio y Producción de Santo Domingo (CCPSD) autorizada a operar como Entidad de Certificación (CA), mediante la Resolución del Consejo Directivo Núm. 169-07 de fecha 23 de agosto de 2007.

Base de los resultados

La presente auditoría se realizó basándonos 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 contiene los requisitos de política general para proveedores de servicios de confianza, esta norma es un requisito para los Organismos de Evaluación de Conformidad que evalúan proveedores de servicios de confianza y la Norma ETSI EN 319 411-1 contiene los requisitos de políticas y seguridad para los proveedores de servicios de confianza que emiten certificados. La misma nos muestra una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. Las normas técnicas fueron redactadas intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ETSI EN 319 401 y ETSI EN 319 411-1 son de forma Neutrales.

Alcance

Esta auditoria incluye todos los controles específicos sobre Infraestructura de Clave Pública (PKI) que comprenden los temas de seguridad informática, seguridad de la información, controles criptográficos y ciclo de vida de los Certificados Digitales, según la normativa vigente en la República Dominicana para las Entidades de Certificaciones.

Plan de Auditoria

Fecha/Hora	Auditor	Área/Función/Proceso/Actividad	Auditado	Lugar
11/03/20 10:00 am	José Raúl Madera	Llegada a organización		Oficina Principal SD
11/03/20 10:15 am 10:30 am	José Raúl Madera	Reunión Apertura	Encargados de áreas	Oficina Principal SD
11/03/20 10:30 am	José Raúl Madera	Análisis Información Documentada		Oficina Principal SD

11:00 am				
11/03/20 11:00 am 11:30 am	Richard Sarmiento	Entrevista/Auditoria procesos de Recursos Humanos/Comunicación Interna	Encargado Recursos Humanos	Oficina Principal SD
11/03/20 11:30 am 12:00 am	José Raúl Madera	Verificación controles técnicos de seguridad física y lógica	Sub-gerente de Seguridad Lógica y Redes/Encargado seguridad Informática	Oficina Principal SD
11/03/20 12:00 am 12:30 am	José Raúl Madera Richard Sarmiento	Almuerzo		Oficina Principal SD
11/03/20 12:30 am 1:00 pm	José Raúl Madera	Verificación ciclo seguro de vida del software	Enc. Desarrollo de Sistemas y Aplicaciones	Oficina Principal SD
11/03/20 1:00pm 1:30pm	José Raúl Madera	Pruebas y Análisis de vulnerabilidades internas/externas	Sub-gerente de Seguridad Lógica y Redes/Encargado seguridad Informática	Oficina Principal SD
11/03/20 1:30 pm 2:00 pm	Richard Sarmiento	Pruebas y Análisis del plan de contingencia y continuidad de negocio	Sub-gerente de Seguridad Lógica y Redes/Encargado seguridad Informática	Oficina Principal SD
12/03/20 9:00 am 10:00 am (GMT-4)	José Raúl Madera Richard Sarmiento Cesar Moline	Reunión Cierre Auditoria (vía videoconferencia)		Oficina Principal SD

Participantes Reunión de Apertura
Lic. Ivan Santana Duval
Ing. Gustavo Díaz

Participantes Reunión de Cierre
Lic. Ivan Santana Duval
Ing. Gustavo Díaz

Lista de Personal Entrevistado
Lic. Ivan Santana Duval
Lic. Yojanny reyes de la Rosa
Ing. José Luis Guzmán
Lic. Bárbara Ramírez

Resumen de la auditoría

En fecha 11 de marzo de 2020, en las instalaciones de la **CCPSD**, sito en la Av. 27 de febrero, Núm. 228, Torre Friusa, La Esperilla de esta Ciudad de Santo Domingo, Distrito Nacional, República Dominicana, 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 servicio y servicios de colocación, además de las Políticas de Seguridad y Protección de Datos.

En ese sentido, se procedió a analizar dicha información documentada con respecto a los criterios exigidos en las normas complementarias sobre Procedimientos de Seguridad, Estándares Tecnológicos, Protección de Datos, Políticas y Procedimientos de Certificación, entre otros.

Se verificó el entorno físico operativo que sirve como recepción de suscriptores para los procesos de acreditación y emisión de Certificados Digitales y el ambiente físico operativo de la CCPSD. Se entrevistaron los responsables en el manejo de la PKI, los señores Gustavo Díaz (Sub-gerente de Seguridad Lógica y Redes) e Ivan José Santana Duval (Oficial de Soluciones Digitales).

Se revisaron los componentes y controles técnicos requeridos por la normativa vigente de acuerdo a los temas sobre la Política de Seguridad Institucional, Organización de la Seguridad, Clasificación y Control de Activos, Seguridad del Personal, Seguridad Física y Ambiental, Gestión de Comunicaciones y Operaciones, Control de Accesos, Desarrollo y Mantenimiento de Sistemas, Administración de la Continuidad del Negocio, puntualizando las revisiones en las áreas de TI, Gestión Humana, Operaciones y Seguridad Física de la empresa.

En adición se ejecutó una herramienta de análisis de vulnerabilidades web al módulo de registro, llamada Owasp-zap, el cual descubrió la existencia de catorce (14) vulnerabilidades catalogada de medio y bajo impacto, las mismas se detallan en este informe.

Sumario de Hallazgo y Observaciones

Dentro de los hallazgos y observaciones encontradas se citan:

Objeto de Control	Situación Encontrada	Recomendaciones	Norma, Numeral e Inciso
Relaciones con suministradores o proveedores	Se observó la falta de políticas de seguridad de la información para suministradores o proveedores	Incluir las políticas de seguridad de la información en las relaciones con los proveedores	Núm. 15/15.1.1 hasta 15.1.3 de la ISO27001 Relaciones con proveedores.
Controles Criptográficos	No cuentan con políticas de uso de los controles criptográficos	Deben desarrollar e implementar políticas sobre el uso de los controles criptográficos para proteger la información.	Núm. 10/10.1.1 hasta 10.1.2 Criptografía y Gestión de clave.
Seguridad de equipos	Se observó que en el DC, tienen algunos gabinetes abiertos y en cuanto al cableado se encuentra desorganizado.	Se recomienda una rápida mejora del cableado del Data Center que se encuentra dentro de la CCPSD, actualización de los distintos shwich	Oportunidad de mejora
Segregación en red	Se comprobó que la red de producción no se encuentra segmentada, en la actualidad es una sola red para todos los empleados.	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	Num. 13.1.3, Gestión de seguridad de red.

Tabla 1: Acciones Correctivas/om

Reporte de vulnerabilidad herramienta Owasp-Zap

Dentro de las alertas encontradas durante el análisis, cincos (5) de ellas se replican

dentro del rango de las alertas bajas y por eso solo se registraran en este informe nueves (9) alertas de medio y bajo impacto:

Resumen de alertas

Nivel de riesgo	Numero de Alertas
Alto	0
Medio	2
Bajo	12

Nivel de alerta: Media
ID de alerta: encabezado X-Frame-Option no se encuentra establecido

Detalles/Descripción Hallazgo	Solución/Recomendaciones
El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.	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).

Nivel de alerta: Media
ID de alerta: Mala configuración entre dominios

Detalles/Descripción Hallazgo	Solución/Recomendaciones
La carga de datos del navegador web puede ser posible, debido a una configuración incorrecta de intercambio de recursos de origen cruzado (CORS) en el servidor web	Asegúrese de que los datos confidenciales no estén disponibles de manera no autenticada (usando la lista blanca de direcciones IP, por ejemplo). Configure el encabezado HTTP "Access-Control-Allow-Origin" en un conjunto de dominios más restrictivo, o elimine todos los encabezados CORS por completo, para permitir que el navegador web aplique la Política del mismo origen (SOP) de una manera más restrictiva.

Nivel de alerta: Baja
ID de alerta: Cookie No HttpOnly Flag

Detalles/Descripción Hallazgo	Solución/Recomendaciones
Se ha establecido una cookie sin la bandera HttpOnly, lo que significa que la cookie puede ser accedida mediante JavaScript. Si un script malicioso puede ser ejecutado en esta página entonces la cookie será accesible y podrá ser transmitida a otro sitio. Si esta es una cookie de sesión entonces el secuestro de sesión podría ser posible.	Asegúrese que la bandera HttpOnly está establecida para todas las cookies.

Nivel de alerta: Baja
ID de alerta: Cookie sin atributo SameSite

Detalles/Descripción Hallazgo	Solución/Recomendaciones

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud 'entre sitios'. El atributo SameSite es una contramedida efectiva para la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y ataques de tiempo.	Asegúrese que la bandera HttpOnly está establecida para todas las cookies.

Nivel de alerta: Baja
ID de alerta: Incompleto o no Cache-control y sistema de encabezado HTTP Pragma

Detalles/Descripción Hallazgo	Solución/Recomendaciones
El cache-control y encabezado HTTP Pragma no ha sido establecido apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.	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.

Nivel de alerta: Baja
ID de alerta: Cookie sin bandera asegurada

Detalles/Descripción Hallazgo	Solución/Recomendaciones
Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.	Cuando una cookie contiene información sensible o es un token de sesión, debería ser siempre pasada usando un canal cifrado. Asegúrese que la bandera asegurada está establecida para cookies conteniendo información sensible.

Nivel de alerta: Baja
ID de alerta: Ausencia de tokens anti-CSRF

Detalles/Descripción Hallazgo	Solución/Recomendaciones
No se encontraron tokens Anti-CSRF en un formulario de envío HTML. Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible. La naturaleza del ataque es que CSRG explota la confianza que un sitio web proporciona a un usuario. Por el contrario, las cadenas de comandos de los sitios cruzados (XSS) explotan la confianza que un usuario proporciona en un sitio web. Al igual que XSS, los ataques CSRG no son de forma necesaria de sitios cruzados, pero hay la posibilidad de que si pueden serlo	Utilice una biblioteca o marco comprobado que no acepte que suceda esta debilidad o que proporcione construcciones que permitan que esta debilidad sea más sencilla de evitar. Por ejemplo, utilice el paquete anti-CSRG como el CSRGuard de una herramienta de vulnerabilidad que desee. Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante. Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS. Identificar las operaciones que sean especialmente peligrosas. Cuando el usuario desarrolla una operación peligrosa, envíe una solicitud de confirmación de forma separada para poder garantizar que el usuario tenga la intención de desarrollar esa operación.

Nivel de alerta: Baja
ID de alerta: No se encuentra encabezado X-Content-Type-Options Header

Detalles/Descripción Hallazgo	Solución/Recomendaciones
El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web compatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.

Nivel de alerta: Baja
ID de alerta: Inclusión de archivos de origen JavaScript Cross-Domain

Detalles/Descripción Hallazgo	Solución/Recomendaciones
Las páginas incluyen uno o más archivos encriptados de un dominio de terceros.	Asegúrese que los archivos de la fuente JavaScript están descargados solo de sus fuentes confiables, y las fuentes no pueden ser controladas por los usuarios finales de la aplicación.

Resumen

Luego de agotar todos los procesos existentes, con la excepción de las situaciones encontradas indicadas en los cuadro anteriores, y de la cual se requiere la realización de una acción correctiva dentro de las primeras seis (6) semanas de recibir este informe para el hallazgo sobre la falta de "segregación en la red de producción y/o de empleados", **se evidenció que la Cámara de Comercio y Producción de Santo Domingo, Inc., ha cumplido de manera satisfactoria con los demás requerimientos que esta auditoría exige, incluyendo el resultado del primer control de vulnerabilidades ejecutado para el 2019, demostrando que sus procedimientos están siendo llevados de forma correcta y de acuerdo a lo establecido en la Ley Núm. 126-02 sobre Comercio Electrónico, Documentos y Firma Digital, su Reglamento de Aplicación y Normas Complementarias**.