
# INFORME AUDITORIA INFRAESTRUCTURA DE CLAVE PÚBLICA AL PROVEEDOR DE SERVICIO DE CONFIANZA LLEIDANET DOMINICANA, SRL. 2020

Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital

Departamento de Firma Digital

27 de julio del 2020

## Equipo de Auditores

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

## Introducción

En fecha 20 de julio del 2020 fue recibida en el Instituto Dominicano de las Telecomunicaciones (INDOTEL) la comunicación identificada con el Núm. 204138, mediante la cual la **Empresa Lleidanet Dominicana SRL** solicita autorización para operar como Proveedores de Servicios de Confianza conforme a lo dispuesto en la Ley Núm. 126-02 sobre Comercio Electrónico, Documento y Firmas Digital, su Reglamento de Aplicación y Normas Complementarias.

Según el Artículo 56 de la Ley Núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales y el Artículo 23 del Reglamento de Aplicación, Decreto 335-03, el INDOTEL está facultado a realizar procedimientos de autorización sobre la prestación de servicios de Certificación Digital, los cuales incluyen la realización de auditorías iniciales para asegurar el correcto funcionamiento y la eficiente prestación del servicio a las Entidades de Certificación (CA), Unidades de Registro y Proveedores de Servicios de Firma Electrónica que quieran operar en la República Dominicana.

Este documento trata sobre la auditoria inicial realizada el 27 de julio del 2020 ha Lleidanet Dominicana SRL, para operar como Proveedor de Servicio sujeto a la prestación de servicios de Entrega Electrónica Certificada y Firmas Electrónicas Avanzadas.

## 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 319 521 V1.1.1 sobre Requisitos de Política y Seguridad para Proveedores de Servicios de Entrega Electrónica Certificada.

## Alcance

Se verificó toda la información documentada relativa a políticas, planes, certificaciones y seguridad de la empresa, analizando y observando procesos de:

- Segregación de funciones administrativas, Segmentación de logs, y registros de acciones en la plataforma ¨Lleidanet Advanced Electronic Signature Services / Click&Sign¨;
- Infraestructura del servicio;
- Procedimientos para el manejo de datos personales del suscriptor;
- Confidencialidad por parte del personal registrador;
- Procedimientos de acreditación de identidad del suscriptor vía remota sobre la plataforma ¨eKYC¨; y
- Reconocimiento de acreditaciones cualificadas según Res. 071-19.
- Escáner al website donde se alojan los formularios y se adjuntan los documentos exigidos por el prestador de servicio de firma electrónica.

## Plan de Auditoria

| Fecha/Hora | Auditor | Área/Función/Proceso/Actividad | Auditado | **Entorno** |
|---|---|---|---|---|
| 27/7/20<br>10:00am<br>10:30am | José Raúl Madera<br>Richard Sarmiento | Reunión Apertura | Encargados de áreas | Remoto |
| 27/7/20<br>10:30am<br>11:30am | Richard Sarmiento | Análisis Información Documentada | Encargado Proyecto | Remoto |
| 27/7/20<br>1:00pm<br>1:30pm | Richard Sarmiento | Análisis operacional de plataforma para Firmas Electrónicas Avanzadas | Encargado de seguridad | Remoto |
| 1:30pm<br>2:00pm | José Raúl Madera | Conocimiento de esquema operativo y de seguridad | Encargado de seguridad | |
| 27/7/20<br>2:00pm<br>3:00pm | Richard Sarmiento | Verificación acreditaciones según Res. 071-19 | Gerente de Cuentas Corporativas | Remoto |
| 27/7/20<br>3:30pm<br>4:30pm | José Raúl Madera<br>Richard Sarmiento | Reunión Cierre Auditoria (vía Videoconferencia) | Gerente General | Remoto |

## Participantes Reunión de Apertura

Pablo Gracia
Oscar Andrés Carrillo
Alan Muñoz
Gloria Salvador
Aryanne Alves
Cesar Moline
José Raúl Madera Oropeza.
Richard Sarmiento.

## Lista de Personal Entrevistado

Pablo Gracia
Gloria Salvador
Aryanne Alves

## Participantes Reunión de Cierre

Pablo Gracia
Gloria Salvador
Aryanne Alves

## Resumen de la auditoría

En fecha 10 de julio del 2020, por medio de 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.

Los sistemas analizados corresponden a las plataformas tecnológicas relacionadas a la prestación de los servicios de Entrega Electrónica Certificada y Firmas Electrónicas Avanzadas. Fueron evaluados los controles de seguridad de dichos entornos operativos, los procedimientos para la generación de las evidencias requeridas sobre la certificación de una entrega electrónica de una comunicación vía correo electrónico, los procedimientos de seguridad asociados a la identificación de los suscriptores que utilizaran Firmas Electrónicas Avanzadas y los métodos de autenticación y comprobación utilizados en la aplicación móvil basados en OTP vía SMS y correo electrónico.

Dentro de los procedimientos de análisis de la información documentada se pudo comprobar el cumplimiento de los requisitos asociados a la Política de Seguridad, Plan de Cese de Actividades, Política de Privacidad, Plan de Continuidad de Negocio y las prácticas para la prestación de servicios de confianza.

A su vez, fueron evaluadas y comprobadas las certificaciones que posee la casa matriz Lleidanetworks Serveis Telematics S.A. en ISO27001:2013 por la casa de certificación BSI, la certificación como Prestador Cualificado de Servicios de Entrega Electrónica de Confianza emitida por el Organismo Evaluador de la Conformidad CERTICAR, S.L., y la certificación para prestar servicios de Firmas Electrónicas Avanzadas por TCAB, pudiendo validar las vigencias y reconocer dichas certificaciones según los criterios dispuestos en norma complementaria por la que se establece la equivalencia regulatoria del sistema dominicano de infraestructura de claves públicas y de confianza con los marcos regulatorios internacionales de servicios de confianza.

En adición se ejecutó la herramienta **OWASP ZAP**, al portal donde están alojados los formularios de solicitud de servicios de Lleidanet, SRL. para el análisis de vulnerabilidades web al módulo de registro, la misma evidenció la existencia de dos (2) alerta de medio impacto, Diez (10) alertas de bajo impacto y Tres (3) alertas informativas, de las Diez (10) alertas de bajo impactos solo se incluirán Tres (3) en este informe como referencia de dichos hallazgo, de todos modos se le remitirá el resultado integro a la parte interesa en ofrecer los servicios ya mencionados y por ultimo las Tres (3) alertas Informativas que se presentan en este informe no se incluirán en dicho 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:

| Nivel de riesgo | Número de alertas |
|---|---|
| Alto | 0 |
| Medio | 2 |
| Bajo | 10 |
| Informativo | 3 |

## Detalles de las distintas alertas encontradas:

**Nivel de alerta**

**Alerta Media:** ***Encabezado X-Frame-Options no 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 otra 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). |

**Alerta Media: Divulgación de error de aplicación.**

| Detalles/Descripción Hallazgo | Solución/Recomendaciones |
|---|---|
| Esta página contiene un mensaje de error de advertencia que podría revelar información sensible como la ubicación del archivo que produjo la excepción no controlada, dicha información puede ser usada para lanzar ataques futuros a la app web, también la alerta podría ser un falso positivo si el mensaje de error es encontrado dentro de una página de doc. | Revisar el código de fuente de esta página. Implementación de páginas de error personalizadas. Considerar implementar un mecanismo para proveer una única referencia/identificación de error para el cliente (navegador) mientras insertando los detalles en el sitio del navegador y no exponiéndolos al usuario. |

**Alerta baja: No se encuentra encabezado X-Content-Type-Options Header**

| | |
|---|---|
| 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 complatible 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. |

**Alerta baja:** ***Ausencia de tokens anti-CSRF.***

| | |
|---|---|
| No se encontraron tokens Anti-CSRF en un formulario de envío HTML.<br>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. La falsificación de las solicitudes ente los sitios también se conocen como CSRF, XSRG, ataques con un solo clic, montaje de sesión, diputado confundido y navegación en alta mar. | Frase: Arquitectura y Diseño<br>Utilice una biblioteca o marco comprobado que no acepte que ocurra esta debilidad o que proporcione construcciones que permitan que esta debilidad sea más sencilla de evitar.<br>Fase: Implementación<br>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.<br>Fase: Arquitectura y Diseño<br>Origina un nonce único para cada uno de los formularios, coloque el nonce en el formulario y confirme la independencia al obtener el formulario. Asegúrese de que el nonce no sea predecible (CWE-330). Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.<br>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.<br>Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.<br>Utilice el control de gestión de la sesión de ESAPI.<br>Este control introduce un elemento para CSRF.<br>No utilice el método GET para ninguna de las solicitudes que puedan desencadenar un cambio de estado.<br>Fase: Implementación<br>Revise que la solicitud se creó en la página esperada. Esto podría quebrar la funcionalidad auténtica, ya que los usuarios o los representantes puede ser que hayan desactivado el envío de Referer por motivos de privacidad. |

**Alerta baja:** ***No se encuentra encabezado X-Content-Type-Options Header.***

| | |
|---|---|
| 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 | 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.<br><br>Si es posible, asegúrese que el último usuario usa un navegador web complatible 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 |

| | |
|---|---|
| contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing. | ejecutar MIME-sniffing. |

**Alerta baja:** ***Cookie No HttpOnly Flag***

| | |
|---|---|
| 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. |

**Alerta baja:** ***Divulgación privada de la IP.***

| | |
|---|---|
| Se ha encontrado una dirección IP privada (como 10.x.x.x, 172.x.x.x, 192.168.x.x) o un nombre de host privado de Amazon EC2 (por ejemplo, ip-10-0-56-78) en el cuerpo de respuesta HTTP. Esta información puede ser útil para nuevos ataques dirigidos a sistemas internos. | Quite la dirección IP privada del cuerpo de la respuesta HTTP. Para los comentarios, utilice el comentario JSP/ASP/PHP en lugar del comentario HTML/JavaScript que puede ser visto por los navegadores cliente. |

## Resumen

Luego de agotar todos los procesos existentes, salvo por algunas situaciones indicadas en el cuadro anterior, se evidencio que **Lleidanet Dominicana, S.R.L.,** ha cumplido de manera satisfactoria con los demás requerimientos que esta auditoria exige, demostrando que la mayoría de sus procedimientos están siendo llevados de forma correcta y de acuerdo a los establecido en la Ley Núm. 126-02 sobre Comercio Electrónico, Documentos y Firma Digital, su Reglamento de Aplicación y Normas Complementarias.