UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"METODOLOGÍA PARA IMPLEMENTAR SEGURIDAD EN SERVICIOS DE CORREO ELECTRÓNICO MEDIANTE LOS MECANISMOS MTA-STS (MAIL TRANSFER AGENT-STRICT TRANSPORT SECURITY) Y SMTP TLS REPORTING (TLSRPT) PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS."

AUTOR: RAYMI HERNÁN DE LA TORRE YAMBERLA

DIRECTOR: MSC. FABIÁN GEOVANNY CUZME RODRÍGUEZ

Ibarra-Ecuador

2022

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003642459		
APELLIDOS Y NOMBRES:	De La Torre Yamberla Raymi Hernán		
DIRECCIÓN:	Cotacachi - Av. El Sol		
EMAIL:	rhdelatorrey@utn.edu.ec		
TELÉFONO FIJO:	062946345	**TELÉFONO MÓVIL:**	0983705213

DATOS DE LA OBRA	
TÍTULO:	Metodología para Implementar Seguridad en Servicios de Correo Electrónico mediante el mecanismo MTA-STS (Mail Transfer Agent-Strict Transport Security) Y SMTP TLS Reporting (TLSRPT) para las Pequeñas y Medianas Empresas
AUTOR:	De La Torre Yamberla Raymi Hernán
FECHA:	08/03/2022
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	[X] **PREGRADO** [ ] **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	Ing. Fabian Cuzme Rodríguez, MSc.

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, 8 de marzo del 2022

EL AUTOR:

Raymi Hernan De La Torre Yamberla

CC:1003642459

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

CERTIFICACIÓN

Ing. Fabian Cuzme Rodríguez, MSc., director del presente Trabajo de Titulacion certifica:

Que, el presente trabajo de titulacion "Metodología para Implementar Seguridad en Servicios de Correo Electrónico mediante el mecanismo MTA-STS (Mail Transfer Agent-Strict Transport Security) Y SMTP TLS Reporting (TLSRPT) para las Pequeñas y Medianas Empresas", fue realizado en su totalidad por el Sr. De La Torre Yamberla Raymi Hernán, bajo mi supervision.

Es todo en cuanto puedo certificar en honor a la verdad.

Ing. Fabian Cuzme Rodríguez, MSc
CC:1311527012
Director

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Dedico esta tesis,

A Dios por bendecirme con la vida, quién supo guiarme dándome fuerzas para seguir adelante durante este proceso de formación profesional.

A mis padres; María Matilde Yamberla y Luís Enrique De La Torre, quienes son los principales pilares en mi vida, por su amor, trabajo y sacrificio durante todos estos años de estudio. Además, son las personas que siempre confiaron en mí, es por ello que este nuevo logro va dedicado hacia ellos.

A mi hermana Nayeli De La Torre, porque al igual que mis padres ha estado siempre brindándome su apoyo y acompañándome en los momentos más difíciles.

Hernán De La Torre

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco,

A mis padres y hermana, por ser los principales promotores en todas mis metas, por confiar y creer en mí. A ellos, mi infinito cariño y gratitud.

A mi tutor y asesores que me guiaron en el desarrollo de este trabajo investigativo, en especial a mi tutor Msc. Fabián Cuzme por su guía, apoyo e ideas que motivaron la presente investigación.

Y para finalizar, también agradezco a todos los amigos que conocí durante todo el proceso universitario, por apoyarme cuando más lo necesité, por sus ayudas y aportes a mi proyecto de tesis, al igual que todos los buenos momentos vividos.

Hernán De La Torre

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

RESUMEN

El presente proyecto de titulación se enfoca en la implementación del estándar de correo electrónico seguro MTA-STS (Mail Transfer Agent Strict Transport Security) y TLS Reporting, cuya función principal es mejorar la seguridad de las conexiones SMTP entre servidores de correo electrónico, con el fin de disminuir las vulnerabilidades de conexiones seguras cifradas mediante Transport Layer Security (TLS).

Como parte inicial del trabajo se realiza un estudio bibliográfico referente a las vulnerabilidades existentes en los sistemas de correo electrónico que usan TLS, del cómo está diseñado MTA-STS para abordar estas vulnerabilidades que ayudan a mitigar distintos tipos de ataques del tipo Man-In-The-Middle (MITM). En función de la fundamentación teórica se determina los requerimientos funcionales y no funcionales aptas para su correcta implementación, una vez definida estos requerimientos se procede a la implementación práctica, es decir activar el estándar MTA-STS y TLS Reporting a un dominio de correo electrónico mediante la configuración de políticas MTA-STS y registros DNS necesarios. Luego se define dos escenarios de prueba las cuales se basan en la recepción exitosa y fallida de correo electrónico cuyos resultados demostraron que al implementar políticas de mta-sts en dominios personalizados en modo de hacer cumplir siempre requerirá conexiones TLS estrictas para entregar el correo electrónico. Finalmente se documenta todo el proceso y se desarrolla una guía técnica especificando qué pasos pueden tomar las organizaciones para implementar el estándar MTA-STS.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ABSTRACT

The present degree Project is focuses on the implementation of the MTA-STS (Mail Transfer Agent Strict Transport Security) and TLS Reporting secure email standard, whose main function is to improve the security of SMTP connections between email servers, in order to decrease the vulnerabilities of secure connections encrypted by Transport Layer Security (TLS).

As an initial part of the work, a bibliographic study is carried out regarding existing vulnerabilities in email systems that use TLS, how MTA-STS is designed to mitigate these vulnerabilities that help to lessen different types of attacks of the type Man-In-The-Middle (MITM). Depending on the theoretical foundation decide the functional and non-functional requirements suitable for proper implementation, after defining the requirements its proceed to practical implementation, that is, activate the MTA-STS standard and TLS Reporting in an email domain by configuring MTA-STS policies and DNS records. Then two test scenarios are defined based on successful and unsuccessful receipt of email whose results showed that when implementing mta-sts policies in custom domains in enforce mode it will always require strict TLS connections to deliver the email. Finally, the whole process is documented and develops a technical guide specifying steps can be taken by organizations to implement the MTA-STS standard.

ÍNDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

Capítulo 1. ANTECEDENTES

Tema

METODOLOGÍA PARA IMPLEMENTAR SEGURIDAD EN SERVICIOS DE CORREO ELECTRÓNICO MEDIANTE LOS MECANISMOS MTA-STS (MAIL TRANSFER AGENT-STRICT TRANSPORT SECURITY) Y SMTP TLS REPORTING(TLSRPT) PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

Problema

Hoy en día, las PYMES son un objetivo del fraude por correo electrónico, al igual que las grandes empresas del sector. Esto se debe principalmente a que la gran mayoría de las PYMES utilizan habitualmente el correo electrónico como herramienta de trabajo(Instituto Nacional de Cyberseguridad, 2020a). Si bien es cierto que las aplicaciones de mensajería instantánea han ganado terreno, sobre todo en un ámbito mucho más personal, el email sigue siendo el más utilizado(Soro, 2019). Para hacernos una idea, se calcula que en un minuto se envían cerca de 197 millones de correos alrededor del mundo, mientras que en ese mismo periodo de tiempo se mandan alrededor de 69 millones de mensajes por WhatsApp y Facebook Messenger(Lewis, 2021). A la vista de una carrera triunfal del email, no sorprende que este medio de comunicación siga siendo el vector de infección más común por parte de los agentes de amenaza, ya que una falta de control sobre estos servicios podría ocasionar diversos ataques a una organización, tales como, mensajes spam, phishing, diseminación de virus, pérdida de información de carácter sensible, entre otros (Cisco Systems, 2019b). La pandemia provocada por el coronavirus no ha hecho más que agudizar el problema a escalas inimaginables ya que ha aumentado el riesgo al

que están sometidas las empresas. En este sentido, ESET elaboró un informe sobre las amenazas informáticas empresariales del segundo trimestre del 2020 en donde se identificó los ataques informáticos que explotan la pandemia, dando como resultado que los principales ataques apuntaban a sitios web y correos electrónicos, más específicamente al aumento en los correos electrónicos de phishing, en donde los cibercriminales se valen de técnicas de ingeniería social para suplantar a personas o empresas de confianza(Chicaiza Valverde, 2020). En esta línea, las empresas del Ecuador también se han enfrentado contra varios incidentes de seguridad distribuidas por medio de cuentas de correo electrónico. Entre los casos más difundidos en redes sociales fueron los masivos correos electrónicos fraudulentos en nombre del Banco Pichincha ocurrido el jueves 18 de febrero del 2021, en donde los atacantes enviaban comunicaciones en nombre del Banco con el fin de obtener la información necesaria para realizar transacciones ilegitimas. Al respecto la entidad a través de un comunicado aseguro estar tomando medidas para prevenir y mitigar este tipo de ataques(El Comercio, 2021). Esto lleva a pensar que, si una empresa grande, que cuenta con múltiples capas de seguridad, puede ser víctima de los ciberataques, las pequeñas y medianas empresas que cuentan con menos recursos no tendrían ninguna esperanza.

Afortunadamente existen algunas formas de garantizar que la empresa esté protegido por medio del correo electrónico seguro, una de ellas corresponde al uso de tecnologías de cifrado, que permite que un e-mail transite en texto cifrado de tal manera que no sea manipulado ni leído por los cyberdelincuentes. Una cosa muy importante que se tiene con el protocolo SMTP (Simple Mail Transfer Protocol) es que el e-mail puede viajar en texto plano ya que el cifrado es opcional. Sin embargo, en 1999 se introdujo el comando STARTTLS a SMTP, proporcionando la función de convertir una conexión no segura a segura por medio del protocolo TLS(Transport

Layer Security)(Kambourakis et al., 2020). La extensión STARTTLS para SMTP que se específica en la RFC 3207 permite negociar un canal TLS entre cliente y servidor además del cifrado de correo electrónico para la transmisión de correo cifrado. Si bien es cierto que esta técnica de cifrado oportunista proporciona una seguridad alta contra los ataques de interceptación pasiva de ataques de trafico intermedio(Hoffman, 2002), STARTTLS tiene dos problemas, la primera es que el cifrado es opcional por lo tanto cualquier atacante puede eliminar partes de una conexión SMTP evitando que ocurra la actualización de la comunicación no cifrada a cifrada lo que ocasionaría ataques de interceptación y degradación. Y la segunda es que STARTTLS no cuenta con un mecanismo para autenticar la identidad de un servidor por lo tanto los servidores de correo SMTP no validarían los certificados(Melnikov, 2016). Esto ocasionaría que los delincuentes informáticos accedan fácilmente a los datos corporativos, no obstante, su uso inapropiado podría ocasionar importantes pérdidas de productividad incluso en la imagen y en la seguridad de la empresa.

Por todas estas razones descritas anteriormente es importante implementar estrictas medidas de seguridad en los sistemas de correo electrónico de tal manera que los datos de una empresa no se vean expuestos. Es por eso que el presente proyecto busca dar a las PYMES una metodología de cifrado de correo electrónico, que se pueda integrar a sus políticas de seguridad, que se basa en dos nuevos estándares de seguridad de internet: MTA-STS (Mail Transfer Agent-Strict Transport Security) y TLS Reporting, que habilita a los servidores de correo electrónico su capacidad de recibir conexiones SMTP seguras utilizando TLS y especificar si los servidores SMTP remitentes deberán rehusar la entrega a host MX que no cuenten con un certificado de servidor confiable, mitigando de esta manera los ataques de degradación y ataques de Man-in-The-Middle. MTA-STS se complementa con SMTP TLS Reporting que le brinda información

sobre qué correos electrónicos se entregan correctamente a través de TLS y cuáles no, enviando los resultados de los informes a una dirección de correo especifica.

Objetivos

Objetivo General

Establecer una metodología de cifrado de un dominio correo electrónico mediante la implementación de los mecanismos MTA-STS y TLS Reporting para mejorar la seguridad a nivel de transporte durante la comunicación SMTP con la finalidad de garantizar la privacidad del tráfico de correo electrónico.

Objetivos Específicos

Estudiar el estado del arte de las principales amenazas a las que se enfrentan los servicios de correo electrónico tradicionales, así como también el estudio los estándares de seguridad: MTA-STS y SMTP TLS Reporting.

Especificar los requerimientos necesarios para el funcionamiento de los estándares en un dominio de correo electrónico.

Definir un escenario de pruebas de acuerdo al análisis de los requerimientos funcionales.

Configurar y publicar la política MTA-STS y los registros DNS necesarios para habilitar el transporte seguro estricto y reportes TLS en un servicio de correo electrónico.

Comprobar la funcionalidad de la implementación de los estándares mediante un Testing de evaluación al dominio de correo con la ayuda de herramientas web de supervisión de nombres de dominio.

Proporcionar un manual técnico para la implementación de los mecanismos MTA-STS y TLS-RPT para un dominio de correo electrónico.

Alcance

El presente proyecto propone mejorar la seguridad del protocolo SMTP al permitir que los dominios de correo opten por un modo que requiera autenticación con certificados públicos válidos y cifrados (TLS) mediante la implementación de dos nuevos estándares de seguridad de internet: MTA-STS (Mail Transfer Agent-Strict Transport Security) y TLS Reporting para las pequeñas y medianas empresas.

La metodología empleada en el desarrollo del presente proyecto corresponde al ciclo de Deming que es un proceso de planificación y optimización diseñado para que las empresas y las organizaciones que lo utilizan mejoren continuamente su productividad ya que garantiza la atención continua sobre la mejora de la calidad(Tang, 2016). Consiste en cuatro etapas que se las ejecuta de forma secuencial y en un cierto orden que son el: Plan, Hacer, Verificar y Actuar, por lo que cada una de ellas tiene una anterior y una posterior. Este ciclo no tiene un fin específico, sino que hay que seguir indefinidamente(Henshall, 2017).

La primera fase del proyecto corresponde al Plan que es un proceso en donde se identifican los problemas específicos que surgen al momento de planificar un proyecto, los recursos necesarios, los requisitos de las partes interesadas, las condiciones de ejecución, y los objetivos finales del proyecto(Escuela Europea de Excelencia, 2021).

Lo primero que se realizará es la recopilación y el análisis de la fundamentación teórica acerca de las amenazas de seguridad en los sistemas de correo electrónico, además del estado del

arte que existen acerca de los mecanismos de transporte seguro estricto y reportes TLS, su soporte entre los principales proveedores de correo electrónico, señalando las falencias que presentan los agentes de transferencia de correo tradicionales que operan bajo la extensión STARTTLS y como se ha implementado el uso de MTA-STS que ayuda a mitigar los ataques del tipo Man-In-The-Middle (MITM), como los ataques de degradación de SMTP y los ataques de suplantación DNS en los sistemas de correo electrónico.

Posterior al análisis de la fundamentación teórica se va a determinar los requerimientos de funcionamiento de acuerdo al análisis de los documentos RFC 8461 y 8460 proporcionados por la IETF y consultas en fuentes bibliográficas referentes al soporte del estándar MTA-STS y TLS Reporting. Una vez que se ha determinado las características del sistema se procede a diseñar un ambiente o un escenario de pruebas para los dominios de correo electrónico de tal manera que se pueda ejecutar y evaluar el envío y recepción del correo electrónico seguro.

Una vez que se ha encontrado la solución al problema y una forma de ejecutar el proceso inicia la etapa de implementación en la práctica(Jimeno Bernal, 2013) que corresponde al ciclo de Hacer que concierne a probar el funcionamiento de los estándares en un dominio de correo electrónico. En este aspecto se procederá a activar el estándar MTA-STS y TLS Reporting a un dominio de correo electrónico mediante la implementación de políticas MTA-STS y registros DNS necesarios de tal manera que el correo que se envía a un dominio este autenticado y cifrado además proporcione los reportes TLS para obtener información de los servidores externos al dominio de correo propio.

En el ciclo de evaluación que corresponde a la comparación, análisis y evaluación de los resultados que se ha obtenido durante la ejecución con los esperados en el ciclo de planificación. Hay que tomar en cuenta que pueden ocurrir problemas imprevistos en esta fase. Por eso, en una

situación perfecta, primero puede intentar incorporar su plan a pequeña escala y en un entorno controlado(Kanbanize, s. f.). Con respecto al proyecto lo primero es comprobar la implementación de las políticas con la ayuda de un agregado de pruebas de MTA-STS que brinda ciertas plataformas web de detección y supervisión de nombres de dominios de correo el cual proporciona diagnósticos, comentarios y recomendaciones si no están configuradas correctamente. Ahora que ha habilitado MTA-STS y TLSRPT (Informes TLS) para el dominio, comenzará a recibir informes de proveedores de correo electrónico compatibles. Estos informes mostrarán la cantidad de correos electrónicos que se entregaron o no con éxito a través de TLS y los motivos de los errores.

Si los elementos definidos en la Planificación son insuficientes, habrá que modificarlos para la próxima vez. La fase de actuación es necesaria para corregir los aspectos negativos obtenidos en la evaluación y puede implicar la modificación de la Planificación(Metodoss, 2016). Si todo fue de acuerdo con el plan y los resultados son satisfactorios, no es necesario desviarse del curso original. Finalmente, una vez que la fase de Evaluación ha concluido con éxito se desarrollará una guía técnica de configuración, que facilite la implementación de los estándares de seguridad de transporte seguro estricto y registros TLS con el objetivo de brindar la orientación necesaria al personal del departamento de TI de una PYME de desarrollar cada uno de los apartados y lineamientos de tal manera que su empresa esté protegida por medio del correo electrónico seguro. Es muy importante no detenerse en la Actuación ni quedarse con la antigua Planificación, sino empezar verdaderamente un nuevo ciclo constantemente con nuevos requerimientos.

Justificación

Cualquier empresa, ya sea una gran corporación o una pequeña pyme, gestiona información de gran valor no solo para la propia empresa, sino también para los cyberdelincuentes. Lamentablemente, el correo electrónico se ha convertido en el medio más habitual para realizar ataques (Gonzalia, 2020), tal es el caso del malware y phishing, que han aprovechado el tema del COVID-19 para lanzar sus campañas fraudulentas que casi a diario se distribuyen por el correo electrónico. En esta línea en una encuesta realizada por ESET en el 2020 revelo que el 44% de los usuarios afirmó haber recibido correos de phishing que utilizaban el tema del covid-19 como anzuelo(ESET Internet Security, 2021). Ante las diferentes y crecientes amenazas, las empresas deben llevar sus estrategias al siguiente nivel no solo para adaptarse a la evolución del fraude, sino también para estar un paso adelante de los delincuentes informáticos, anticipando las amenazas emergentes y posibles vulnerabilidades en los dispositivos y las redes. De esta manera los equipos de seguridad y antifraude podrán potenciar sus estrategias para sacar ventaja de las más recientes y mejores herramientas con las que cuenta el sector (Datta, 2021).

La seguridad del correo electrónico es una disciplina de múltiples capas que involucra varios tipos de software y tecnología. Hay varias formas de garantizar la seguridad de las cuentas de correo electrónico empresariales, pero es importante combinar la educación de los empleados con políticas y procedimientos de seguridad integrales(Barracuda Networks, 2010). La tecnología MTA-STS ha surgido con el fin de corregir las vulnerabilidades del cifrado opcional del protocolo SMTP. El mecanismo MTA-STS permite a los proveedores de servicios de correo hacer cumplir la seguridad de la capa de transporte con un cifrado TLS para proteger las

conexiones SMTP(Greenwald, 2019). Con la implementación MTA-STS, les informa a los remitentes que su servidor de correo electrónico acepta la entrega segura de correo electrónico utilizando SMTP sobre STARTTLS y que el correo electrónico no debe entregarse a través de una conexión SMTP insegura gracias a los registros TLS(Mills, 2021).

Si se activa MTA-STS se mejora la seguridad del correo electrónico al proteger a los destinatarios, remitentes de correo electrónico y usuarios de dominios de ataques de phishing que es una táctica muy exitosa para que los hackers obtengan lo que quieren(Ferreira, 2021), El email phishing tiene un impacto enorme en las campañas de email marketing que afecta la marca y la reputación de una empresa lo cual ocasionaría enormes pérdidas financieras que amenaza la existencia misma de la empresa(Cruz, 2017).

MTA-STS requiere un servidor web habilitado para HTTPS con un certificado válido, registros DNS y un mantenimiento constante, lo que hace que el proceso de despliegue sea largo, lento y complicado(De Graaff, 2021), Por tal motivo en el presente proyecto se busca proporcionar un manual técnico para la implementación de estos estándares de seguridad en los servicios de correo electrónico se ayudara a las PYMES a facilitar la activación de los mecanismos MTA-STS y TLS Reporting para su servidor de correo empresarial con la finalidad de garantizar la privacidad de trafico de correo electrónico.

Capítulo 2. FUNDAMENTACIÓN TEÓRICA

Este capítulo corresponde a un estudio bibliográfico preliminar. Por lo que el marco teórico expuesto aquí servirá como base en el presente proyecto para desarrollar un estudio congruente, el cual valide las determinaciones tomadas durante la ejecución del proyecto.

2.1. Seguridad en Correo Electrónico

El correo electrónico se mantiene como una herramienta esencial para la vida cotidiana actual, que puede servir al menos para poder registrar distintas cuentas para todos esos servicios, aplicaciones y redes sociales existentes. Su uso tan masificado hace que los atacantes se interesen en vulnerar estos servicios. Por lo tanto, la seguridad en correo electrónico es un tema muy importante que no hay que descuidar(Shcherbakova, 2019).

La seguridad en el correo electrónico ha pasado por una serie de etapas desde su creación. En la década de 1980 surge el protocolo SMTP el cual no cuenta con las capacidades necesarias para asegurar una comunicación por correo. Para mejorar la seguridad se introdujo en el 2002 el protocolo SMTP STARTTLS para cifrar la comunicación entre el servidor y el cliente de correo, pero resultó que no era capaz de mitigar amenazas de ataques de intermediario (MITM) y de degradación de conexión(Fernández, 2018). Hoy en día los esfuerzos se centran en los nuevos mecanismos de seguridad ante los ciberataques como los protocolos SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) y MTA-STS (Mail Transfer Agent-Strict Transport Security) para luchar contra la suplantación de identidad, el phishing y otros ciberataques que amenazan los servicios en la internet (Foster et al., 2015).

Si bien existen muchas personas haciendo uso legítimo del servicio de correo, también hay personas que aprovechan este servicio para usos ilegítimos, en donde existen un sin número de amenazas, las mismas que se han incrementado debido a que las personas no prestan la suficiente atención al abrir su correo por el desconocimiento de los riesgos que existen.

2.1.1. Amenazas en la comunicación por correo electrónico

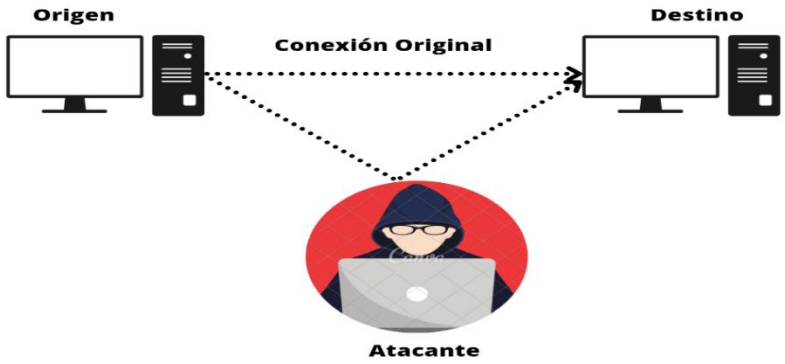
En este mundo digitalizado, la protección del correo electrónico es imprescindible para la infraestructura de ciberseguridad de cualquier empresa, sin embargo, casi todo el delito cibernético se basa en el correo electrónico o lo emplea como parte del proceso(Petcu, 2021). Entre los peligros más comunes asociados al correo electrónico se tiene:

2.1.1.1. Eavesdropping

La Figura 1 ejemplifica un ataque de escucha clandestina, el atacante escucha pasivamente las comunicaciones de la red para obtener acceso a información privada o datos confidenciales del correo electrónico(Teng et al., 2012).

Figura 1.

Ataque Eavesdropping



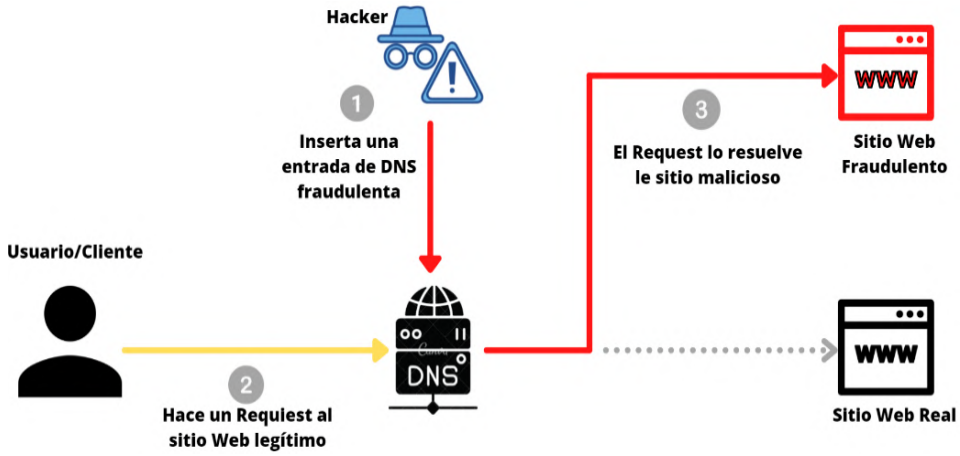
Nota. Un atacante olfatea o fisgonea información transmitida por un dispositivo. Adaptada de (Lakhtaria, 2015).

2.1.1.2. Suplantación DNS

Debido a que el DNS es un sistema no cifrado, un atacante podría modificar los registros MX hacia un servidor de correo desconocido desviando fácilmente el trafico DNS en la red tal como se presenta en la Figura 2; de esta manera el servidor de correo enviaría el e-mail al servidor de correo del cyberdelincuentes (Ramesh et al., 2010).

Figura 2.

Esquema de un Ataque DNS Spoofing



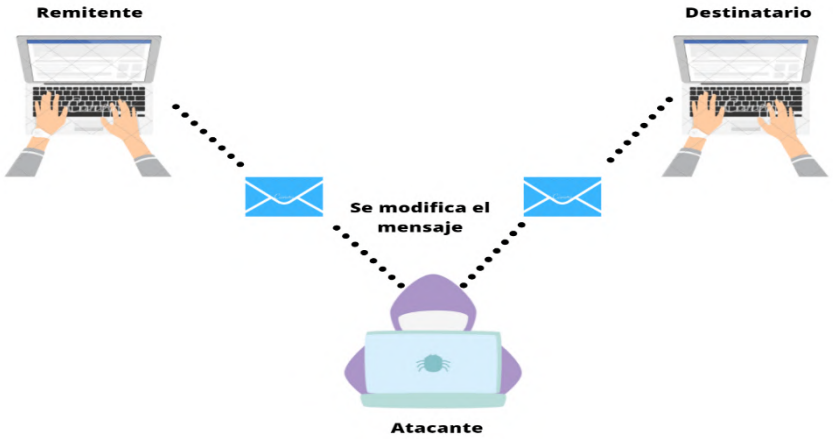
Nota. Un atacante manipula vulnerabilidades conocidas dentro del sistema de nombres de dominio (DNS). Adaptada de (Okta, 2021).

2.1.1.3. Modificación del mensaje

Si un atacante captura el e-mail también puede alterar el contenido de su mensaje si no está cifrado. En la Figura 3 se muestra que cualquier persona que tenga derechos administrativos sobre cualquiera de los servidores SMTP, no solo puede leer su mensaje sino también puede modificarlo(Lux Scientiae, 2015).

Figura 3.

Ataques Pasivos: Modificación del Mensaje



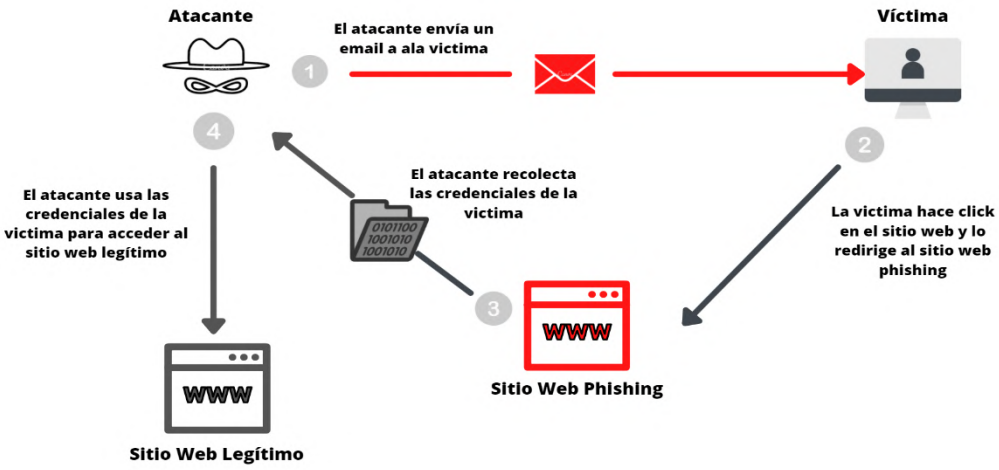
Nota. Un atacante trata de reenviar mensajes que ya habían sido previamente transmitidos tras haberlos modificado. Adaptada de (Internet Security, 2020).

2.1.1.4. Phishing

Considerado como el ataque más común a través del correo electrónico, utilizado para robar información confidencial como contraseñas, PINES de cajeros automáticos y otras credenciales bancarias. El ataque se origina por medio de un correo electrónico que finge ser de confianza, estos correos electrónicos invitan a hacer clic en los enlaces para abrir algún archivo adjunto o responder algún tipo de mensaje, el cual contiene un malware para actos malintencionados(Gory et al., 2014). Todo este proceso se lo puede observar en la Figura 4.

Figura 4.

Esquema de un Ataque de Phishing



Nota. Un atacante intenta de robar información confidencial, generalmente nombres de usuario, contraseñas, números de tarjetas de crédito, información de cuentas bancarias u otros datos importantes para utilizar o vender la información robada. Adaptado de (Mezquita, 2019).

2.1.1.5. Man-In-The-Middle

Comprende un tipo de ataque que se basa en interceptar una comunicación entre dos o más equipos, pudiendo suplantar la identidad de uno u otro según sea necesario para robar la información y modificarla. Esto puede ocurrir en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc. No solo tratan de vigilar las conversaciones privadas, sino que también pueden orientar toda la información dentro de sus equipos terminales(Instituto Nacional de Cyberseguridad, 2020b).

Los cyberdelincuentes que utilizan esta táctica se dirigen a cuentas de correo electrónico de grandes organizaciones, especialmente instituciones financieras y bancos. Una vez que obtengan acceso a importantes cuentas de correo electrónico, supervisarán las transacciones para que su eventual ataque sea mucho más convincente. Por ejemplo, pueden esperar un escenario en el que el cliente envíe dinero y responda falsificando la dirección de correo electrónico de la empresa, con sus propios datos bancarios en lugar de los de la empresa(Publico, 2017). De esta manera, el cliente cree que está enviando su pago a la empresa, pero en realidad lo está enviando directamente al pirata informático. De esta forma en la Figura 5 se presenta un ataque de intermediario entre el usuario y la aplicación.

Figura 5.

Esquema de un Ataque Man in The Middle

Nota. Un atacante se posiciona en una conversación entre un usuario y una aplicación, ya sea para escuchar a escondidas o hacerse pasar por una de las partes. Adaptado de (Qureshi, 2019).

2.1.2. Uso seguro del Correo Electrónico

La ciberseguridad es un tema de gran importancia, pero a menudo se pasa por alto cuando nos engañamos a nosotros mismos haciéndonos creer que "no nos va a pasar nada". El hecho es

que cualquier persona con una cuenta de correo electrónico es muy susceptible de estar expuesta a ataques cibernéticos.

En el último informe de la Evaluación de riegos de seguridad de correo electrónico de Mimecast se identificó que 1 de cada 72 correos electrónicos contienen URL malicioso, en donde además se estima que el 11% de todos los correos electrónicos contiene algún tipo de malware(Email Security Risk Assessment, 2019). Enviar correos electrónicos es un hábito diario en nuestras vidas, por lo que la bandeja de entrada es un excelente lugar para comenzar a construir una estrategia de ciberseguridad. Evitar la negligencia e informarse sobre las prácticas seguras de correo electrónico para evadir a los piratas informáticos y evitar ser víctima de diversas amenazas de seguridad.

Existen numerosos consejos a seguir para usar el correo electrónico de forma segura, muchos de ellos de sentido común.

2.1.2.1. Usar diferentes cuentas de correo electrónico

Es recomendable usar múltiples cuentas de correo dependiendo de la situación por ejemplo una cuenta para recibir correos de poca relevancia como avisos comerciales, entre otros; una cuenta de correo exclusivamente para temas relacionados con el oficio y una cuenta de correo electrónico para ser expuesta en internet usándola para distintas suscripciones y demás fuentes de información(Universidad de Jaén, 2020).

2.1.2.2. No enviar ni receptar información privada

Es de suma importancia ser prudente a la hora de enviar información de carácter sensible por correo electrónico. El correo electrónico transita por la internet antes de llegar al destino, por lo que es muy probable que un atacante lo intercepte y lo lea(Cisco Systems, 2019a).

2.1.2.3. Utilizar una copia oculta BCC

Al enviar correos electrónicos a un grupo diverso de personas sin usar el campo “BCC” ponemos en peligro la privacidad y la seguridad. De esta forma un Spammer puede conseguir todos los correos electrónicos de los destinatarios en inmediatamente lanzar ataques de Spam o Phishing(Sistemex, 2015).

2.1.2.4. Prudencia a la hora de responder correos

Los clientes de correo suelen tener por defecto la opción de contestar sólo al remitente, pero muchas veces por alguna u otra situación podemos seleccionar la opción de “Contestar a todos”. De esta forma se incluye la respuesta a todos los clientes pudiendo tener graves consecuencias(Digital Guide IONOS, 2019).

2.1.2.5. Revisar el reenvío de correos

El reenvío de correos es una opción muy útil para responder a alguien sin escribir un texto muy extenso, pero si el correo llega a un Spammer informático puede asaltar una gran cantidad de direcciones de correo electrónico y enviar contenido con Spam a las direcciones de correo robadas(HubSpot, 2021).

2.1.2.6. Cifrar los correos electrónicos

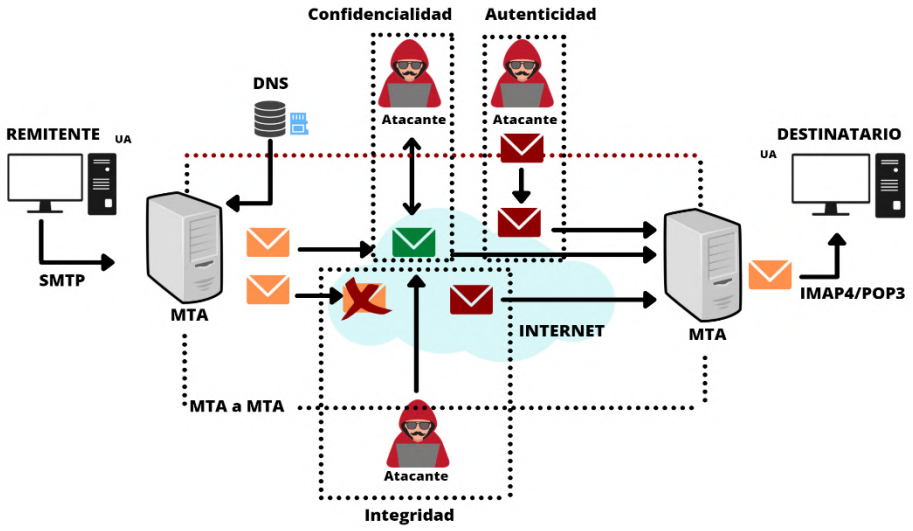
Es necesario utilizar distintas técnicas de cifrado de correo y controlar toda la información confidencial para lo cual se debe disponer de un certificado digital. De esta manera se logra proteger contenido sensible de ser leído por un usuario desconocido, exceptuando al destinatario original. (Shet, 2021).

2.1.3. Aspectos de Seguridad

Es deber de los proveedores de correo electrónico proteger propiedades de seguridad específicas, como, la confidencialidad, autenticidad e integridad de los mensajes al interactuar con otros proveedores, esta necesidad está estrechamente relacionada con el nivel de confianza que un usuario final puede entablar con su proveedor. Esto se debe simplemente a que el usuario final ordinario no puede ser informado directamente sobre las prácticas de seguridad seguidas por su proveedor. Por ejemplo, el protocolo SMTP no requiere que los MTA se autentiquen, asumiendo que cada correo electrónico recibido es legítimo. Por lo tanto, el repertorio de ataques de red disponibles para el oponente pasivo o activo va desde escuchar a escondidas el canal de comunicación o Man-in-The-Middle (MITM), hasta configurar un MTA deshonesto para lanzar campañas de Spam o Phishing (Shitole & Divekar, 2019). En la figura 6 se muestra brevemente y da una representación de alto nivel de los ataques contra las propiedades de seguridad de interés.

Figura 6.

Representación de Alto Nivel de Ataques Contra la Confidencialidad, Autenticidad e Integridad.



Nota. Adaptado de (Kambourakis et al., 2020)

2.1.3.1. Confidencialidad

El atacante puede despojar o distorsionar el anuncio de TLS que obliga el extremo receptor para volver al texto sin cifrar, incluso si se crea el túnel TLS. De esta manera el MTA de salida no autentica el entrante mediante un certificado de servidor confiable, entonces un atacante activo puede actuar como un MITM personificando cada extremo de la conexión con el otro. Esto permitiría al agresor ver y manipular cualquier mensaje a voluntad.

2.1.3.2. Autenticidad

Se puede abusar de esta falta de autenticación para falsificar identidades de correo electrónico, es decir, enviar correos electrónicos fingiendo ser otra persona. Para llevar a cabo este ataque, el atacante malintencionado no requiere manipulación con las comunicaciones en red de un servidor legítimo, lo que simplifica su ejecución.

El Phishing es una de las técnicas maliciosas que pueden aprovechar las identidades falsificadas para llevar a cabo ataques, por ejemplo, haciéndose pasar por el departamento de TI de un banco, red social, minorista en línea, etc. y solicitar a la víctima para iniciar sesión en su cuenta utilizando un enlace proporcionado en el correo electrónico.

2.1.3.3. Integridad

Los mensajes, incluida la dirección del remitente, que durante el tránsito entre MTA no se pueden garantizar si no se aplican las medidas adecuadas, como las firmas digitales. Claramente, no es factible asegurar que el mensaje recibido es idéntico al original; un atacante activo es capaz de manipular tanto el contenido del mensaje y los metadatos asociados, como el remitente y destinatario a lo largo de cualquier salto entre los MTA implicados.

2.1.4. Estándares de Seguridad

Desde el desarrollo inicial de los principales protocolos de correo electrónico (SMTP, POP3 e IMAP), han aparecido diferentes propuestas basados en nuevos protocolos y / o extensiones de los anteriores para abordar las vulnerabilidades del correo electrónico. Si bien han recibido numerosas actualizaciones y mejoras estas casi siempre no son implementadas, por razones de costo o desconocimiento(Sánchez & Draper-Gil, 2019). Se ha identificado un conjunto de protocolos de seguridad modernos que pueden ayudar a mitigar las vulnerabilidades de los servicios de correo electrónico las cuales se presentan a continuación.

2.1.4.1. Extensión STARTTLS

Una de las extensiones de cifrado de correo electrónico más utilizadas es STARTTLS. Es una capa TLS (SSL) sobre la comunicación de texto sin formato, lo que permite a los servidores de correo electrónico actualizar su comunicación de texto sin formato a la comunicación encriptada(Li & Gillula, 2018).

2.1.4.2. Marco de políticas del remitente (SPF)

Protocolo que permite a los proveedores de correo electrónico anunciar una lista de hosts autorizados para enviar correos electrónicos en su nombre. Los registros SPF son publicado como TXT tipo RR en la zona DNS del correo electrónico proveedor, y por lo tanto dependen directamente de la integridad del DNS. Solo se permite un SPF TXT RR por dominio, pero este registro puede enumerar varios servidores autorizados(Kitterman, 2014).

2.1.4.3. The Domain Keys Identified Mail (DKIM)

El Correo Identificado con Claves de Dominio es un estándar que permite al MTA receptor validar el origen y contenido de un correo electrónico. DKIM utiliza firmas digitales para vincular el mensaje de correo electrónico con su origen, es decir, el titular de la clave privada correspondiente. Un proveedor de correo electrónico que soporte de DKIM contiene una o más claves privadas, y publica sus claves públicas asociadas como DNS TXT RR con la URL *<selector>*. *_domainkey.* <*Domain*>, donde el parámetro selector es una cadena arbitraria elegida por el remitente(Crocker et al., 2011).

2.1.4.4. Domain Name System Security Extensions (DNSSEC)

Las Extensiones de Seguridad del Sistema de Nombres de Dominio comprende un conjunto de especificaciones que básicamente proporcionan los medios para autenticar registros DNS. El uso de DNSSEC asegura que los RR de DNS sean válidos y no han sido modificados o manipulados, aumentando el nivel de confianza. Teniendo en cuenta que la integridad de los RR TXT de DNS SPF, DKIM y DMARC dependen de la seguridad de la infraestructura DNS subyacente, DNSSEC es la base para la transmisión segura de correo electrónico(Weiler & Blacka, 2013).

2.1.4.5. DNS-based Authentication of Named Entities (DANE)

La Autenticación basada en DNS de Entidades Nombradas es un mecanismo que vincula certificados a nombres de dominio. Es decir, en lugar de depender de las Autoridades de Certificación (CA), el DANE confía en DNSSEC para publicar claves públicas y certificados para su uso durante el protocolo de enlace TLS(Hoffman & Schlyter, 2012).

DANE alivia dos problemas básicos; la relación a menudo poco clara entre un dominio de servidor de correo electrónico entrante y el servidor SMTP autorizado para ese dominio, y el hecho de que por confiar en el certificado presentado por el servidor entrante, el remitente debe confiar en un gran número de CA, pero hasta ahora, no hay una lista universalmente acordada de las CA existentes (Dukhovni & Hardaker, 2015b).

2.1.4.6. SMTP Mail Transfer Agent Strict Transport Security (MTA-STS)

Es un mecanismo para publicar directivas de políticas con respecto al uso de conexiones TLS y la validación de certificados X.509. MTA-STS se desarrolla como una alternativa al uso de DANE, considerando que la implementación de DNSSEC no es sencilla y puede ser propenso a errores (Shulman & Waidner, 2017) y, a veces, poco práctico. Es decir, a diferencia del DANE, MTA-STS se basa en CA (PKIX) y no exige DNSSEC. Fue diseñado para reparar un agujero existente en el protocolo STARTTLS que permitía que la comunicación se no se cifre a través de que un atacante pudiera eliminar partes de la sesión SMTP (como la respuesta “250 STARTTLS”). Esto se logra al traer DNS como un tercero para verificar las conexiones(dmarcian, 2021).

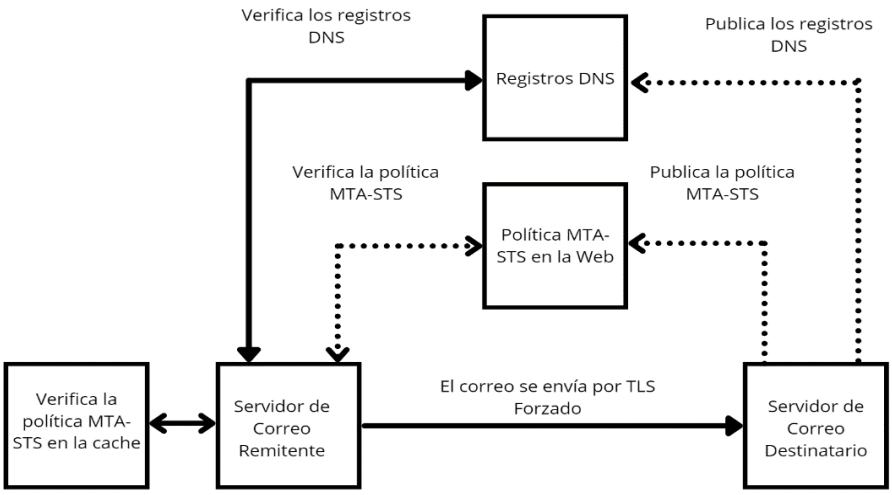
2.2. MTA-STS (Mail Transfer Agent-Strict Transport Security)

La seguridad de transporte estricta se basa en las autoridades de certificación (CA) y no requieren DNSSEC, a costa de correr el riesgo de degradaciones maliciosas. Además, proporciona una política en modo de "enforce", se solicitará a los servidores de correo externos que envíen informes diarios. Estos informes contienen información sobre los problemas detectados cuando se conectan al dominio. También incluyen información sobre las políticas de MTA-STS que se han detectado, así como estadísticas de tráfico, datos sobre las conexiones fallidas y los mensajes que no se han podido enviar. La principal motivación de MTA-STS es proporcionar un mecanismo basado en dominios para garantizar la seguridad del transporte incluso cuando la implementación de DNSSEC es indeseable o poco práctico(D Margolis et al., 2018).

El protocolo MTA-STS opera mediante un registro DNS que le dice a los servidores de correo que consulten su archivo de políticas por medio de HTTPS desde un subdominio definido. Este archivo contiene una lista de los servidores receptores que están autenticados y aprobados para receptar mensajes y además define la política de aplicación para los mensajes entrantes. En la primera conexión a un nuevo servidor, se guarda la huella digital del certificado en una base de datos local para referencia futura. En cada establecimiento posterior de una conexión a este servidor, el certificado se comparará con esta huella digital local(United Kingdom Public Sector Government, 2021). La Figura 7 describe el esquema de funcionamiento del estándar MTA-STS en un dominio de correo entrante.

Figura 7.

Diagrama de Operación de MTA-STS



Nota. Adaptado de (United Kingdom Public Sector Government, 2021)

2.2.1. Terminología

La RFC 8461 define los siguientes términos los cuales serán útiles para la compresión de la tecnología MTA-STS:

- ***Política MTA-STS:*** un compromiso del dominio de políticas para admitir TLS autenticado con PKIX para los hosts MX especificados.
- ***Dominio de política:*** el dominio para el que se define una política MTA-STS. Este es el dominio del siguiente salto; al enviar correo a "*alice@example.com*", normalmente sería "example.com", pero esto puede ser anulado por reglas de enrutamiento explícitas.
- ***Host de política:*** el host HTTPS que aloja a la política MTA-STS para un dominio de políticas.
- ***Remitente o MTA de envío:*** El MTA de SMTP que envía un mensaje de correo electrónico

2.2.2. Tecnologías Relacionadas

La autenticación basada en DNS de un registro TLS de entidades designadas (DANE) descrito en la RFC7672 es similar, ya que DANE también está diseñado para actualizar cifrado no autenticado o transmisión de texto sin formato a transmisión cifrada autenticada y resistente a la degradación, en lugar de depender de las Autoridades de Certificación (CA), el DANE confía en DNSSEC para publicar claves públicas y certificados para su uso durante el protocolo de enlace TLS. Las extensiones de seguridad del sistema de nombres de dominio (DNSSEC) agregan al origen de los datos de pruebas de autenticación, integridad de datos e inexistencia de datos al Sistema de Nombres de Dominio (DNS). DANE aprovecha la infraestructura DNSSEC para publicar claves públicas y certificados para su uso con el Protocolo de seguridad de capa Transporte (TLS) a través del registro DNS tipo "TLSA". Con DNSSEC, cada dominio solo puede responder por las claves de sus subdominios delegados(Dukhovni & Hardaker, 2015a).

En cambio la tecnología MTA-STS posibilita a los proveedores de servicios de correo proclamar su capacidad para establecer conexiones SMTP seguras basadas en Transport Layer Security (TLS) además de precisar si los servidores SMTP remitentes deben negarse a entregar correos a servidores SMTP destinatarios que no cuenten con un certificado de servidor legítimo (Comply, 2020).

2.2.3. Exhibición de Políticas

El servicio de correo electrónico emisor verificará el registro del sistema de nombres de dominio (DNS) del servicio de correo electrónico receptor para ver si hay una política de MTA-STS. Este archivo de política se la obtiene mediante una URL alojado en un servidor Web HTTPS y se autentica con los certificados en conjunto con los servidores de correo

receptores(PowerDMARC, 2020). Para descubrir si un dominio de destinatario implementa MTA-STS, un remitente necesita solo resolver un registro TXT.

2.2.3.1. Registros TXT

El registro TXT de MTA-STS es un registro con el nombre "_mta-sts" en el dominio de políticas. Para el dominio "example.com", este registro será "_mta-sts.example.com"(Schwittmann et al., 2019). La norma RFC 8461 manifiesta que los registros TXT de MTA-STS Deben ser US-ASCII, pares clave / valor separados por punto y coma que contienen los siguientes campos:

- *"v"* (texto sin formato, obligatorio): actualmente, solo se admite "STSv1".
- *"id"* (texto sin formato, obligatorio): una cadena corta que se utiliza para realizar un seguimiento de la política actualizaciones. El id puede ser cualquier valor alfanumérico con una longitud máxima de 32 caracteres. El valor para "id" se debe modificar cada vez que el archivo de política se modifique(Email Security Geek, 2020).

El valor del texto tiene una estructura muy simple:

v=STSv1; id=20200206T010101;

De acuerdo a la estructura TXT debe comenzar con el campo sts-version; el orden de otros campos no es significativo. Los registros TXT "_mta-sts" no son resueltos por el resolver, para aquellos registros que no comienzan con "v = STSv1;" en otras palabras se descartan. También si el número de registros resultantes es ninguno, o si el registro resultante es sintácticamente inválido.

2.2.3.2. Política MTA-STS

La política MTA-STS es un archivo de texto que se sirve mediante HTTPS. Se debe configurar un servidor web para servir el archivo de política(Gersch et al., 2017). El nombre DNS del host de políticas está construido anteponiendo ***"mta-sts"*** al dominio de políticas, de la siguiente forma ***https://mta-sts.[domain]/.well-known/mta-sts.txt***(Mailhardener, s. f.-a). Este recurso contiene los siguientes pares clave / valor separados por CRLF:

- *Versión:* Siempre debe ser el primer campo, actualmente, solo se admite "STSv1".
- *Modos:* comprende tres modos de operación que son "enforce", "testing" o "none", que indica el comportamiento esperado de un MTA de envío en el caso de una política falla de validación.
- *max_age:* Esto especifica la vida útil máxima de la política en segundos (valor máximo de 31557600).
- *mx:* uno o más campos que contienen los nombres de todos los servidores de dominio MX permitidos. Los patrones válidos pueden ser ya sea nombres completamente especificados ("example.com") o sufijos con el prefijo un comodín ("*.example.net").

Para el dominio *"example.com"* la política debe estar disponible en la siguiente ubicación: ***https://mta-sts.example.com/.well-known/mta-sts.txt***.

La política en sí es bastante sencilla; y quedaría redactada de la siguiente manera:

version: STSv1
mode: testing
mx: mail.example.com
*mx: *.example.net*
mx: backupmx.example.com
max_age: 604800

2.2.3.3. Obtención de una política por HTTPS

Los órganos de políticas se recuperan, mediante el envío de MTA a través de HTTPS, durante el enlace TLS iniciado para obtener una nueva política actualizada del Policy Host, el servidor HTTPS del Policy Host debe presentar un certificado X.509 que sea válido para los "mta-sts" (p. Ej., "mta-sts.example.com") debe encadenar a una CA raíz en la que confíe el MTA remitente y no caducado. Se espera que los MTA de envío utilicen un conjunto de CA confiables similares a los de los navegadores web ampliamente implementados(Australian Cyber Security Centre, 2020).

2.2.4. Validación de políticas

De acuerdo a Helme (2020), un MTA remitente que respete MTA-STS Debe comprobar si:

- Al menos uno de los patrones "mx" de la política coincide con el seleccionado host mx.
- El servidor de correo del destinatario es compatible con STARTTLS y ofrece un certificado PKIX TLS que es válido para ese host.

2.2.5. Aplicación de políticas

Una política MTA-STS se aplica según el valor del campo "modo" de la política. Se puede configurar de tres modos diferentes que son “enforce”, “testing” y “none”, esta aplicación da a entender el comportamiento esperado del servidor de correo electrónico remitente en caso de que se produzca una falla en la validación de la política(Leeman, 2019).

- *Enforce (hacer cumplir):* en este modo, el receptor MTA nunca debe entregar el mensaje a los hosts que no coinciden con su MX, fallas en la validación del certificado o que no sean compatibles con STARTTLS.

- *Testing (prueba):* en este modo, el remitente MTA implementa la especificación TLSRPT (informes de TLS) para enviar un informe indicando fallas en la aplicación de políticas (siempre que TLSRPT también sea implementado por el dominio del destinatario); en cualquier caso, los mensajes pueden entregarse como si no hubiera fallas de validación de MTA-STS.
- *None (ninguno):* El servidor tratará la política como si no tuviera ninguna política activa.

2.2.6. Informe de fallas

MTA-STS está diseñado para usarse junto con TLS Reporting (TLSRPT) para garantizar que la implementación de dominios pueda detectar casos tanto de benignidad y fallas maliciosas para asegurar que los errores que indiquen un ataque activo sean detectables(The Hacker News, 2021) como tal, los remitentes que también implementan TLSRPT debe tratar los siguientes eventos como fallas de notificación:

- La política HTTPS recupera fallas cuando está presente un registro TXT válido.
- La política busca fallas de cualquier tipo cuando existe una política válida en la caché de políticas, excepto si el modo de esa política es "none".
- Intentos de entrega en los que un MX configurado no admite STARTTLS o no presenta certificado que lo valide de acuerdo con la política aplicada, excepto si el modo de esa política es "none".

2.2.7. Consideraciones Operacionales

Es importante conocer las formas de manipulación de las operaciones de la política MTA-STS las cuales se las puede lograr mediante actualizaciones de la política y los registros

TXT y en caso de usar servicios de alojamiento únicamente desde un panel de administración respectivo(James, 2021).

2.2.7.1. Actualización de políticas

Para la actualización de la política se requiere que el propietario realice cambios en dos lugares: el registro TXT *"_mta-sts*" en la zona DNS del dominio de política y en el punto final HTTPS correspondiente. Como resultado, los destinatarios deben esperar que los remitentes sigan utilizando una política hasta que ambos puntos finales HTTPS y TXT se actualicen y el TTL del registro TXT se ha aprobado(D Margolis et al., 2018).

2.2.7.2. Delegación de políticas

Los propietarios de dominios normalmente delegan el alojamiento SMTP a una organización, como un ISP o un servidor web. En tal caso, si se desea delegar una política MTA-STS a una misma organización, se puede lograr con algunos cambios (DuoCircle, 2021).

- Primero, el dominio de políticas debe apuntar al registro "_mta-sts", a través de CNAME, al registro "_mta-sts" mantenido por el proveedor. Esto permite al proveedor controlar la actualización de la señalización(sslmate, 2020).
- En segundo lugar, el dominio de políticas debe señalar la ubicación de la política "conocida" al proveedor. Esto se puede hacer configurando los "mta-sts" registrados en una dirección IP o CNAME especificada por el proveedor(Danmarg, 2021).

2.2.7.3. Eliminar MTA-STS

Con el fin de facilitar la exclusión voluntaria de MTA-STS a un dominio, y para distinguir claramente entre fallas que indican ataques y aquellos que indican tales exclusiones, MTA-STS implementa el modo "none", que permite que las políticas validadas con autoridad del

dominio de políticas ya no desean implementar MTA-STS y puede en el futuro, eliminar los respectivos registros TXT y puntos finales de la política por completo(Google, 2021b).

Un flujo de trabajo sugerido para eliminar MTA-STS comprende lo siguiente:

- Publicar una nueva política con "modo" igual a "none" y una pequeña "max_age" (por ejemplo, un día).
- Publicar un nuevo registro TXT para activar la obtención de una nueva política.

Al momento de que las políticas configuradas ya han expirado con respecto al parámetro "max_age" muchas veces las políticas se superponen con las otras almacenadas en la cache, por lo tanto, se debe eliminar el registro TXT y la publicación HTTPS respectivamente.

2.2.8. Consideraciones de seguridad

SMTP MTA-STS intenta contrarrestar la acción de un atacante activo que intenta interceptar o manipular el correo entre hosts que admitan STARTTLS. Hay dos clases de ataques considerados:

- Frustrar la negociación de TLS (por ejemplo, eliminando la respuesta "250 STARTTLS " de un servidor o alteración de la sesión de negociación TLS). Esto daría lugar a que se produjera la sesión SMTP sobre texto plano, a pesar de que ambas partes admiten TLS(Valsorda, 2015).
- Hacerse pasar por el servidor de correo de destino, por lo que el remitente podría entregar el mensaje a un impostor, quien luego podría monitorear y / o modificar mensajes a pesar de usar TLS oportunista. Esta suplantación se puede lograr falsificando el registro MX del DNS para el dominio del destinatario o redirigiendo las conexiones del cliente destinado al servidor destinatario(Baaten, 2019).

MTA-STS puede frustrar tales ataques solo si el remitente puede obtener previamente y almacenar en caché una política para el dominio del destinatario, y solo si el atacante no puede obtener un certificado válido que cumple con esa política.

2.3. SMTP TLS Reporting

El protocolo TLS-RPT se define en la RFC 8460 y se desarrolló para ampliar MTA-STS y DANE como un mecanismo de notificación. Los mensajes enumerados en el informe pueden ayudar a identificar errores de configuración o incluso ataques activos a las sesiones TLS entre los MTA de ambas partes. Al hacerlo, el informe cubre los errores que ocurren en las áreas de enrutamiento, resolución de nombres DNS, Negociación de parámetros STARTTLS o validación de políticas. Para habilitar TLS-RPT, un administrador necesita establecer otro registro TXT para el dominio de políticas en *smtp. tls. [dominio]*. *[tld]*(Daniel Margolis et al., 2018).

2.3.1. Informe de políticas

Un dominio publica un registro en su DNS indicando que desea recibir informes. Estas políticas SMTP TLSRPT se distribuyen a través del DNS de la zona del dominio de política como registros TXT (similar a los Políticas de autenticación, informes y conformidad de mensajes (DMARC)) bajo el nombre *"_smtp._tls"*(Kucherawy & Zwicky, 2015). Los registros TLS contienen las siguientes directrices:

- *"v"*: define la versión de TLSRPT, actualmente soporta únicamente la versión 1 por lo que valor debe ser igual a "TLSRPTv1.
- *"rua":* Se debe enviar información sobre los resultados de la validación de políticas aun correo electrónico recientemente creado, se admiten dos esquemas: "mailto" y "https". Como con DMARC, el dominio de políticas puede especificar una lista separada por comas de URI.

En el caso de "https", los informes deben enviarse a través de POST al URI especificado. Los remitentes de informes pueden ignorar errores de validación de certificados al enviar informes a través de HTTPS POST. Para la opción de "mailto", los informes deben enviarse a la dirección de correo electrónico especificada.

Para habilitar los informes SMTP TLS, se debe agregar un registro DNS de tipo TXT al subdominio ***_smtp. _tls. [Domain].*** Los informes se envían a la dirección especificada en el registro DNS(Mailhardener, s. f.-b).

2.3.1.1. Informe usando mailto

Considerando el dominio example.com los informes se envían a la dirección especificada en el registro DNS.

_smtp._tls.example.com. EN TXT \
"v = TLSRPTv1; rua = mailto: informes@example.com"

2.3.1.2. Informe usando HTTPS

El uso del esquema HTTPS requiere un servidor web habilitado para HTTPS con un certificado válido para el dominio, el MTA que informa lo hará a POST través de HTTPS.

_smtp._tls.example.com. EN TXT \
*"v = TLSRPTv1; *
rua = https: //reporting.example.com/v1/tlsrpt "

2.3.2. Esquema de reportes

El informe está compuesto como un archivo de texto formato codificado en Internet Formato JSON (I-JSON)(Grandstream Networks, 2020). Los informes proporcionados contienen los siguientes parámetros:

- La organización responsable del informe.
- Un identificador único para el informe.
- El intervalo de fechas en el que se recopilaron los resultados.
- Nombre e información de contacto de la parte denunciante.
- Los diversos resultados de la política.

2.3.2.1. Marco de tiempo del informe

El informe debe cubrir un día completo, de 00: 00-24: 00 UTC. Esto debe permitir una correlación más fácil de los eventos de falla. Para evitar sobrecargar involuntariamente el sistema que procesa los informes, estos deben entregarse después de cierto retraso, quizás varias horas(Scaife, 2019).

2.3.2.2. Resumen de entregas

Según Daniel Margolis et al. (2018) manifiesta que las entregas de los reportes se definen de la siguiente manera:

- *"total-Success-session-count":* esto indica que el MTA de envío pudo negociar con éxito una conexión TLS compatible con la política y sirve para proporcionar un "latido" para recibir dominios que significa que la presentación de informes es funcional y tabulado correctamente.
- *"total-failure-session-count":* esto indica que el MTA de envío no pudo establecer correctamente una conexión con la plataforma receptora. Elaborará un informe sobre los intentos fallidos de negociación.

2.3.2.3. Tipo de fallas

Los informes SMTP TLS se utilizan para informar fallas durante la negociación SMTP TLS. Según las validaciones descritas por Brotman et al. (2018) con respecto a STARTTLS Validation Result Types se tiene las siguientes tipos de resultados:

- **Fallos de negociación TLS**

Un error de negociación TLS del cliente se refiere a que una conexión TLS iniciada por el cliente no pudo establecer una sesión con el equilibrador de carga. Los errores de negociación TLS ocurren cuando los clientes intentan conectarse a un equilibrador de carga mediante un protocolo o cifrado que la política de seguridad del equilibrador de carga no admite(Amazon Web Services, 2020). Según la norma RFC 8460 fallos más comunes durante la fase de negociación TLS son las que se detallan en la Tabla 1.

Tabla 1.

Descripción de los Fallos en la Negociación TLS

Valor	Descripción
starttls-not-supported	El MTA destinatario no admite STARTTLS
certificate-host-mismatch	El certificado del MTA destinatario no coincide con el nombre del host mx.
certificate-not-trusted	El certificado del MTA destinatario no es de confianza para el remitente.
certificate-expired	El certificado del MTA destinatario venció.
validation-failure	Cualquier falla de validación general que no coincida con ninguna de las categorías anteriores

- **Fallas Relacionadas al DNS**

La DNSSEC y la cadena de confianza CA / TLS han sido independientes y no están vinculadas entre sí. Esto ha provocado problemas de seguridad relacionados con la información de la base de datos de DNS o con el emisor de CA que se ve comprometido(Hogg, 2014). Las fallas más notables según el estándar RFC 8460 se registran en la Tabla 2

Tabla 2.

Descripción de los Fallos Relacionado al DNS

Valor	Descripción
tlsa-invalid	Indica un error de validación en el registro TLSA asociado con una política del DANE.
dnssec-invalid	Indica que no se incluyeron registros válidos devuelto por el validador recursivo.
dane-required	Indica que el sistema de envío está configurado para requerir registros DANE TLSA para todos los hosts MX del dominio de destino, pero no había registros TLSA validados por DNSSEC para el host MX que es el tema del informe.

- **Fallos relacionados con MTA-STS**

Este tipo de fallos hace referencia a la dificultad de obtener y validar la política MTA-STS por parte del remitente por errores en la configuración del servidor web que aloja la política, errores de sintaxis en el archivo TXT de la política y problemas en los certificados digitales de los servidores. Los fallos más importantes en relación a MTA-STS según la RFC 8460 son las que se especifican en la Tabla 3.

Tabla 3.

Descripción de los Fallos con MTA-STS

Valor	Descripción
sts-policy-fetch-error	El remitente no pudo obtener la política MTA-STS a través de HTTPS.
sts-policy-invalid	La política MTA-STS se pudo recuperar, pero no validar. Esto suele indicar algún error de sintaxis en la política.
sts-webpki-invalid	No se pudo recuperar la política MTA-STS debido a un problema de validación de PKI. Esto indica un problema con el certificado proporcionado por el servidor web que aloja el archivo de política MTA-STS.

2.3.3. Informe de diagnóstico JSON

El informe se compone de un archivo de texto sin formato codificado en JSON. El informe debe cubrir un día completo, de 00: 00-24: 00 UTC, que según Evans et al. (2015) permitirá una correlación más fácil ante los eventos de falla y evitar la sobrecarga del proceso de informes, por tal razón los informes se deberán entregar después de algún retraso.

Según Tim Bray (2017) los informes agregados deben contener los siguientes campos:

- *"organization-name":* la organización responsable del reporte.
- *"date-time":* la fecha-hora indica las horas de inicio y finalización del rango del informe. El informe debe ser para un día UTC completo, 00: 00-24: 00.
- *"dirección de correo electrónico":* la información de contacto de la parte responsable para el informe.
- *"report-id":* Único identificado para el reporte.
- *"policy-type":* La política que se aplicó al dominio. Las tres opciones válidas hasta ahora: "*tlsa*", "*sts*" y "*no-policy-found*".
- *"policy-string":* Una codificación de la política aplicada como una matriz de cadenas JSON.
- *"policy-domain":* El dominio de política contra el cual se define la política MTA-STS o DANE.
- *"mx-host":* Para sts: el patrón de nombres de host MX de la política aplicada que se proporciona como una matriz JSON de cadenas.
- *"result-type":* Tipos de resultado.
- *"ip-address":* La dirección IP del MTA remitente.
- *"receiving-mx-hostname":* el nombre de host del MTA MX receptor registro con el que el MTA remitente intentó negociar una Conexión STARTTLS.
- *"receiving-ip":* La dirección IP de destino que se resolvió desde MX para la sesión saliente.
- *"total-successful-session-count":* El número de sesiones (intentadas) que coinciden con el tipo de resultado exitoso.
- *"total-failure-session-count":* El número de sesiones (intentadas) que coinciden con el tipo de resultado fallido.

- *"failure-reason-code":* Un campo de texto para incluir un código de error o mensaje de error relacionado con TLS.

En la Figura 8 se detalla el informe de reporte JSON:

Figura 8.

Esquema de un Informe TLSRPT (JSON)

```
{
    "organization-name": "Google Inc.",
    "date-range": {
        "start-datetime": "2019-12-11T00:00:00Z",
        "end-datetime": "2019-12-11T23:59:59Z"
    },
    "contact-info": "smtp-tls-reporting@google.com",
    "report-id": "2019-12-11T00:00:00Z_example.com",
    "policies": [
        {
            "policy": {
                "policy-type": "sts",
                "policy-string": [
                    "version: STSv1",
                    "mode: enforce",
                    "mx: mail1.example.com",
                    "mx: mail2.example.com",
                    "max_age: 86401"
                ],
                "policy-domain": "example.com"
            },
            "summary": {
                "total-successful-session-count": 773,
                "total-failure-session-count": 0
            }
        }
    ]
}
```

Nota. Este informe muestra que el MTA de Google (para Gmail y G Suite) detectó con éxito una política MTA-STS para el dominio example.com y que hubo 773 sesiones TLS exitosas (correos electrónicos entregados desde el MTA de Google a su dominio) durante el período del informe. Tomada de (JamieWeb, 2019).

2.3.4. Entrega de informes

Los reportes se pueden enviar por medio de correo electrónico o mediante un Post HTTP.

2.3.4.1. Nombre del archivo de informe

La norma RFC 8460 recomienda nombrar al archivo mediante el siguiente argumento:

nombre de archivo = *remitente "!" dominio-política "!" start-timestamp "!" marca de tiempo final ["!" Identificación única] "." extensión*

Por ejemplo, esta es un posible nombre de archivo para un informe comprimido al dominio de políticas *"example.net"* del MTA de envío *"mail.sndr.example.com":*

"mail.sndr.example.com! example.net! 1470013207! 1470186007! 001.json.gz"

2.3.4.2. Compresión

El reporte debe estar sujeto a una compresión ***gzip*** tanto para correo electrónico y transporte HTTPS. Al no aplicar esta técnica puede ocasionar que un informe de gran tamaño sea demasiado proceso para el receptor(Deutsch, 1996).

2.3.4.3. Medios de entrega de informes TLS

El reporte se puede enviar por correo electrónico. Para lograr que los informes sean analizables por los receptores, se define un tipo de nivel superior *"multipart / report"*, agregando un nuevo parámetro "report-type =" tlsrpt "". En su interior, hay dos partes: la primera parte es legible por humanos, normalmente "texto / sin formato", y la segunda parte es legible por máquina con un nuevo tipo de medio definido llamado "application / tlsrpt + json". Si es comprimido, el informe debe utilizar el tipo de medio "aplicación / tlsrpt + gzip "(Daniel Margolis et al., 2018).

El reporte puede ser entregado vía Post HTTPS. Si está comprimido, el informe debe usar el tipo de medio "application / tlsrpt + gzip"; de lo contrario debe usar el tipo de medio "application / tlsrpt + json"(Melnikov & Dukhovni, 2018). El sistema receptor debe devolver una respuesta "satisfactoria" del servidor HTTPS, normalmente un código HTTP 200 o 201. No se espera que el sistema receptor procese informes en el momento de la recepción y puede almacenarlos para su procesamiento en un determinado tiempo.

2.3.4.4. Reintento de entrega

En caso de haber falla en la entrega, independientemente del método utilizado, el remitente debe intentar volver a enviarlo después de 24 horas al intento inicial. Como se indicó anteriormente, los informes son opcionales, por lo que, si bien es ideal intentar una nueva entrega, no es necesario.

2.3.5. Consideraciones de seguridad

Los informes SMTP TLS proporcionan visibilidad de las configuraciones erróneas o ataques de interceptación del correo entre host que soportan STARTTLS(Fenton, 2019). Existen algunos riesgos de seguridad presentados por la existencia de este canal de informes:

- *Inundación del extremo URI del informe agregado (rua):* un atacante podría inundar el punto final con tráfico de informes excesivo y evitar que el dominio receptor acepte informes adicionales.
- *Contenido que no es de confianza:* un atacante podría inyectar código malicioso en el informe, explotando cualquier vulnerabilidad en el manejo de informes al sistema del dominio receptor.
- *Informar espionaje:* un atacante podría crear un registro TLSRPT falso para recibir estadísticas sobre un dominio que el atacante no posee.

- *Ignorar la validación HTTPS al enviar informes:* al informar configuraciones erróneas benignas, es probable que un servidor SMTP esté mal configurado o también puede significar un servidor HTTPS mal configurado; como resultado, los reportes que requieren validez HTTPS en el punto final de reporte pueden no alertar a los administradores sobre tales configuraciones incorrectas. Por el contrario, en el caso de un ataque real, un atacante que desea crear una brecha en los informes podría interceptar informes HTTPS, con la misma facilidad, simplemente frustrar la resolución del Registro TLSRPT TXT o establecimiento de la sesión TCP al HTTPS final(Hoffman, 1999).

Capítulo 3. DISEÑO DEL SISTEMA

Este capítulo corresponde al análisis y desarrollo de la arquitectura del sistema, que, siguiendo la metodología General de Deming correspondiente a la fase de planificación, consiste en determinar las características y requerimientos del sistema. Inicialmente se abordará la explicación del propósito general del sistema, luego en base a la metodología RAD se define el proceso de desarrollo de la arquitectura del sistema, el cual se encargará de especificar las características del producto final, basado en sus componentes y la interacción entre ellas, el principio de operación, la implementación junto a las pruebas de validación del estándar MTA-STS y TLS Reporting.

3.1. Descripción General del Sistema

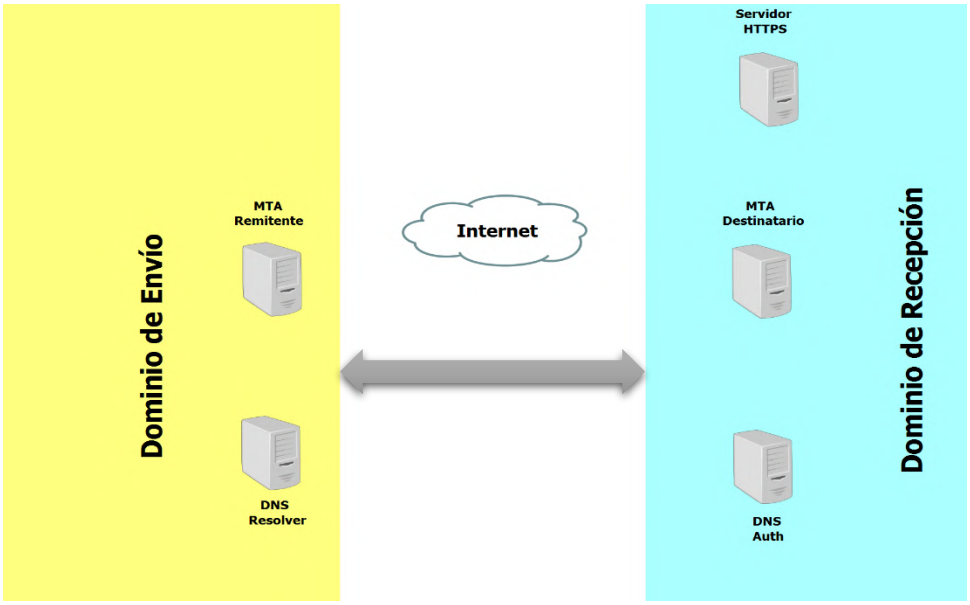
Cuando se envía un correo electrónico, el servidor de correo electrónico (MTA) destinatario determinará dónde entregar el correo electrónico consultando los registros MX del dominio receptor a través de DNS. Con MTA-STS, las direcciones MX obtenidas a través de DNS se comparan con las que se encuentran en el archivo de política MTA-STS, que se encuentra alojada en un sitio web HTTPS.

3.2. Arquitectura del sistema

La arquitectura general del sistema corresponde a un servidor de correo remitente y destinatario las cuales se comunican entre sí para establecer una conexión encriptada. Para describir el proceso de comunicación entre Agentes de Transferencia de Correo (MTA) que admiten Transporte Seguro Estricto se recurrió a una arquitectura servidor-servidor en donde se identifica el dominio de envió y de recepción con sus respectivos componentes, la cual se ilustra en la Figura 9.

Figura 9.

Arquitectura General del Sistema



Nota. Adaptado de (Hardaker & Dukhovni, 2019)

El desarrollo de la arquitectura implica dar forma al sistema, para lo cual es necesario definir un modelo de desarrollo de aplicaciones ágiles, que se traduce en un proceso secuencial para crear los diseños de forma rápida y barata de tal forma que pueda satisfacer las necesidades empresariales(Bunge, 2002). Según Salazar (2014) la Metodología RAD (Rapid Application Development) es considerada una de las mejores para agilizar los procesos de desarrollo de aplicaciones y dar forma al diseño, además de definir un marco para desarrollar el proyecto. Por esta razón se utilizará éste modelo de desarrollo rápido de aplicaciones, la cual según Campaña (2015) consta de las siguientes fases: Planificación de requisitos, Diseño, Construcción y transición.

A continuación, se describe el proceso de desarrollo en cada una de las etapas:

3.2.1. Requerimientos

En esta etapa se recolecta la información y se documenta los requerimientos que influyen en cada uno de los componentes del dominio de recepción. Para este apartado se ha elaborado un informe correspondiente al análisis de los requerimientos que se documenta en el ANEXO 1.

Lo primero que se ha hecho es especificar los requerimientos funcionales y no funcionales para los servicios del dominio de recepción. A continuación, en la Tabla 4 que fue extraída del ANEXO 1 se detalla cada uno de los requerimientos funcionales (RQ_F#) y no funcionales (RQ_NF#) de los servicios que forman parte del dominio de correo entrante.

Tabla 4.

Requerimientos Funcionales y no Funcionales del Dominio

Servicio	Nro.	Requerimiento	*Clasificación*	Descripción
Hosting	RQ_F1	Certificado de seguridad SSL	Funcional	Contar con un certificado SSL para los dominios y subdominios.
	RQ_F2	Seguridad General	Funcional	Deben incluir las características básicas de seguridad para preservar la integridad del hosting.
	RQ_F3	Dominio	Funcional	Brindar un dominio registrable con un nombre específico.
	RQ_F4	Interfaz	Funcional	Incluir una adecuada interacción y administración de los usuarios con la aplicación.
	RQ_F5	Integración a servicios de alojamiento basados en la nube.	Funcional	Permitir el alojamiento del dominio a un nuevo espacio de trabajo digital integrado.

	RQ_NF6	Almacenamiento	No funcional	Una buena cantidad de almacenamiento de datos para el servicio de alojamiento web.
	RQ_NF7	Soporte	No funcional	Una atención rápida al cliente las 24 horas, los 7 días de la semana en caso de fallas en el hosting.
Servidor Web alojado	RQ_F8	Admitir SSL/HTTPS	Funcional	Corresponde a un servidor web basado en el protocolo HTTPS con un certificado SSL.
	RQ_F9	Certificado válido y firmado por una Autoridad certificadora de confianza.	Funcional	El servidor debe disponer de un certificado valido emitido por una autoridad de confianza(CA) para proteger el sitios web.
	RQ_NF10	Rendimiento	No funcional	Comprende una buena velocidad de carga y estabilidad del sitio web.
	RQ_NF11	Usabilidad	No funcional	El servidor debe contar con una buena usabilidad que permita al usuario navegar de forma sencilla y cómoda.
Servidor de correo alojado	RQ_F12	Admitir conexión segura TLS	Funcional	Requieren que el correo se transmita a través de una conexión segura TLS.
	RQ_F13	Versión TLS 1.2 o superior	Funcional	Posibilidad de habilitar Transport Layer Security (TLS) 1.2 o versiones superiores para proteger las conexiones entre servidores.
	RQ_F14	Certificado válido y firmado por una Autoridad certificadora de confianza	Funcional	Los certificados deben estar firmados por una autoridad de certificación raíz que los considera de confianza.

RQ_F15	Certificados digitales no caducados	Funcional	En caso de que él certificado esté caducado proceder a renovarlo.
RQ_F16	Soporte MTA-STS y TLS Reporting	Funcional	Proveer soporte nativo para MTA-STS relacionado a la publicación y resolución de políticas además del soporte para reportes TLS en el dominio.
RQ_NF17	Usabilidad	No funcional	Brindar una buena experiencia de navegación de la plataforma al usuario en términos de eficiencia y rapidez.
RQ_NF18	Rendimiento	No funcional	Una fluidez al momento de entablar conexiones entre servicios de correo.
RQ_NF19	Portabilidad	No funcional	Una gestión de preferencia basada completamente en la nube.
RQ_NF20	Seguridad	No funcional	Integración de funcionalidades para proteger el acceso al correo electrónico.
RQ_NF21	Fiabilidad	No funcional	Comprende un entorno muy seguro y fiable.
RQ_NF22	Soporte	No funcional	Soporte para temas de problemas de administración todos los días de año.

En base al análisis de la Tabla 2 del ANEXO 1 correspondiente a la Tabla comparativa de requerimientos entre HostGator y GoDaddy que son las plataformas de alojamiento en la nube a comparar, se estableció que HostGator cumple con mayor robustez que GoDaddy cada uno de

los requerimientos identificados, por esto se opta por utilizar un dominio registrado proporcionado por HostGator que a su vez servirá para configurar el sitio web.

Se ha elaborado una tabla resumen en donde se validan cada uno de los requerimientos funcionales y no funcionales para el servicio web y de hosting en base a las plataformas utilizables; la cual se la ilustra en la Tabla 5.

Tabla 5.

Comparativa de Requerimientos para las Plataformas de Hosting

Servicio	Nro. Requerimiento	Proveedor	
		HostGator	GoDaddy
Hosting	RQ_F1	✓	**X**
	RQ_F2	✓	**X**
	RQ_F3	**X**	✓
	RQ_F4	✓	✓
	RQ_F5	✓	✓
	RQ_NF6	✓	✓
	RQ_NF7	✓	**X**
Web	RQ_F8	✓	**X**
	RQ_F9	✓	**X**
	RQ_NF10	✓	✓
	RQ_NF11	✓	✓

Para este proyecto se pretende montar un servidor de correo electrónico propio de tal manera que el dominio de correo pueda enviar y recibir emails seguros de un usuario@nombre_dominio.com. Para esto se determinó las características que debe tener el servicio de correo para emplear MTA-STS y TLS Reporting que según Misle (2020) es propio de algunas proveedores de correo electrónico profesional, por esta razón lo ideal es registrar el dominio en ciertas plataformas de servicios de internet para adquirir ésta funcionalidad avanzada para correo electrónico empresarial.

Por ello al igual que con el Hosting Web se ha identificado los requerimientos funcionales y no funcionales que debe cumplir el servidor de correo destinatario. El estudio se lo ha hecho en base a tres proveedores de alojamiento de dominio para correo electrónico empresarial que son: Google Workspace, Yahoo! Mail y Microsoft Exchange. En la Tabla 3 del ANEXO 1 que corresponde a la comparativa de requerimientos entre las tres proveedoras, se ha determinado que Google Workspace es la mejor opción por que cumple en mayor medida todos los requerimientos solicitados, además es el único de los tres que cuenta con el soporte para MTA-STS y TLS Reporting, es así que se inclina por adquirir una suscripción a Google Workspace cuya funcionalidad MTA-STS se encuentra disponible para los administradores del servicio en cualquier plan.

La Tabla 6 detalla la validación de los requerimientos funcionales y no funcionales para el servicio de correo con las tres plataformas analizadas.

Tabla 6.

Comparativa de Requerimientos Para el Servidor de Correo a Utilizar

Servicio	Nro. Requerimiento	Proveedor		
		Google Workspace	Yahoo! Mail	Microsoft Exchange
Correo	RQ_F12	✓	✓	✓
	RQ_F13	✓	✓	✓
	RQ_F14	✓	✓	✓
	RQ_F15	✓	✓	✓
	RQ_F16	✓	**X**	**X**
	RQ_NF17	✓	**X**	**X**
	RQ_NF18	✓	✓	**X**
	RQ_NF19	✓	✓	**X**
	RQ_NF20	✓	✓	✓
	RQ_NF21	✓	**X**	✓
	RQ_NF21	✓	✓	✓

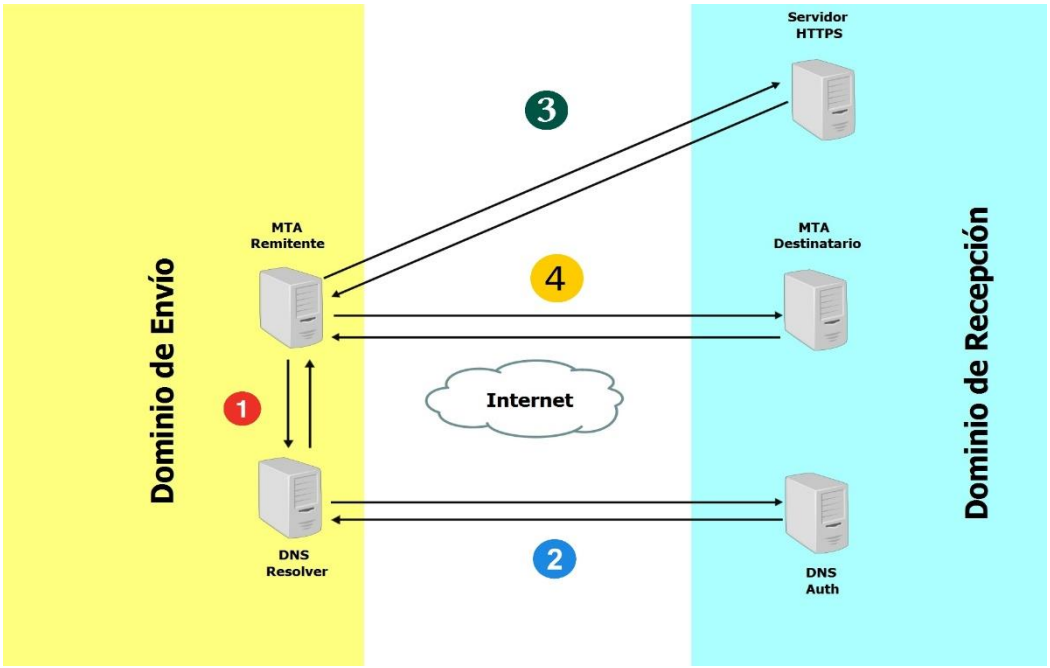
3.2.2. Diseño

Esta fase consiste en definir explícitamente la arquitectura del sistema, en donde se enumera los componentes del sistema, las funciones de cada componente y el proceso de interacción entre las mismas tal y como se indica en la Figura 10. Este trabajo se centra en la implementación de los mecanismos MTA-STS y TLS Reporting para el servicio de correo

entrante; por consiguiente, se hace uso de un Agente de Transferencia de correo denominada MTA para la recepción de emails de un determinado dominio de correo. Además, se sabe que para implementar MTA-STS se requiere un servidor web habilitado para HTTPS con un certificado válido emitido por una CA de confianza, de tal manera que el contenido pueda visualizarse en internet de manera segura. También se debe gestionar los registros MX de zonas que definen la funcionalidad del protocolo mediante el DNS Autorizado. Es decir, en la parte del destinatario se hace uso de tres servicios las cuales son: el servidor de correo MTA, un servidor HTTPS y el DNS. Para la parte del remitente se requiere de un servidor de correo MTA por donde se enviará los mensajes de email y también del DNS que sea capaz de resolver los registros que el DNS Autorizado ha publicado.

Figura 10.

Comunicación entre los Dominios de Envío y Recepción.



A continuación, se especifica en que consiste los componentes del servidor de recepción y de envío.

3.2.2.1. Dominio de Recepción

El Dominio de correo destinatario es en donde se implementará las políticas MTS-STS por medio de un servidor web seguro, además de los registros DNS necesarios para activar el protocolo de transporte seguro estricto y los reportes TLS. El dominio entrante consta de los siguientes elementos:

- ***DNS Auth***

Corresponde al Sistema de nombres de dominio (DNS) del servicio de correo electrónico, éste almacena los registros que notifica la existencia de una política MTA-STS y el mecanismo de reportes TLS.(United Kingdom Public Sector Government, 2021).

- ***Servidor Web HTTPS***

El servidor web Hosting almacenará una política MTA-STS, la cual se lo debe publicar en un subdominio especial con el nombre de *mta-sts* y una ruta especial conocida. La política contiene una lista de servidores de correo electrónico (MX) a los que conectarse(Dubrovin, 2020).

- ***Servidor de correo entrante***

Una vez que se ha activado MTA-STS en el dominio, éste solicita a los servidores externos o remitentes que le envíen mensajes de correo solo si la conexión esta autenticada con un certificado valido y cifrada con TLS 1.2 o superior(Google, 2021a).

3.2.2.2. Dominio de Envío

El dominio de correo remitente solicita los respectivos registros y la política DNS por medio de HTTPS (comprobando el certificado). La política obtenida se almacena directamente en la caché en caso de que un atacante bloquee el acceso a ella o falsifique el registro DNS(Dubrovin 2020). El dominio saliente tiene los siguientes elementos:

- ***DNS Resolver***

Verifica, resuelve y solicita los registros ***_mta-sts***, ***_smtp. _tls***, que contiene la política MTA-STS y los reportes TLS que identifica de forma única una versión de política en particular. El archivo de texto resuelto se almacenará en la memoria cache del servidor de correo saliente(Ristic, 2019).

- ***Servidor de correo saliente***

Éste verificará el registro DNS del servidor de correo entrante para determinar si hay una política MTA-STS de un determinado dominio en una ruta conocida. Si el servidor no tiene una política almacenada en su caché el servidor descargará automáticamente la política de la ruta conocida del dominio entrante(Mailhardener, s. f.-a).

3.2.3. Construcción

En esta etapa se adecua las características específicas del sistema junto a algunos detalles para llevar a cabo el modelo de construcción. La construcción de la aplicación debe consistir en una serie de pasos que se debe seguir para el proceso de integración de las funcionalidades del sistema. Aquí se desarrollan todos los procedimientos de operación y se elaboran los manuales de administración para un usuario final, todo esto con la finalidad de asegurar su correcto funcionamiento a partir de la verificación(Cillero, 2019).

En esta línea se detallará el proceso de implementación de los estándares en un dominio de correo electrónico de recepción mediante el uso de las plataformas de trabajo especificadas en la parte de requerimientos. El servidor de correo destinatario MTA funcionará en base al dominio registrado que se nos ha proporcionado HostGator, este dominio se lo debe registrar y validar en Google Workspace mediante una serie de pasos que involucra la adición de algunos registros DNS proporcionados por Google directamente en el panel de administración de HostGator, una vez validado el dominio se deberá esperar un tiempo prudencial hasta que los nuevos registros DNS añadidos sean propagados en el dominio.

Además, se requiere un servidor web HTTPS con un certificado válido, de tal manera que el contenido pueda visualizarse en internet de manera segura. Para ello se debe realizar los ajustes pertinentes del dominio obtenido en HostGator para que los sitios sean visibles en la internet. Primero se definirá la política correspondiente a MTA-STS, para eso se procede a crear un archivo de texto el cual tendrá una estructura específica con respecto a las configuraciones del DNS, este archivo de texto lo guardamos para utilizarlo más adelante. Después se configura el servidor HTTPS para entregar el archivo en el formato correcto, para esto primero se crea un subdominio con el nombre de *mta-sts,* en esta ruta se define un directorio denominado *well-known* que es en donde se cargará el archivo de texto TXT que contiene la política anteriormente creada. Es decir, para un dominio *"example.com"*, la URL que aloja la política será: ***https://mta-sts.example.com/.well-known/mta-sts.txt***. Y finalmente para activar MTA-STS, se debe actualizar la configuración del dominio con dos registros TXT de DNS añadido a los subdominios que son: *"_mta-sts"* y "*_smtp. _tls"*. Una vez que los registros DNS se haya establecido y propagado, MTA-STS se habilitará con la política configurada y comenzará a recibir informes TLS en la dirección que se especificó.

A continuación, se detalla el proceso de implementación mediante un diagrama de flujo que se observa en la Figura 11.

Figura 11.

Diagrama de Flujo para Implementar MTA-STS y TLS-RPT

Una vez que se haya terminado de ajustar su configuración se procede a probar su implementación basado en un agregado de pruebas MTA-STS que brinda ciertas páginas web que funciona al ejecutar la evaluación del dominio; en concreto se hará un test de evaluación al dominio para comprobar que todo este configurado correctamente, caso de encontrar errores se procederá a corregirlos en base al análisis de los resultados que proporcionará la plataforma web.

3.2.4. Transición

En esta última etapa se le permite al equipo de desarrollo mover todos sus componentes del sistema para un entorno de producción en vivo de tal manera que se pueda determinar su funcionamiento; adicionalmente se deberán llevar a cabo todas las pruebas pertinentes(Gómez Zea, 2016).

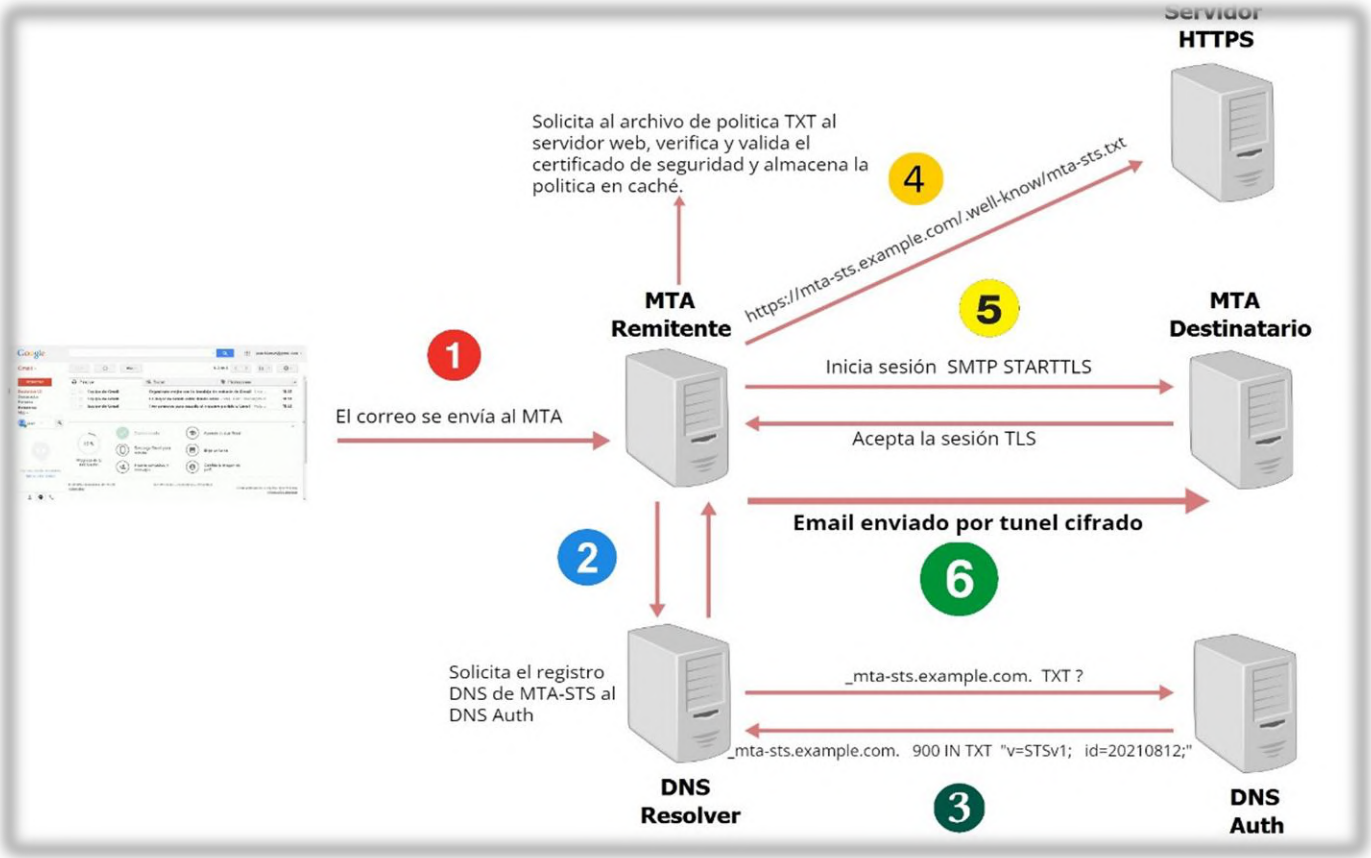
Por ende, es importante especificar el funcionamiento del sistema en función del envío y recepción del correo para comprobar la funcionalidad del protocolo en el sistema de dominios de correo electrónico.

El proceso de funcionamiento de todo el sistema se detallará a continuación. Al configurar MTA-STS en un dominio, se solicita a los servidores externos que envíen emails a nuestro dominio solo cuando la conexión SMTP se encuentren autenticadas y cifradas. El proceso de conexión inicia cuando dos agentes de transferencia de correo intercambian mensajes, en este caso un dominio de correo remitente enviará un correo a nuestro dominio que ha publicado una política MTA-STS. El servidor de correo remitente enviará un mensaje de email desde el agente de usuario de correo, este mensaje se almacenará en el MTA Remitente el cual se encargará de enviar el correo al MTA Destinatario. El MTA Remitente busca el archivo de política TXT de MTA-STS en su DNS Resolver, si encuentra una política almacenada en su cache el mensaje se enviará rápidamente por TLS estricto, en el caso de que no haya ninguna

política almacenada en su caché, El DNS resolver pregunta y solicita el archivo TXT al DNS Auth, el DNS Auth devuelve el contenido del campo MTA-STS al DNS del remitente. Luego el MTA remitente solicita la política de seguridad TXT al servidor HTTPS en donde se verifica el certificado de seguridad TLS X509 para después almacenar la política en su cache DNS, el MTA remitente valida el certificado X509, y luego se inicia la sesión TLS estricta con el MTA Destinatario para finalmente establecer un túnel de comunicación cifrado entre los MTA y enviar el correo de manera segura. Todo el proceso de comunicación basado en el mecanismo MTA-STS se lo detalla en la figura 12.

Figura 12.

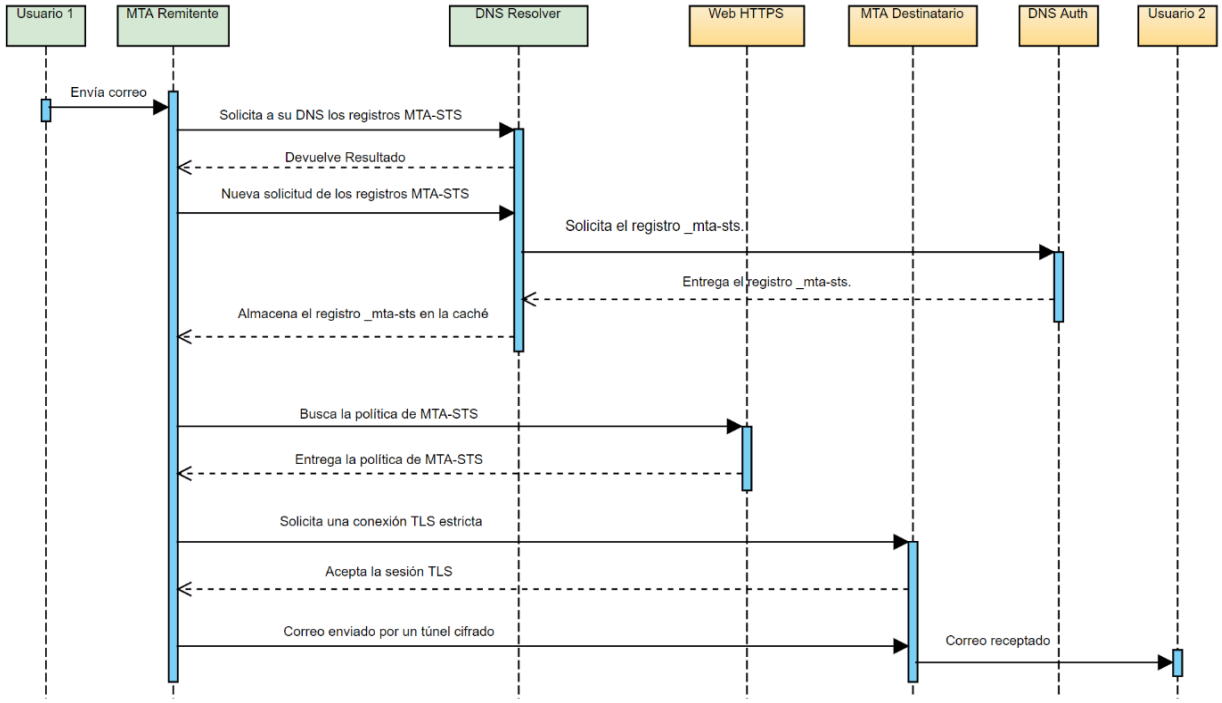
Esquema de Funcionamiento del Sistema con MTA-STS



De igual forma en la Figura 13 se representa todo este proceso mediante un diagrama de secuencias para un mayor entendimiento.

Figura 13.

Diagrama de Secuencias de la Operación de MTA-STS



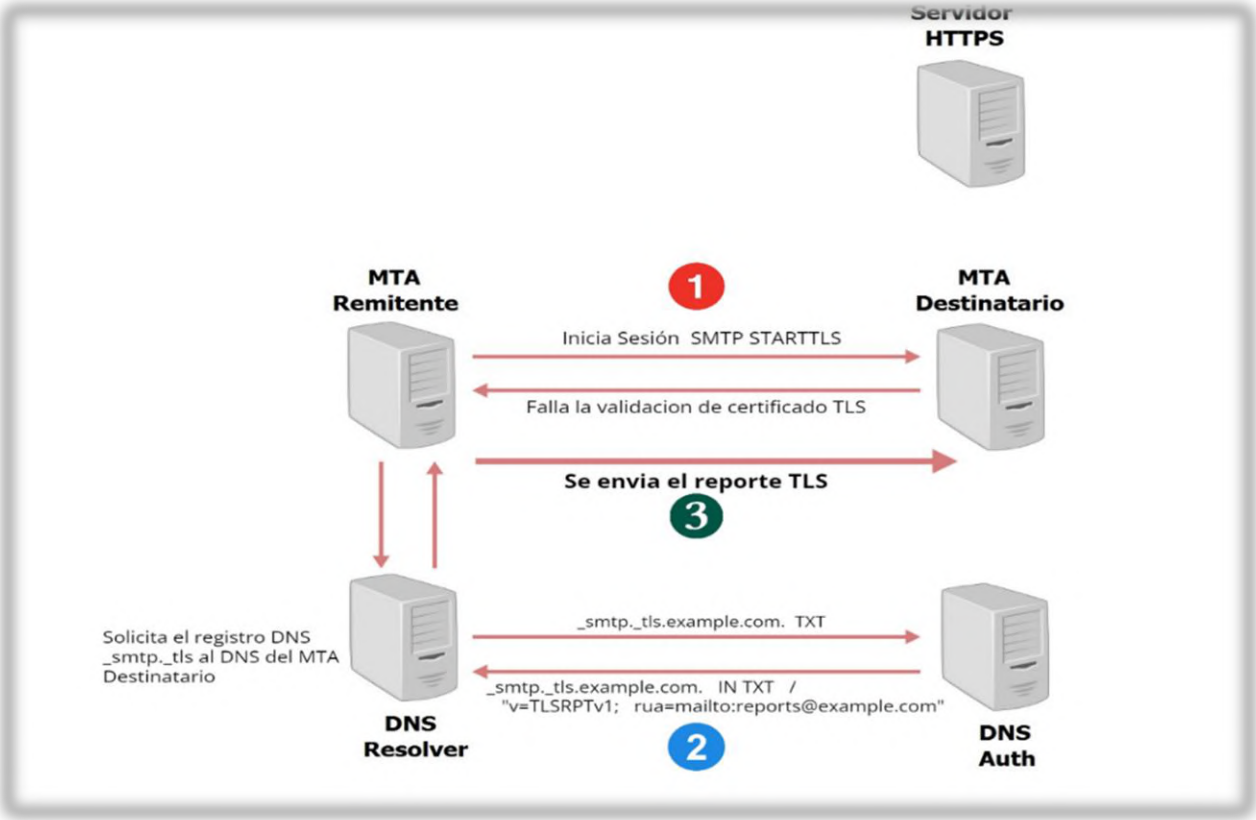
Al igual que MTA-STS, TLS Reporting es un estándar que proporciona notificaciones TLS acerca de los problemas de conectividad y algunas discrepancias durante la comunicación entre agentes de correo. Una vez que se habilita las notificaciones TLS, se envía informes diarios sobre los problemas de conexión que experimentan el servidor de correo saliente al momento de enviar correos electrónicos al servidor de correo entrante.

Para activar los reportes TLS se debe publicar un registro DNS con el nombre *_smtp._tls*, en el panel de administración del servidor DNS, este registro manifiesta porque medio y hacia qué dirección se debe enviar los informes TLS-RPT. Los servicios de envío de correo

electrónico verifican el registro y, si existe, enviarán un informe a la dirección proporcionada. Los informes son agregados, por lo que solo obtendrá por día de cada servicio de envío. En la Figura 14, se representa el esquema de funcionamiento del protocolo TLS-RPT en el sistema de dominio de correo de emisión y recepción.

Figura 14.

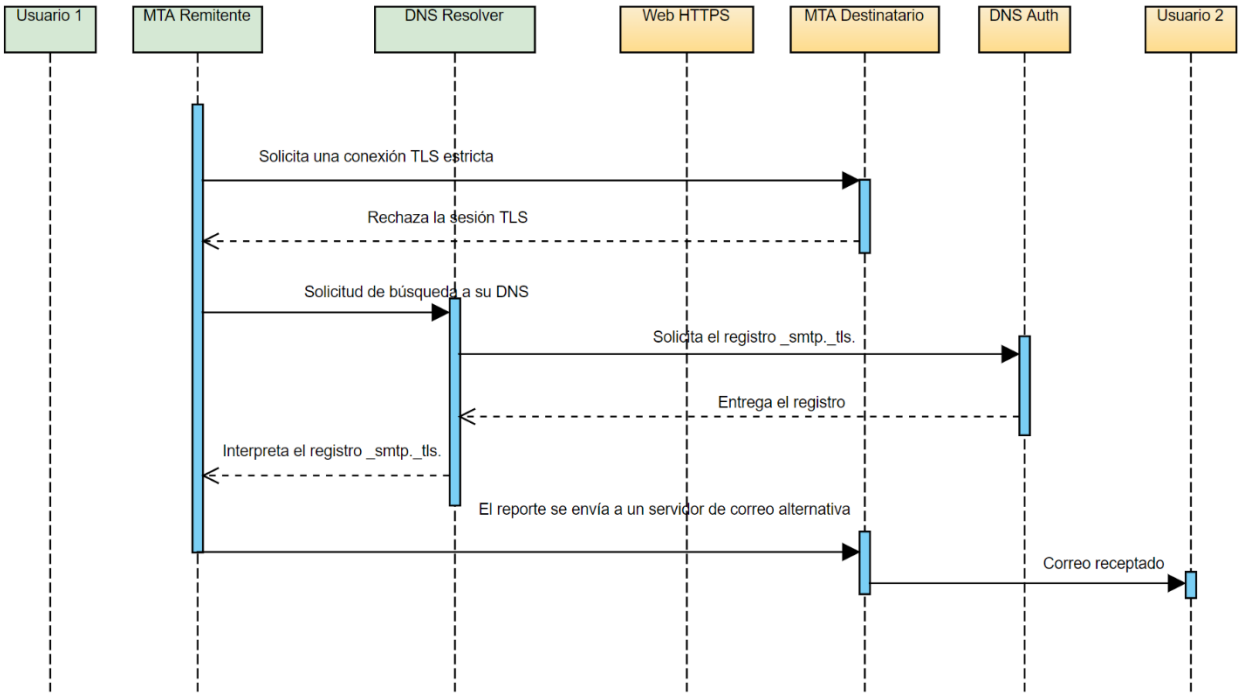
Esquema de Funcionamiento del Sistema con TLS Reporting



Este proceso de entrega de reportes TLS se la puntualiza en un diagrama de secuencias la misma que se visualiza en la Figura 15.

Figura 15.

Esquema de Funcionamiento del Sistema con TLS Reporting



En siguiente capítulo referente a la implementación y pruebas se detallará las pruebas realizadas tomando en cuenta un escenario de pruebas en correspondencia a algunas consideraciones que se definirán posteriormente.

Capítulo 4. IMPLEMENTACIÓN Y PRUEBAS

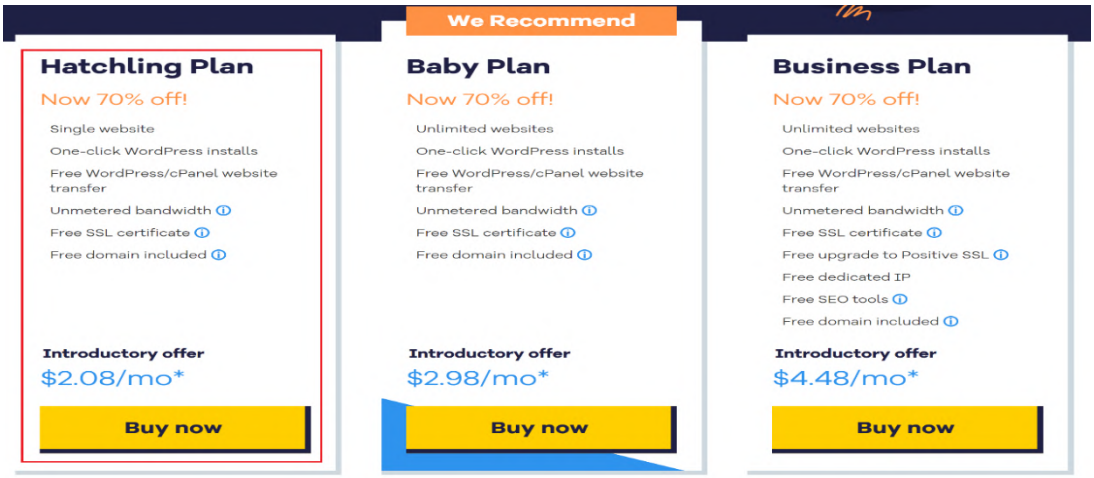
Este capítulo abarca el proceso para la implementación del estándar MTA-STS y TLS Reporting en un dominio de correo, proceso que se logra en base a la Figura 11 correspondiente al diagrama de flujo para implementar los estándares, la cual está definida en la fase de construcción de la arquitectura del sistema descrita en el capítulo anterior. Finalmente se procede a la definición de un escenario de pruebas con la finalidad de comprobar la recepción del correo electrónico seguro. Además, se desarrollará una guía técnica de configuración, que facilite la implementación de los estándares de seguridad MTA-STS y TLS Reporting la cual se especifica en el anexo 3.

4.1. Contratación del Hosting

Contratar el hosting es un proceso de gran relevancia para el funcionamiento del sitio web, el mismo que debe estar asociado a un nombre de dominio. De modo que lo primero que se ha hecho es la adquisición del hosting y posterior registro de un dominio. Para esto se priorizó el plan básico de HostGator, la contratación del servicio se lo hace directamente en la página web de HostGator ingresando a las opciones de “Web Hosting”, en los planes que se observa en la Figura 16 se selecciona el plan más económico denominado “Hatching Plan”.

Figura 16.

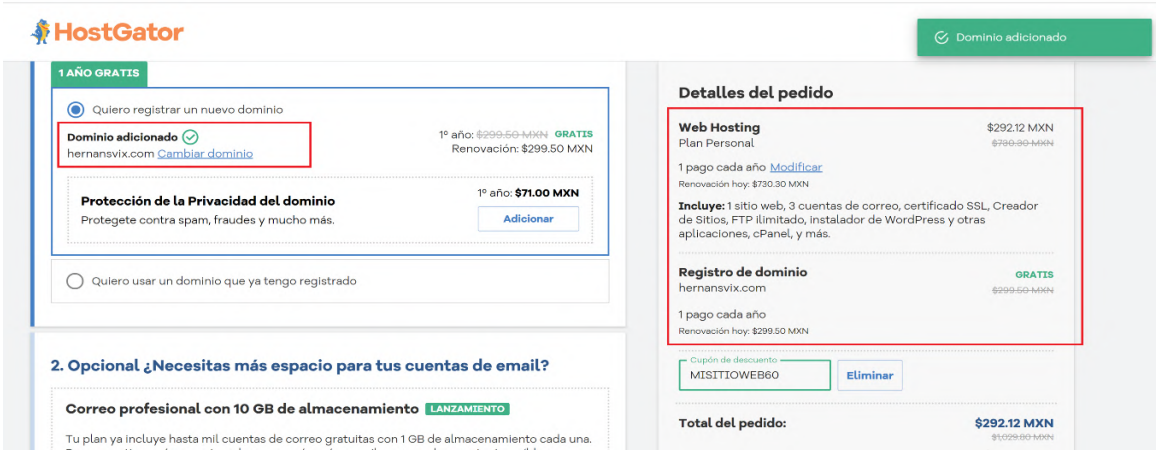
Planes de Hosting Disponibles en HostGator.com



En la pestaña correspondiente al registro del dominio la cual se la observa en la Figura 17, se ha registrado un nuevo dominio denominado *hernansvix.com* de tal manera que el sitio web en la internet se identifique con el dominio creado.

Figura 17.

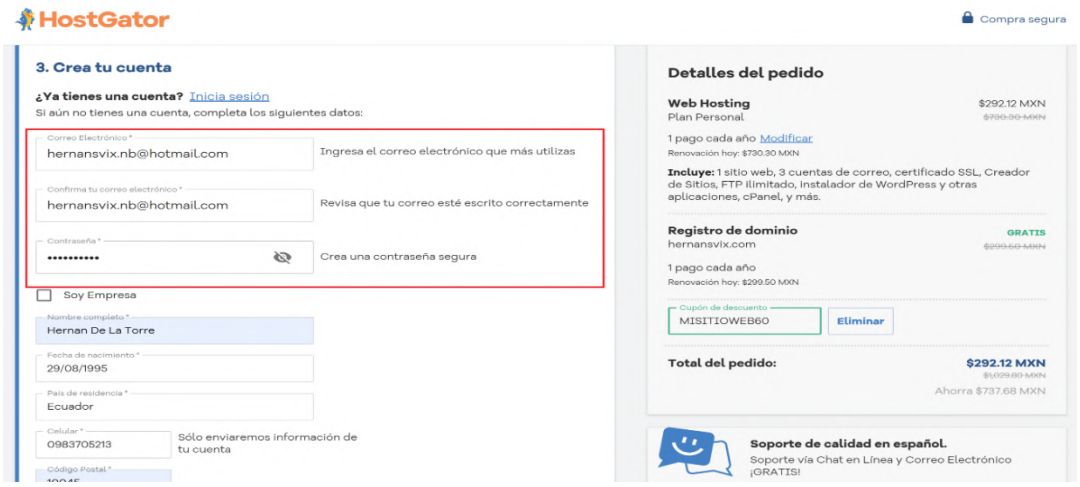
Pestaña Para el Registro de un Nuevo Dominio



Hecho esto se validará un nombre de usuario y contraseña para ingresar al Portal Cliente del Hosting. Para lo cual se debe completar un formulario igual al de la Figura 18 con algunos datos.

Figura 18.

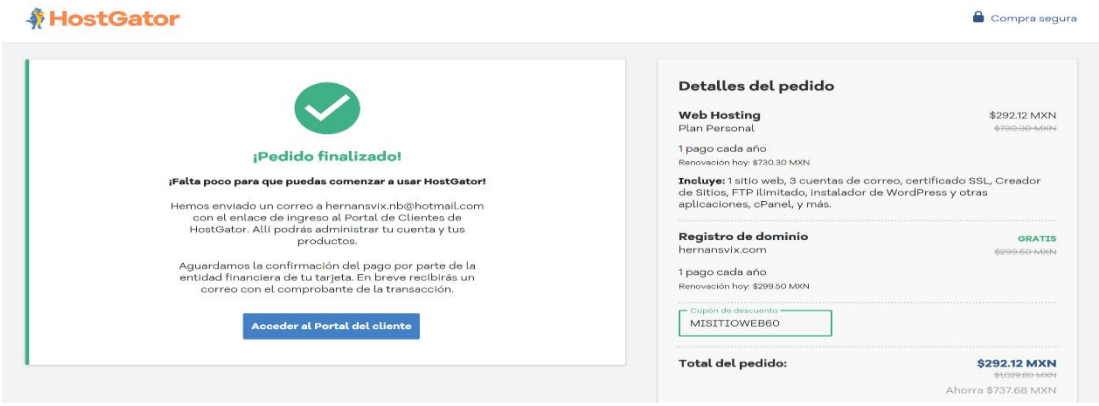
Pestaña Para Crear la Cuenta de HostGator



Para finalizar la compra se acepta los términos y condiciones del servicio y habrá finalizado el proceso de compra, tal como se ve en la Figura 19.

Figura 19.

Pestaña Finalización de la Compra del Hosting



4.2. Configuraciones del Dominio/Hosting Web

En este apartado se realiza las configuraciones preliminares del dominio y del sitio web, las cuales permitirán activar los servicios en internet.

4.2.1. Ajustes Preliminares del Dominio

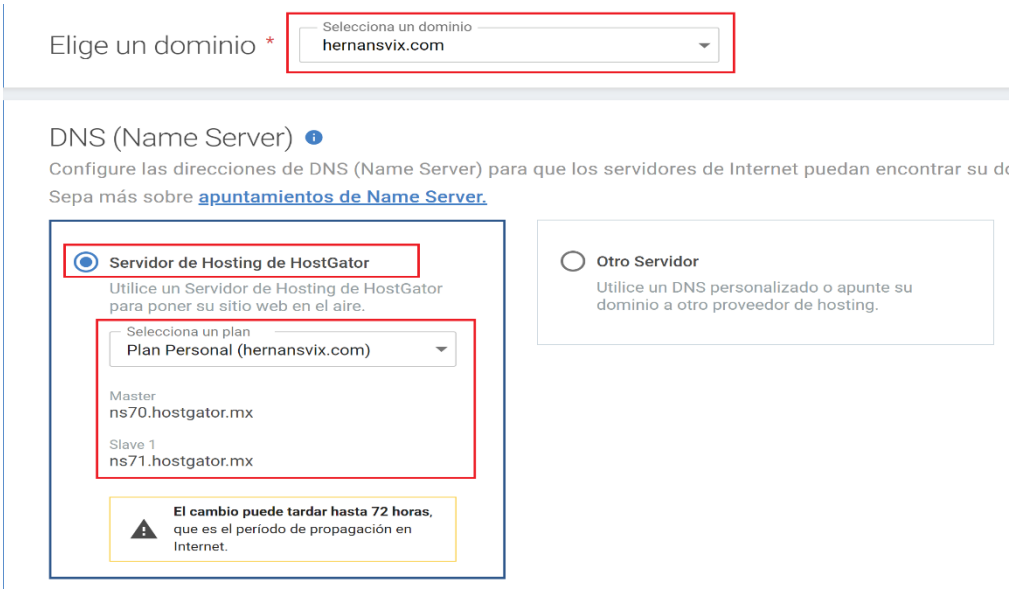
Es importante configurar las direcciones DNS (Name Server) para que los servidores de la internet puedan localizar el dominio en la red mundial. Por lo que se debe validar los registros del tipo NS correspondientes al plan contratado. Para realizar este proceso ingresamos al cPanel con las respectivas credenciales como se detalla en la Figura 20, en la opción de dominios seleccionamos el plan y automáticamente saldrán los registros correspondientes la cual se visualiza en la Figura 21, basta con hacer clic la opción de *Servidor de Hosting de HostGator*, y a automáticamente se valida los dos registros correspondientes.

Figura 20.

Página Principal cPanel

Figura 21.

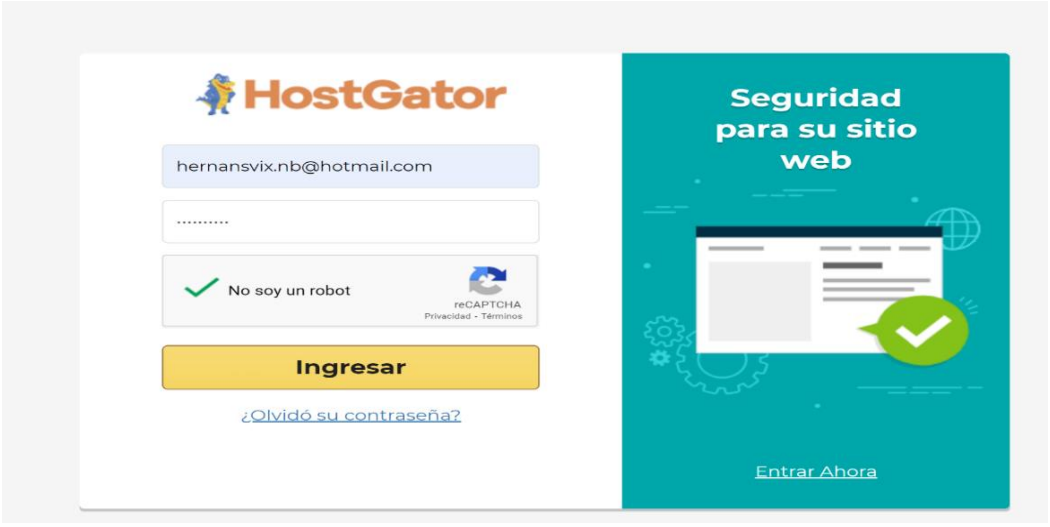
Opción de Dominios para Validar los Registros del Tipo NS



Para determinar si el dominio está registrado en la internet se ingresa al Portal Cliente con la cuenta de registro de HostGator tal como se indica en la Figura 22.

Figura 22.

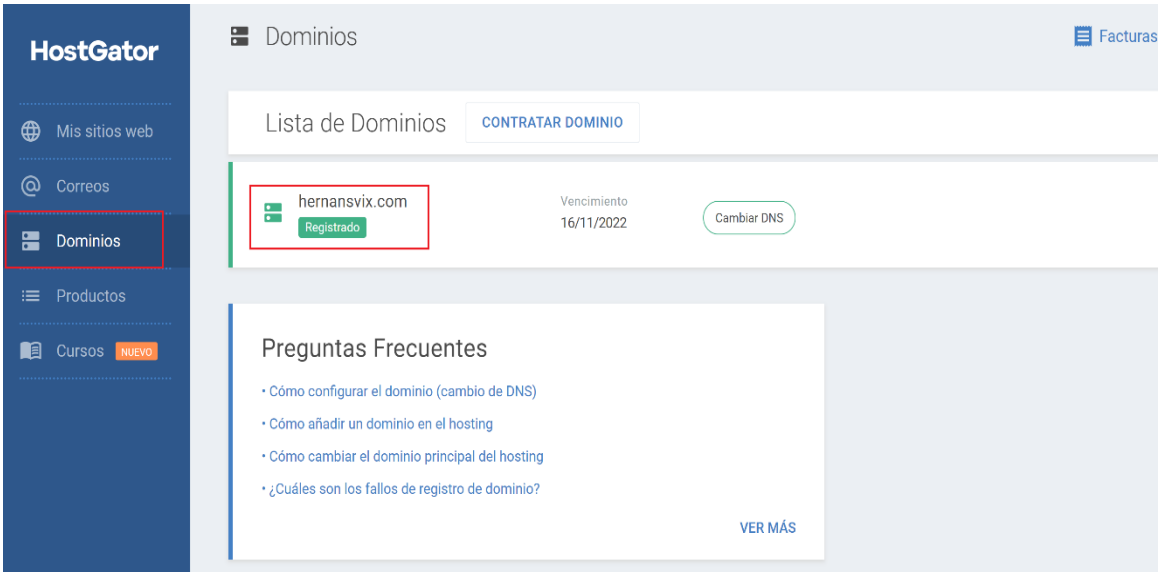
Login en el Portal Cliente de HostGator



Dentro de la página principal, se localiza la opción de dominios, y dentro de esa opción se observa que el dominio de *hernansvix.com* está registrado en la internet, tal y como refleja la Figura 23.

Figura 23.

Pestaña Verificación Dominio



4.2.2. Ajustes Preliminares del Sitio Web

Una vez registrado el dominio se procede a realizar algunos ajustes preliminares del Sitio Web de tal forma que el sitio este activo y sea accesible en la web.

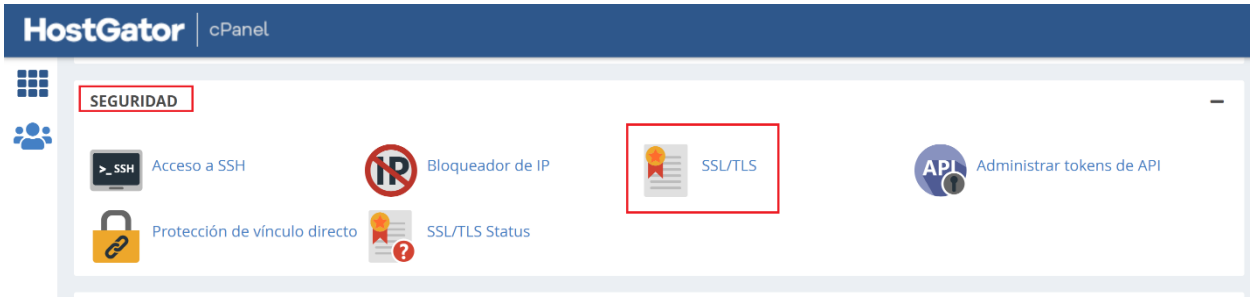
4.2.2.1. Instalación Certificado de Seguridad SSL

El certificado SSL proporciona la parte de autenticación de la identidad del sitio y garantizar a los visitantes que naveguen de forma segura. El plan de hosting contratado incluye un certificado SSL gratuito para todos los dominios y subdominios. Para la instalación se requieren acciones ya que está no se instala automáticamente.

Para configurar el certificado de seguridad SSL primero iniciamos sesión en el cPanel, para ubicarnos en la configuración SSL/TLS de las opciones de Seguridad la cual se la ilustra en la Figura 24.

Figura 24.

Opciones de Seguridad en el cPanel



En la Figura 25 muestra ventana de Solicitar nuevo Certificado SSL dentro de las opciones de seguridad, registramos los datos de la empresa relacionada al dominio adquirido para enviar la solicitud de petición del certificado una vez que la solicitud ha sido procesada el certificado de seguridad se encontrara en estado activo cuyo proceso se observa de la Figura 26 a Figura 27.

Figura 25.

Pestaña para Solicitar Certificado SSL

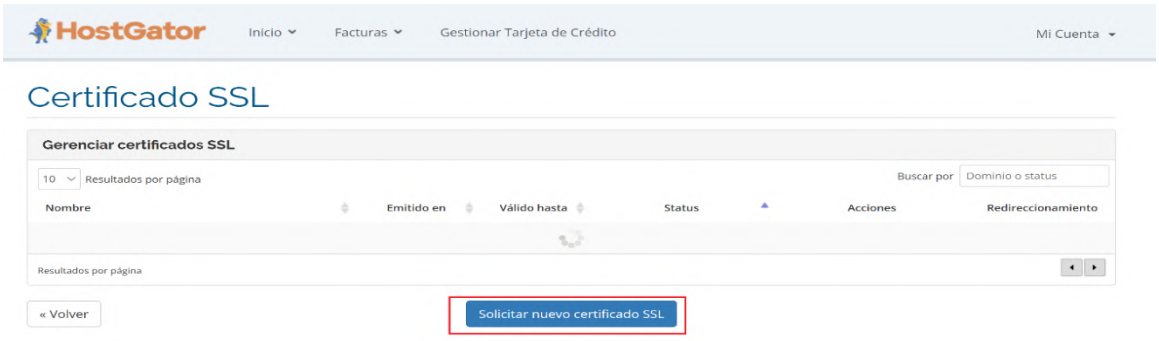


Figura 26.

Datos para Solicitar el Certificado SSL

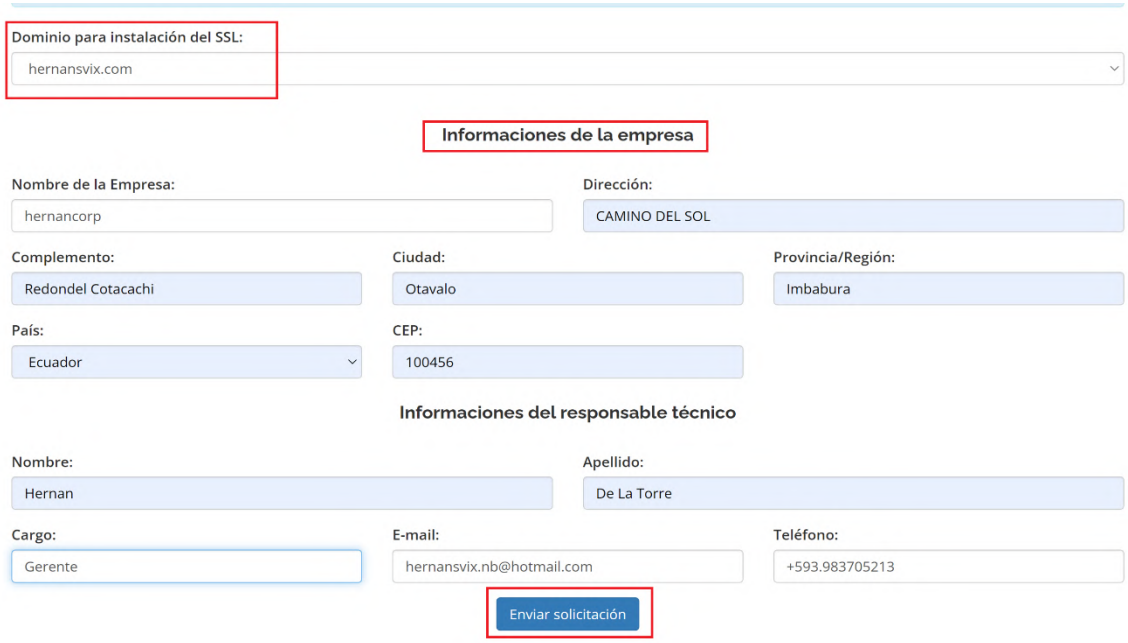
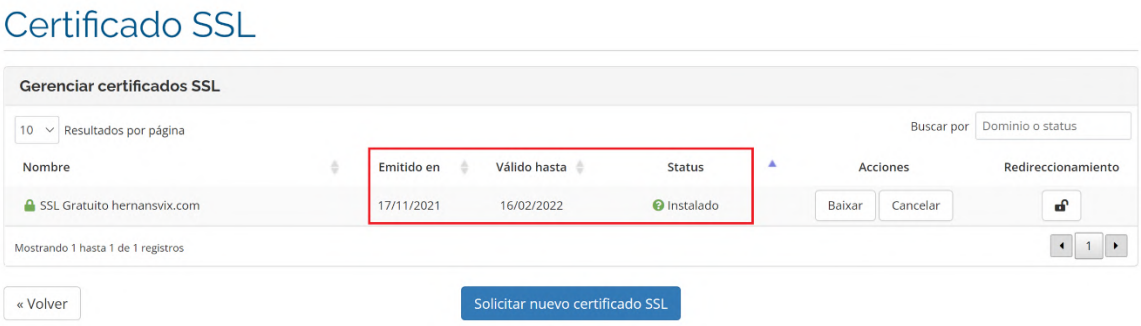


Figura 27.

Certificado SSL Instalado



4.2.2.2. Ajustes de Redirección Automática de HTTP a HTTPS

Después de la instalación del certificado SSL en el dominio es necesario configurar un redireccionamiento por medio del protocolo seguro. En caso contrario, la web funciona con HTTP y HTTPS a la vez, lo cual es riesgoso para los datos alojados en la internet. Por esta razón es necesario redireccionar el sitio a HTTPS de manera permanente.

Para hacer la redirección HTTPS ingresamos al cPanel como se visualiza en la Figura 28, buscamos la opción de Administrador de Archivos.

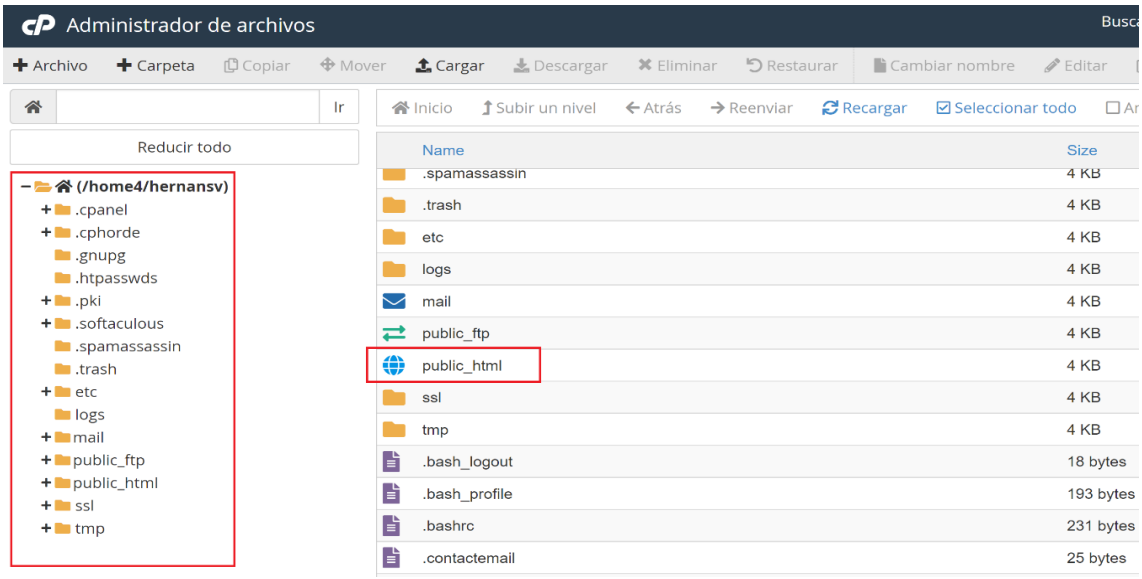
Figura 28.

Pestaña cPanel de HostGator

Enseguida se despliega un panel que contiene todos los archivos almacenados en directorio raíz como se indica en la Figura 29, lo que interesa es buscar los archivos que alojan los sitios web, para esto se busca la carpeta public_html.

Figura 29.

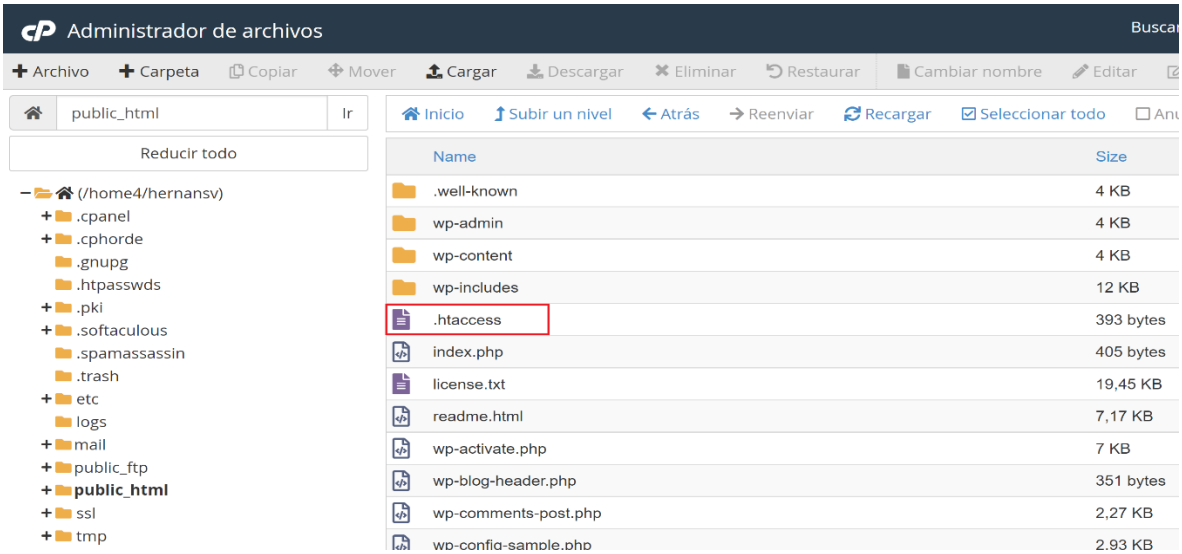
Directorio Raíz home4/hernansv



Dentro de la carpeta public_html que se identifica en la Figura 30, ubicamos el archivo TXT genérico denominado .htaccess.

Figura 30.

Archivo .htaccess



Dentro del archivo .htaccess se añade la siguiente sentencia de código:

RewriteEngine On

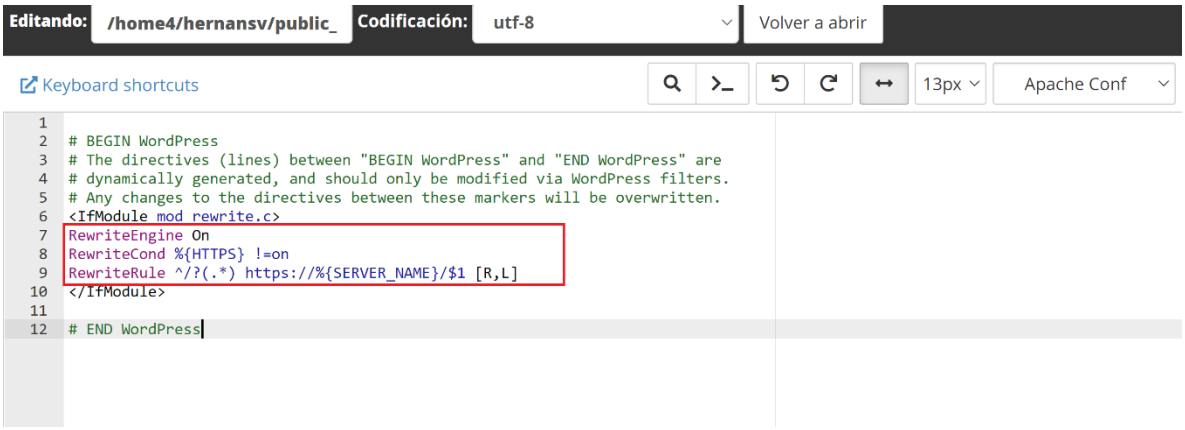
RewriteCond %{HTTPS}! =on

RewriteRule ^/? (. *) https://%{SERVER_NAME} /$1 [R, L]

Estas líneas de código indican una redirección automática en estado ON para los sitios del dominio mediante el protocolo HTTPS, esta configuración se visualiza en la Figura 31.

Figura 31.

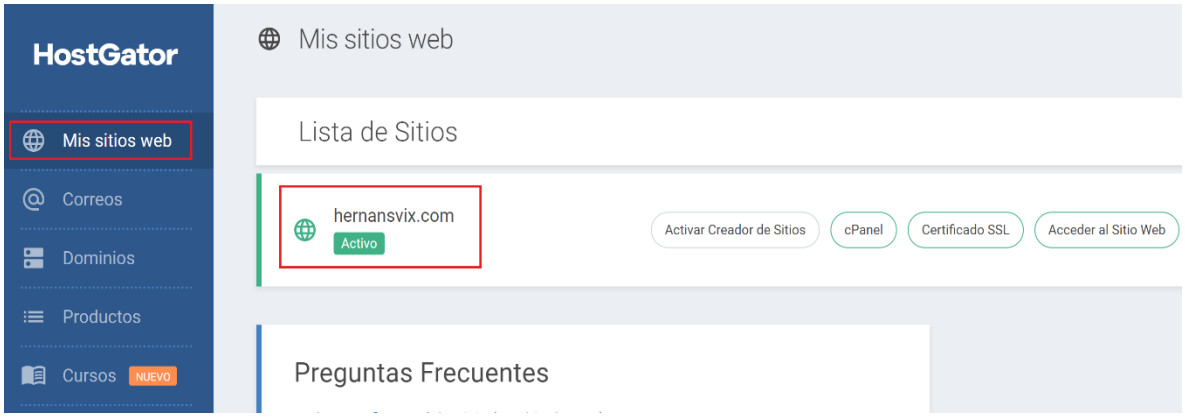
Visualización del Código HTML ON



En base a estas configuraciones se determinar el funcionamiento del sitio en la internet, para verificar si el sitio web está activo se inicia sesión en Portal Cliente y luego, dentro de la página principal en la opción de mis sitios web se determina que el sitio web de *hernansvix.com* está totalmente activo tal y como se plasma en la Figura 32.

Figura 32.

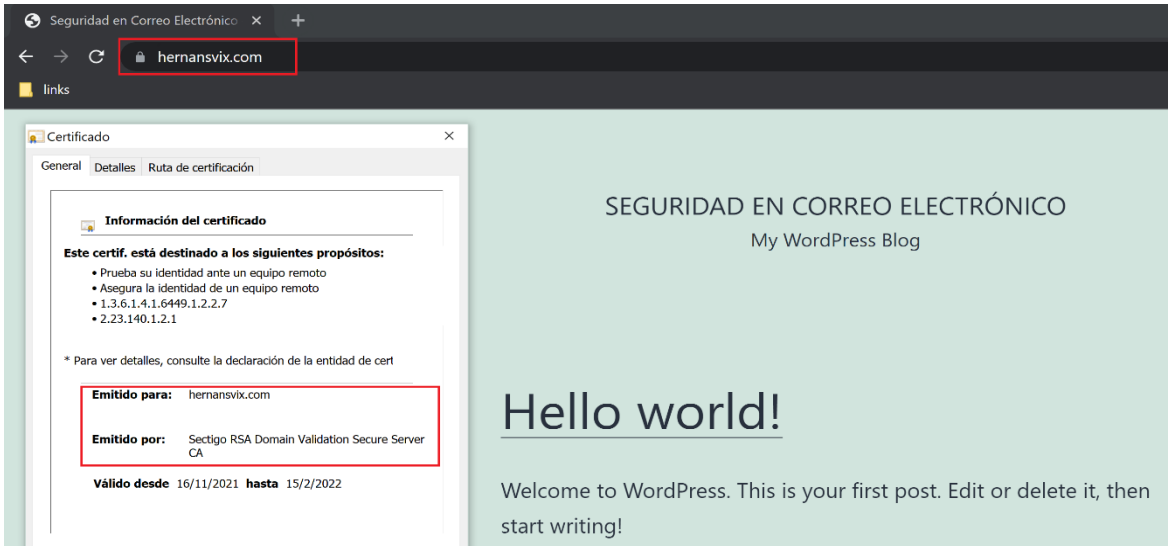
Pestaña que Indica que el Sitio hernansvix.com está Activo



Con estos ajustes al hosting web se procede a verificar si el sitio está activo en la web, en este caso se verificar la seguridad del sitio en base a su certificado digital. En la Figura 33 se observa la página web del dominio *hernansvix.com*, así mismo el certificado digital emitido por Sectigo.

Figura 33.

Testing del Sitio hernansvix.com en el Navegador



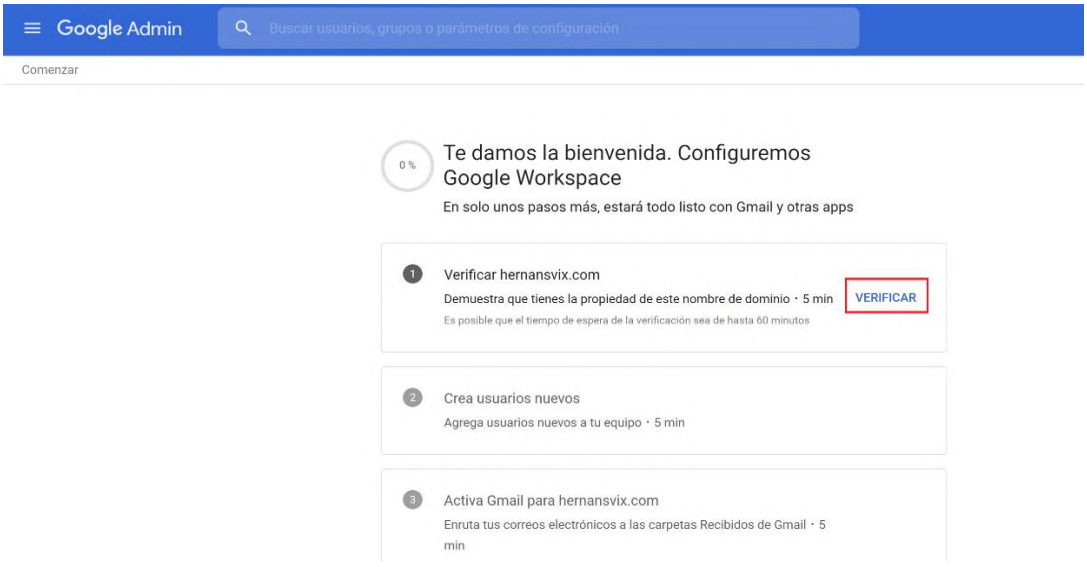
4.3. Sincronización del Dominio en Google Workspace

De acuerdo al diagrama de implementación de los estándares MTA-STS y TLS Reporting descritos en el capítulo anterior, para registrar y validar el dominio en Google es necesario cumplir correctamente las configuraciones preliminares del dominio y hosting web, configuraciones que ya se las ha hecho correctamente en los apartados anteriores.

Después de que el dominio está registrado y el sitio web activo se procede a sincronizar el dominio *hernansvix.com* con los servicios avanzados de Google Workspace para adquirir las funcionalidades de seguridad avanzada de Gmail. Para empezar lo primero que se debe realizar es crear una cuenta de administrador en base al dominio hernansvix.com, este proceso se lo detalla en la sección 2.1 del ANEXO 2. Una vez que se ha definido la cuenta de administrador inmediatamente se nos ubica en la página de Configuración de Google Workspace la cual se la observa en la Figura 34.

Figura 34.

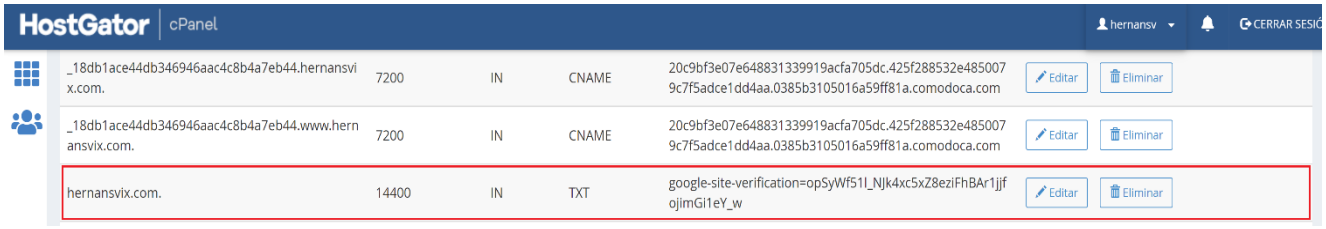
Pestaña Principal de Opciones de Verificación de Dominios



El proceso de validación se inicia con la verificación del dominio *hernansvix.com* cuyo proceso completo se lo especifica en la sección 2.2 del ANEXO 2. La Validación se lo hará mediante la adición de un registro TXT cuyo valor de código es *google-site-verification=opSyWf51l_NJk4xc5xZ8eziFhBAr1jjfojimGi1eY_w*. En la Figura 35 se observa como el registro está alojado en la tabla del Editor de Zonas del hosting.

Figura 35.

Registro TXT de Google en la Tabla de Editor de Zonas del Hosting



Luego inicia la fase de activación de Gmail para el dominio de *hernansvix.com*, de igual manera todo el proceso de activación se la descrito en la sección 2.3 del ANEXO 2. Para activar Gmail en el dominio se debe agregar 5 registros del tipo MX, las cuales se especifican en la Tabla 7 que fue extraída del ANEXO 2.

Tabla 7.

Valores de los registros MX en Google Workspace

Valor/Respuesta/Destino	Prioridad
ASPMX.L.GOOGLE.COM	1
ALT1.ASPMX.L.GOOGLE.COM	5
ALT2.ASPMX.L.GOOGLE.COM	5
ALT3.ASPMX.L.GOOGLE.COM	10
ALT3.ASPMX.L.GOOGLE.COM	10

Una vez creado todos estos registros, procedemos a verificar en el Editor de Zonas del Hosting que los registros consten en la respectiva tabla de Zonas tal y como se detalla en la Figura 36.

Figura 36.

Registros MX de Google en la Tabla de Editor de Zonas del Hosting

Una vez que se ha agregado los registros MX de Google, se podrá recibir correos electrónicos en la bandeja de entrada de Gmail desde clientes de correo electrónico de servidores externos.

4.4. Configuración del Estándar MTA-STS y TLS Reporting

La implementación del estándar MTA-STS y TLS Reporting se lo hará para el dominio registrado en Google Mail. A continuación, se detallará los pasos para la configuración de los estándares en el dominio.

4.1.1. Crear una política de MTA-STS

La política de MTA-STS (un archivo txt), define los servidores de correo electrónico que utilizan MTA-STS en el dominio destinatario. Los servidores de correo admitidos se conectarán automáticamente a la web para recuperar el archivo.

MTA-STS ofrece dos modos de política: el modo de prueba y obligatorio. El modo de prueba MTA-STS únicamente permite recibir informes TLS sobre problemas en la política de MTA-STS, lo cual puede ayudar a solventar problemas de seguridad existentes. De otra forma el modo obligatorio además de recibir los reportes TLS aplica el cifrado obligatorio al recibir correos electrónicos. Esto evita que los mensajes sean modificados o manipulados mientras están en tránsito(Papazyan, 2021). Para garantizar un funcionamiento normal del estándar se lo configurará en modo obligatorio.

En primer lugar, se debe crear un archivo de política del estándar MTA-STS utilizando información de la organización en donde se ha registrado el dominio de correo que sería el de Google Workspace. El campo versión debe incluirse al principio del archivo de texto, mientras que los demás campos pueden incorporarse en cualquier orden. Luego especificar los registros

MX de Google en la política de MTA-STS. Además de precisar el tiempo de vida útil de la política MTA-STS, cuya sugerencia es colocar un tiempo de *604800*(1 semana).

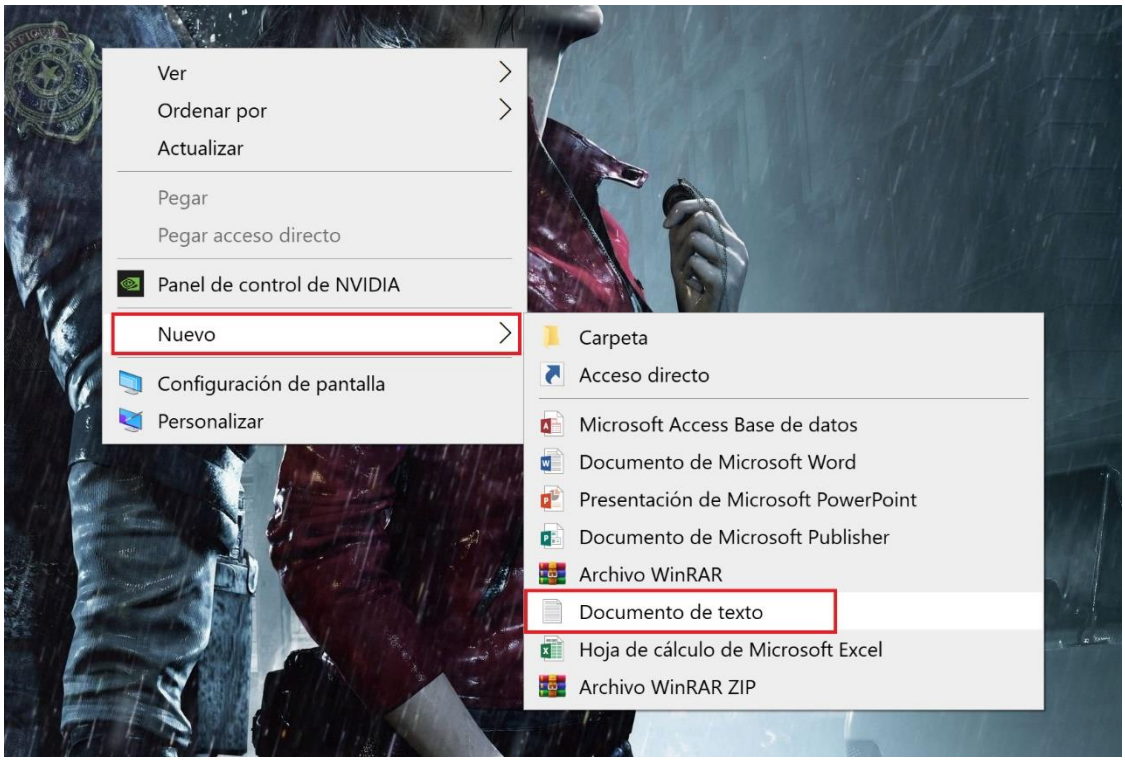
El archivo de políticas del MTA-STS es en esencia un simple archivo de texto, que de acuerdo a las consideraciones anteriores tendrá el siguiente aspecto:

version: STSv1
mode: enforce
mx: ALT4.ASPMX.L.GOOGLE.COM
mx: ALT2.ASPMX.L.GOOGLE.COM
mx: ASPMX.L.GOOGLE.COM
mx: ALT1.ASPMX.L.GOOGLE.COM
mx: ALT3.ASPMX.L.GOOGLE.COM
max_age: 604800

Para definir el archivo de texto primero se crea un texto sin formato en el escritorio del ordenador dando clic derecho en la pantalla principal, seleccionar la opción nuevo y documento de texto tal y como se indica en la Figura 37.

Figura 37.

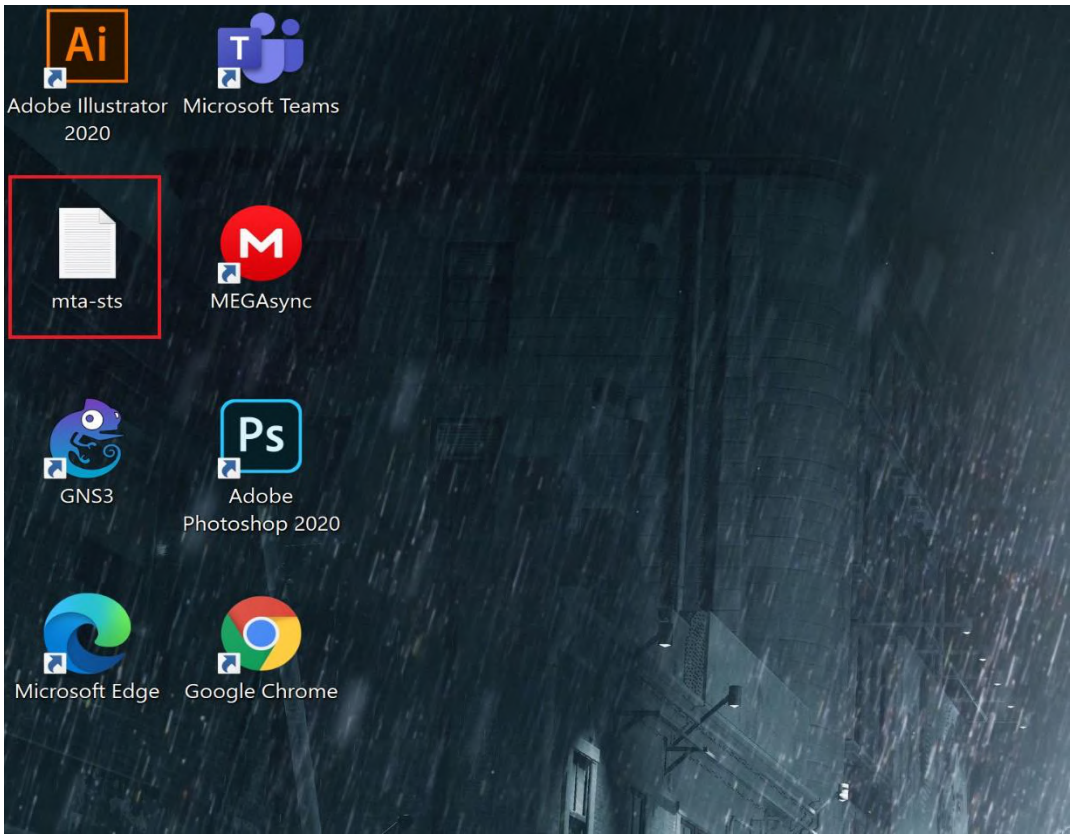
Creación de un Documento de Texto en el Escritorio



Inmediatamente el documento de texto se ubica en el escritorio del ordenador, este archivo lo renombraremos con el nombre de *mta-sts.txt*, este documento se lo visualiza en el Figura 38.

Figura 38.

Documento de Texto Renombrado con el Nombre mta-sts



Luego se abre el documento de texto y se escribe el contenido que será el correspondiente al cuerpo de la política MTA-STS definida anteriormente, el contenido del archivo de texto *mta-sts* se ilustra en la Figura 39. Guardamos el archivo de texto para utilizarla después.

Figura 39.

Contenido del Documento de Texto mta-sts.txt

En este apartado, se creó el archivo de configuración MTA-STS deseado y se lo guardó en el escritorio. En el siguiente paso, se subirá el archivo de texto al servidor web público para que los servidores de correo externos puedan acceder a él.

4.1.2. Publicar una política de MTA-STS en la Web

Para que el archivo de configuración del MTA-STS se pueda descubrir automáticamente por los servidores de correo externos, debe ser alojado exactamente en el camino correcto, se debe usar el subdominio sobre HTTPS y la ruta conocida; de lo contrario, la configuración no funcionará.

Para añadir una política al servidor web del dominio *hernansvix.com* hay que crear un subdominio con el nombre de *mta-sts*. Antes que nada, se debe iniciar sesión en el panel de administración del Hosting, dirigirnos a la opción de subdominio en la función de dominio, la misma que se recalca en la Figura 40.

Figura 40.

Opción Subdominio del cPanel

Dentro de la opción subdominio se encuentra la función de crear un subdominio, aquí se ingresa el nombre del subdominio que será *mta-sts*, luego más abajo seleccionamos el dominio principal(*hernansvix.com*) que aloja el subdominio e inmediatamente el cuadro de texto raíz de documento muestra la URL del subdominio tal y como se expresa en la Figura 41.

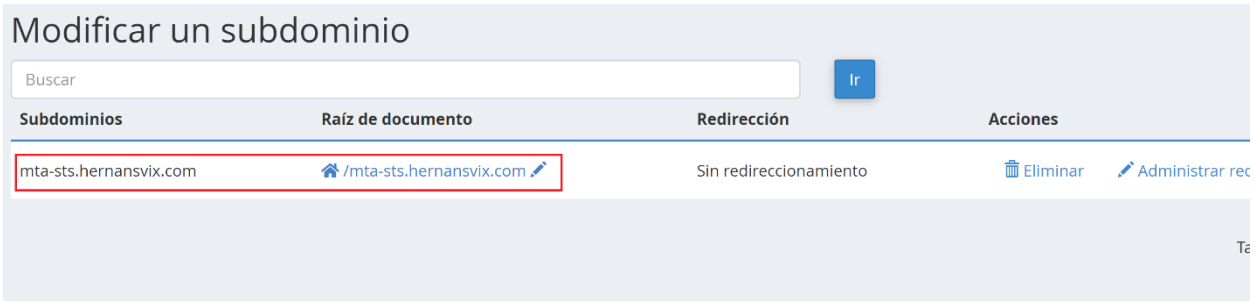
Figura 41.

Parámetros Para Crear un Subdominio

Una vez que ya se ha establecido el subdominio damos clic en crear y el subdominio ya estará visible en la parte final de la pestaña crear subdominio, en la Figura 42 se observa el subdominio ya creado.

Figura 42.

Raíz de Documento que Contiene al Subdominio



El siguiente paso es crear un directorio llamado *well-known* en el subdominio, para ello nos ubicamos en la opción de administrador de archivos en la pestaña principal del cPanel la cual es visible en la Figura 43.

Figura 43.

Opción Administrador de Archivos en el cPanel

Una vez dentro de la opción Administrador de archivos ubicamos la carpeta que tiene el subdominio creado, esto se visualiza en la Figura 44. Luego hacemos clic dentro de la carpeta del subdominio en donde no tiene ningún tipo de archivo alojado que haga referencia a ese subdominio, esto se lo puede ver en la Figura 45.

Figura 44.

Archivos que Contiene la Carpeta del Subdominio.

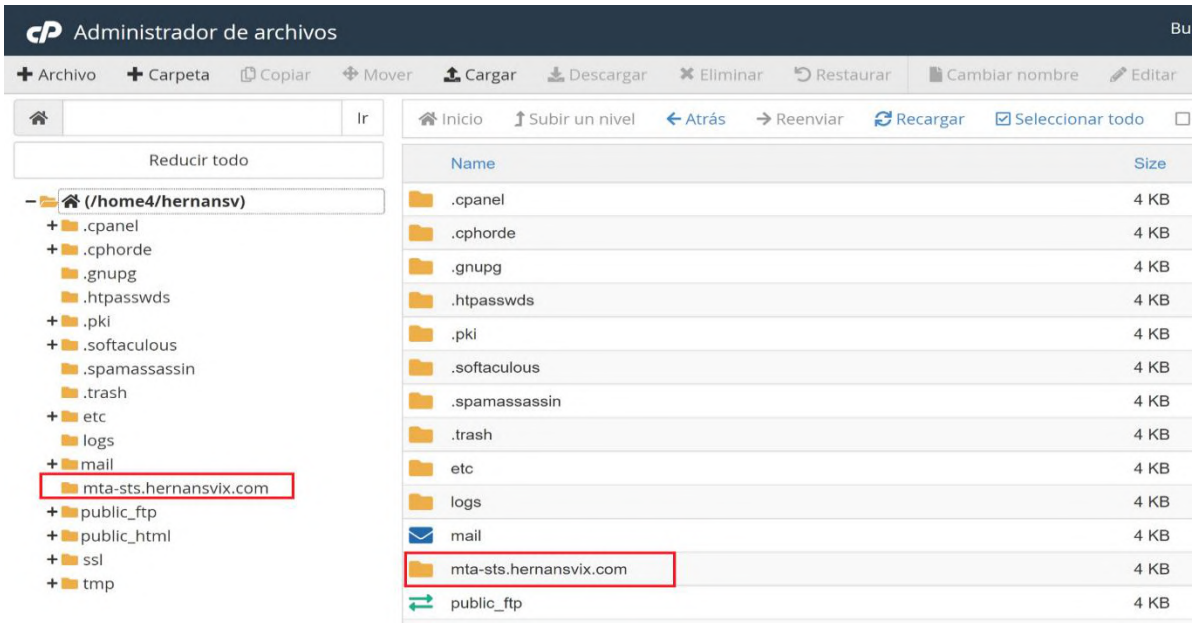
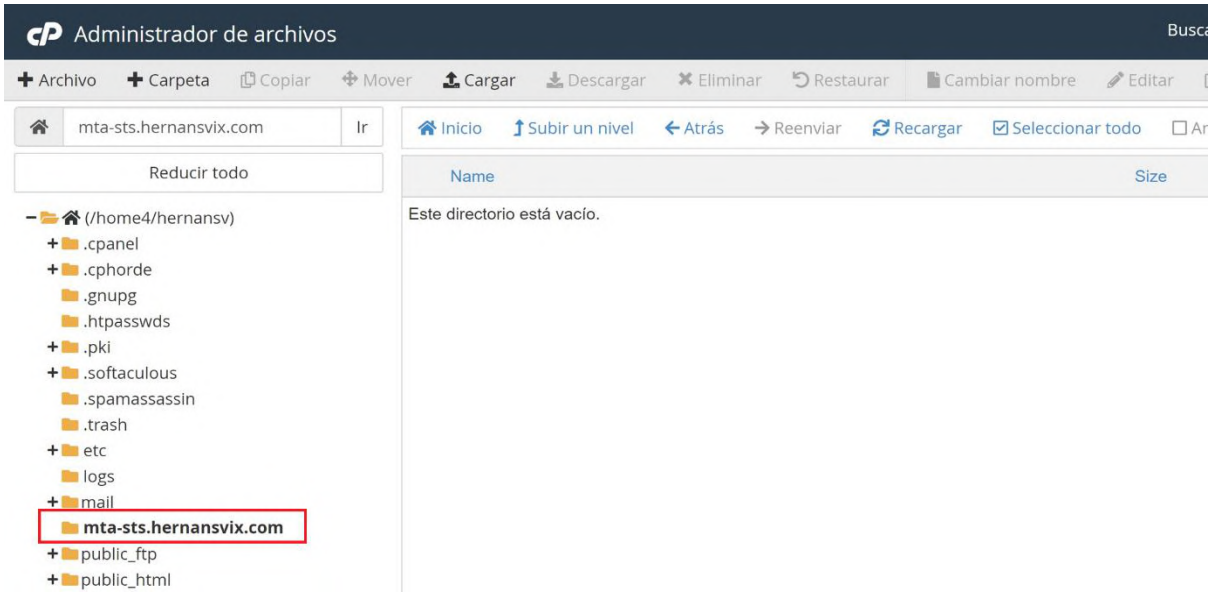


Figura 45.

Contenido de la Carpeta mta-sts.hernansvix.com



Dentro del directorio *mta-sts.hernansvix.com* se procede a crear un directorio, para eso se hace clic en la opción superior *Carpeta*, enseguida se despliega un cuadro de dialogo en donde se deberá especificar el nombre del directorio que debe ser *well-known* tal y como muestra la Figura 46. Enseguida dar clic en *Create New Folder* para crear el directorio.

Figura 46.

Cuadro de Dialogo para Crear el Directorio

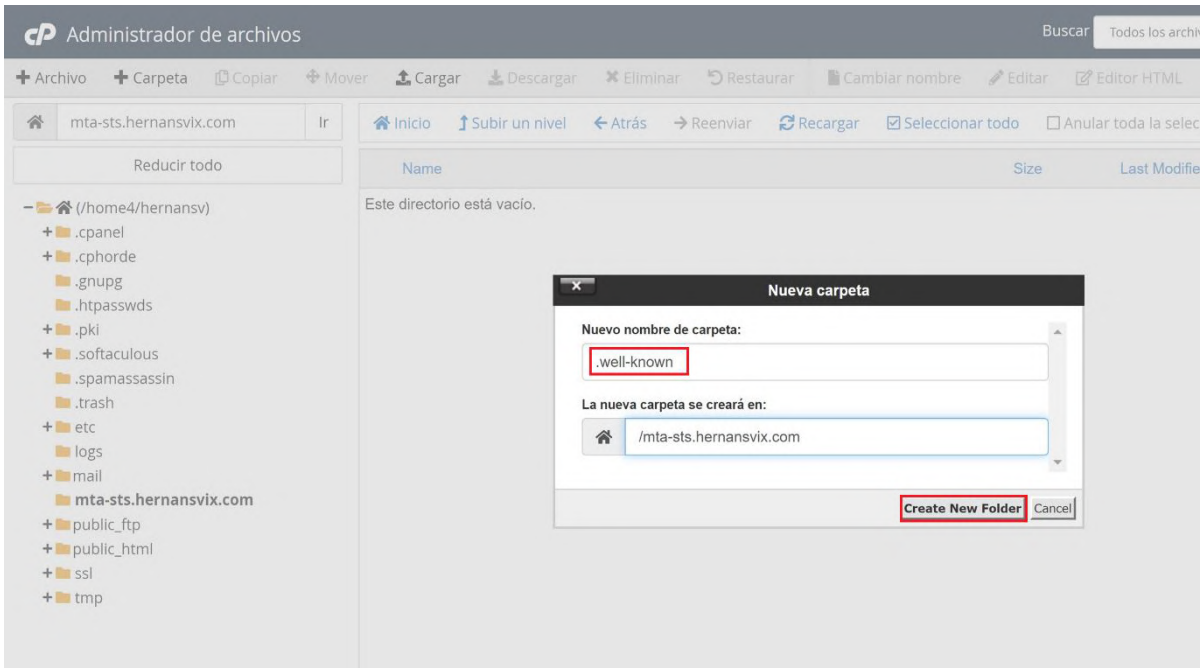
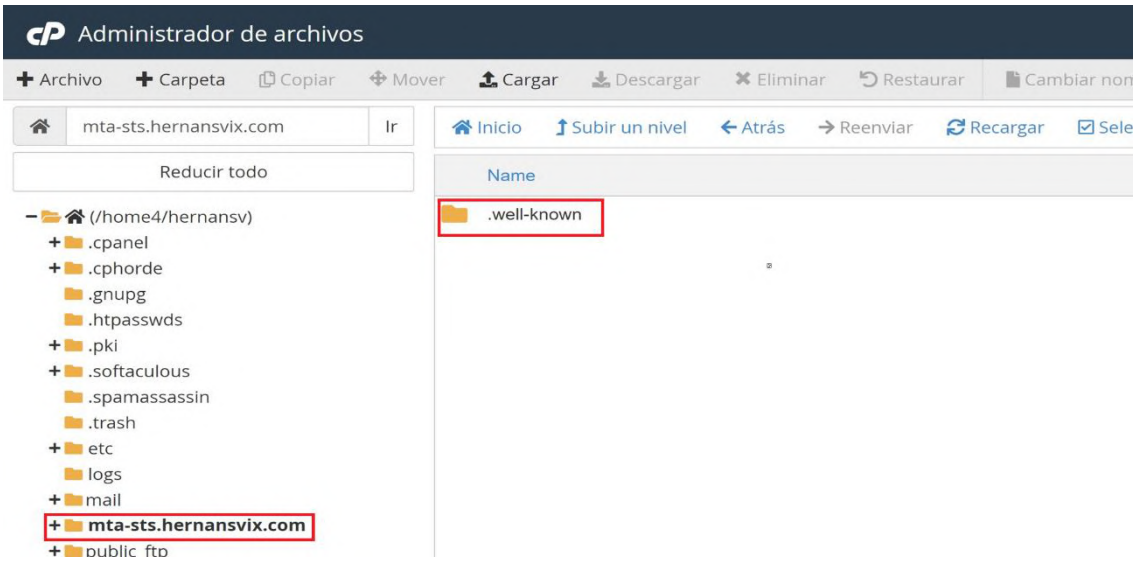


Figura 47.

Directorio well-known en mta-sts.hernansvix.com



El directorio estará disponible dentro de *mta-sts.hernansvix.com*, como se ilustra en la Figura 47, ahora dentro del directorio se debe cargar el archivo de política que se creó anteriormente, para este paso dar clic en la opción *Cargar* en la parte superior del Administrador de archivos, enseguida se carga una pestaña para subir el archivo, aquí seleccionamos subir archivo y se busca el documento de texto con el nombre *mta-sts*, esto se lo representa en la Figura 48. La Figura 49 detalla cómo el documento de texto ha sido cargado totalmente en el directorio.

Figura 48.

Proceso de Subir el Documento mta-sts.txt

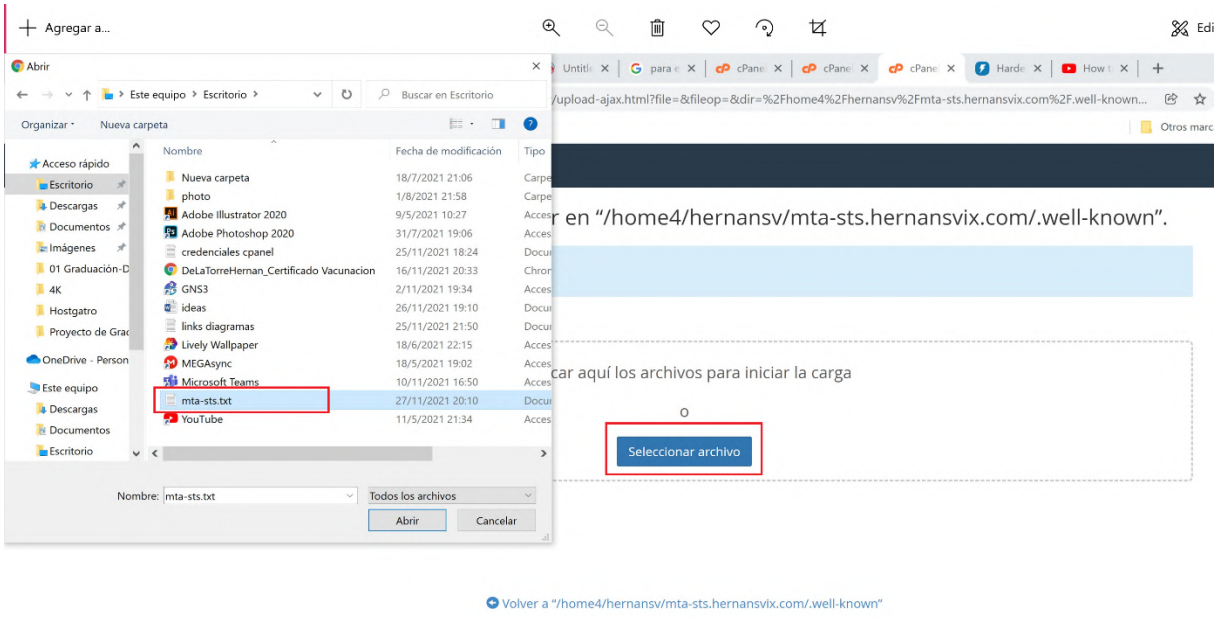
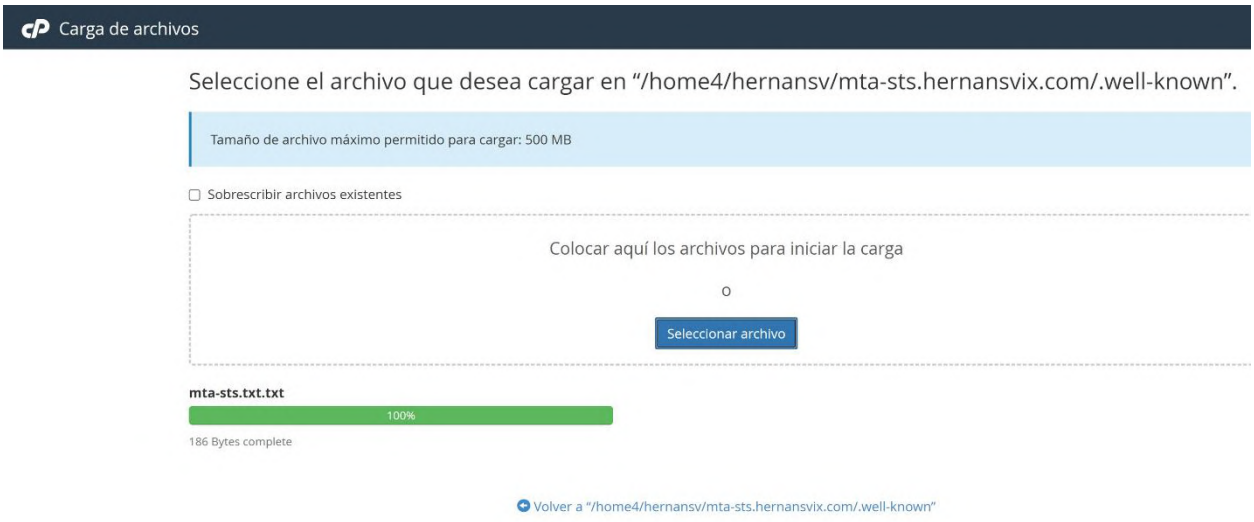


Figura 49.

Documento Cargado al 100%



Una vez que el archivo de texto *mta-sts* se ha cargado totalmente, éste ya estará ubicado dentro del directorio *well-known* que se observa en la Figura 50. Con todos estos ajustes hechos la URL de la política de MTA-STS correspondiente al dominio *hernansvix.com* será: *https://mta-sts.hernansvix.com/.well-known/mta-sts.txt.* Al ingresar al enlace se encuentra la política publicada en la web tal y como se observa en la Figura 51.

Figura 50.

Documento de Texto mta-sts.txt en el Directorio well-known

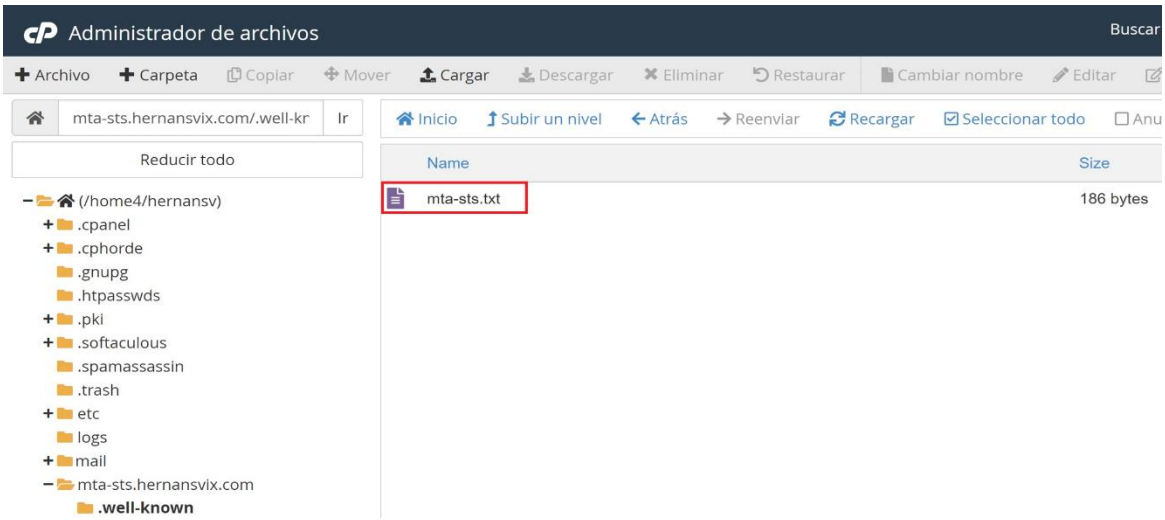
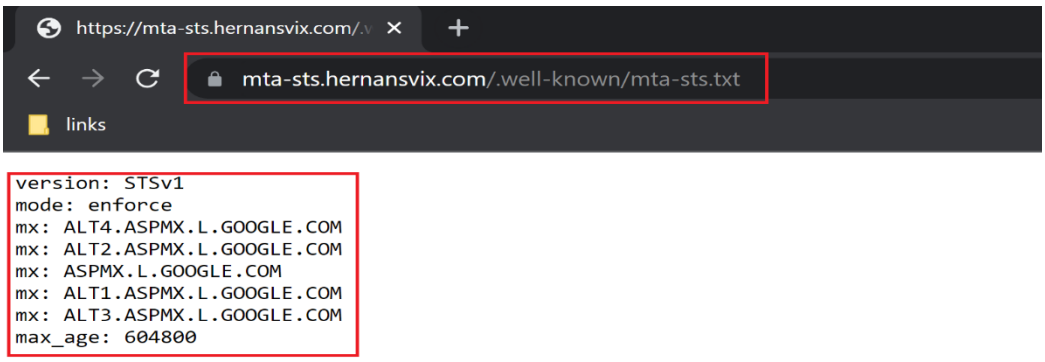


Figura 51.

Política mta-sts.txt Publicada en la Internet



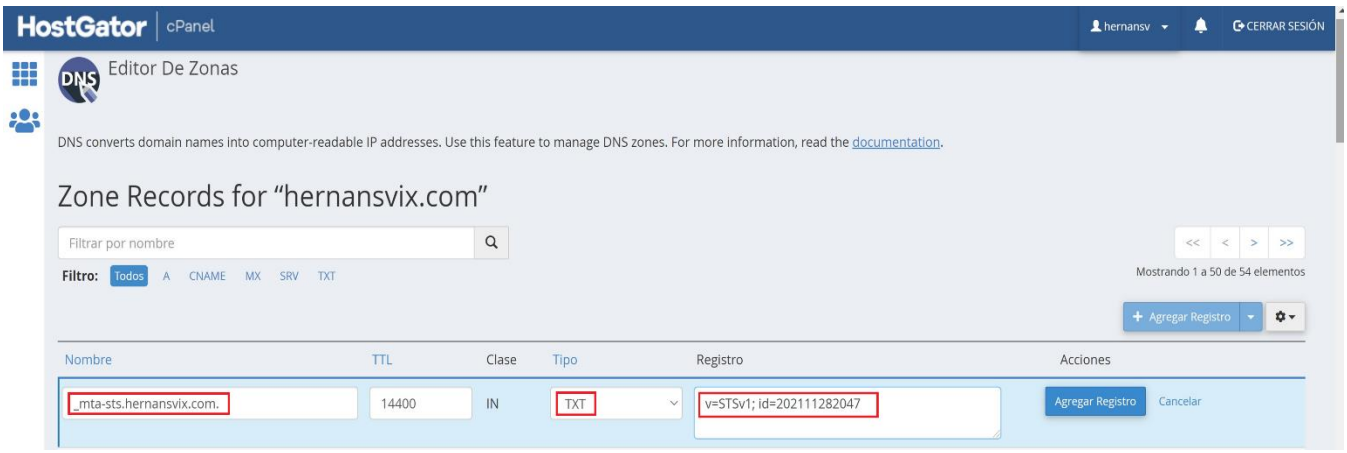
4.1.3. Activar MTA-STS y las notificaciones TLS

Para activar el estándar MTA-STS y TLS Reporting en el dominio de recepción de correo, se debe actualizar la configuración DNS del hosting mediante dos registros TXT, las cuales son: *_mta-sts* y *_smtp. _tls* seguido del nombre de dominio. Esto posibilita que los servidores de correo externos envíen correos electrónicos al dominio cuando estén autenticados y cifrados con TLS 1.2 o superior.

Lo primero es iniciar sesión en el cPanel del hosting, en las configuraciones del editor de zonas del dominio se crea el siguiente registro: *_mta-sts.hernansvix.com*, utilizando el siguiente valor: *v=STSv1; id=202111282047;* en donde el id debe constar de entre 1 y 32 caracteres alfanuméricos. Este proceso se la representa en la Figura 52.

Figura 52.

Creación del Registro _mta-sts.hernansvix.com

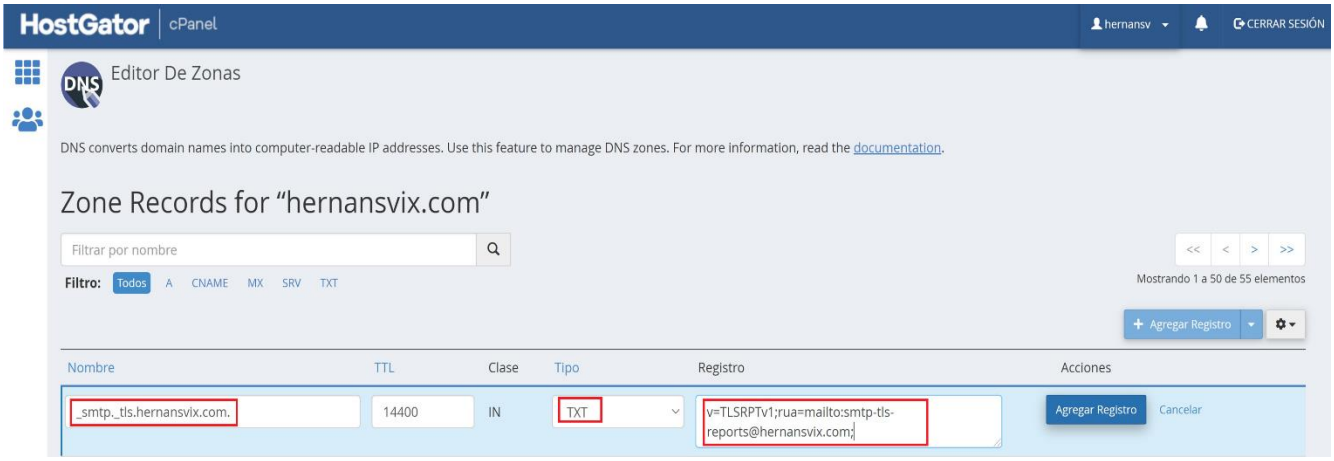


Con respecto al registro de TLS Reporting, se añade el siguiente registro: *_smtp._tls.hernansvix.com*. Cabe recalcar que las notificaciones se receptaran vía correo electrónico con el parámetro *mailto* a la dirección *smtp-tls-reports@hernansvix.com*, De esta

forma el valor del registro es: *v=TLSRPTv1;rua=mailto:smtp-tls-reports@hernansvix.com;* la creación del registro se la indica en la Figura 53.

Figura 53.

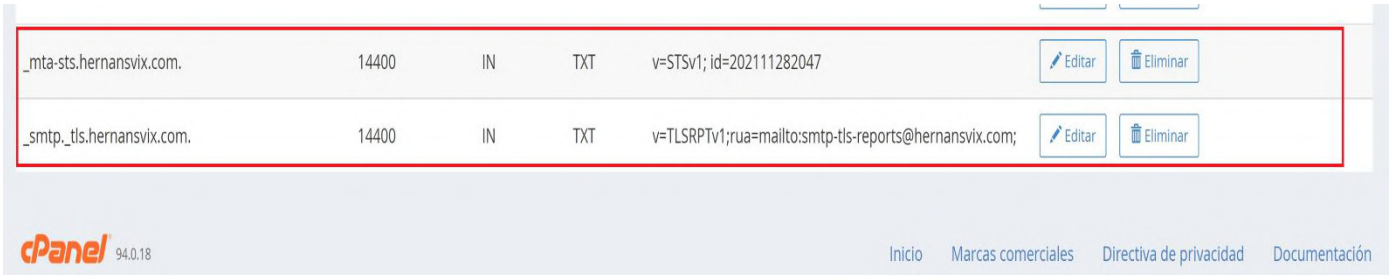
Creación del Registro _smtp._tls.hernansvix.com



Una vez que se ha añadido ambos registros al hosting se debe verificar que estos registros consten en la tabla del Editor de Zonas del hosting, estos registros se visualizan en la Figura 54.

Figura 54.

Registros TXT Añadidos en el Editor de Zonas del Hosting



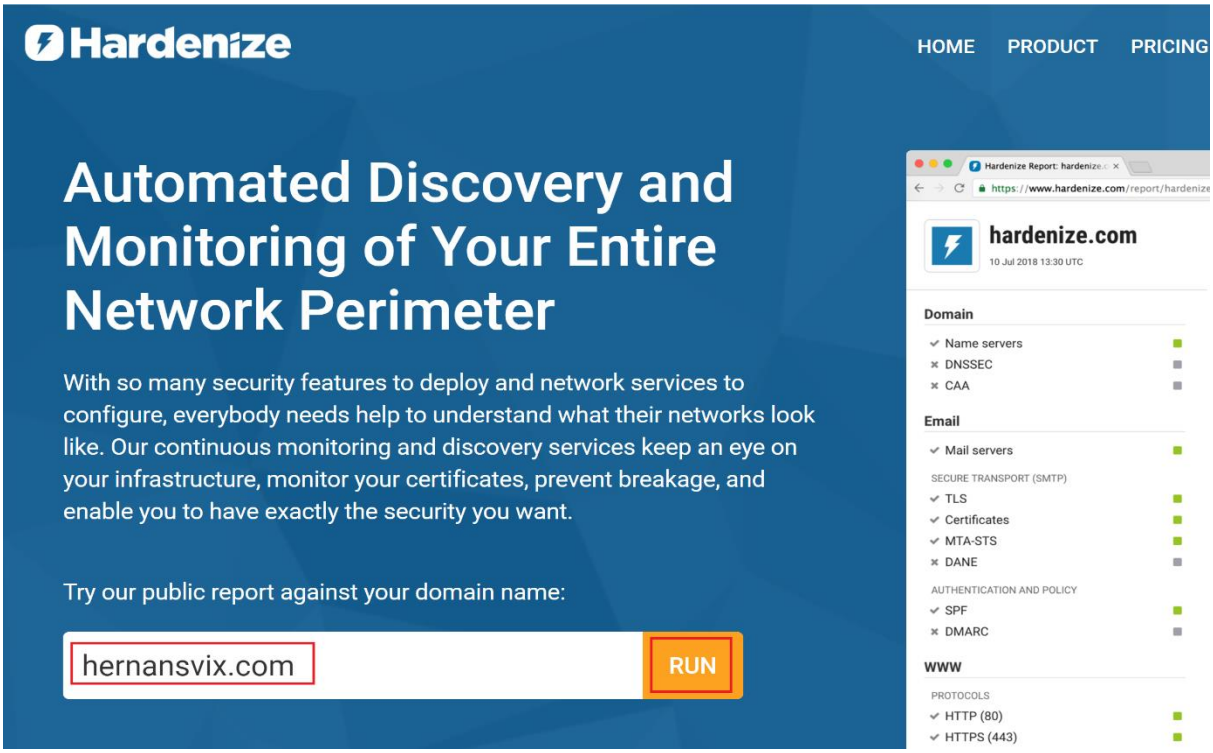
4.1.4. Verificación de la configuración de MTA-STS y TLS Reporting

Para asegurarse de que los ajustes de MTA-STS y TLS Reporting están configurados correctamente, se debe validar la configuración de MTA-STS en las plataformas web de supervisión de nombres de dominio DNS. La validación de las configuraciones se lo hecho en la página web: *https://www.hardenize.com/*.

En la página principal de *hardenize* se escribe el dominio *hernansvix.com* la cual se la ilustra en la Figura 55, luego se hace clic en *run*; esto permitirá generar un informa público con respecto al estado de seguridad de los servicios del dominio.

Figura 55.

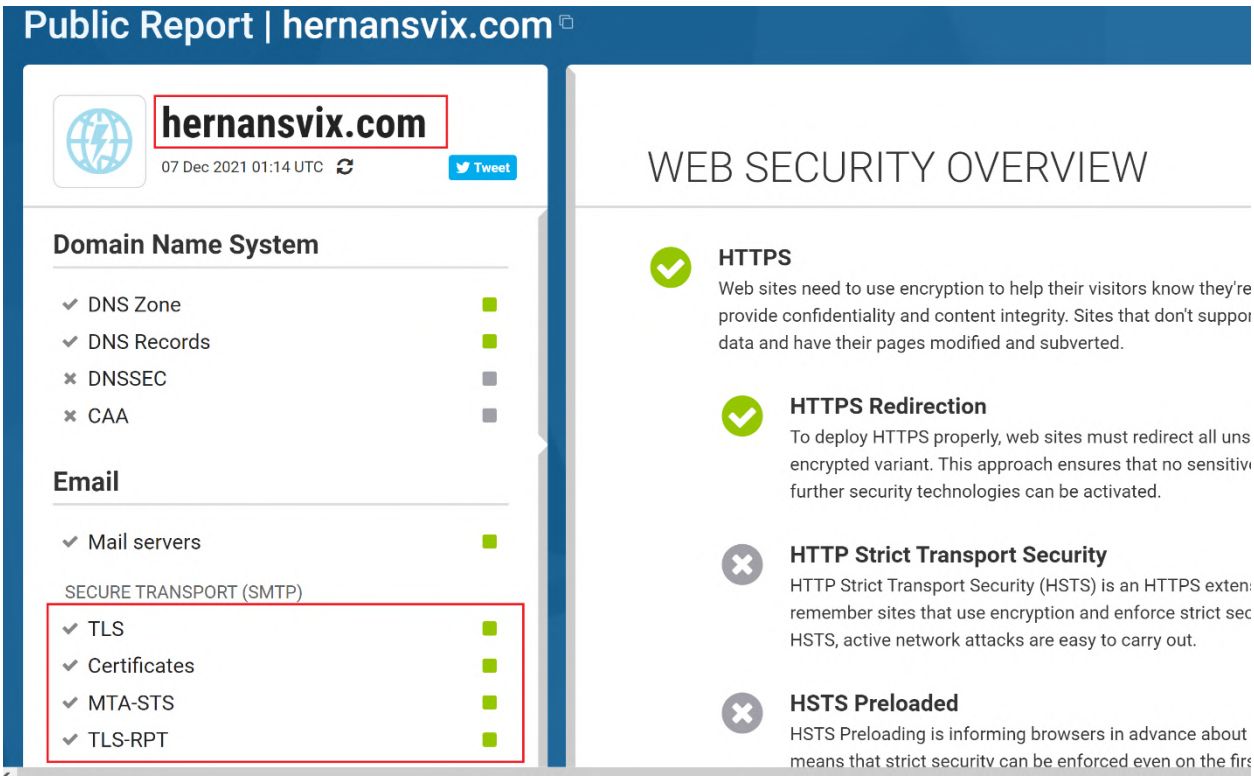
Testing del Dominio hernansvix.com en Hardenize



Enseguida se representará el estado de seguridad del servicio de correo electrónico de *hernansvix.com*, en la pestaña de presentación se puede observar que el estándar MTA-STS y TLS Reporting están habilitados correctamente, esta información se la expone en la Figura 56.

Figura 56.

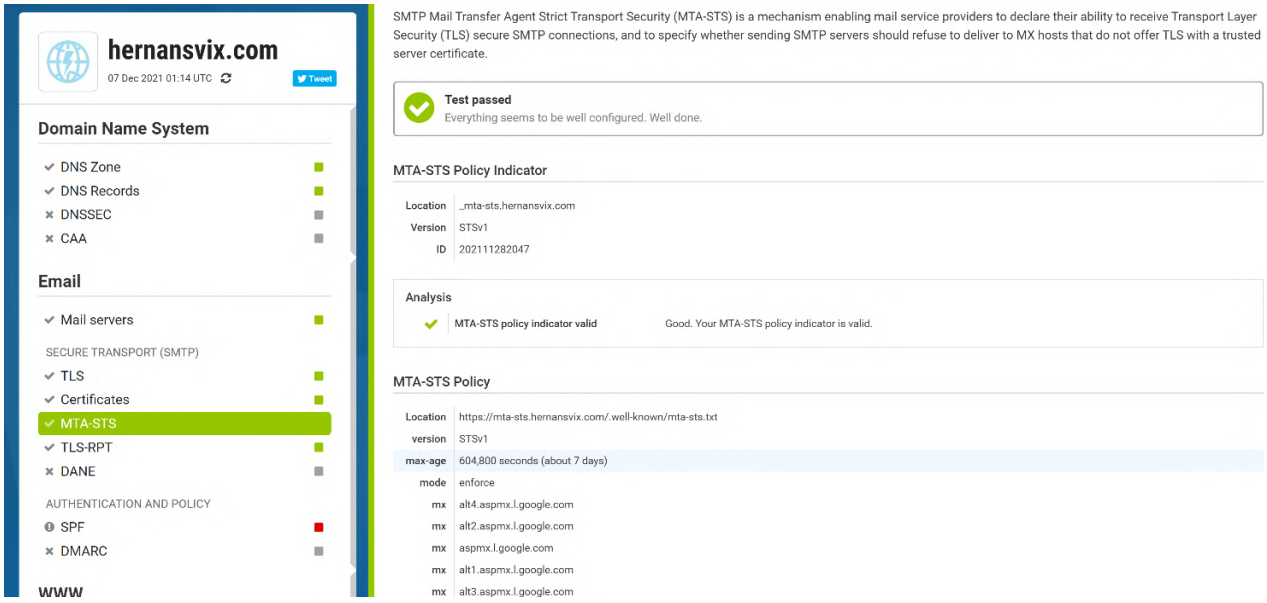
Reporte Público Correspondiente a hernansvix.com



En la Figura 57 se puede observar los datos correspondientes a la política de MTA-STS alojada en el registro DNS, en esta parte se visualiza las configuraciones tal cual se las definió al momento de crear y configurar la política y el respectivo registro TXT.

Figura 57.

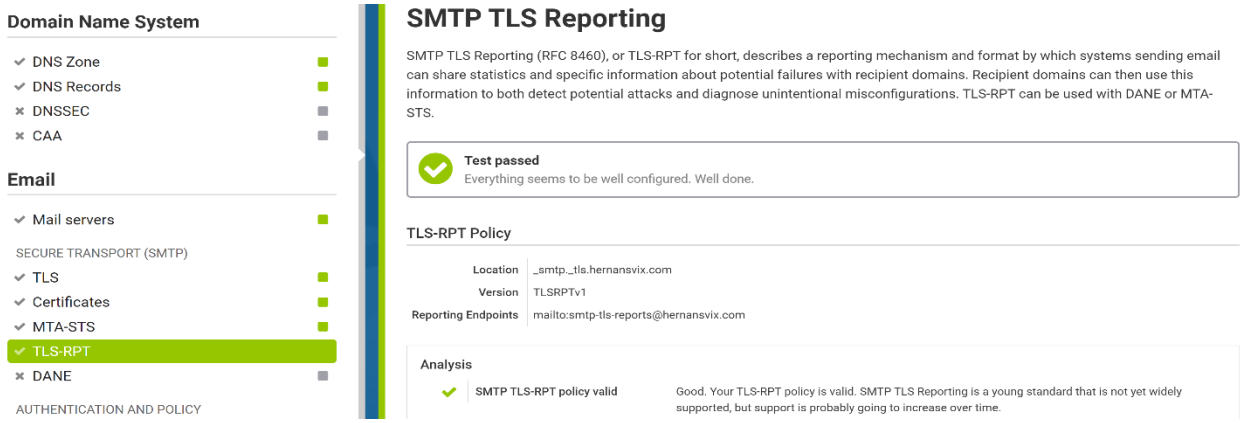
Reporte de las Configuraciones de MTA-STS para hernansvix.com



Las configuraciones para el registro *_smtp._tls.hernansvix.com* que hace referencia a TLS Reporting también ha pasado la prueba de validación de configuración tal y como se la aclara en a Figura 58.

Figura 58.

Reporte de las Configuraciones de TLS Reporting para hernansvix.com



4.5. Escenario de Pruebas

El estándar MTA-STS, informa a los servidores remitentes que su servidor de correo acepta la recepción segura de correo electrónico utilizando conexiones TLS estrictas, siempre y cuando se trabaje con una política en modo de *hacer cumplir,* y que el correo electrónico nunca debe entregarse a través conexiones TLS inseguras. Al configurar una política en el modo *hacer cumplir*, el servidor destinatario exige a los servidores externos que admiten MTA-STS que examinen si la conexión SMTP está cifrada y autenticada.

En este aspecto se ha planteado dos escenarios de prueba, en donde el *escenario 1* se representa un envío exitoso desde un servidor externo que admite MTA-STS de manera nativa y que es capaz de verificar las conexiones seguras con dominios que también admite MTA-STS. De otra manera en el *escenario 2* se induce a una falla en el archivo de política de MTA-STS y los registros MX del dominio destinatario, de tal manera que un servidor de envío falle en él envió del mensaje de correo hacia el servidor destinatario.

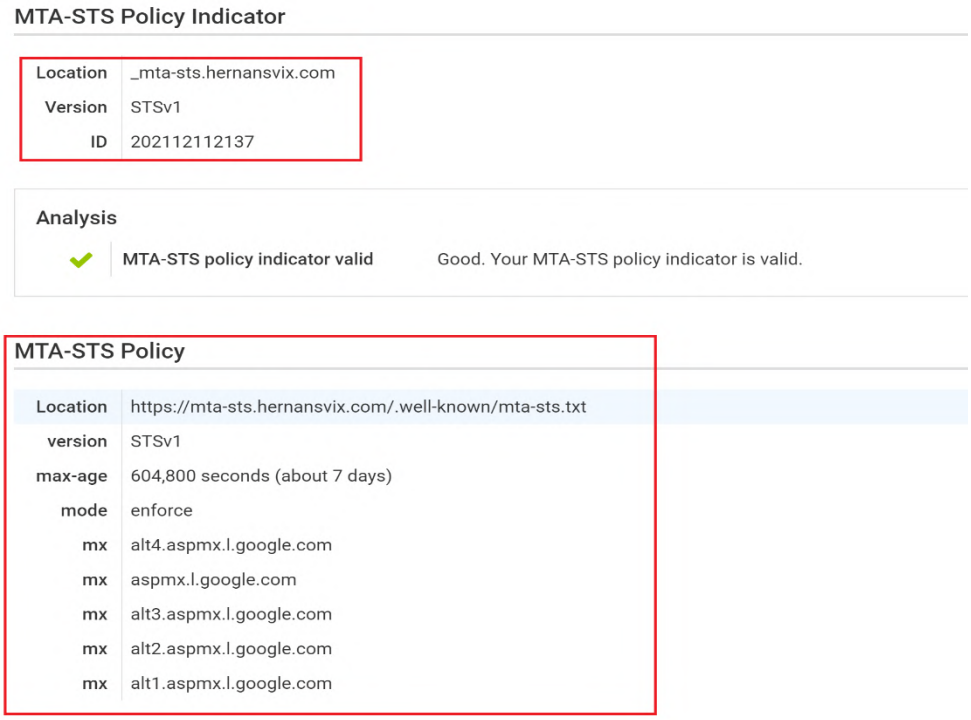
4.5.1. Escenario 1

En esta sección se representa un caso en donde la entrega del correo desde un dominio que admite MTA-STS hacia *hernansvix.com* que también admite MTA-STS sea exitosa. Esta prueba se lo hará utilizando los servidores de correo SMTP de *Outlook.com,* que son de los pocos que admiten MTA-STS de manera nativa. A continuación, se describe los parámetros de configuración de *hernansvix.com*:

Lo primero es validar las configuraciones MTA-STS de *hernansvix.com* mediante el testing del dominio en *hardenize.com*, el resultado se la detalla en la Figura 59.

Figura 59.

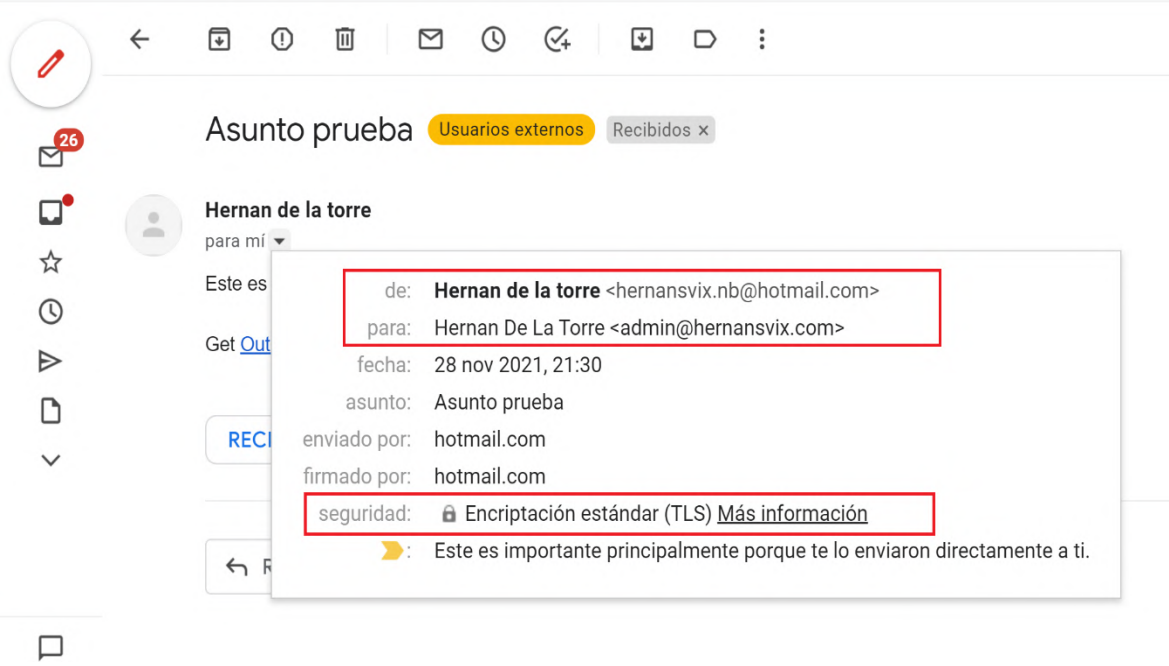
Indicador de Configuraciones de MTA-STS para hernansvix.com



Con las configuraciones correctas para el dominio *hernansvix.com*, el correo que se envía desde los servidores de *Outlook.com* será mediante una conexión cifrada. Dicho esto, se procede a enviar un correo desde el servicio de *Outlook.com* a *hernansvix.com.* Para determinar el estado de recepción del mensaje se verifica la bandeja de entrada de Gmail, aquí se especifica las direcciones de correo de recepción y envió, así mismo la conexión cifrada TLS que es aplicada por el estándar MTA-STS, esta información se la ilustra en la Figura 60.

Figura 60.

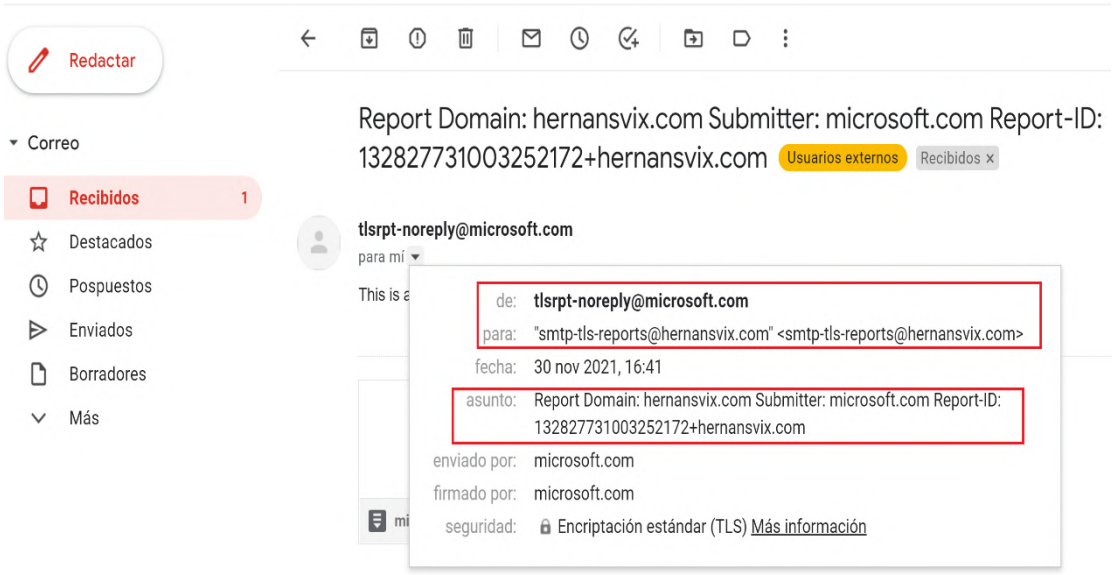
Estado de Entrega del Mensaje a admin@hernansvix.com



Así mismo se ha receptado la notificación TLS dirigida al administrador de domino cuya dirección es *smtp-tls-reports@hernansvix.com*, tal y como se indicó en los registros TLS Reporting durante su configuración, en la Figura 61 se representa el correo receptado en la bandeja de entrada.

Figura 61.

Documento de Reporte TLS en la Bandeja de smtp-tls-reports@hernansvix.com



A continuación, se procede a descargar el archivo adjunto que contiene el reporte TLS. En ese documento se verifica que el dominio de *hernansvix.com* está configurado correctamente, ya que especifica la política configurada en *mta-sts.hernansvix.com* la cual coinciden con el archivo alojado en el servidor HTTPS. En el reporte se informa que fue enviado desde la organización de Microsoft más específicamente desde la dirección *tlsrpt-noreply@microsoft.com*, la cual gestiona los reportes para el dominio de *hotmail.com*, en el estado del informe se observa que no hubo ningún problema la enviar los mensajes de correo hacia *hernansvix.com*, ya que resalta el mensaje de *total-successful-session-count,* lo que significa que el MTA remitente pudo negociar una conexión TLS compatible con la política de comunicación MTA-STS. El contenido del reporte TLS se lo observa en la Figura 62.

Figura 62.

Reporte TLS Emitido para hernansvix.com


```
{"organization-name":"Microsoft Corporation",
"date-range":
{"start-datetime":"2021-11-29T00:00:00Z",
"end-datetime":"2021-11-29T23:59:59Z"
},

"contact-info":"tlsrpt-noreply@microsoft.com",
"report-id":"13282773100325217 2+hernansvix.com",
"policies":[
{
"policy":{
"policy-type":"sts",
"policy-string":[
"version: STSv1",
"mode: testing",
"mx: ALT4.ASPMX.L.GOOGLE.COM",
"mx: ALT2.ASPMX.L.GOOGLE.COM",
"mx: ASPMX.L.GOOGLE.COM",
"mx: ALT1.ASPMX.L.GOOGLE.COM",
"mx: ALT3.ASPMX.L.GOOGLE.COM",
"max_age: 604800"
],
"policy-domain":"hernansvix.com"
},
"summary":{
"total-successful-session-count":2,
"total-failure-session-count":0
}
}
]
}
```


4.5.2. Escenario 2

Para esta sección se representa el caso donde la entrega de correo electrónico es fallida, cuando el mensaje de correo electrónico enviado desde el dominio de *Outlook.com* no supera las comprobaciones de MTA-STS.

Para esta prueba se induce a errar las conexiones TLS mediante configuraciones incorrectas en el archivo de políticas de *mta-sts.txt*. Esto provocará que el correo electrónico no

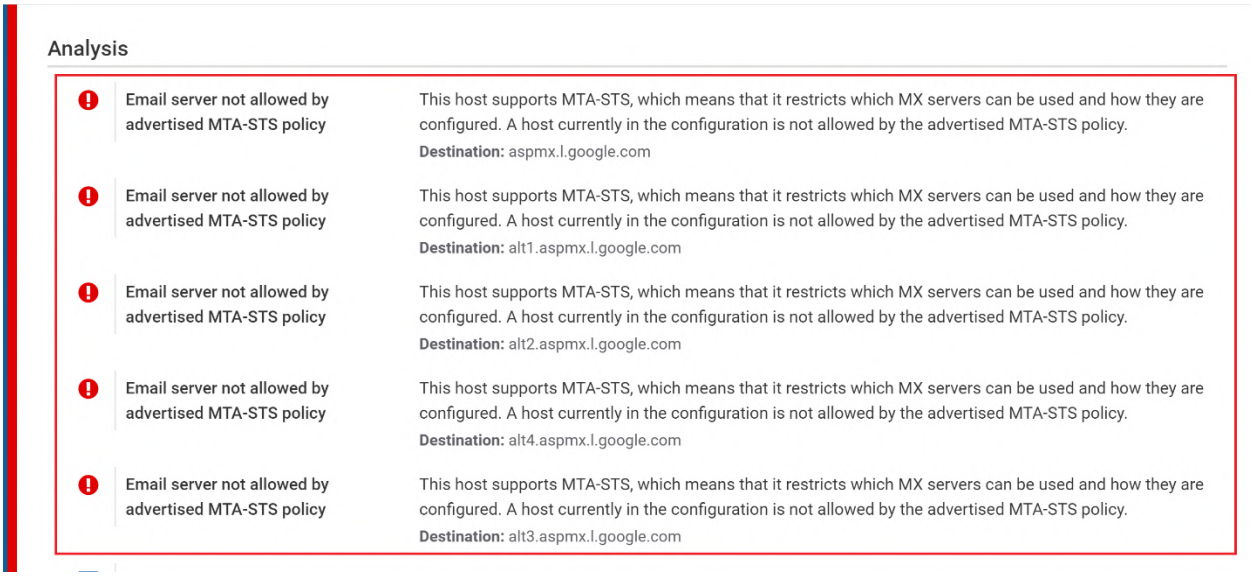
se entregue por la política de *hacer cumplir* impuesta por el servidor. En este escenario se prueba con un archivo de política que anuncia registros MX incorrectos. Los parámetros de configuración de *hernansvix.com* son:

- Política de MTA-STS: servidor mx de terceros deliberadamente incorrecto, pero existente en el archivo mta-sts.
- Registro DNS: Servidores MX correctos.

Ahora se procede a validar las configuraciones de *hernanasvix.com* con el archivo de política incorrecto que contiene los falsos servidores MX. El resultado del Testing del dominio en *hardenize.com* se lo especifica en la Figura 63.

Figura 63.

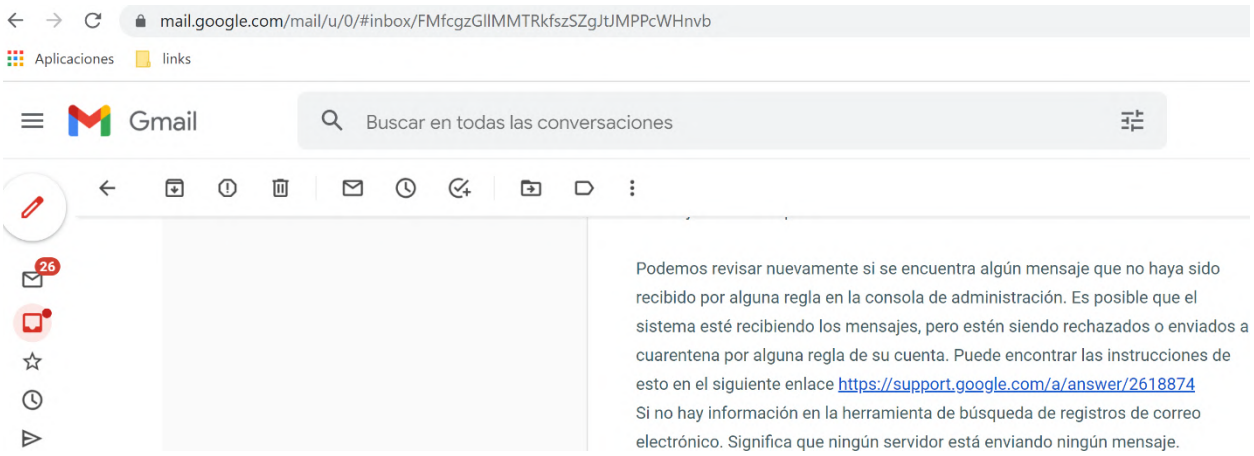
Testing Fallido de MTA-STS del Dominio hernansvix.com



En la Figura 63 se indica los errores de validación para MTA-STS las cuales manifiestan que no coinciden con los registros de Google al cual está vinculado al dominio. A continuación, se procede a enviar un correo desde una cuenta de *Outlook.com* a una cuenta de *hernansvix.com*. El mensaje enviado no fue receptado por el buzón de *hernansvix.com*, con este motivo Google ha enviado un correo de alerta en donde manifiesta que ciertos mensajes de correo han sido rechazados por el servidor, el mensaje se muestra en la Figura 64.

Figura 64.

Mensaje de Alerta de Google



En la notificación de Google además proporciona un enlace para verificar las configuraciones de correo electrónico erróneas. El enlace proporciona información acerca de las configuraciones de MTA-STS del dominio, en donde detecta errores en el archivo de política la misma que especifica que los registros MX no coinciden con los que se informan en la política de STS, lo cual es correcta ya que se modificó los destinos de host MX hacia servidores de correo desconocidos. En la Figura 65 se representa el estado de MTA-STS proporcionado por Google.

Figura 65.

Estado de Servicio MTA-STS Proporcionado por Google.

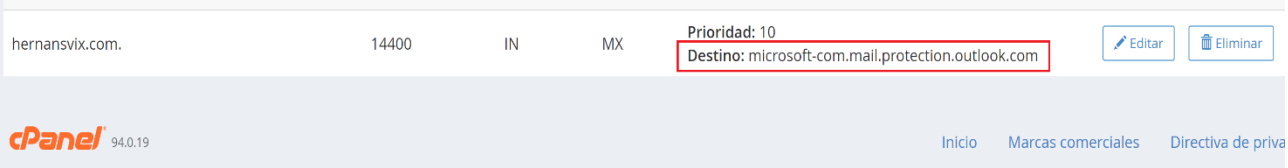
De igual modo se incita al fallo del estándar MTA-STS mediante errores en los registros MX del servidor de correo. Los parámetros de configuración de *hernansvix.com* son:

- Política de MTA-STS: servidor mx correcto, pero existente en el archivo *mta-sts*.
- Registro DNS: Servidores MX incorrectos.

Para ello lo primero es apuntar a otro servidor de destino mediante la adición de nuevos registros MX, es decir apuntar a los servidores de *Outlook.com*, mediante el registro *microsoft-com.mail.protection.outlook.com*. En la Figura 66 se nota el cambio realizado desde el panel de administración del Hosting.

Figura 66.

*Tabla de Zona de Dominio con el Nuevo Registro MX***.**



Después de la propagación del nuevo registro MX, inmediatamente notifica una alerta de configuración en el servidor de correo, pues al actualizar las configuraciones DNS la bandeja de correo Gmail de *hernansvix.com* fue suspendida temporalmente debido a inconsistencias con sus configuraciones, además el estándar MTA-STS detecta un error en su política, ya que esta no coincide con el registro MX de Outlook, a causa de este error los mensajes de correo no serán entregados por el servidor de envío ya que lo detecta como un servidor con errores en su validación de política STS. En la Figura 67 se contempla el error en el estado de validación de MTA-STS.

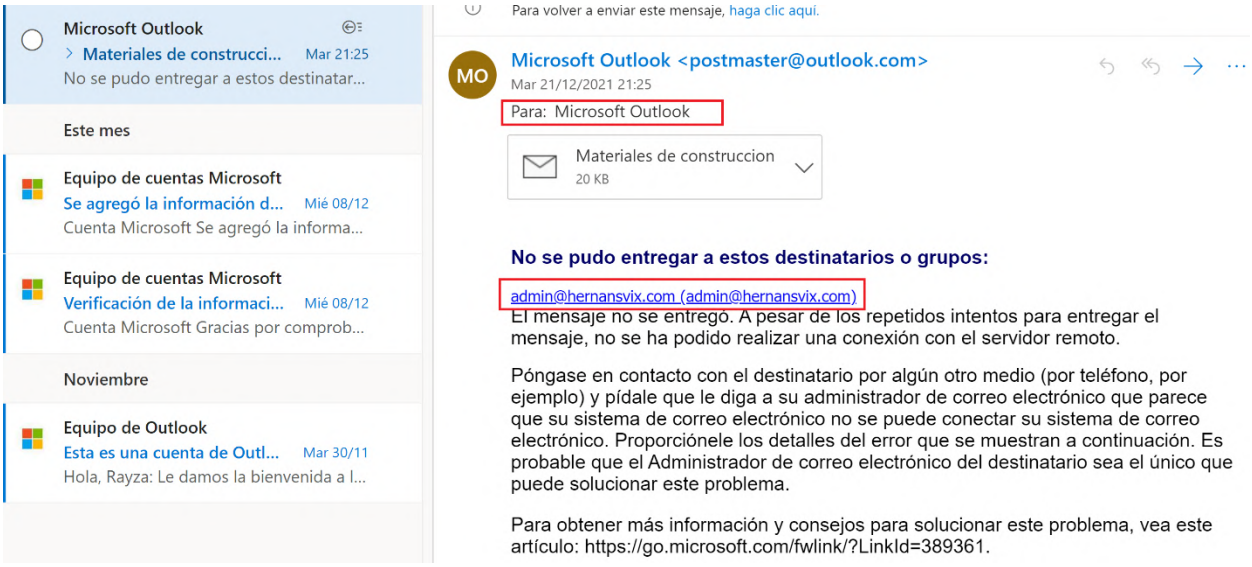
Figura 67.

Error de Validación de MTA-STS.

Además, se ha receptado un correo electrónico a la cuenta de *Outlook.com* el cual informa acerca de errores de conectividad ala cuenta *admin@hernansvix.com*, especificando que a pesar de repetidos intentos de envío del mensaje de correo no se ha podido establecer una comunicación con el servidor o dominio *hernansvix.com*. En la Figura 68 se observa el correo electrónico receptado en la cuenta de *raymitr@outlook.com.*

Figura 68.

Correo Electrónico Receptado en la Cuenta de Outlook.com



4.5.3. Análisis de Ambos Escenarios

En el primer escenario se ha implementado una política de MTA-STS en modo de *hacer cumplir* con todas las configuraciones correctas para el dominio de *hernansvix.com.* Para las pruebas de envió se ocupó los servicios de *Outlook.com*, en este escenario el correo electrónico se transporta a través de una conexión segura ya que ambos servidores soportan MTA-STS, además se ha recibido un reporte TLS donde se notifica la entrega segura del mensaje de correo mediante el comando *total-successful-session-count,* la cual especifica que el servidor externo de *Outlook.com* si pudo negociar una conexión TLS segura con el dominio *hernansvix.com.*

En el escenario 2 se indujo a una falla en las configuraciones de MTA-STS. Con este fin primero se ha configurado un archivo de política erróneo en donde sus registros MX con coinciden con los agregados en la zona de dominios del hosting, como resultado los mensajes de correo no pudieron ser receptados ya que el servidor de *Outlook.com* detecto una anomalía en la

política MTA-STS, por consiguiente no se ha podido establecer una conexión segura TLS, además se ha recibido un correo de notificación en donde se especificó el error acerca de la no coincidencia de los registros MX en el archivo de política. Después se ha modificado deliberadamente los registros MX de Google para agregar nuevos registros que apunten a los servidores de *outloook.com,* en este caso tampoco se ha podido receptar los mensajes de email ya que se ha deshabilitado el buzón de Gmail para el dominio *hernansvix.com,* esto se debe a que los registros MX añadidos no están registrados ni validados con el dominio en los servidores de Outlook. Además, después de un tiempo se ha receptado un mensaje notificando el error de conectividad con el dominio de *hernansvix.com,* en donde se especifica que a pesar de varios intentos de entrega no fue posible establecer una conexión con el servidor remoto. En definitiva, con el escenario 2 se ha intentado redirigir el correo entrante mediante falsificación DNS en donde se ha observado que los mensajes no se entregarán a un destino incorrecto. De modo que el correo electrónico está protegido contra las malas acciones.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El estudio bibliográfico permite analizar los contenidos más relevantes sobre el cual se sustenta el presente proyecto de investigación. Abordando las vulnerabilidades introducidas al enviar mensajes de correo usando STARTTLS, del cómo está diseñado MTA-STS para solventar dichas vulnerabilidades y que pasos pueden tomar las organizaciones para implementar el estándar.

Para la realización de este proyecto de titulación fue necesario apoyarse en una metodología adecuada de tal manera que se describa adecuadamente cada uno de los pasos para solucionar el problema de investigación, en este caso mejorar la privacidad del tráfico de correo electrónico con MTA-STS.

La implementación de los estándares de seguridad MTA-STS y TLS Reporting en un dominio de correo responde a un adecuado análisis de los requerimientos, de tal manera que puedan proveer la funcionalidad requerida.

Una organización puede anunciar el nombre del host de su servidor de correo en una página web segura separada, lo que significa que un atacante no puede simplemente subvertir las entradas DNS del servidor, ya que estas se comparan con las que se encuentran en el archivo de política MTA-STS y debido a que los MTA almacenan las políticas en su cache, hace que sea poco probable que suceda un ataque de suplantación DNS.

MTA-STS garantiza el intercambio de correos encriptados. Sin embargo, no protege el correo electrónico de alguien que tenga acceso al servidor, ya que los mensajes de correo se

almacenan en los servidores en texto plano. Por esta razón cualquiera que tenga acceso a los archivos del servidor podrán leerlos.

En el caso de prueba con un archivo de política que menciona registros mx incorrectos, no se entregaron los correos electrónicos como se esperaba, además el remitente de prueba no recibió ningún mensaje sobre problemas de entrega. Sin embargo, al revisar la parte técnica el servidor mencionó un error de validación fallida de errores mta-sts, aunque lo legible es que la dirección de destino no coincidía con el servidor destino, lo cual desencadenaría a errores en su DNS. Por lo cual confusamente lo identifica como error de interpretación mta-sts.

Hay que tener en cuenta que, si bien muchos de proveedores de correo electrónico empresarial ya han implementado el estándar MTA-STS, todavía no existe un soporte completo de todos los proveedores. Para aquellos que aún no lo implementan, los mensajes de correo se seguirán enviando en todos los casos.

Considerando la baja participación de MTA-STS y TLS Reporting, las entradas de correo de las notificaciones pueden ser muy bajas debido al bajo número de mensajes enviados por los usuarios a un determinado dominio. También hay que tener en cuenta que lastimosamente no todos los proveedores de correo electrónico utilizan ya esta función y es posible que no se recepte reportes con los proveedores de correo que no son compatibles.

Recomendaciones

Implementar MTA-STS implica un trabajo relativamente alto, por ello las organizaciones deben avanzar en su implementación con mucho cuidado; ya que si se activa los controles demasiado rápidos es posible que no se recepte los correos electrónicos. Para mitigar este riego, siempre se recomienda trabajar con una política MTA-STS en modo de prueba y configurar los

Informes TLS. Se debe monitorear el tráfico de correo entrante durante un tiempo prolongado para identificar y solucionar errores con el dominio.

Al momento de configurar la política siempre se debe incluir primero el campo versión, mientras que los demás campos pueden incorporarse en cualquier orden. De no incluir primero el valor versión la política no tendrá ninguna acción.

Si se configura una política MTA-STS en modo de prueba, es recomendable que el campo *max_age* tenga un valor de entre 604800 y 1209600 (entre 1 y 2 semanas), de tal forma que la configuración MTA-STS no caduque rápidamente.

Es bueno asegurarse de tener las configuraciones de TLS correctas en el servidor de correo electrónico, es decir, asegurase de contar con el soporte de TLS 1.2 o superior y de que sus certificados sean válidos o de lo contrario se perderán todos los correos electrónicos entrantes.

Siempre que se modifica el cuerpo de la política MTA-STS, el valor de id en el registro TXT debe actualizarse a un valor nuevo y único, lo que indica a los MTA que se estableció una nueva política.

Cada dominio configurado debe tener un archivo de política independiente. El cuerpo de las políticas puede ser similar, pero estas deben alojarse por separado dependiendo del dominio o subdominio correspondiente.

Si bien es cierto que el estándar MTA-STS ayuda a mitigar los ataques de intermediario y garantizar que los mensajes se cifren durante la transmisión ésta solo cifra las conexiones entrantes por esta razón siempre será bueno implementar seguridad extra para conexiones salientes como: SPF o DKIM, es decir todo bajo un mismo trecho.

Bibliografía

Amazon Web Services. (2020, enero 31). *Why do I get a client SSL/TLS negotiation error when I try to connect to my load balancer?* https://aws.amazon.com/es/premiumsupport/knowledge-center/elb-fix-ssl-tls-negotiation-error/

Australian Cyber Security Centre. (2020). *Implementing Certificates , TLS , HTTPS and Opportunistic TLS*. *December*, 1-19. https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-https-and-opportunistic-tls

Baaten, D. (2019, noviembre 20). *Better mail security with DANE for SMTP*. https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/

Barracuda Networks. (2010). *What is Email?*. https://www.barracuda.com/glossary/email-security

Bott, E. (2020, septiembre 15). *Microsoft 365 vs Google Workspace (formerly G Suite): Which productivity suite is best for your business?* https://www.zdnet.com/article/office-365-vs-g-suite-which-productivity-suite-is-best-for-your-business/

Bray, T. (2017). *The JavaScript Object Notation (JSON) Data Interchange Format* (T. Bray (ed.); Número 8259). https://doi.org/10.17487/RFC8259

Brotman, A., Margolis, D., & Dukhovni, V. (2018, septiembre 28). *STARTTLS Validation Result Types*. https://www.iana.org/assignments/starttls-validation-result-types/starttls-validation-result-types.xhtml

Bunge, M. (2002). ¿Qué es y para qué Sirve la Epistemología? En *EPISTEMOLOGÍA* (pp. 21-

33). https://www.incentro.com/es-es/blog/stories/metodologia-rad-desarrollo-rapido-aplicaciones/

Campaña, R. (2015). El proceso de desarrollo rápido de aplicaciones (DRA) de software: Un aporte práctico en el Instituto Geográfico Militar. *ResearchGate, April 2015*, 9. https://www.researchgate.net/publication/303839299_El_proceso_de_desarrollo_rapido_de_aplicaciones_DRA_de_software_Un_aporte_practico_en_el_Instituto_Geografico_Militar

Chicaiza Valverde, C. (2020, agosto 28). *ESET presenta su informe de amenazas del segundo trimestre del 2020*. Canal News Ecuador. https://canalnewsecuador.com/2020/08/28/eset-presenta-su-informe-de-amenazas-del-segundo-trimestre-del-2020/

Cillero, M. (2019). *Construcción del Sistema de Información ÍNDICE*. http://cc.etsii.ull.es/ftp/antiguo/INGSOF2/Metricav3/CSIPROC.PDF

Cisco Systems. (2019a). *Correo electrónico : haga clic con precaución*. https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/email-security-spa-final-version.pdf

Cisco Systems. (2019b). *Defiéndase contra amenazas críticas de la actualidad*. https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cybersecurity-series-threat.pdf

Comply, R. (2020, abril 26). *Do we need SMTP MTA Strict Transport Security (MTA-STS)?* https://blog.paranoidpenguin.net/2020/04/smtp-mta-strict-transport-security/

Crocker, D., Hansen, T., & Kucherawy, M. (2011). DomainKeys Identified Mail (DKIM) Signatures. En D. Crocker, T. Hansen, & M. Kucherawy (Eds.), *document RFC 6376, Proposed Standard, Internet Engineering Task Force.* https://doi.org/10.17487/rfc6376

Cruz, K. (2017, octubre 5). *La Importancia de la Seguridad en el Email Marketing - Benchmark Email*. https://www.benchmarkemail.com/es/blog/la-importancia-de-la-seguridad-en-el-email-marketing/

Danmarg. (2021, junio 20). *STS-Mate*. https://github.com/danmarg/sts-mate

Datta. (2021, febrero 17). *18 millones de malware y correos electrónicos de phishing relacionados con Covid-19 son enviados diariamente*. Datta Business Innovation. https://datta.com.ec/articulo/18-millones-de-malware-y-correos-electronicos-de-phishing-relacionados-con-covid-19-son-enviados-diariamente

De Graaff, B. (2021, julio 21). *Zimbra SkillZ: Enhance email confidentiality using MTA-STS*. https://blog.zimbra.com/2021/07/zimbra-skillz-enhance-email-confidentiality-using-mta-sts/

Deutsch, P. (1996). *GZIP file format specification version 4.3*. https://doi.org/10.17487/rfc1952

Digital Guide IONOS. (2019, agosto 5). *La respuesta automática perfecta*. https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/la-respuesta-automatica-perfecta/

dmarcian. (2021, abril 1). *MTA-STS*. https://dmarcian.com/mta-sts/

Dubrovin, V. (2020, septiembre 2). *Dive into Email Security: MTA-STS Policies*. https://habr.com/en/company/mailru/blog/517544/

Dukhovni, V., & Hardaker, W. (2015a). SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS). En *document RFC 7672* (Número 7672). https://doi.org/10.17487/RFC7672

Dukhovni, V., & Hardaker, W. (2015b). The DNS-Based Authentication of Named Entities

(DANE) Protocol: Updates and Operational Guidance. En *document RFC 7671, Proposed Standard, Internet Engineering Task Force*. https://doi.org/10.17487/RFC7671

DuoCircle. (2021). *What Is MTA-STS - Combined With TLS-RPT Protocol Ensures Encryption And Prevent Interception Of Emails*. https://www.duocircle.com/resources/what-is-mta-sts

El Comercio. (2021, febrero 18). *Banco Pichincha advierte de correos fraudulentos que buscan obtener información para realizar «transacciones ilegítimas»*. https://www.elcomercio.com/actualidad/negocios/banco-pichincha-correos-transacciones-ilegitimas.html

Email Security Geek. (2020, febrero 10). *Hosting your MTA-STS policy using GitHub Pages*. https://emailsecurity.blog/hosting-your-mta-sts-policy-using-github-pages

Email Security Risk Assessment. (2019). *Quarterly Report | August 2019* (Vol. 5, Número March). https://mti.com/wp-content/uploads/2020/11/MTI-Mimecast-Email-Security-Risk-Assessment-WP.pdf

Enclyne. (2019). *What You Need To Know About Office 365's TLS 1.2 Rollout*. https://www.enclyne.com/what-you-need-to-know-about-office-365s-tls-1-2-rollout/

Escuela Europea de Excelencia. (2021, julio 28). *¿En que consiste el ciclo PDCA para la mejora continua?* https://www.escuelaeuropeaexcelencia.com/2020/07/en-que-consiste-el-ciclo-pdca-para-la-mejora-continua/

ESET Internet Security. (2021). Security Report Latinoamerica 2021. En *Welivesecurity*. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Evans, C., Palmer, C., & Sleevi, R. (2015). Public Key Pinning Extension for HTTP. En *document RFC 7469, Proposed Standard, Internet Engineering Task Force*. https://doi.org/10.17487/RFC7469

Fenton, J. (2019). *SMTP Require TLS Option*. https://doi.org/10.17487/RFC8689

Fernández, M. (2018). *¿Seguridad en el correo electrónico: Es SMTP STS un paso fundamental?* https://blog.mailfence.com/es/smtp-sts-un-paso-fundamental-para-la-seguridad-en-el-correo-electronico/

Ferreira, J. (2021, mayo 21). *Why Important AAA Standards, such as MTA-STS, are Essential for Email Security*. https://www.anubisnetworks.com/blog/why_aaa_standards_are_a_must_have_for_email_security

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S., & Levchenko, K. (2015). *Security by Any Other Name*. 450-464. https://doi.org/10.1145/2810103.2813607

Gersch, J., Massey, D., & Rose, S. (2017). DANE Trusted email for supply chain management. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2017-Janua*, 2896-2905. https://doi.org/10.24251/hicss.2017.350

Gomez Zea, J. M. (2016). Implementando scrum+ rad para la gestión y desarrollo de proyectos de software en equipos de trabajo con personal limitado y eventual. *Programación Matemática y Software*, *8*, 52-64.

Gonzalia, D. (2020, junio 18). *Email: políticas de seguridad para las pyme*. https://www.interbel.es/email-politicas-de-seguridad-para-las-pyme/

Google. (2019, abril 10). *Google Workspace Updates: Gmail making email more secure with MTA-STS standard*. https://workspaceupdates.googleblog.com/2019/04/gmail-making-email-more-secure-with-mta-sts.html

Google. (2021a). *Acerca de MTA-STS y los informes de TLS - Ayuda de Administrador de Google Workspace*. https://support.google.com/a/answer/9261504?hl=es

Google. (2021b). *Turn off MTA-STS*. https://support.google.com/a/answer/9711996?hl=en&ref_topic=9261406

Google Support. (2021). *Configurar los registros MX del correo electrónico de Google Workspace*. https://support.google.com/a/answer/140034?hl=es

Gory, M., Mohideen, M., & Banu, S. (2014). E-Mail Phishing -An open threat to everyone. *International Journal of Scientific and Research Publications*, *4*(2), 2250-3153.

Grandstream Networks. (2020). *CDR and REC API Guide*. https://www.grandstream.com/hubfs/Product_Documentation/ucm6xxx_cdr_rec_api_guide.pdf?hsLang=en

Greenwald, R. (2019, mayo 23). *What is MTA-STS, and how can it make my emails more secure?* Insource Services.INC. https://www.insourceservices.com/what-is-mta-sts-and-how-can-it-make-my-emails-more-secure/

Hardaker, W., & Dukhovni, V. (2019). *SMTP Security Options*. *June*.

Helme, S. (2020, febrero 5). *Improving email security with MTA-STS*. https://scotthelme.co.uk/improving-email-security-with-mta-sts/

Henshall, A. (2017, junio 30). *How to Use The Deming Cycle for Continuous Quality*

Improvement. Process. https://www.process.st/deming-cycle/

Hoffman, P. (1999). *SMTP Service Extension for Secure SMTP over TLS* (Número 1). https://doi.org/10.17487/rfc2487

Hoffman, P. (2002, febrero). *SMTP Service Extension for Secure SMTP over Transport Layer Security*. document RFC 3207, RFC 7817, Proposed Standard, Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc3207

Hoffman, P., & Schlyter, J. (2012). The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. En *document RFC 6698, RFCs 7218, 7671, Proposed Standard, Internet Engineering Task Force*. https://doi.org/10.17487/RFC6698

Hogg, S. (2014, abril 14). *DNS-based Authentication of Named Entities (DANE)*. https://blogs.infoblox.com/ipv6-coe/dns-based-authentication-of-named-entities-dane/

HubSpot. (2021, marzo 26). *Reenvía un mensaje de correo electrónico a un correo alojado en la bandeja de entrada de conversaciones.* https://knowledge.hubspot.com/es/conversations/connect-a-hosted-email-to-your-conversations-inbox

Ictea. (2021). *¿Qué es el alojamiento web ?* https://www.ictea.com/cs/index.php?rp=%2Fknowledgebase%2F7%2FiQue-es-el-alojamiento-web-.html&language=portuguese-br

Instituto Nacional de Cyberseguridad. (2020a). *Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario*.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf

Instituto Nacional de Cyberseguridad. (2020b, julio 16). *El ataque del "Man in the middle" en la empresa, riesgos y formas de evitarlo*. https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

Internet Security. (2020, junio 10). *Active and Passive Attacks: Differences and prevention*. https://www.internetsecurity.tips/active-and-passive-attacks-differences-and-prevention/

James. (2021, junio 17). *Using AWS to help secure your email domain: the MTA-STS website*. https://blog.james.rcpt.to/2021/06/17/using-aws-to-help-secure-your-email-domain-the-mta-sts-website/

JamieWeb. (2019, diciembre 27). *Securing Inbound Email Transport with MTA-STS and STARTTLS-Everywhere*. https://www.jamieweb.net/blog/securing-inbound-email-transport-with-mta-sts-and-starttls-everywhere/

Jimeno Bernal, J. (2013, agosto 23). *Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua*. Grupo PDCA Home. https://www.pdcahome.com/5202/ciclo-pdca/

Kambourakis, G., Gil, G. D., & Sanchez, I. (2020). What Email Servers Can Tell to Johnny: An Empirical Study of Provider-to-Provider Email Security. *IEEE Access, 8*, 130066-130081. https://doi.org/10.1109/ACCESS.2020.3009122

Kanbanize. (s. f.). *What is Plan-Do-Check-Act (PDCA) Cycle?* Recuperado 11 de agosto de 2021, de https://kanbanize.com/lean-management/improvement/what-is-pdca-cycle

Kitterman, S. (2014). Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. En *document RFC 7208, Proposed Standard, Internet Engineering Task Force*. https://doi.org/10.17487/RFC7208

Kucherawy, M., & Zwicky, E. (2015). *Domain-based Message Authentication, Reporting, and Conformance (DMARC)* (M. Kucherawy & E. Zwicky (eds.)). https://doi.org/10.17487/rfc7489

Kumar, S. (2021, junio 4). *Hostgator Vs Bluehost - Which Is The Best Web Hosting?* https://theguidex.com/hostgator-vs-godaddy-compared/

Lakhtaria, K. I. (2015). Next generation wireless network security and privacy. *Next Generation Wireless Network Security and Privacy*, *October*, 1-372. https://doi.org/10.4018/978-1-4666-8687-8

Leeman, F. (2019, abril 18). *MTA-STS explained*. https://www.uriports.com/blog/mta-sts-explained/

Lewis, L. (2021, abril 13). *Infographic: What Happens In An Internet Minute 2021*. Merge. https://www.allaccess.com/merge/archive/32972/infographic-what-happens-in-an-internet-minute

Li, S., & Gillula, J. (2018, junio 25). *Announcing STARTTLS Everywhere: Securing Hop-to-Hop Email Delivery*. https://www.eff.org/deeplinks/2018/06/announcing-starttls-everywhere-securing-hop-hop-email-delivery

Lux Scientiae. (2015, marzo 31). *The Case for Email Security: Why it is insecure and how to protect youself*. https://luxsci.com/blog/the-case-for-email-security.html

Mailhardener. (s. f.-a). *MTA-STS*. Recuperado 27 de septiembre de 2021, de https://www.mailhardener.com/kb/mta-sts

Mailhardener. (s. f.-b). *SMTP TLS reporting*. Recuperado 27 de septiembre de 2021, de https://www.mailhardener.com/kb/smtp-tls-reporting

Margolis, D, Risher, M., Ramakrishnan, B., Brotman, A., & Jones, J. (2018). SMTP MTA Strict Transport Security (MTA-STS). En *document RFC 8461*. https://doi.org/10.17487/RFC8461

Margolis, Daniel, Brotman, A., Ramakrishnan, B., Jones, J., & Risher, M. (2018). SMTP TLS Reporting. En *document RFC 8460*. https://doi.org/10.17487/RFC8460

Melnikov, A. (2016). Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols. *Ietf*, *7817*, 1-13. https://doi.org/10.17487/RFC7817

Melnikov, A., & Dukhovni, V. (2018, mayo 2). *I-D Action: draft-ietf-uta-smtp-tlsrpt-19.txt*. https://uta.ietf.narkive.com/2Tt1HGok/i-d-action-draft-ietf-uta-smtp-tlsrpt-19-txt

Metodoss. (2016). *Metodología PDCA – Ciclo Deming*. Metodología PDCA – Ciclo Deming. https://metodoss.com/metodologia-pdca-ciclo-shewhart-deming/

Mezquita, T. (2019, diciembre 16). *Phishing*. https://cyberhoot.com/cybrary/phishing/

Microsoft Support. (2021). *POP, IMAP, and SMTP settings*. https://support.microsoft.com/en-us/office/pop-imap-and-smtp-settings-8361e398-8af4-4e97-b147-6c6c4ac95353

Mills, M. (2021, marzo 29). *MTA-STS and SMTP TLS: How They Improve Email Security*. https://itigic.com/mta-sts-and-smtp-tls-how-they-improve-email-security/

Misle, F. (2020, septiembre 28). *Increase SMTP security and trust with MTA-STS*.

https://blog.redsift.com/email/dmarc/increase-smtp-security-and-trust-with-mta-sts/

National CyberSecurity Centre. (2021, agosto 18). *Using MTA-STS to protect the privacy of your emails*. https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/using-mta-sts-to-protect-the-privacy-of-your-emails

Okta. (2021). *DNS Poisoning (DNS Spoofing): Definition, Technique & Defense*. https://www.okta.com/identity-101/dns-poisoning/

Papazyan, S. (2021, octubre 5). *¿Cómo se soluciona el problema de «falta la política MTA-STS»?* https://powerdmarc.com/es/how-to-fix-mta-sts-policy-is-missing/

Petcu, A. (2021, marzo 5). *Email Protection 101: What You Need to Know About Secure Communication*. https://heimdalsecurity.com/blog/email-protection/

PowerDMARC. (2020, diciembre 9). *What is MTA-STS and Why Do You Need It?* TEAM. https://powerdmarc.com/what-is-mta-sts-and-why-do-you-need-it/

Publico, R. (2017, marzo 1). *What is a Man-in-the-Middle Attack and How Can You Prevent It?* GlobalSign. https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack

Qureshi, N. (2019, noviembre 11). *How to make sure no man-in-the-middle attack can harm you*. https://thehacktoday.com/how-to-make-sure-no-man-in-the-middle-attack-can-harm-you/

Ramesh, P., Bhaskari, D., & Satyanarayana, C. (2010). A Comprehensive Analysis of Spoofing. *International Journal of Advanced Computer Science and Applications*, *1*(6), 158-159. https://doi.org/10.14569/ijacsa.2010.010623

Ristic, I. (2019, abril 23). *Introducing MTA Strict Transport Security (MTA-STS)*. https://www.hardenize.com/blog/mta-sts

Roy, D. (2020). *G Suite Vs Microsoft Exchange Online*. https://www.infiflex.com/g-suite-vs-microsoft-exchange-online

Salazar, P. (2014). *Universidad Nacional De Trujillo Facultad De Ciencias Físicas Y Matemáticas*.

Sanchez, I., & Draper-Gil, G. (2019). My Email Communications Security Assessment (MECSA). *Publications Office of the European Union, 2019*. https://doi.org/10.2760/166203

Scaife, J. (2019, septiembre 6). *How To Configure MTA-STS and TLS Reporting for Your Domain Using Apache on Ubuntu 18.04*. https://www.digitalocean.com/community/tutorials/how-to-configure-mta-sts-and-tls-reporting-for-your-domain-using-apache-on-ubuntu-18-04

Schwittmann, L., Wander, M., & Weis, T. (2019). Domain impersonation is feasible: A study of CA domain validation vulnerabilities. *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, 544-559. https://doi.org/10.1109/EuroSP.2019.00046

Shcherbakova, T. (2019, agosto 29). *Cómo utilizan el phishing para robar cuentas de correo electrónico*. https://www.kaspersky.es/blog/email-account-stealing/19155/

Shet, M. (2021, abril 26). *9 Servicios y aplicaciones de correo electrónico cifrado para una mejor privacidad*. https://geekflare.com/es/encrypted-email-services-apps/

Shitole, H. P., & Divekar, P. S. Y. (2019). Secure Email Software using e-SMTP. *International Research Journal of Engineering and Technology (IRJET)*, *6*(3), 3967-3971.

https://www.irjet.net/archives/V6/i3/IRJET-V6I31087.pdf

Shulman, H., & Waidner, M. (2017). One key to sign them all considered vulnerable: Evaluation of DnSsec in the internet. *Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2017*, 131-144.

Similar Tech. (2021). *G Suite VS Yahoo Business Email*. https://www.similartech.com/compare/g-suite-vs-yahoo-business-email

Sistemex. (2015, marzo 17). *¿Cómo evitar recibir correos SPAM?* https://whm.mx/new/2015/03/17/evitar-recibir-spam/

Soro, X. (2019, octubre 22). *Cómo identificar el phishing, la principal amenaza para las empresas*. https://hablemosdeempresas.com/pymes/identificar-phishing-suplantacion-identidad-ciberseguridad/

Squirrel, M. (2021, agosto 18). *HostGator Vs GoDaddy – What Happens When Top Hosts Go Head-To-Head?* https://digital.com/best-web-hosting/vs/hostgator-godaddy/

sslmate. (2020, noviembre 12). *Monitor and Automate MTA-STS with Cert Spotter*. https://sslmate.com/blog/post/mta_sts_monitoring_and_automation

Startup Guide IONOS. (2021, junio 25). *Google Workspace vs. Microsoft 365*. https://www.ionos.es/startupguide/productividad/google-workspace-vs-microsoft-365/

Tang, D. (2016, diciembre 12). *Continuous Improvement 101: The Deming Cycle (PDCA)*. Flevy Blog - Operations & Supply Chain. https://flevy.com/blog/continuous-improvement-101-the-deming-cycle-pdca/

Teng, J., Gu, W., & Xuan, D. (2012). Defending Against Physical Attacks in Wireless Sensor

Networks. En *Handbook on Securing Cyber-Physical Critical Infrastructure* (1st editio, pp. 251-279). Elsevier. https://doi.org/10.1016/B978-0-12-415815-3.00010-8

The Hacker News. (2021, agosto 30). *How Does MTA-STS Improve Your Email Security?* https://thehackernews.com/2021/08/how-does-mta-sts-improve-your-email.html

United Kingdom Public Sector Government. (2021, marzo 15). *Using the Mail Transfer Agent Strict Transport Security (MTA-STS) protocol in your organisation*. https://www.gov.uk/government/publications/email-security-standards/using-the-mail-transfer-agent-strict-transport-security-mta-sts-protocol-in-your-organisation

Universidad de Jaén. (2020). *Guías de seguridad uja*.

Valsorda, F. (2015, marzo 31). *The sad state of SMTP encryption*. https://blog.filippo.io/the-sad-state-of-smtp-encryption/

Weiler, S., & Blacka, D. (2013). Clarifications and Implementation Notes for DNS Security (DNSSEC). En S. Weiler & D. Blacka (Eds.), *document RFC 6840, Proposed Standard, Internet Engineering Task Force*. https://doi.org/10.17487/rfc6840

ANEXOS

Anexo1. Informe del Análisis de Requerimientos

METODOLOGÍA PARA IMPLEMENTAR SEGURIDAD EN SERVICIOS DE CORREO ELECTRÓNICO MEDIANTE EL MECANISMO MTA-STS (MAIL TRANSFER AGENT-STRICT TRANSPORT SECURITY) Y SMTP TLS REPORTING(TLSRPT) PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

ANÁLISIS DE REQUERIMIENTOS

Versión: 0100

Fecha: 09/12/2021

HOJA DE CONTROL

Proyecto	METODOLOGÍA PARA IMPLEMENTAR SEGURIDAD EN SERVICIOS DE CORREO ELECTRÓNICO MEDIANTE EL MECANISMO MTA-STS (MAIL TRANSFER AGENT-STRICT TRANSPORT SECURITY) Y SMTP TLS REPORTING (TLSRPT) PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS		
Entregable	Análisis de Requerimientos		
Autor	Raymi Hernán De La Torre Yamberla		
Versión/Edición	0100	**Fecha Versión**	22/10/2021
Aprobado por	Msc. Fabián Geovanny Cuzme Rodríguez	**Fecha Aprobación**	05/11/2021
Firma Director			

Objetivo de la actividad

Identificar y analizar las especificaciones funcionales, no funcionales y de plataformas requeridas para la implementación de los mecanismos MTA-STS y SMTP TLS REPORTING en un dominio de correo electrónico.

Antecedentes

Es posible mejorar la seguridad de correo electrónico empresarial activando en el dominio MTA Strict Transport Security (MTA-STS), un mecanismo que requiere que el correo que se envía al dominio esté autenticado y cifrado. De igual manera se puede activar los informes TLS para obtener información acerca de las conexiones de los servidores externos a un determinado dominio, con esta información se puede identificar y solucionar problemas de seguridad con el servidor de correo(National CyberSecurity Centre, 2021).

Si bien su uso aún no está muy extendido entre los proveedores de correo electrónico debido a que es un protocolo relativamente nuevo, solo algunas de las grandes corporaciones de alojamiento de correo electrónico empresarial admiten dicho protocolo de seguridad. Google Mail se ha convertido en el primer proveedor en admitir y validar los mecanismos MTA-STS y TLS Reporting, pues varios empleados de Google son coautores de los respectivos reportes de estudio en donde se especifica dicha tecnología. Sin embargo, se debe tener en cuenta que, si bien algunos de los principales servicios de correo electrónico han creado soporte para MTA-STS, todavía no existe un soporte completo para todos los proveedores. Para aquellos que aún no lo admiten, los correos electrónicos se seguirán enviando en todos los casos (Misle, 2020).

Las comunicaciones SMTP entre servidores de correo electrónico son más seguras cuando el servidor externo o de envío admite MTA-STS y el servidor destinatario implementa una política MTA-STS configurada en modo obligatorio(D Margolis et al., 2018).

Según Google. (s. f.) cuando se activa MTA-STS en un dominio, se solicita a los servidores de correo externos que envíen correos al dominio solamente si la conexión SMTP cumpla con los siguientes requisitos:

- La comunicación este autenticada con un certificado público válido.
- Este cifrada con TLS 1.2 o una versión superior.

En resumen, MTA-STS impone la transferencia de correos electrónicos a través de una ruta encriptada TLS. En caso de que no se pueda establecer una conexión encriptada, el correo electrónico no se entrega en absoluto, en lugar de ser entregado en texto sin cifrar.

El proceso de desarrollo de los requerimientos funcionales parte del análisis de las documentaciones RFC 8461 y RFC 8460. El cual manifiesta que para poder integrar los

mecanismos de transporte seguro estricto y notificaciones TLS a un dominio de correo electrónico estas deben cumplir algunas características de tal manera que sean comprensibles y cumplan el objetivo de ayudar a los desarrolladores a implementar los estándares de la manera correcta.

Requerimientos Funcionales y No Funcionales

Según Margolis et al. (2018) para implementar MTA-STS en un servicio de correo electrónico se requiere un servidor web habilitado para HTTPS con un certificado válido, de tal manera que el contenido pueda visualizarse en internet. Para esto no hay mejor forma que tenerlos a buen recaudo dentro de la nube de información, por lo tanto, se puede optar por un plan de Hosting que incluya alojamiento web personalizado bajo un nombre de dominio que permita una total flexibilidad para crear una página web y adaptarla de acuerdo a las necesidades. Además, se necesitará un servidor de correo electrónico para el envío y recepción de emails el cual funcionará en base al dominio registrado. Cada uno de estos servicios debe cumplir ciertos requerimientos funcionales basados en algunos aspectos de seguridad las cuales permitirán integrar los mecanismos MTA-STS y TLS Reporting a un dominio de correo. Así mismo se analiza los requerimientos no funcionales que surgen de acuerdo a las necesidades de presupuesto, interoperabilidad, seguridad general, etc.

En la Tabla 1 se detalla cada uno de los requerimientos funcionales y no funcionales de un servicio de hosting, servidor web y de correo.

Tabla 1

Tabla de requerimientos funcionales y no funcionales de los servicios.

Servicio	Nro.	Requerimiento	*Clasificación*	Descripción
Hosting	RQ_F1	Certificado de seguridad SSL	Funcional	Contar con un certificado SSL para los dominios y subdominios.
	RQ_F2	Seguridad General	Funcional	Deben incluir las características básicas de seguridad para preservar la integridad del hosting.
	RQ_F3	Dominio	Funcional	Brindar un dominio registrable con un nombre especifico.
	RQ_F4	Interfaz	Funcional	Incluir una adecuada interacción y administración de los usuarios con la aplicación .
	RQ_F5	Integración a servicios de alojamiento basados en la nube.	Funcional	Permitir el alojamiento del dominio a un nuevo espacio de trabajo digital integrado.
	RQ_NF6	Almacenamiento	No funcional	Una buena cantidad de almacenamiento de datos para el servicio de alojamiento web.
	RQ_NF7	Soporte	No funcional	Una atención rápida al cliente las 24 horas, los 7 días de la semana en caso de fallas en el hosting.
Servidor Web alojado	RQ_F8	Admitir SSL/HTTPS	Funcional	Corresponde a un servidor web basado en el protocolo HTTPS con un certificado SSL.
	RQ_F9	Certificado válido y firmado por una Autoridad certificadora de confianza.	Funcional	El servidor debe disponer de un certificado valido emitido por una autoridad de confianza(CA) para proteger los sitios web.

	RQ_NF10	Rendimiento	No funcional	Comprende una buena velocidad de carga y estabilidad del sitio web.
	RQ_NF11	Usabilidad	No funcional	El servidor debe contar con una buena usabilidad que permita al usuario navegar de forma sencilla y cómoda.
Servidor de correo alojado	RQ_F12	Admitir conexión segura TLS	Funcional	Requieren que el correo se transmita a través de una conexión segura TLS.
	RQ_F13	Versión TLS 1.2 o superior	Funcional	Posibilidad de habilitar Transport Layer Security (TLS) 1.2 o versiones superiores para proteger las conexiones entre servidores.
	RQ_F14	Certificado válido y firmado por una Autoridad certificadora de confianza	Funcional	Los certificados deben estar firmados por una autoridad de certificación raíz que los considera de confianza.
	RQ_F15	Certificados digitales no caducados	Funcional	En caso de que él certificado esté caducado proceder a renovarlo.
	RQ_F16	Soporte MTA-STS y TLS Reporting	Funcional	Proveer soporte nativo para MTA-STS relacionado a la publicación y resolución de políticas además del soporte para reportes TLS en el dominio.
	RQ_NF17	Usabilidad	No funcional	Brindar una buena experiencia de navegación de la plataforma al usuario en términos de eficiencia y rapidez.

RQ_NF18	Rendimiento	No funcional	Una fluidez al momento de entablar conexiones entre servicios de correo.
RQ_NF19	Portabilidad	No funcional	Una gestión de preferencia basada completamente en la nube.
RQ_NF20	Seguridad	No funcional	Integración de funcionalidades para proteger el acceso al correo electrónico.
RQ_NF21	Fiabilidad	No funcional	Comprende un entorno muy seguro y fiable.
RQ_NF22	Soporte	No funcional	Soporte para temas de problemas de administración todos los días de año.

Requerimientos de Plataforma

A continuación, se definirá las plataformas de trabajo basados en los requerimientos funcionales, esto se lo hará en base a una comparación entre las principales plataformas las cuales permiten establecer las condiciones necesarias para implementar los mecanismos MTA-STS y TLS Reporting a un dominio de correo.

Dominio/Hosting Web

Planes de hosting los hay de diferentes tamaños, herramientas y precios, pero se sugiere buscar el punto justo entre espacio de almacenamiento, cantidad de casillas de email y soporte. Algunos planes de hosting, pero no los gratuitos incluyen un nombre de dominio para que sea más fácil acceder al sitio. Si no viene incluido, es el usuario quien tiene que registrar un dominio mediante un registrador o bien usar un subdominio de la misma compañía(Ictea, 2021).

HostGator y GoDaddy son probablemente las figuras más conocidas en el mercado de servicios en línea. Estas comprenden dos opciones populares para cualquiera que inicie un sitio de alojamiento web. Sin embargo, HostGator ofrece precios más económicos y paquetes de alojamiento con todo incluido. GoDaddy, por otro lado, es más caro y está orientado a los usuarios comerciales (Squirrel, 2021).

En la siguiente Tabla 2 se detalla sus funcionalidades y su relación con los requerimientos funcionales y no funcionales para determinar un verdecito y seleccionar la mejor opción.

Tabla 2

Tabla comparativa de requerimientos entre HostGator y GoDaddy

Requerimiento	HostGator	GoDaddy	Veredicto
RQ_F1	★★★★☆	☆☆☆☆☆	HostGator, a diferencia de GoDaddy, ofrece un certificado SSL.
RQ_F2	★★★☆☆	★☆☆☆☆	Ambos proveedores carecen de opciones de seguridad gratuitas y muchas herramientas son de pago. Sin embargo HostGator cuenta con un firewall a nivel de servidor sin importar el plan.
			GoDaddy, brinda un mejor

RQ_F3	★★☆☆☆	★★★★☆	servicio de dominios que HostGator, porqué no solo te brinda el dominio principal, sino que también 99 sub-dominios a diferencia de HostGator que brinda 35 sub-dominios.
RQ_F4	★★★★★	★★★★★	Ambos proveedores ofrecen una combinación de interfaz de usuario nativa y cPanel que es muy fácil de usar.
RQ_F5	★★★★★	★★★★★	Ambos proveedores ofrecen registro y validación de dominios para servicios de terceros.
RQ_NF6	★★★☆☆	★★★☆☆	GoDaddy y HostGator ofrece 100 GB de almacenamiento gratuito.
RQ_NF7	★★★★★	★☆☆☆☆	La atención al cliente de HostGator es mejor. Su chat en vivo es rápido y su equipo muy útil. Por otro lado, el chat de GoDaddy es lento.
RQ_F8	★★★★★	☆☆☆☆☆	A diferencia de GoDaddy los planes de alojamiento HostGator incluye un certificado SSL gratuito que proporciona seguridad para los dominios y subdominios del sitio web.
			HostGator ofrece seguridad para

RQ_F9	★★★★★	☆☆☆☆☆	cifrar comunicaciones con certificados gratuitos de Sectigo.
RQ_NF10	★★★★☆	★★★★☆	El tiempo de actividad del 99,99% de HostGator fue ligeramente mejor que el 99,98% de GoDaddy. La respuesta promedio estuvo del lado de GoDaddy: 341 ms en comparación con los 525 ms de HostGator.
RQ_NF11	★★★★☆	★★★★☆	GoDaddy y HostGator están bastante igualados en lo que respecta a la usabilidad y ambos tienen problemas similares para configurar una cuenta.

Nota. Adaptado de (Kumar, 2021).

En esta comparación de HostGator y GoDaddy, se observa que HostGator ofrece las mejores características con respecto a los requerimientos funcionales y no funcionales para el servicio de alojamiento web. Por lo tanto, se opta por adquirir el plan más básico denominado Hatchling a $2.75/mes.

Servicio de correo alojado Personalizado

Para este proyecto se pretende montar un servidor de correo electrónico propio de tal manera que nuestro dominio de correo pueda enviar y recibir emails de un usuario@nombre_dominio.com para lo cual es recomendable registrar un dominio en ciertas plataformas para adquirir herramientas avanzadas para correo electrónico empresarial.

Para la implementación MTA-STS se necesita un nombre de dominio ya configurado para recibir correos, utilizando un servicio de correo alojado, como G-Suite u otros proveedores. De acuerdo a los antecedentes las funcionalidades MTA-STS y TLS Reporting son exclusivas de muy pocos proveedores de alojamiento de servicios digitales entre los cuales destaca Google Workspace, Yahoo! Mail y Microsoft Exchange. A continuación, en la Tabla 3 se detalla las funcionalidades de las tres plataformas de acuerdo a los requerimientos funcionales y no funcionales.

Tabla 3

Tabla comparativa de requerimientos entre Google Workspace, Yahoo! Mail y Microsoft Exchange.

Requerimiento	Google Workspace	Yahoo! Mail	Microsoft Exchange	Veredicto
RQ_F12	★★★★★	★★★★★	★★★★★	Los tres proveedores de correo alojado ofrecen de forma predeterminada transmisión segura de correo basado en TLS(Microsoft Support, 2021).
RQ_F13	★★★★★	★★★★☆	★★★★☆	Google, Yahoo! y Microsoft ofrecen versiones TLS 1.2, sin embargo solo Google mail da soporte para TLS 1.3(Enclyne, 2019).
RQ_F14	★★★★★	★★★★★	★★★★★	Los tres proveedores brindan certificados emitidos por una autoridad certificadora(CA)(Similar Tech, 2021).
RQ_F15	★★★★★	★★★★★	★★★★★	Los certificados digitales no caducan al menos que se suspenda el servicio.
RQ_F16	★★★★★	★★☆☆☆	☆☆☆☆☆	Solo Google cuenta con un soporte nativo de MTA-STS, Microsoft lo implementará en un futuro, y Yahoo! a pesar de tener soporte, no

				se puede incluir políticas en el dominio(Ristic, 2019).
RQ_NF17	★★★★☆	★★★★☆	★★★☆☆	Google tiene una interfaz más deductiva y de rápida integración mientras que Microsoft brinda un diseño menos familiar al igual que Yahoo! Mail(Startup Guide IONOS, 2021).
RQ_NF18	★★★★★	★★★★☆	★★☆☆☆	Microsoft Exchange tiene una velocidad que está a la par con el servidor de correo electrónico de Google al igual que Yahoo!(Bott, 2020).
RQ_NF19	★★★★★	★★★★★	★★☆☆☆	Yahoo! y Google se gestionan completamente en la nube, mientras que Microsoft Exchange depende de una aplicación instalada en la PC(Roy, 2020).
RQ_NF20	★★★★★	★★★★☆	★★★★☆	Las tres plataformas ofrecen seguridad a nivel de correo electrónico empresarial. Pero google ofrece funciones de seguridad adicionales(Bott, 2020).
RQ_NF21	★★★★★	★★☆☆☆	★★★★★	Yahoo! tienen una reputación un poco fiable tras sufrir algunas violaciones a su seguridad mientras que Google y Microsoft casi no han experimentado violaciones a sus sistemas de seguridad(Roy, 2020).
RQ_NF22	★★★★★	★★★★★	★★★★★	Todas ofrecen un buen soporte durante todos los días del año.

De acuerdo a la tabla anterior los tres proveedores cumplen en mayor medida con los criterios funcionales y no funcionales de seguridad de un servidor de correo basado en la nube, pero se observa que Yahoo! Mail no ofrece los mismos niveles de organización y fiabilidad que

Google Workspace o Microsoft Exchange. De estos, Google Workspace actualmente cuenta con un soporte nativo de MTA-STS, Microsoft lo implementará en un futuro y Yahoo! Mail indica soporte, pero no cuenta con una herramienta para publicar políticas. La función de seguridad MTA-STS está disponible para los administradores de Google Workspace (anteriormente G-Suite) en todas sus ediciones o planes. Los administradores de Workspace pueden optar por configurar políticas de MTA-STS y generar informes para el correo entrante en su servidor DNS. Si bien los administradores podían hacer esto anteriormente, será más impactante ahora que Gmail está aplicando las políticas de MTA-STS(Google, 2019).

La elección del mejor proveedor de correo electrónico se basa especialmente en el soporte de los protocolos MTA-STS y TLS Reporting, por lo tanto, Google Workspace es la más indicada, además de brindar mejores funciones de comunicación y colaboración. De esta manera se opta por adquirir el plan Business Starter a $5.40.

Anexo2. Registro de Nombre de Dominio

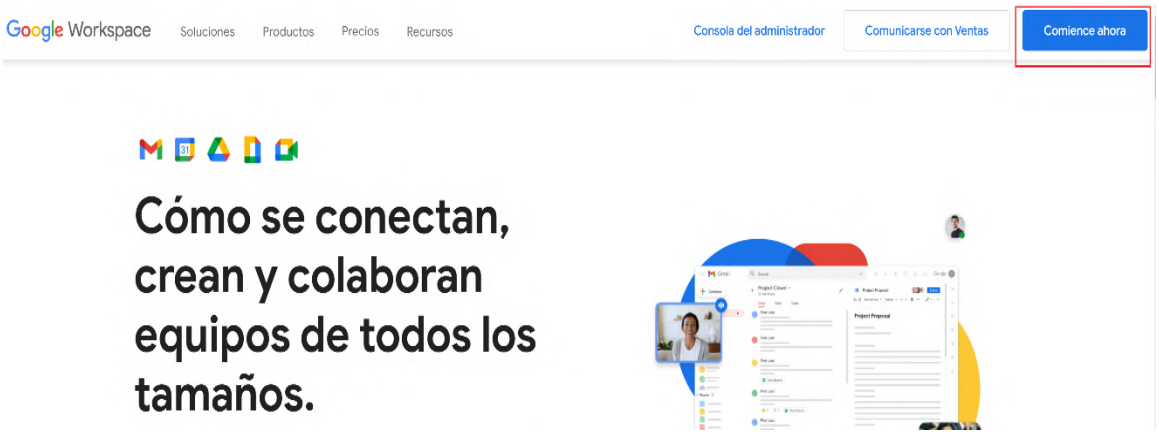
2. Registro del Dominio en Google Workspace

2.1. Validar una cuenta de administrador

Para registrar y validar la cuenta de Google en función al dominio adquirido en HostGator primero ingresamos al enlace https://workspace.google.com/intl/es-419_ar/ y se muestra la página principal tal como en la Figura 1, y seleccionamos la opción Comenzar ahora.

Figura 1

Página Principal de Google Workspace



Después se ingresa algunos datos preliminares que corresponde a la información de contacto en las respectivas pestañas como en la Figura 2 y 3.

Figura 2

Registro de Datos Preliminares

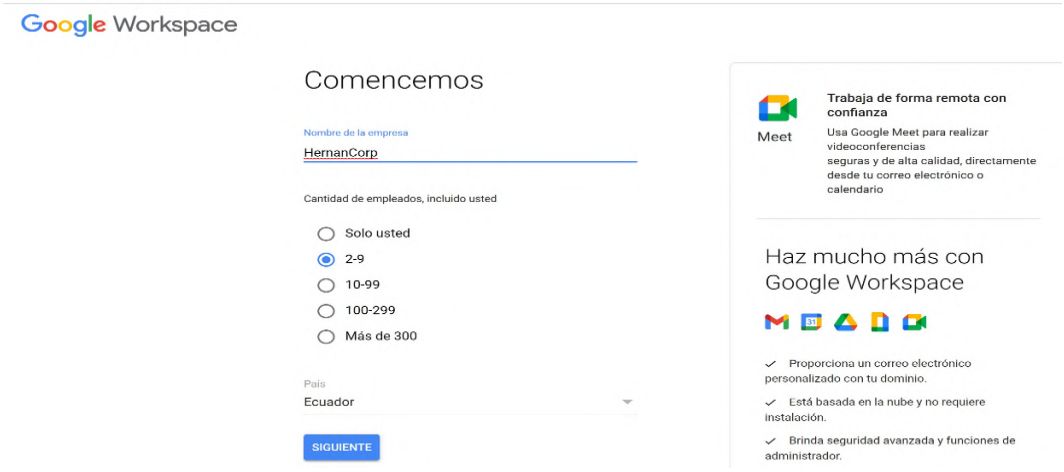
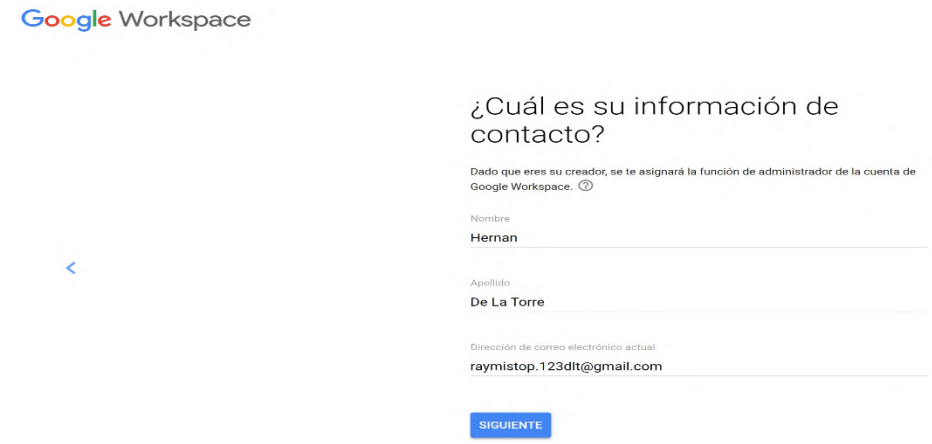


Figura 3

Registro de Información de contacto



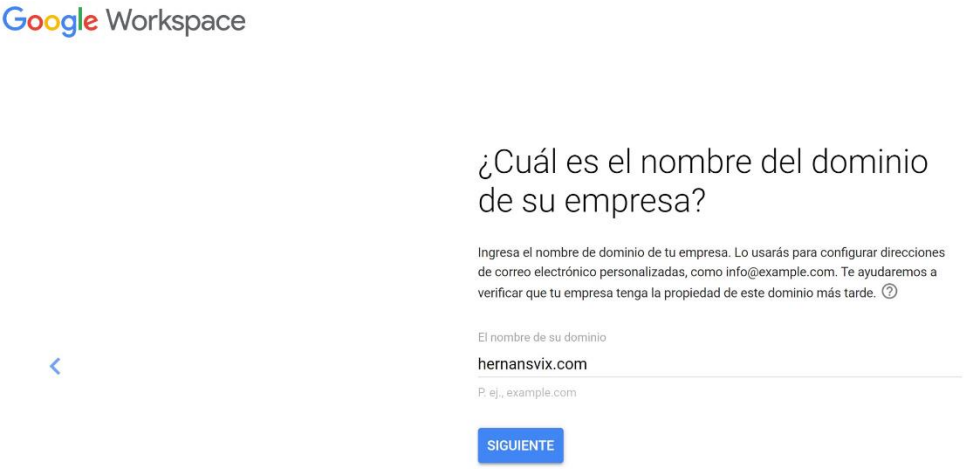
A continuación, ingresamos el dominio para configurar una cuenta de Google. Google Workspace da la opción de comprar un dominio, pero al tener ya un dominio registrado en HostGator hacemos clic en ya tengo un dominio, ingresamos el nombre de hernansvix.com para que Google Mail identifique el mismo cada paso se lo detalla en las Figuras 4 y 5.

Figura 4

Información del dominio

Figura 5

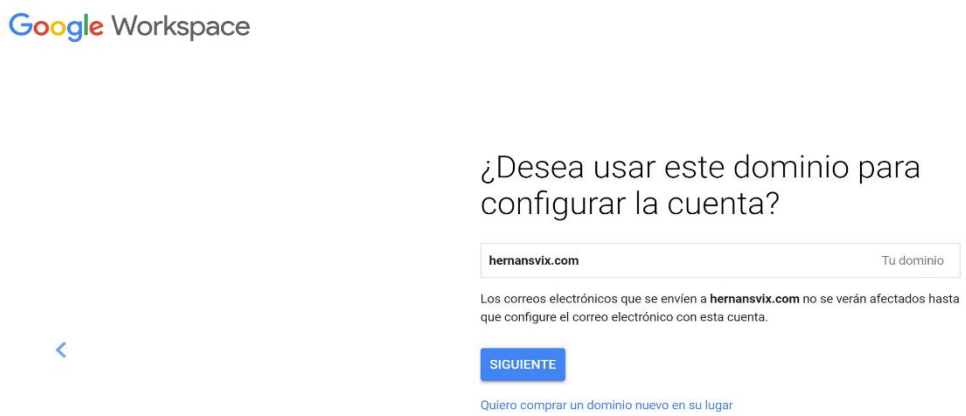
Registro del dominio hernansvix.com



Después se confirma el dominio que va a validar para adquirí una cuenta de Google como se ilustra en la Figura 6.

Figura 6

Confirmación del nombre de dominio



La Figura 7 indica cómo se configura las credenciales de acceso para la cuenta principal de administrador, aceptamos los términos de servicio y damos clic en Aceptar y Continuar. Después de validar las credenciales de acceso la cuenta ya estará creada como muestra la Figura 8.

Figura 7

Registro de datos para la cuenta de administrador

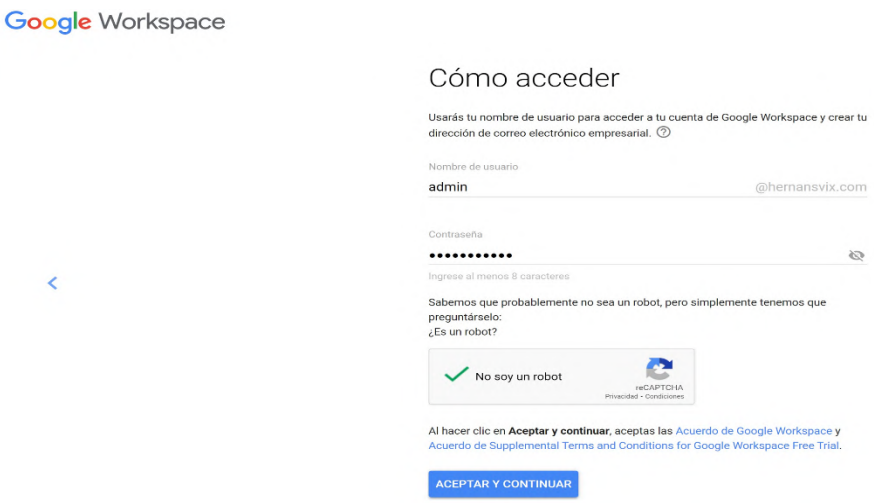
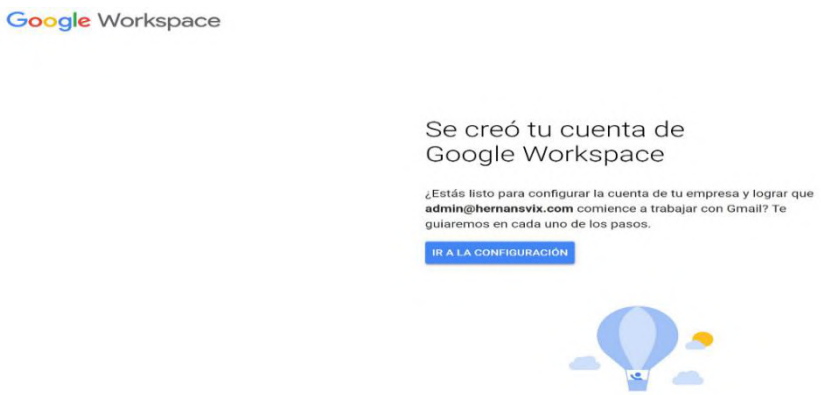


Figura 8

Pestaña de creación de cuenta exitosa



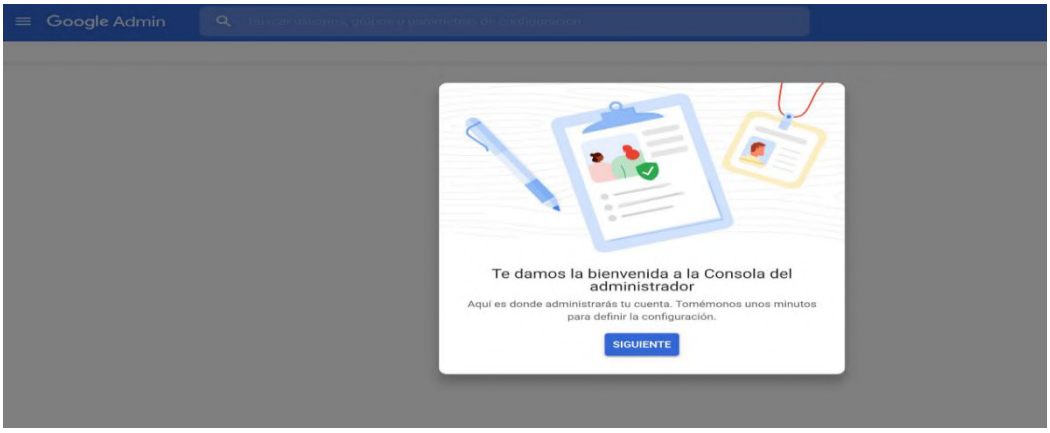
Finalizada la creación de cuanta ya se tendrá acceso a la consola de administración en donde se procederá a registrar y validar el dominio hernansvix.com en los servicios de Google.

2.2. Verificar el dominio hernansvix.com

Con el acceso a la consola de administración nos dirigimos al panel de administración cuya pestaña principal se indica en la Figura 9.

Figura 9

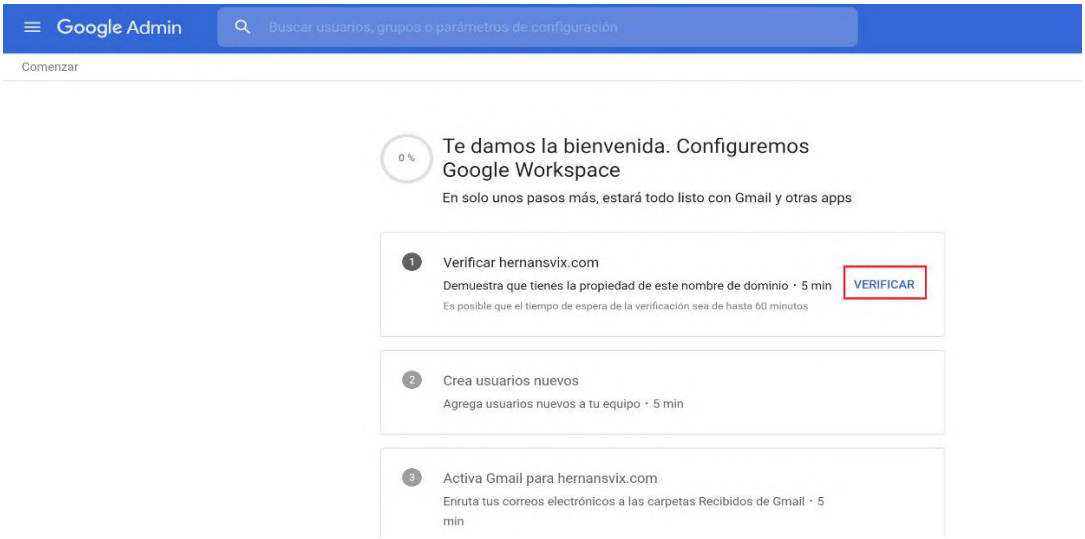
Página de Consola de administración de Google



Una vez dentro de las opciones se despliega tres pasos necesarios para validar el dominio igual que en la Figura 10, en primera instancia vamos a validar el dominio para eso seleccionamos la primera opción de verificar *hernansvix.com*.

Figura 10

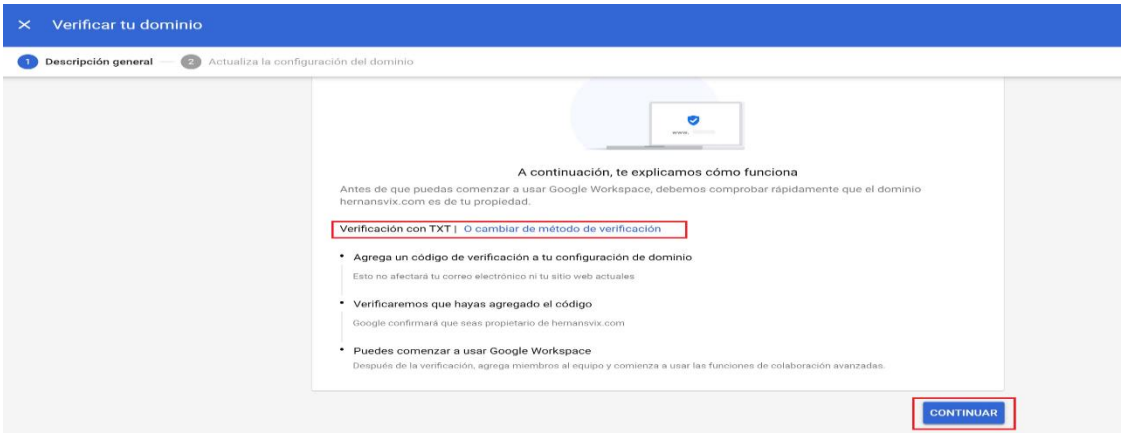
Pestaña Principal de opciones de Verificación de dominios



La verificación del dominio se lo hará mediante la adición de registros TXT que dirigen el tráfico de Internet al nombre del dominio y que deben apuntar a los servidores de Google. Una vez seleccionado la forma de verificación damos clic en continuar tal y como se muestra en la Figura 11.

Figura 11

Pestaña de verificación TXT



La adición de los registros TXT se lo hará desde el cPanel del Hosting. Por esta razón primero se debe iniciar sesión en el Panel de administración del dominio de HostGator, luego vamos a la pestaña de dominios y seleccionamos la opción de Editor de zonas tal como describe la Figura 12, en esta pestaña ejecutamos la acción de administrar y nos redirige a la Zona de Registros en donde se alojan todos los registros DNS del dominio principal, en las Figuras 13 y 14 se representa las acciones para acceder a la zona de dominio.

Figura 12

Opciones de editor de zonas

Figura 13

Panel de administración de dominios

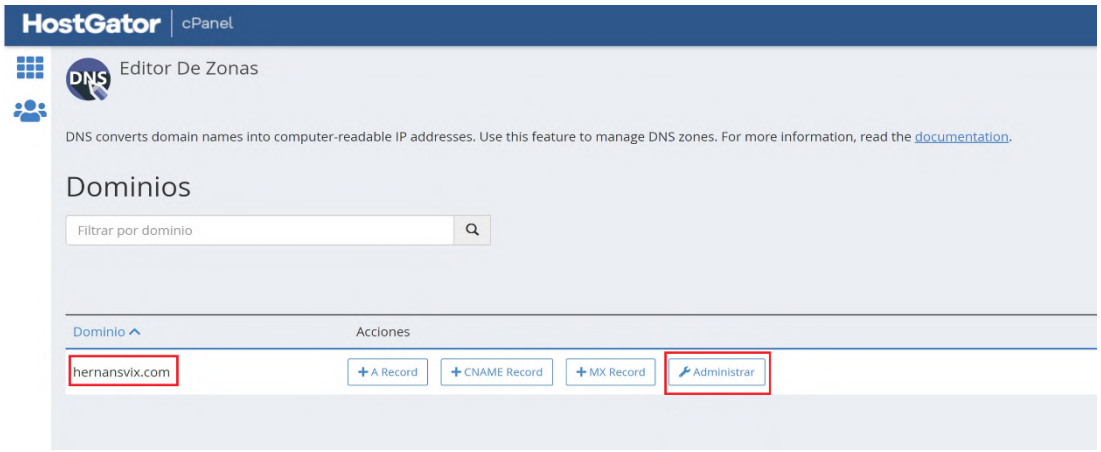
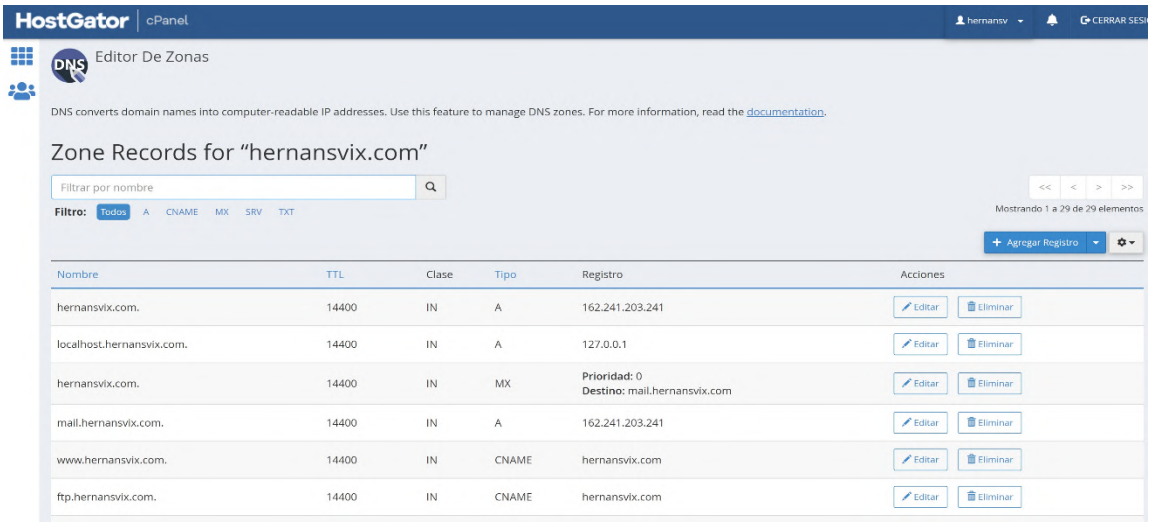


Figura 14

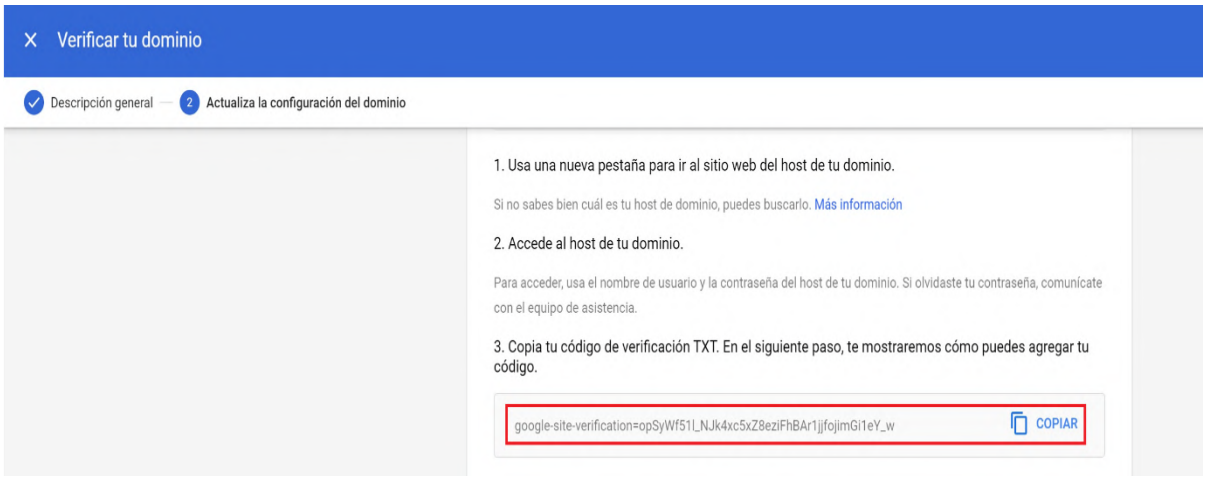
Tabla de registros DNS del Hosting



En la consola de administración de Google se observa una serie de pasos para verificar el dominio basado en el registro TXT. Se debe copiar el código de verificación que se observa en la Figura 15 para agregar a las configuraciones de zona del hosting.

Figura 15

Actualización de configuración del dominio con un registro TXT



En el cPanel seleccionamos la opción de agregar registros, en donde se especifica el tipo de registro, el código de registro y el nombre, para luego crear el nuevo registro el proceso se lo detalla de la figura 16 a la figura 18.

Figura 16

Agregación del registro TXT

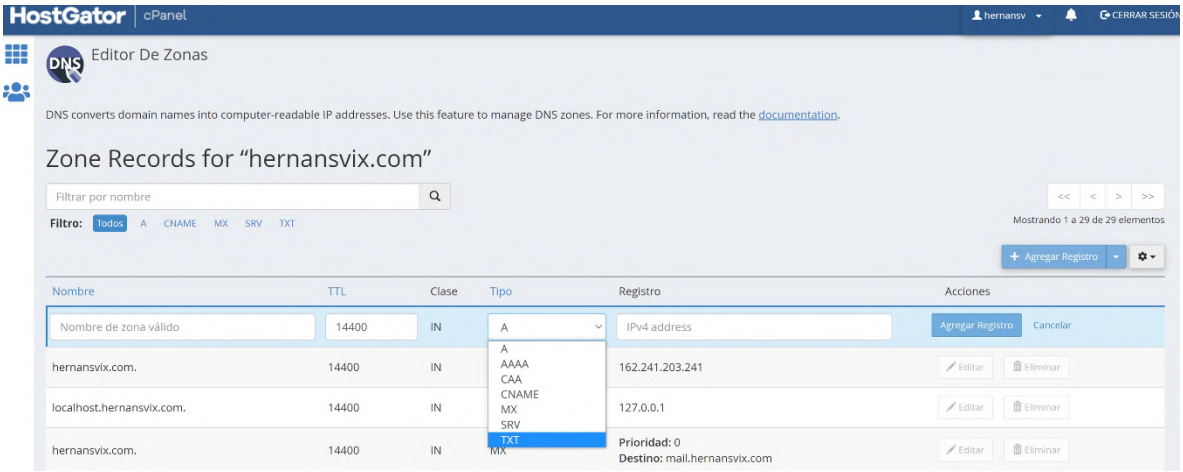


Figura 17

Modificación de los parámetros del registro TXT

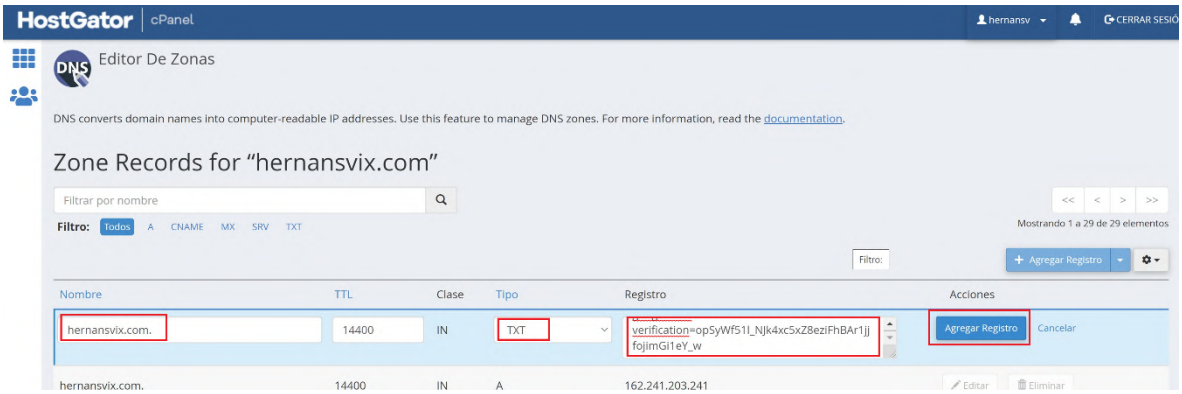
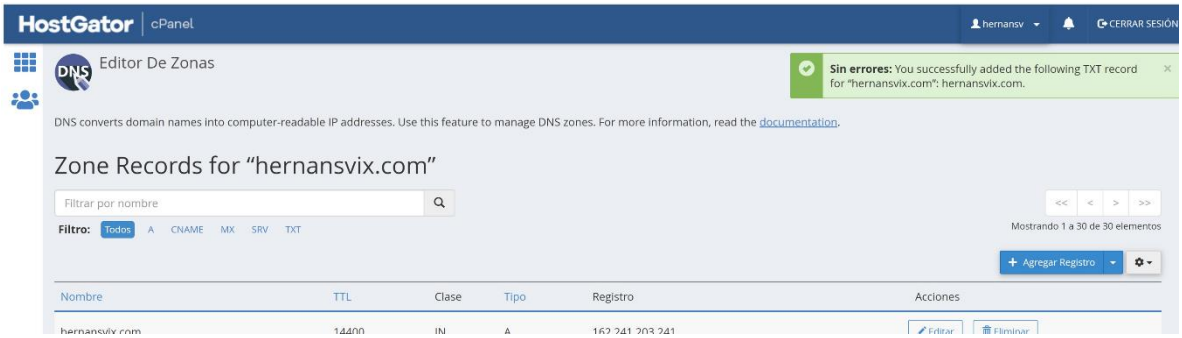


Figura 18

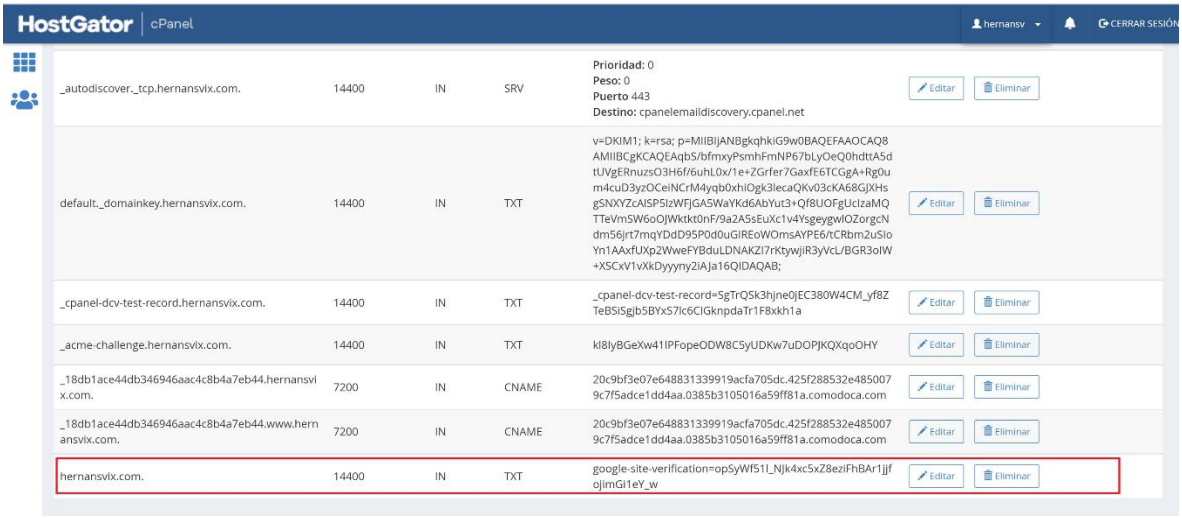
Creación del registro TXT



En la Figura 19 se visualiza el registro en la tabla de registros del Hosting.

Figura 19

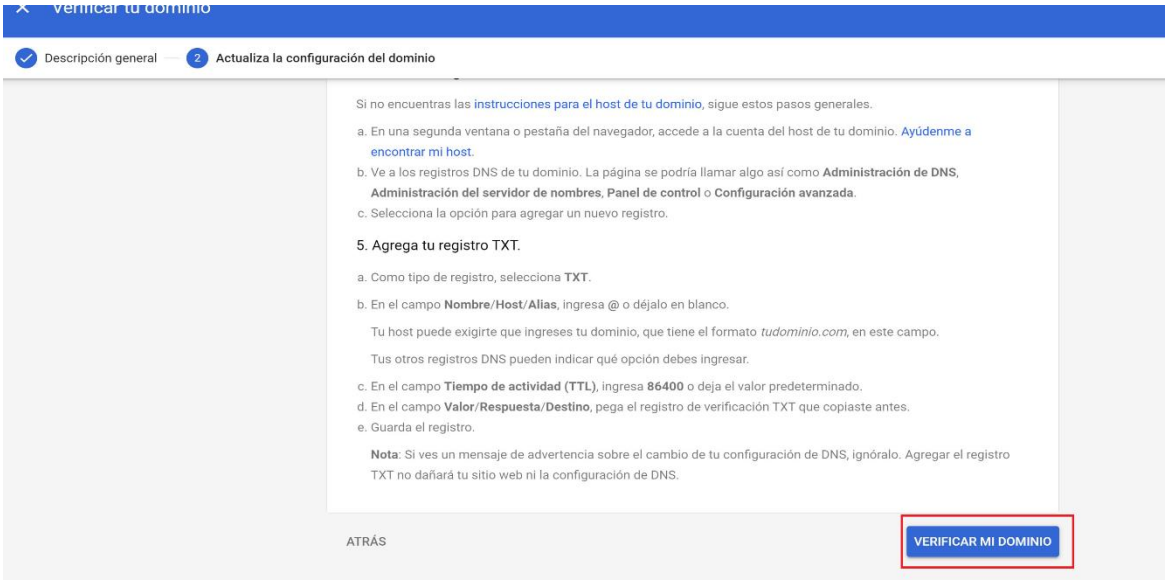
Visualización del registro TXT en la tabla de registros



Después damos clic en verificar dominio en la pestaña de verificación de Google como en la Figura 20, este proceso puede tardar entre 10 a 15 min.

Figura 20

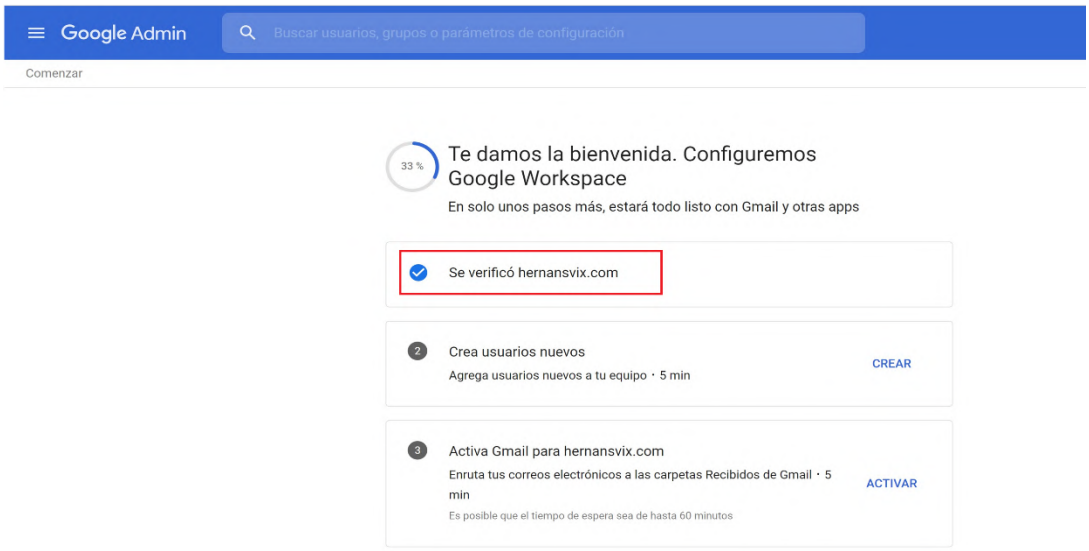
Pestaña de verificación del dominio



Hecho esto el dominio queda totalmente registrado en Google Workspace la cual se la ilustra en la Figura 21.

Figura 21

Pestaña en donde indica la verificación del dominio



2.3. Activar Gmail para hernansvix.com

Una vez que se ha verificado el dominio, se procede a configurar Gmail con Google Workspace para obtener todas las funcionalidades avanzadas de correo electrónico que proporciona Gmail.

En la página de Bienvenida de Google Workspace la cual se muestra en la Figura 22, ubicamos la tercera opción que corresponde a activar Gmail para hernansvix.com, damos clic en activar, luego aceptamos los términos de servicios y continuamos.

Figura 22

Sitio de bienvenida de Google Workspace

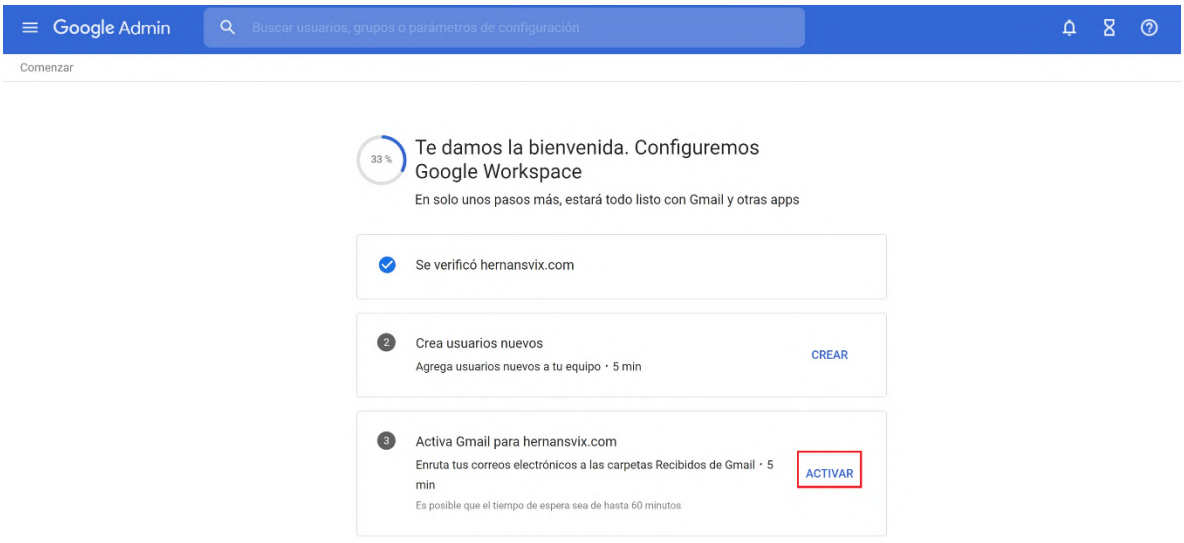
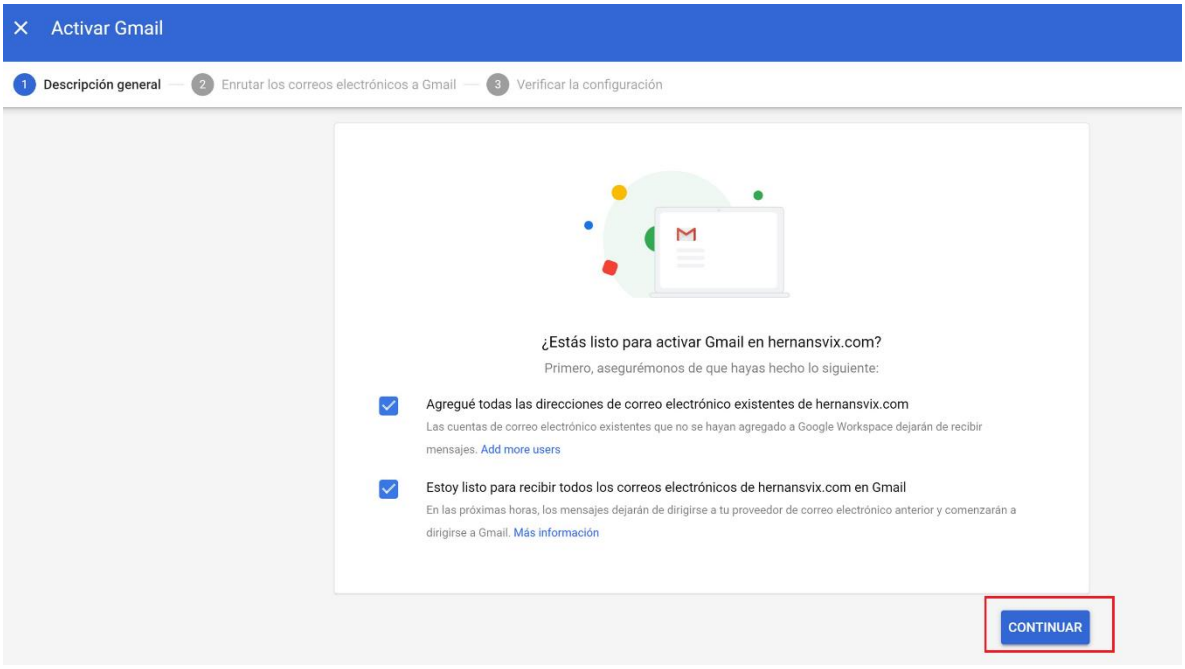


Figura 23

Pestaña que contiene las condiciones para el servicio de Gmail



De igual manera que al agregar el código TXT, se va a agregar los registros MX para utilizar los servidores MTA de Gmail. Según Google Support (2021) las entradas MX de Google son las que se representan en la Tabla 1.

Tabla 1

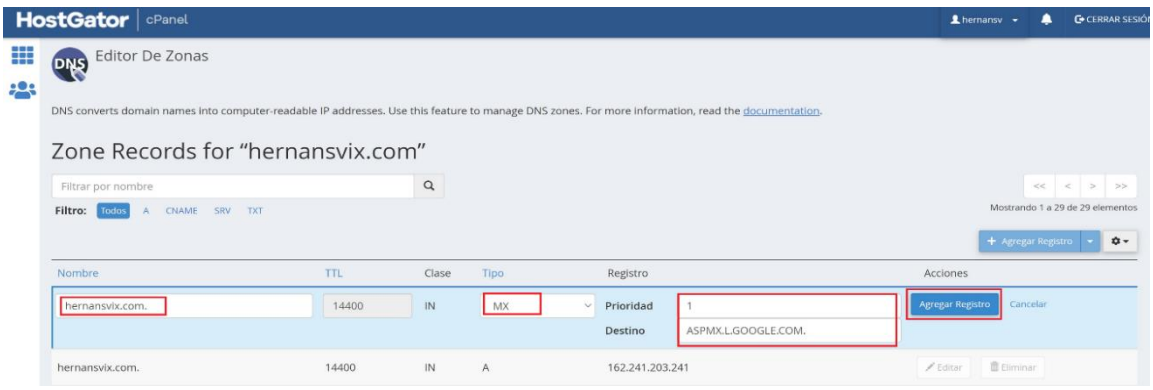
Valores de los registros MX en Google Workspace

Valor/Respuesta/Destino	Prioridad
ASPMX.L.GOOGLE.COM	1
ALT1.ASPMX.L.GOOGLE.COM	5
ALT2.ASPMX.L.GOOGLE.COM	5
ALT3.ASPMX.L.GOOGLE.COM	10
ALT3.ASPMX.L.GOOGLE.COM	10

La Figura 24 indica la agregación del primer registro MX que es ASPMX.L.GOOGLE.COM con prioridad de 1.

Figura 24

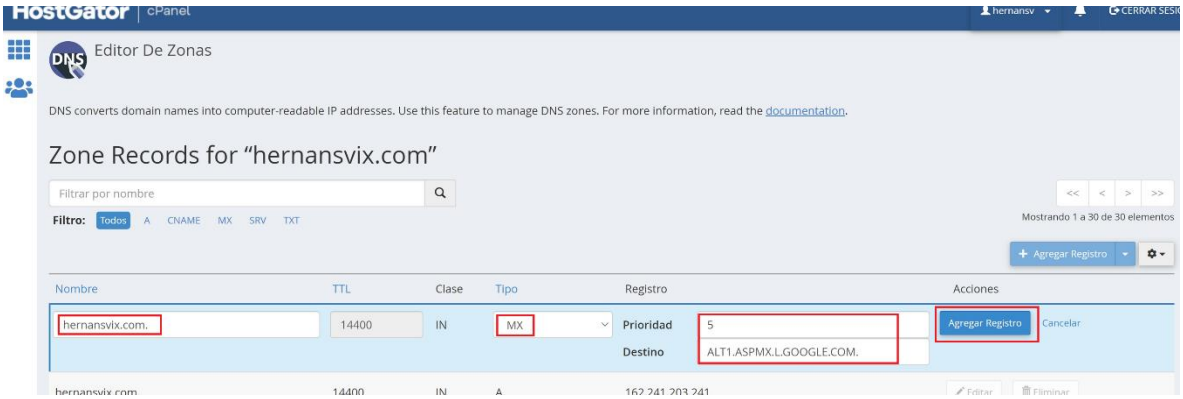
Agregación del primer registro MX



El segundo registro MX que se agrega es ALT1.ASPMX.L.GOOGLE.COM con prioridad de 5 al igual que en la Figura 25

Figura 25

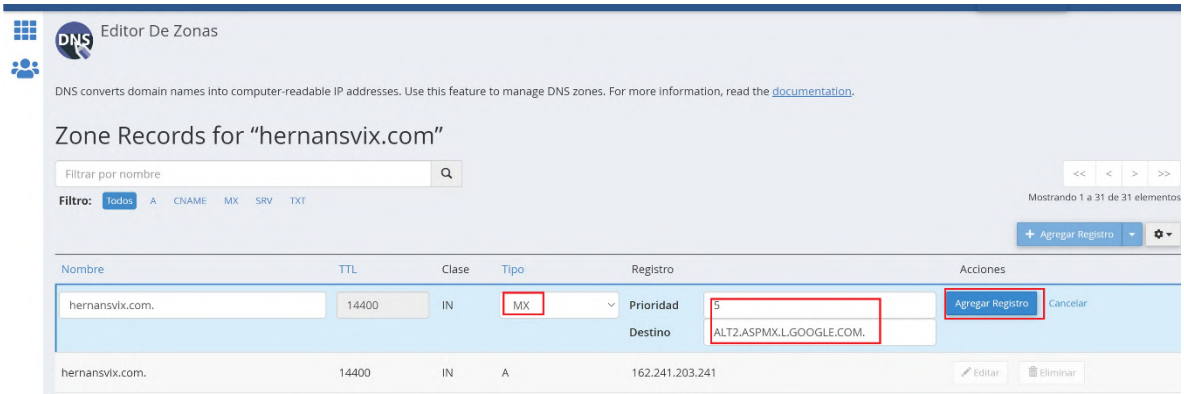
Agregación del segundo registro MX



El siguiente registro MX que se agrega es ALT2.ASPMX.L.GOOGLE.COM con prioridad de 5 al igual que en la Figura 26.

Figura 26

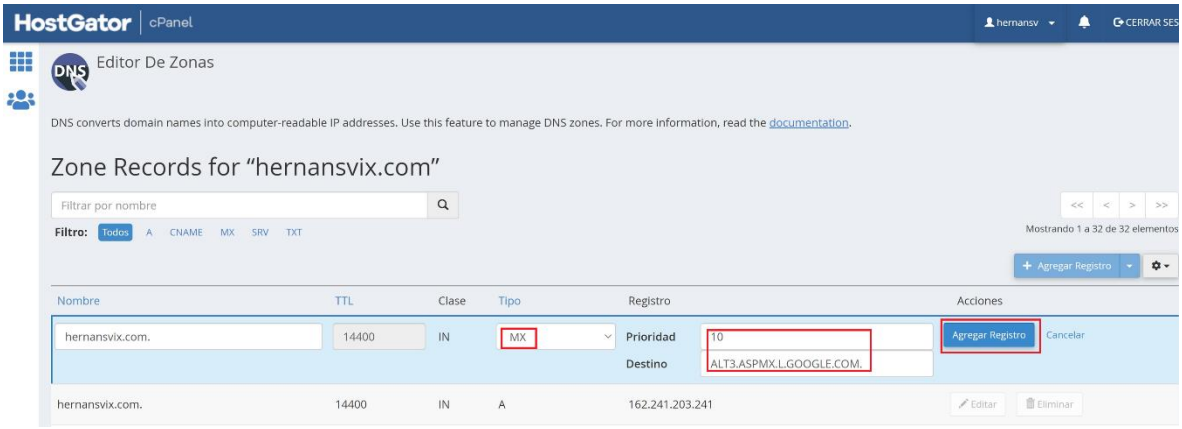
Agregación del tercer registro MX



El siguiente registro MX que se agrega es ALT3.ASPMX.L.GOOGLE.COM con prioridad de 10 tal y como se observa en la Figura 27.

Figura 27

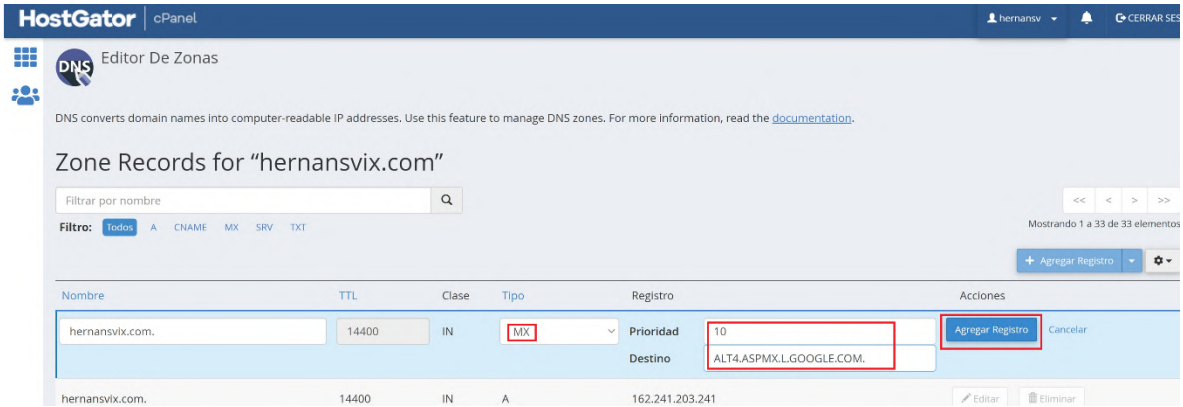
Agregación de cuarto registro



Y el último registro es ALT4.ASPMX.L.GOOGLE.COM con prioridad de 10 la cual se observa en la Figura 28.

Figura 28

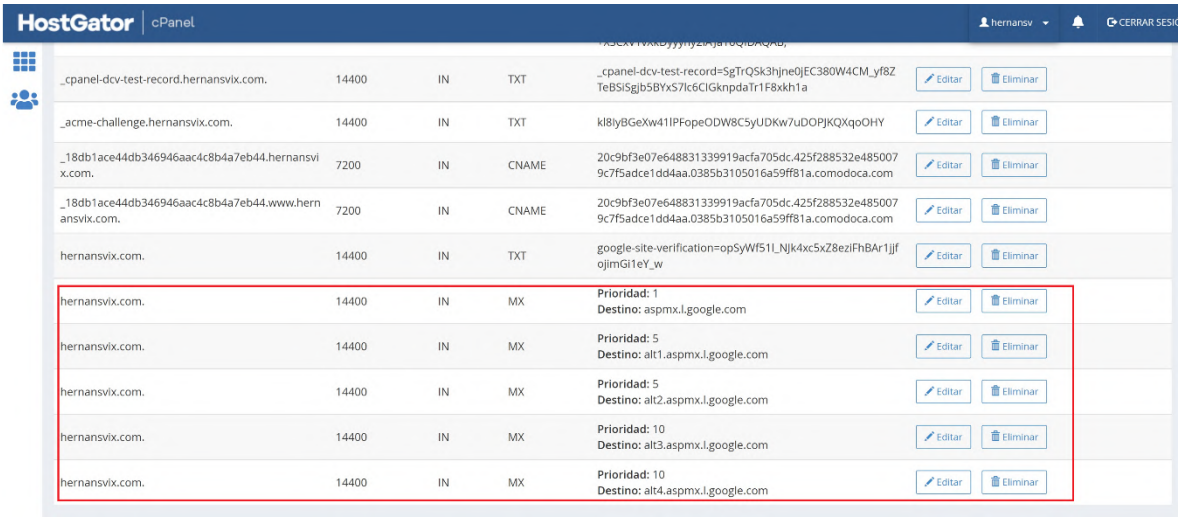
Agregación del último registro MX



Se verifica que todos los registros MX consten en la tabla de registros del dominio como en la Figura 29.

Figura 29

Sitio Web HTTPS seguro



Validamos la configuración de los registros MX en el panel de administración de Google Workspace. En la Figura 30 se muestra la comprobación de los registros añadidos en el cPanel.

Figura 30

Proceso de verificación de los registros MX

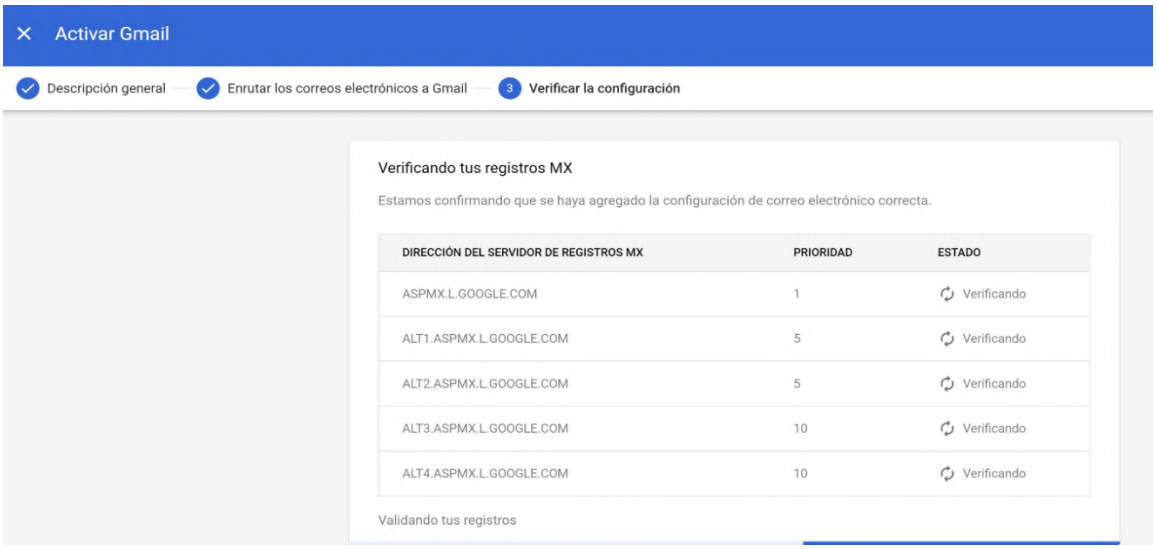
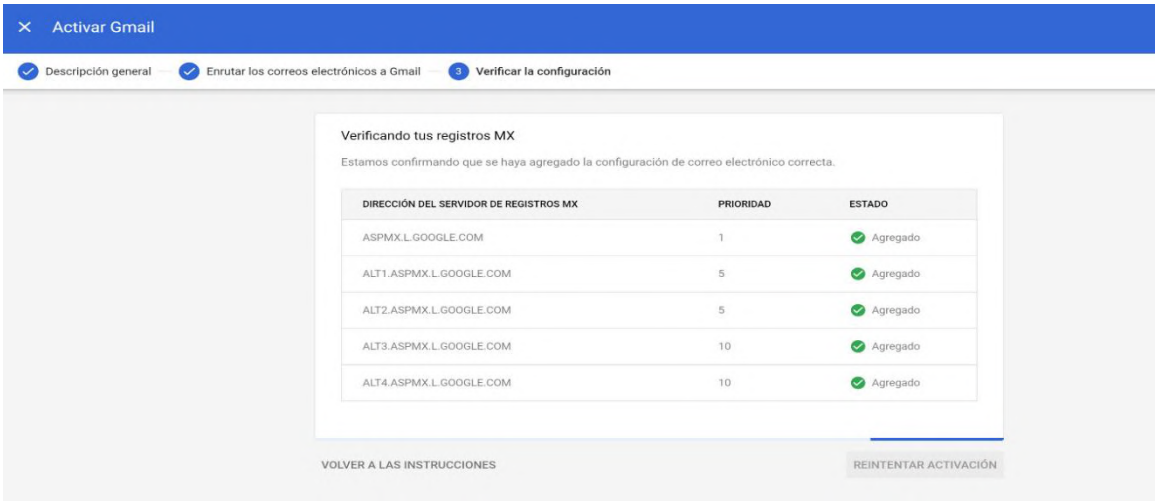


Figura 31

Proceso de verificación de los registros MX exitosos



De esta manera Gmail ya estará activado para el dominio hernansvix.com que se indica en la Figura 32, se debe esperar un periodo de tiempo hasta que los cambios en la zona de DNS

del hosting surtan efecto, luego nos redirige a la pestaña de confirmación de configuración de Google Workspace la misma que se ilustra en la Figura 33.

Figura 32

Pestaña que indica la activación de Gmail para hernansvix.com

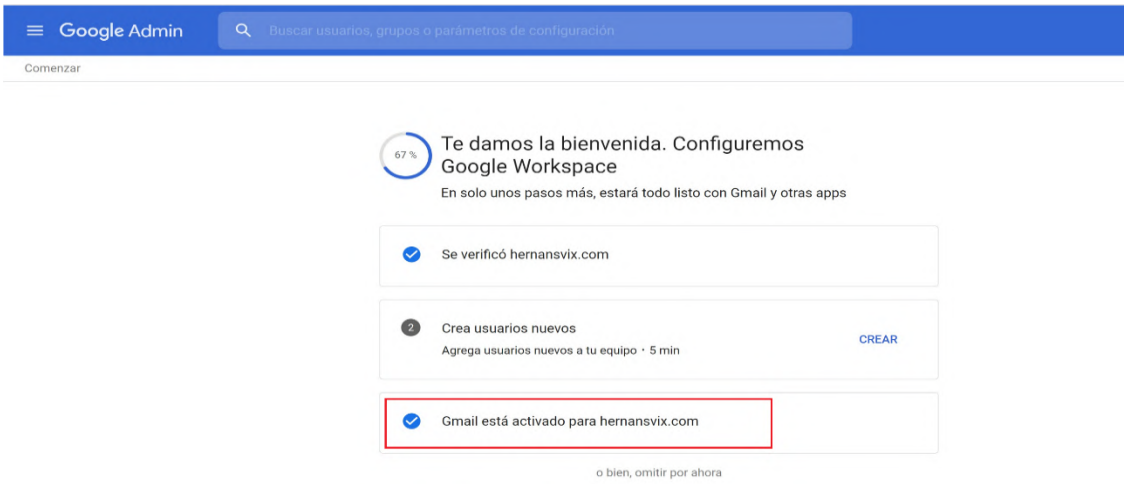
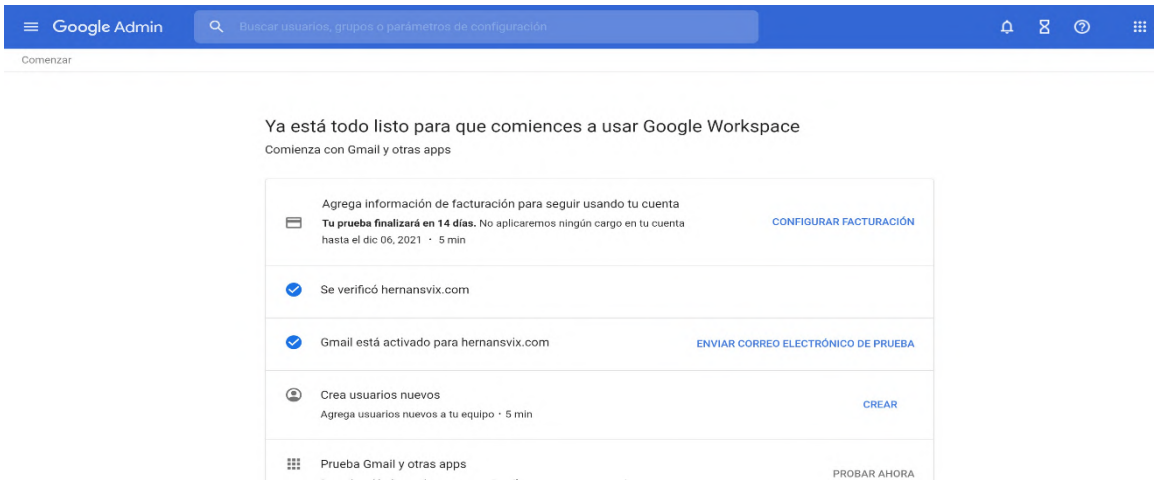


Figura 33

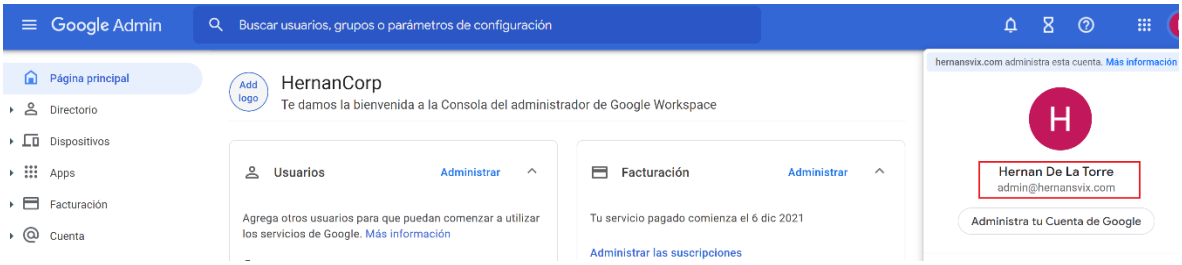
Pestaña de acceso a Google Workspace



Finalmente, procedemos a iniciar sesión en *admin.hernansvix.com* con su respectivo nombre de usuario y contraseña y nos ubicará en la página principal de Google Admin la misma que se observa en la Figura 34.

Figura 34

Página inicial de Google Admin.



Anexo3. Manual Técnico de Implementación de MTA-STS y TLS Reporting

METODOLOGÍA PARA IMPLEMENTAR SEGURIDAD EN SERVICIOS DE CORREO ELECTRÓNICO MEDIANTE EL MECANISMO MTA-STS (MAIL TRANSFER AGENT-STRICT TRANSPORT SECURITY) Y SMTP TLS REPORTING (TLSRPT) PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

Manual de Técnico de Implementación

Versión: 0100

Fecha: 09/12/2021

HOJA DE CONTROL

Proyecto	METODOLOGÍA PARA IMPLEMENTAR SEGURIDAD EN SERVICIOS DE CORREO ELECTRÓNICO MEDIANTE EL MECANISMO MTA-STS (MAIL TRANSFER AGENT-STRICT TRANSPORT SECURITY) Y SMTP TLS REPORTING (TLSRPT) PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS		
Entregable	Manual Técnico		
Autor	Raymi Hernán De La Torre Yamberla		
Versión/Edición	0100	**Fecha Versión**	09/12/2021
Aprobado por	Msc. Fabián Geovanny Cuzme Rodríguez	**Fecha Aprobación**	16/12/2021
Firma Director			

GLOSARIO

Término	Descripción
Hosting	Es un servicio que permite alojar toda la información de un sitio web en un servidor .
Dominio	Dirección única que recibe un sitio web en la internet.
MTA	Agente de Transferencia de Correo
Registro TXT	Es un registro DNS que proporciona información de texto a dominios externos las mismas que se puede utilizar con distintos fines.
Registro MX	Dirigen el correo de un dominio a los servidores de correo entrantes del dominio.
Política MTA-STS	Un compromiso del dominio de políticas para admitir TLS autenticado con PKIX para los hosts MX especificados.
Dominio de Política	El dominio para el que se define una política MTA-STS
Host de Política	El host HTTPS que sirve a la política MTA-STS para un dominio de políticas.
MTA de envío	El MTA de SMTP que envía un mensaje de correo electrónico.

DESCRIPCIÓN DEL SISTEMA

Objetivo

Establecer los pasos necesarios para aumentar la seguridad de los servicios de correo electrónico mediante la aplicación de los estándares MTA-STS y TLS Reporting con la finalidad de brindar la orientación necesaria para su implementación al personal del departamento de TI de una PYME.

Alcance

En el presente documento se especifica cada uno de los pasos para configurar los estándares de seguridad que inicia desde las configuraciones preliminares del dominio/hosting, para luego activar los mecanismos de transporte seguro estricto y reportes TLS mediante el registro y activación del dominio en Google Workspace para finalmente verificar el estado de MTA-STS y TLS Reporting desde la consola de administración de Google Admin.

Funcionalidad

El estándar MTA-STS se activa mediante un registro TXT que especifica que un servidor de correo externo puede extraer un archivo de política de un subdominio definido. Este archivo de política se publica utilizando HTTPS en lugar de DNS ya que HTTPS no es susceptible a ataques MITM como lo es DNS (Mishra, 2017). MTA-STS hace uso de un servidor web HTTPS para alojar el archivo de política y un registro DNS de tipo TXT para indicar su soporte con MTA-STS (Gersch et al., 2017). Un servidor de correo emisor comprobará la existencia del registro DNS de MTA-STS en el dominio que se encuentra en la dirección del remitente. Si se encuentra el registro DNS, el servidor de correo remitente obtendrá el archivo de política MTA-

STS a través de HTTPS del servidor web, si lo hace, el correo electrónico se envía a través de una conexión cifrada.

Requisitos

Requisitos del servidor de correo

Los servidores de correo entrante deben cumplir con los siguientes requisitos:

- Soporte para el comando STARTTLS.
- Utilizar versión TLS 1.2 o superior.
- Contar con certificados no caducados con certificados firmados por autoridades certificadoras.

Requisitos del servidor Web

El servidor Web que contenga la política del estándar MTA-STS debe cumplir los siguientes requisitos:

- Admitir SLL/HTTPS.
- Contener un certificado digital firmado por una autoridad certificadora que lo considere de confianza.

MAPA DEL SISTEMA

Modelo del Sistema

La arquitectura del sistema corresponde a un servidor de correo remitente y destinatario las cuales se comunican entre sí para establecer una un túnel de comunicación cifrada. Para describir el proceso de comunicación entre Agentes de Transferencia de Correo (MTA) que admiten Transporte Seguro Estricto se recurrió a una arquitectura servidor-servidor en donde se identifica el dominio de envió y de recepción con sus respectivos componentes, la cual se ilustra en la Figura 1.

Figura 1

Arquitectura General del Sistema

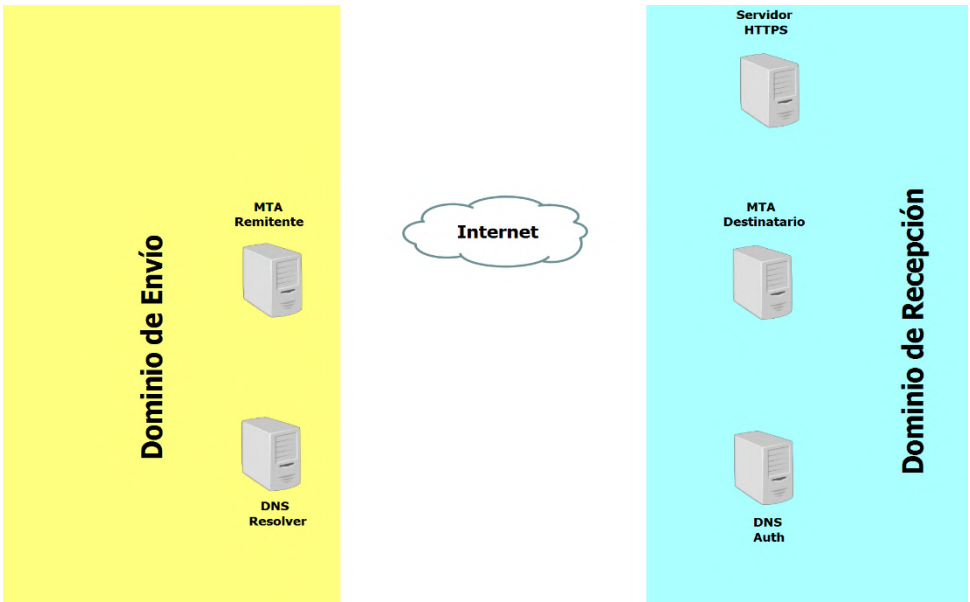
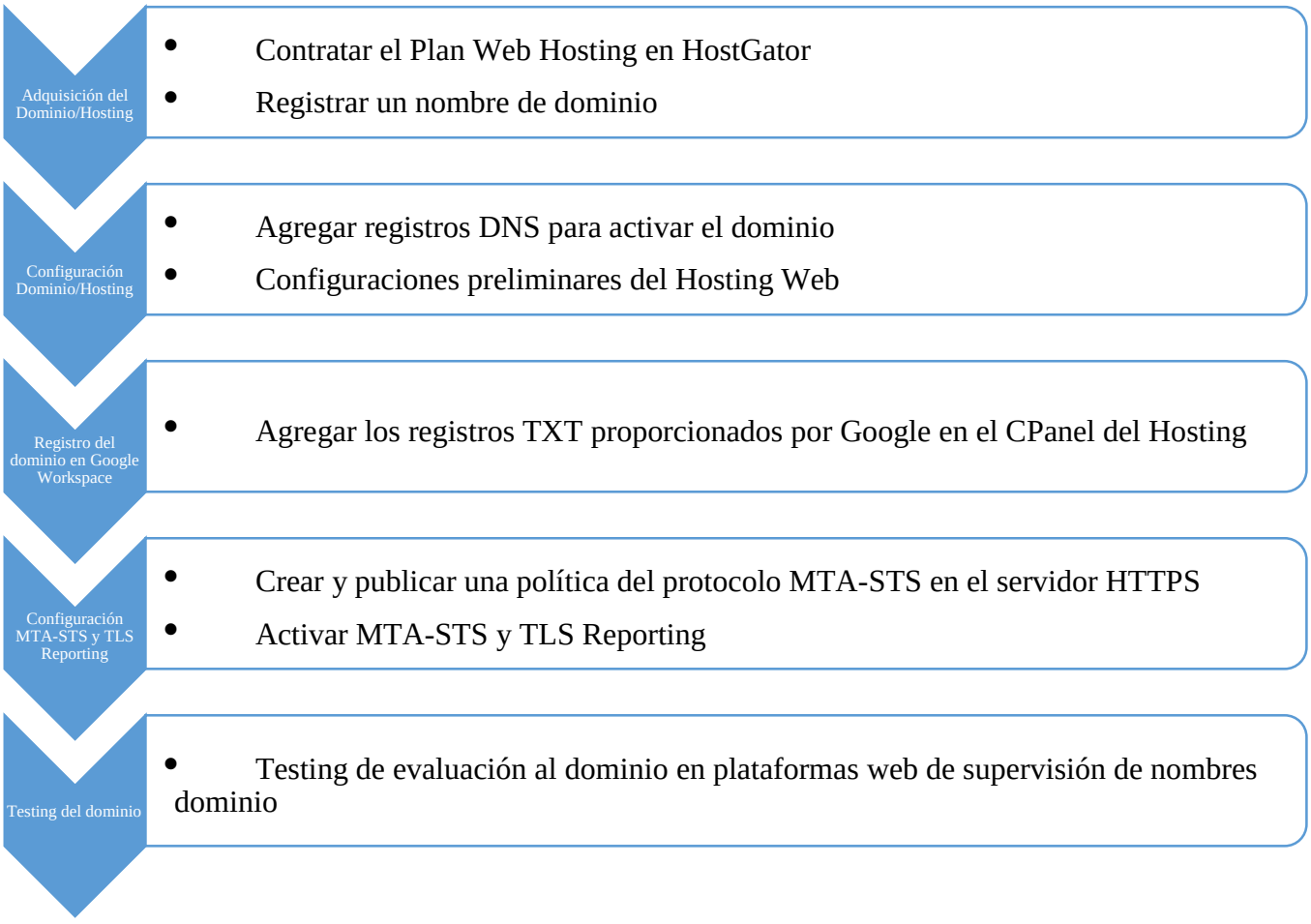


Diagrama de Implementación

En este apartado se hará una descripción de la implementación de MTA-STS y TLS Reporting mediante diagramas en formato libre con un enfoque top-Down la cual se la ilustra en la Figura 2.

Figura 2

Diagrama del proceso de implementación del estándar MTA-STS y TLS Reporting



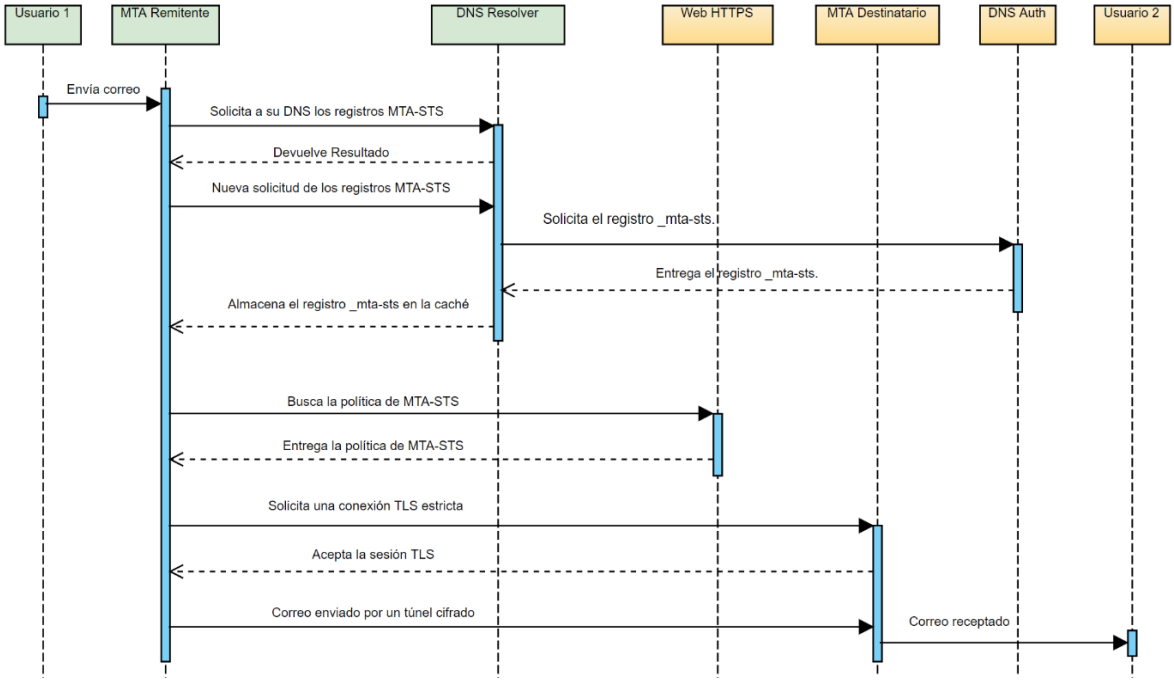
Diagramas de Interacción

En este punto se describirá la interacción del usuario-sistema por medio de un diagrama de secuencias, en donde se han de representar los procesos más significativos de MTA-STS y TLS Reporting.

Si un MT envía un mensaje de correo a example@dominio.com el MTA realiza una consulta a su DNS para verificar a qué MTA debe enviarse el correo. La solicitud DNS se envía con la finalidad de verificar los registros TXT y el archivo de política, la misma que se aloja en un servidor web seguro. A continuación, el MTA remitente entabla una comunicación con el MTA destinatario en base al resultado de las consultas de los registros DNS, preguntando si el servidor receptor acepta el cifrado TLS. Si lo hace, el correo se envía por medio de un túnel cifrado; sin embargo, si no lo hace, el MTA emisor no entabla la conexión segura TLS y el mensaje se envía en texto plano. En la Figura 3 se representa el proceso de comunicación entre MTA´s con MTA-STS en un diagrama de secuencias.

Figura 3

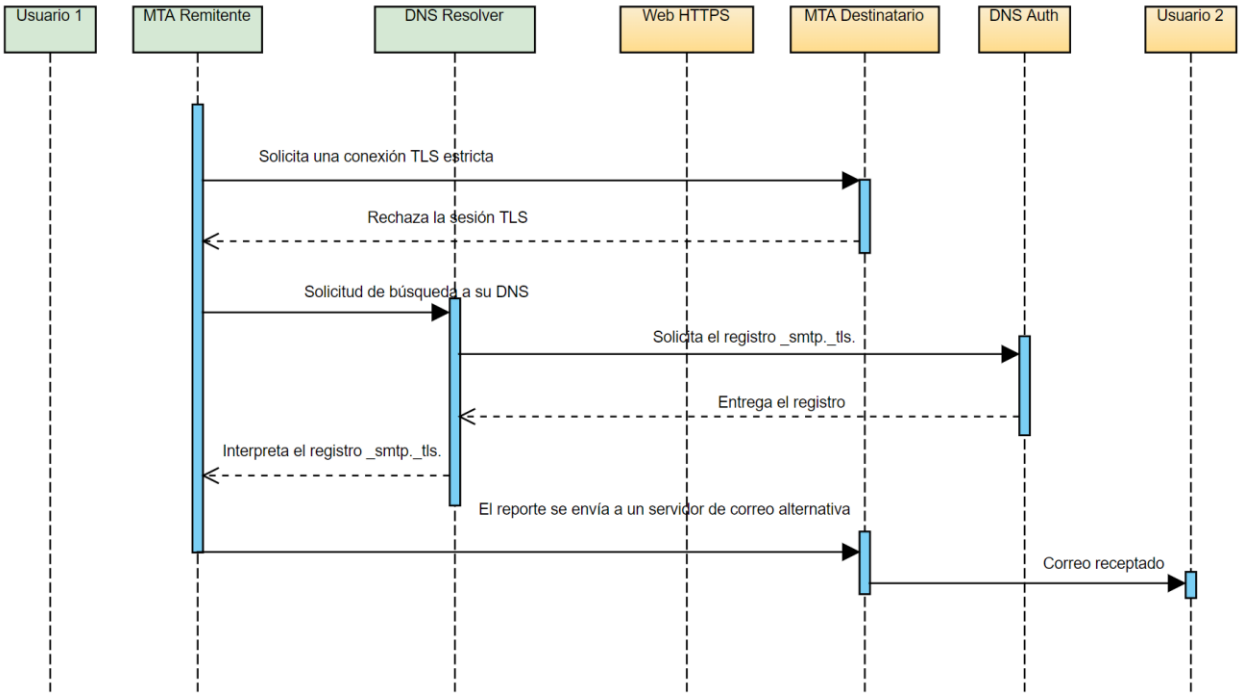
Diagrama del proceso de implementación del estándar MTA-STS y TLS Reporting.



Antes de enviar un correo electrónico a un dominio, un MTA que admita TLS Reporting verificará la existencia de un registro DNS del tipo TXT. Si lo encuentra, el MTA notificará periódicamente los detalles sobre el éxito o el fracaso de la entrega de correo electrónico al dominio a través de una conexión segura. Los informes se envían a la dirección especificada en el registro DNS. En la Figura 4 se representa el proceso de entrega de un reporte cuando la conexión falla.

Figura 4

Esquema de funcionamiento del sistema con TLS Reporting



DESARROLLO DEL MANUAL TÉCNICO

En esta sección se describirá todos los pasos para implementar los protocolos MTA-STS y TLS Reporting, cuya implementación sé que basa en el diagrama Top-Down descrito en la Figura 2.

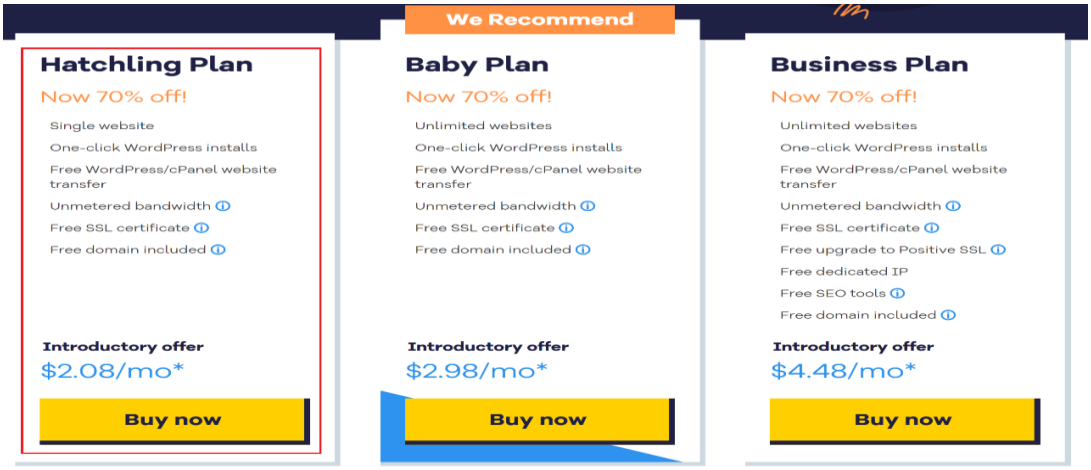
Adquisición Dominio/Hosting

Contratación del Hosting

Contratar el hosting es un proceso de suma importancia para el funcionamiento del sitio web, el mismo que debe estar asociado a un nombre de dominio. Por este motivo lo primero es la adquisición del hosting y posterior registro de un dominio. Se eligió el plan básico de HostGator ya que cumple correctamente con los requerimientos de funcionalidad para el sitio web, la contratación del servicio se lo hace directamente en la página web de HostGator ingresando a las opciones de “Web Hosting”, en los planes que se observa en la Figura 5 se selecciona el plan más económico denominado “Hatching Plan”.

Figura 5

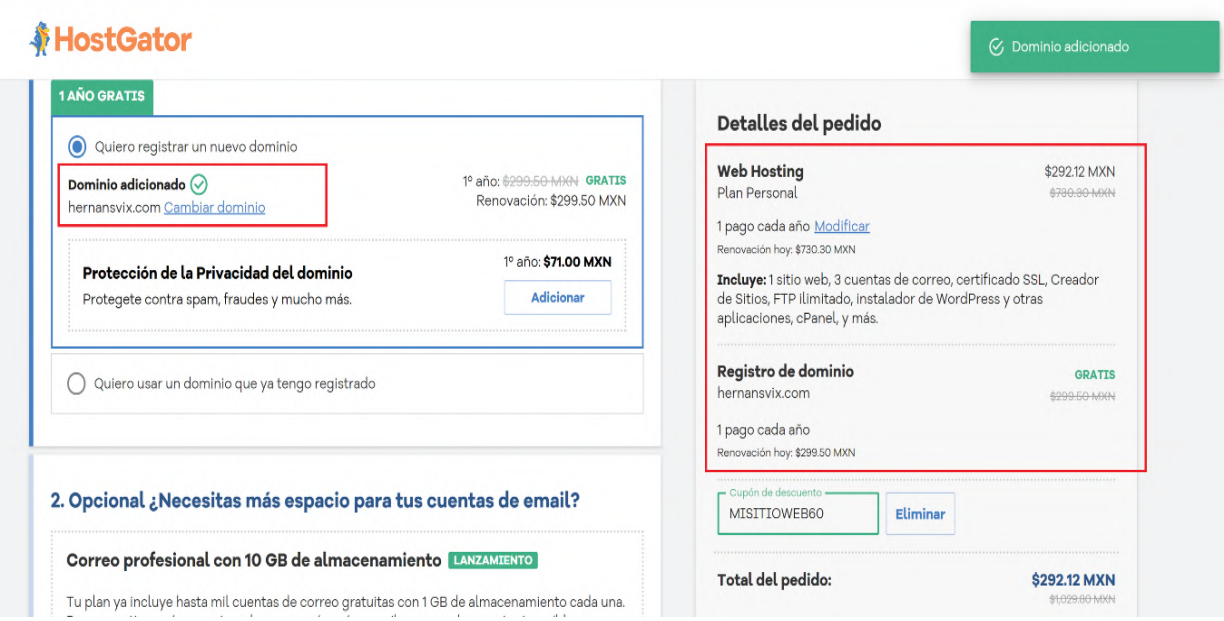
Planes de Hosting Disponibles en HostGator.com



En la siguiente pestaña se procede al registro del dominio tal cual se la observa en la Figura 6, en este caso se ha registrado hernansvix.com de tal manera que el sitio web en la internet se identifique con éste dominio creado.

Figura 6

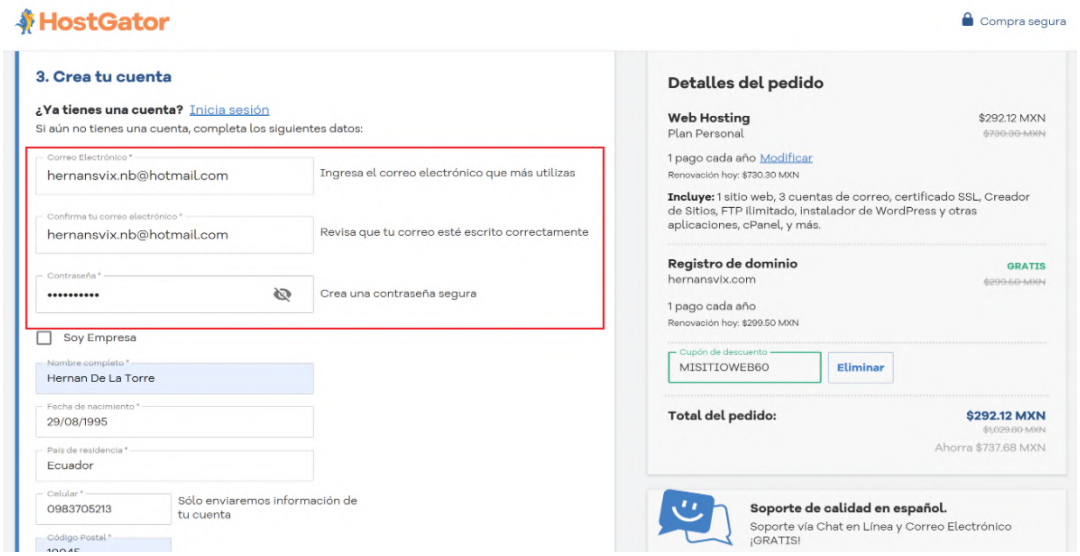
Pestaña para el registro de un nuevo dominio



Luego se validará un nombre de usuario y contraseña para ingresar al Portal Cliente del Hosting. Para lo cual se debe completar un formulario igual al de la Figura 7 con ciertos datos.

Figura 7

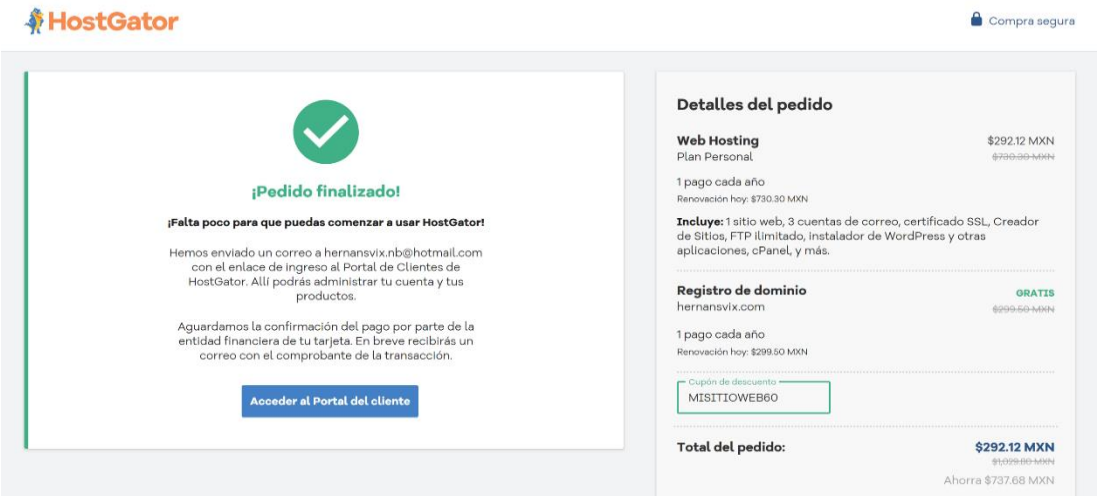
Pestaña para crear la cuenta de HostGator



Para finalizar la compra se acepta los términos y condiciones del servicio y habrá finalizado el proceso de compra, cuya pestaña se verá tal como en la Figura 8.

Figura 8

Pestaña finalización de la compra del Hosting



Configuración Dominio/Hosting Web

Configuraciones Generales del dominio

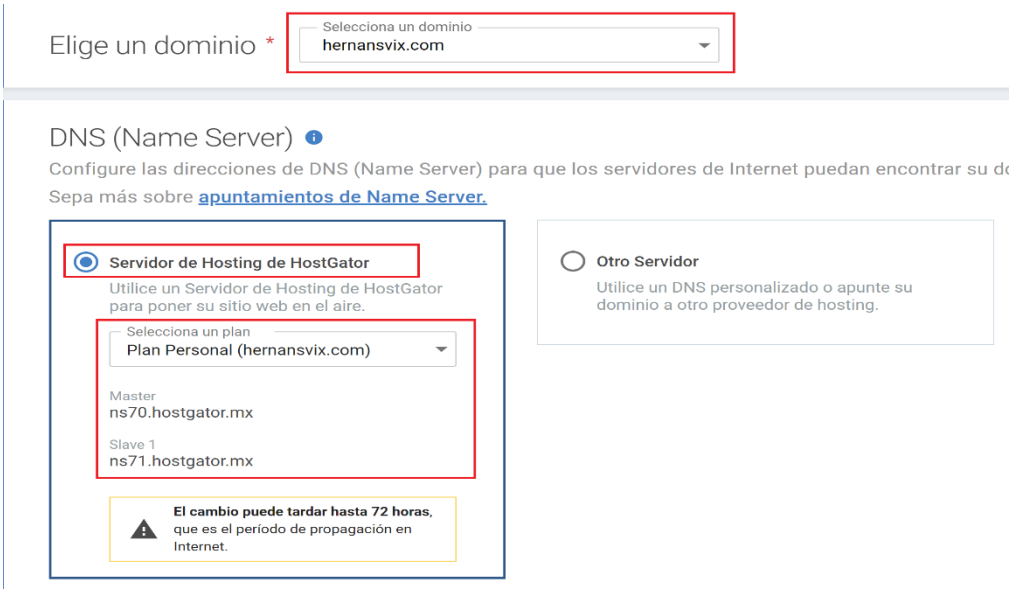
Es importante configurar las direcciones DNS (Name Server) para que los servidores de la internet puedan localizar el dominio en la red mundial. Por lo que se debe validar los registros del tipo NS correspondientes al plan contratado. Para realizar este proceso ingresamos al cPanel con las respectivas credenciales como se detalla en la Figura 9, en la opción de dominios seleccionamos el plan y automáticamente saldrán los registros correspondientes la cual se visualiza en la Figura 10, basta con hacer clic la opción de Servidor de Hosting de HostGator, y a automáticamente se valida los dos registros correspondientes.

Figura 9

Página principal cPanel

Figura 10

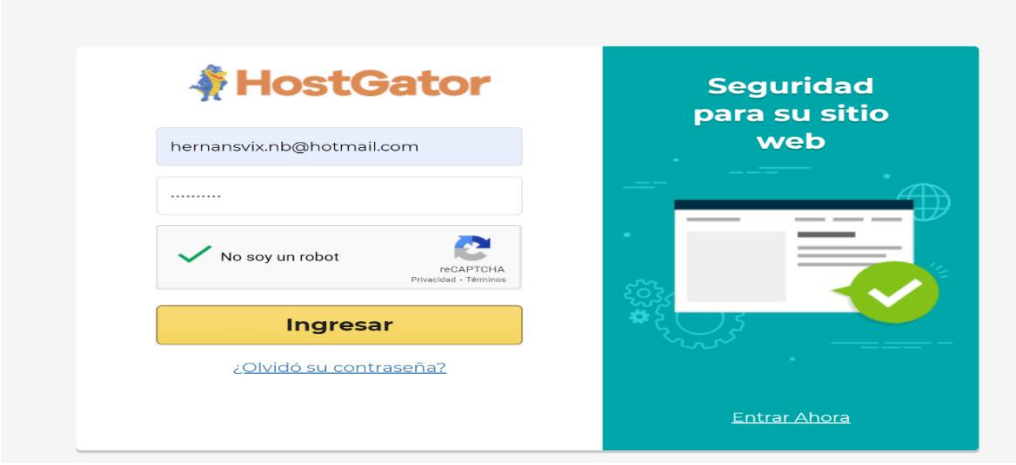
Opción de dominios para validar los registros del tipo NS



Para determinar si el dominio está registrado en la internet se ingresa al Portal Cliente con la cuenta de registro de HostGator tal como se indica en la Figura 11.

Figura 11

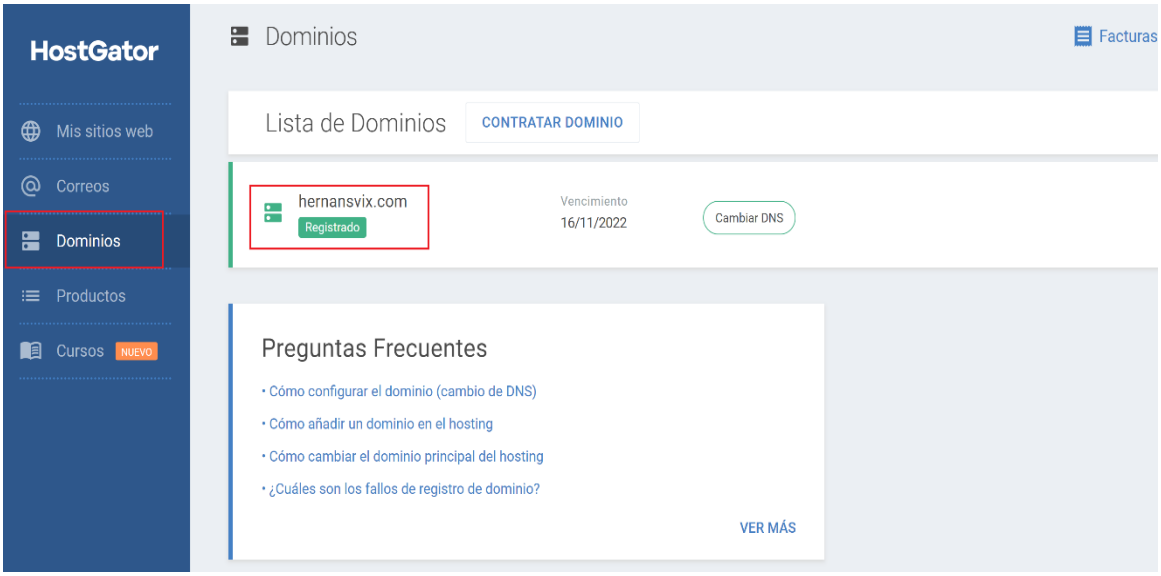
Login en el Portal Cliente de HostGator



Dentro de la página principal, se localiza la opción de dominios, y dentro de esa opción se observa que el dominio de *hernansvix.com* está registrado en la internet, tal y como refleja la Figura 12.

Figura 12

Pestaña Verificación Dominio



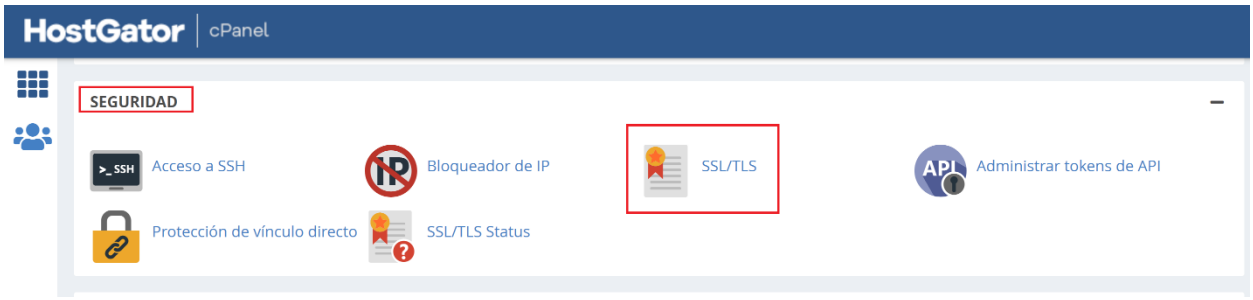
Configuraciones Generales del Hosting Web

Antes de configurar el sitio web se debe reforzar su seguridad mediante el certificado de seguridad SSL. El certificado SSL va a cumplir la función de autenticar la identidad del sitio y garantizar a los visitantes que se encuentran en una página legítima. El plan de hosting contratado incluye un certificado SSL gratuito para todos los dominios y subdominios. Para la instalación se requieren acciones ya que está no se instala automáticamente.

Para configurar el certificado de seguridad SSL primero iniciamos sesión en el cPanel, para ubicarnos en la configuración SSL/TLS de las opciones de Seguridad la cual se la ilustra en la Figura 13.

Figura 13

Opciones de Seguridad en el cPanel



En la Figura 14 muestra ventana de Solicitar nuevo certificado SSL dentro de las opciones de seguridad, registramos los datos de la empresa relacionada al dominio adquirido para enviar la solicitud de petición del certificado una vez que la solicitud ha sido procesada el certificado de seguridad se encontrara en estado activo cuyo proceso se observa de la Figura 15 a Figura 16.

Figura 14

Pestaña Verificación Dominio

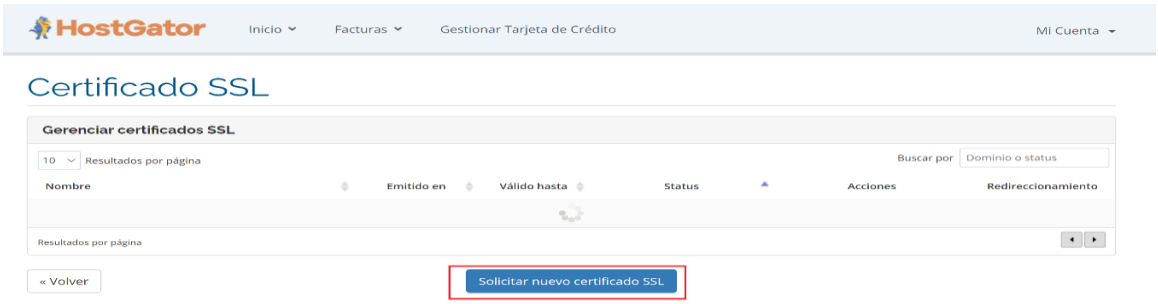


Figura 15

Datos para solicitar el certificado SSL

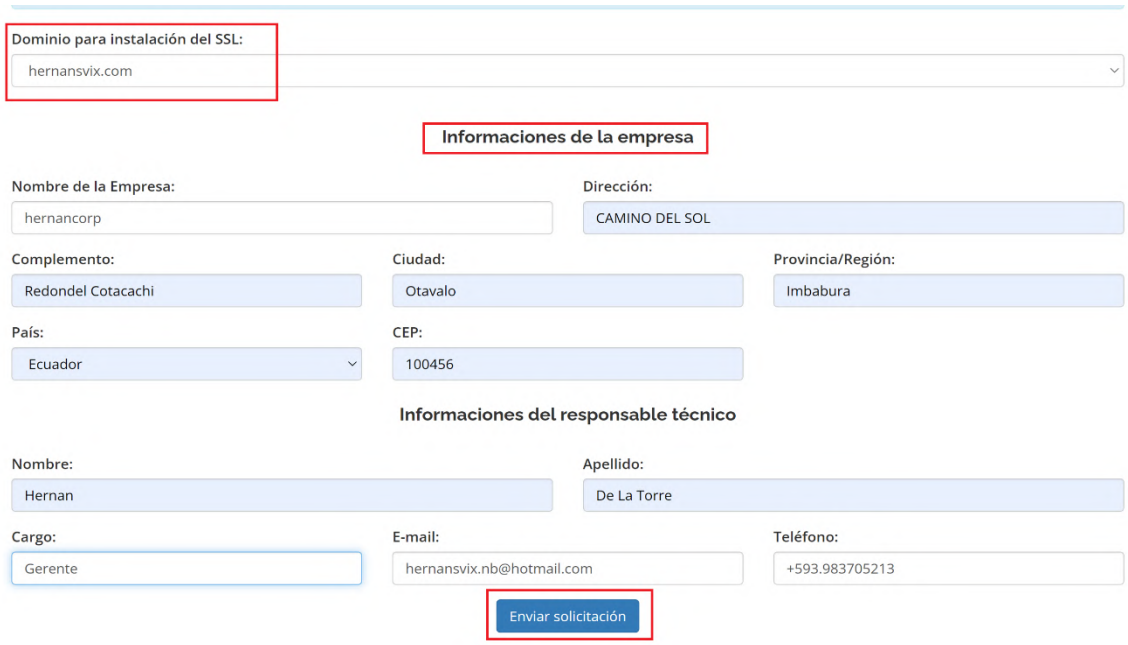
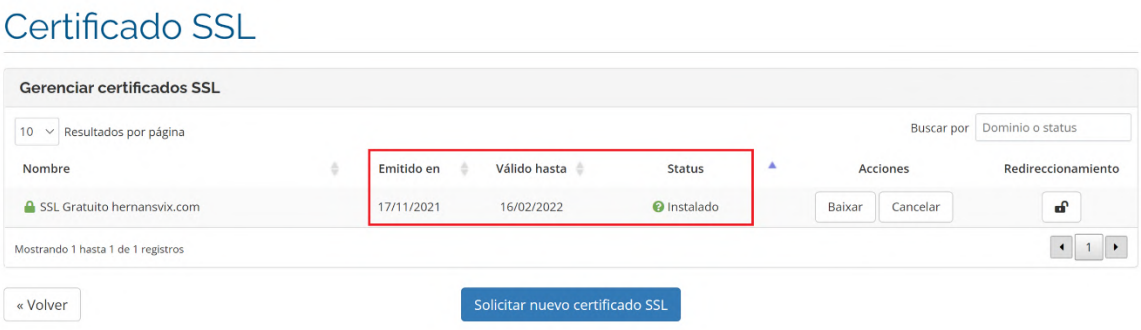


Figura 16

Certificado SSL instalado



Después de la instalación del certificado SSL en el dominio es necesario configurar un redireccionamiento por medio del protocolo seguro. En caso contrario, la web funciona con HTTP y HTTPS a la vez, lo cual es riesgoso para los datos alojados en la internet. Por esta razón es necesario redireccionar el sitio a HTTPS de manera permanente.

Para hacer la redirección HTTPS ingresamos al cPanel como se visualiza en la Figura 17, buscamos la opción de Administrador de Archivos.

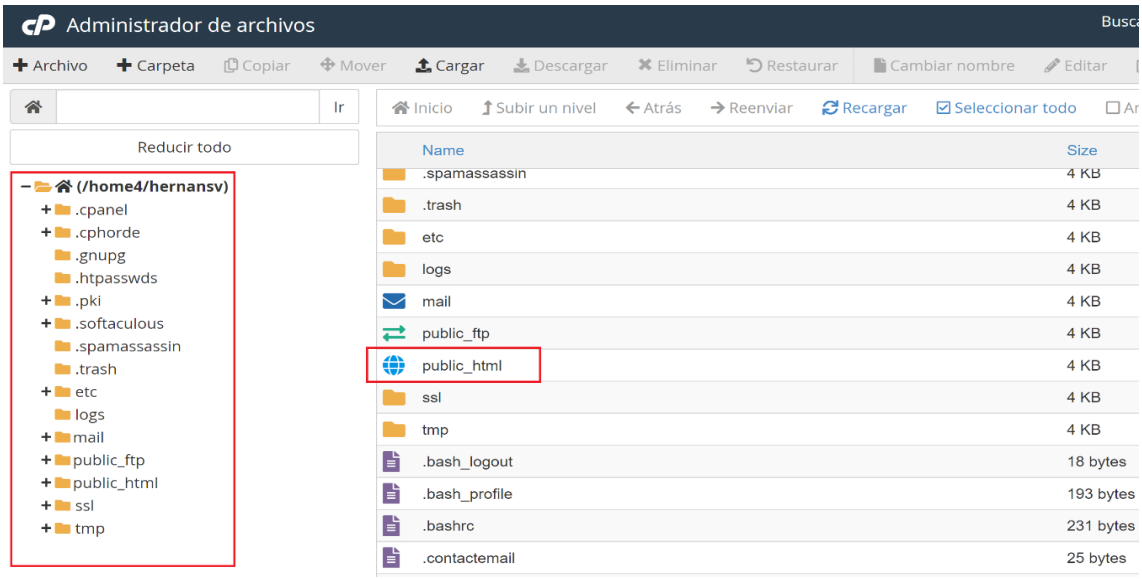
Figura 17

Pestaña cPanel de HostGator

Enseguida se despliega un panel que contiene todos los archivos almacenados en directorio raíz como se indica en la Figura 18, lo que interesa es buscar los archivos que alojan los sitios web, para esto se busca la carpeta public_html.

Figura 18

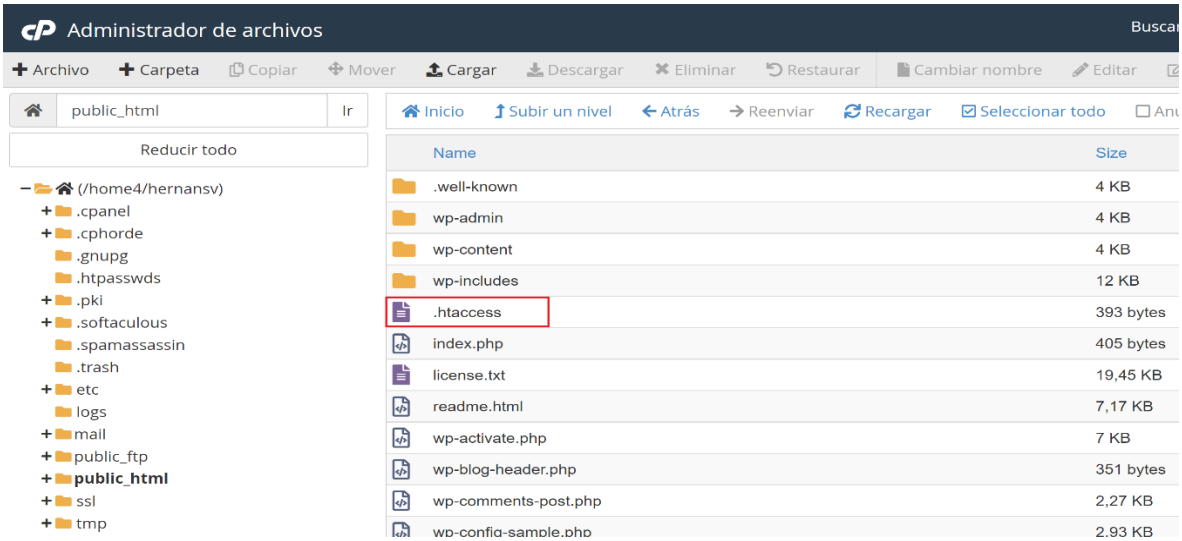
Directorio raíz home4/hernansv



Dentro de la carpeta public_html que se identifica en la Figura 19, ubicamos el archivo TXT genérico denominado .htaccess.

Figura 19

Archivo .htaccess



Dentro del archivo .htaccess se añade la siguiente sentencia de código:

RewriteEngine On

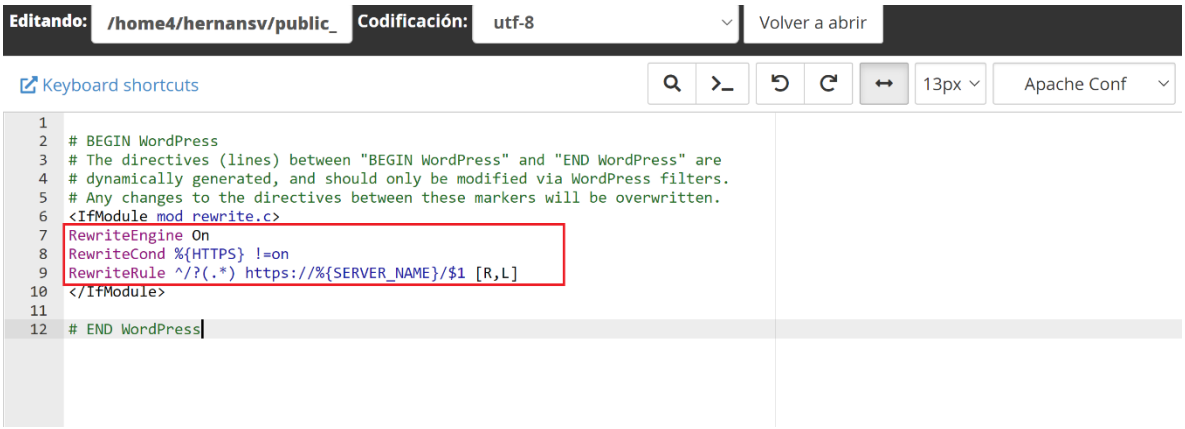
RewriteCond %{HTTPS}! =on

*RewriteRule ^/? (. *) https://%{SERVER_NAME} /$1 [R, L]*

Estas líneas de código indican una redirección automática en estado ON para los sitios del dominio mediante el protocolo HTTPS, esta configuración se visualiza en la Figura 20.

Figura 20

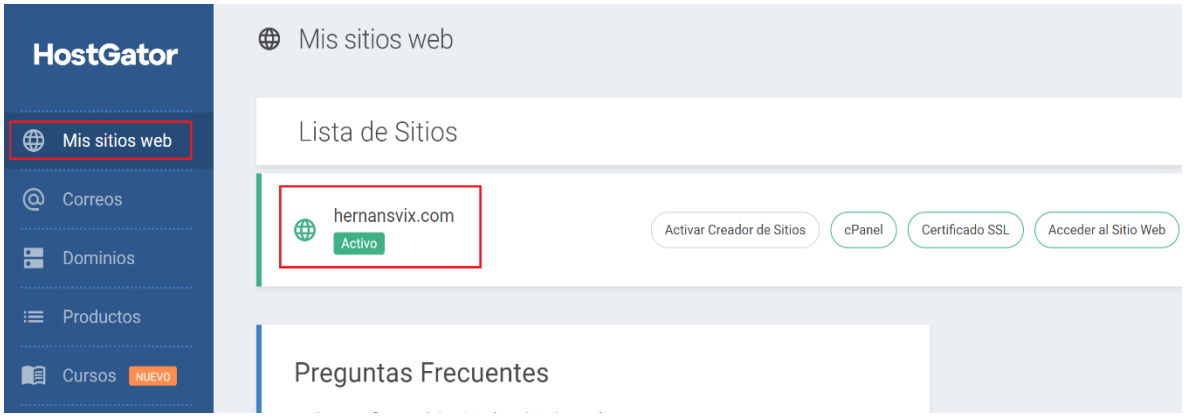
Visualización del código HTML ON



En base a estas configuraciones se determinar el funcionamiento del sitio en la internet, para verificar si el sitio web está activo se inicia sesión en Portal Cliente y luego, dentro de la página principal en la opción de mis sitios web se determina que el sitio web de *hernansvix.com* está totalmente activo tal y como se plasma en la Figura 21.

Figura 21

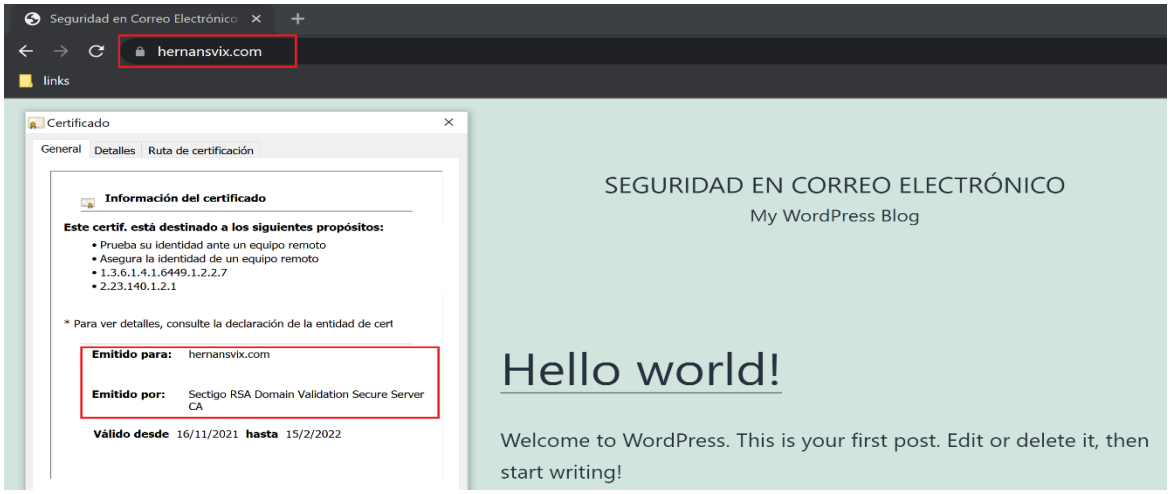
Pestaña que indica que el sitio hernansvix.com está activo



Con estos ajustes al hosting web se procede a verificar si el sitio está activo en la web, en este caso se verificar la seguridad del sitio en base a su certificado digital. En la Figura 22 se observa la página web del dominio *hernansvix.com*, así mismo el certificado digital emitido por Sectigo.

Figura 22

Testing del sitio hernansvix.com en el navegador



Registro del Dominio en Google Workspace

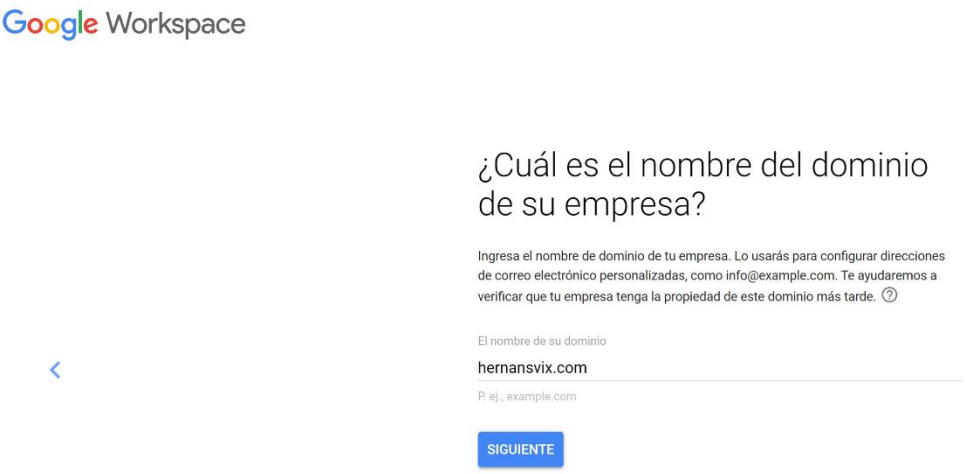
Verificación del Dominio

Después de que el dominio está registrado y el sitio web activo se procede a sincronizar el dominio *hernansvix.com* con los servicios avanzados de Google Workspace para adquirir las funcionalidades de seguridad avanzada de Gmail. Para empezar lo primero que se debe realizar es crear una cuenta de administrador en base al dominio hernansvix.com. Para registrar y validar la cuenta de Google en función al dominio adquirido en HostGator primero ingresamos al enlace https://workspace.google.com/intl/es-419_ar/.

A continuación, ingresamos el dominio para configurar una cuenta de Google. En la pestaña visualizada en la Figura 23 se ingresa el nombre de *hernansvix.com* para que Google Mail identifique el mis

Figura 23

Pestaña registro del dominio



La Figura 24 indica cómo se configura las credenciales de acceso para la cuenta principal de administrador, aceptamos los términos de servicio y damos clic en Aceptar y Continuar. Después de validar las credenciales de acceso la cuenta ya estará creada como muestra la Figura 25.

Figura 24

Pestaña registro del dominio

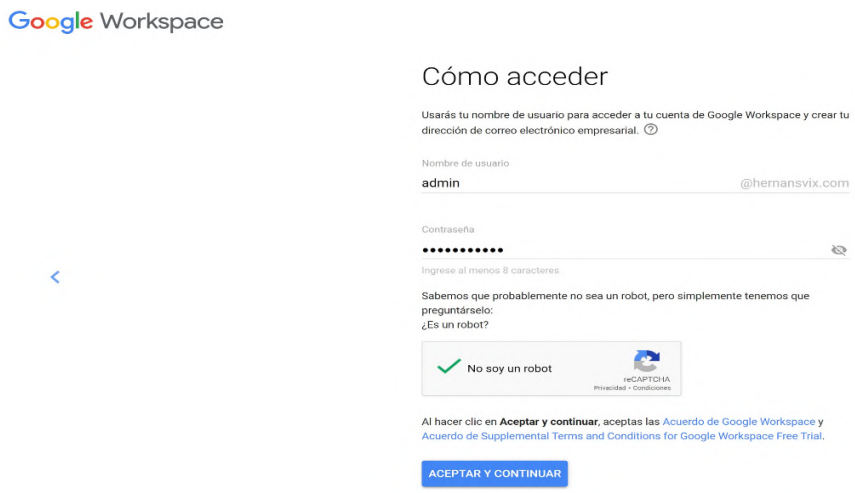
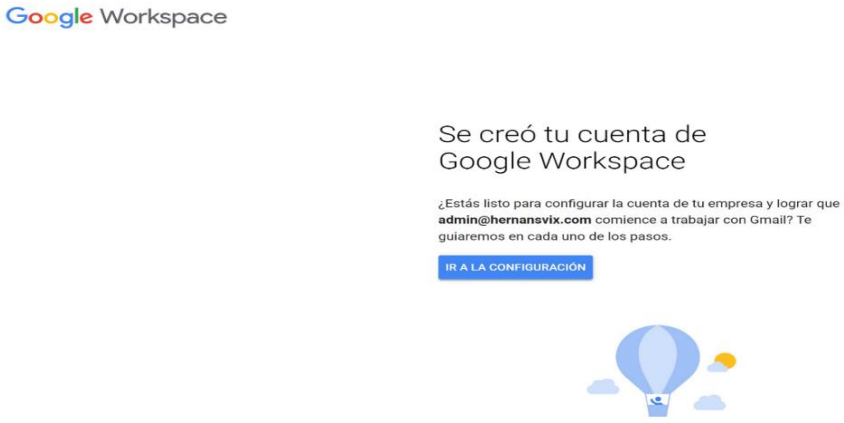


Figura 25

Pestaña registro del dominio

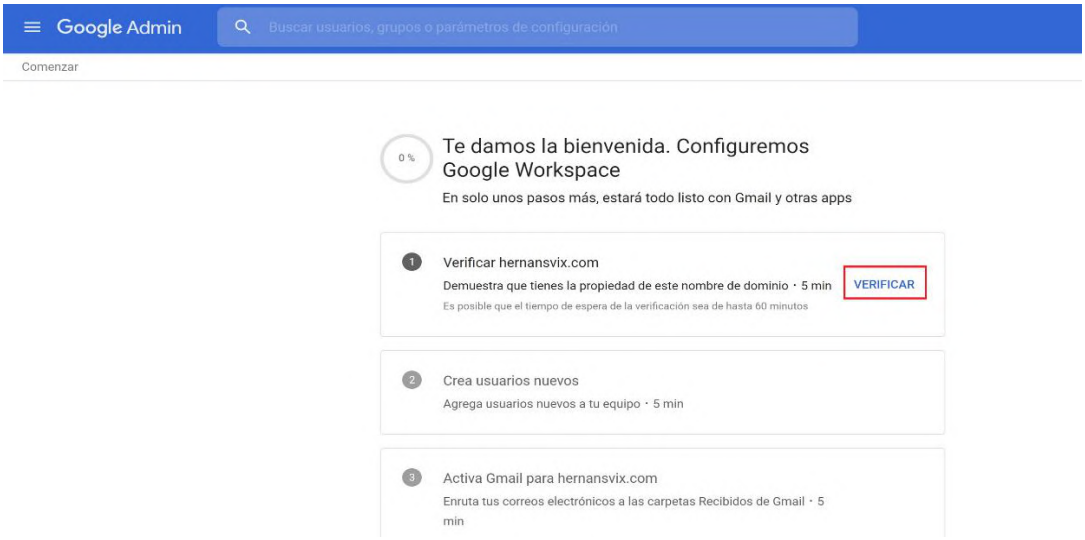


Finalizada la creación de cuanta ya se tendrá acceso a la consola de administración en donde se procederá a registrar y validar el dominio *hernansvix.com* en los servicios de Google. En la página preliminar de Google Admin se inicia a verificar el dominio en Google.

Una vez dentro de las opciones se despliega tres pasos necesarios para validar el dominio como se observa en la Figura 26, en primera instancia se va a validar el dominio para eso seleccionamos la primera opción de verificar *hernansvix.com*.

Figura 26

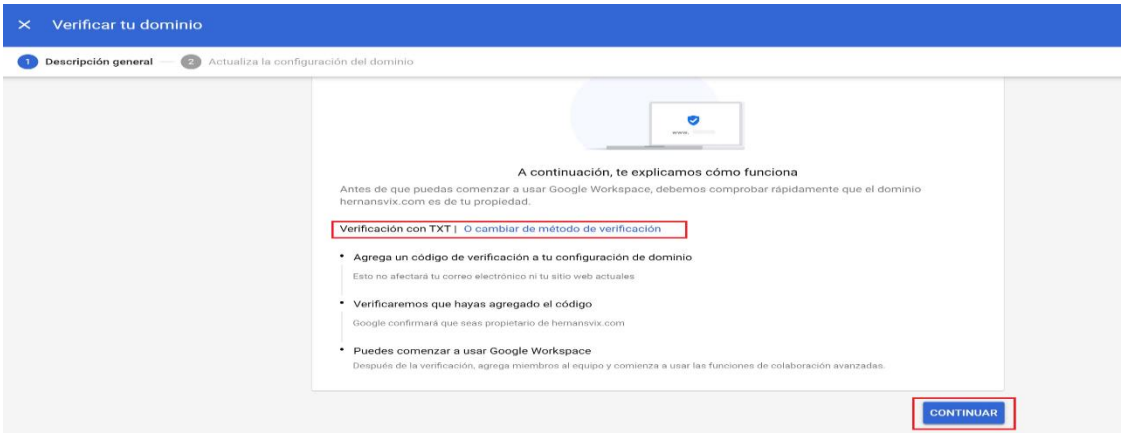
Pestaña registro del dominio



La verificación del dominio se lo hará mediante la adición de registros TXT que dirigen el tráfico de Internet al nombre del dominio y que deben apuntar a los servidores de Google. Una vez seleccionado la forma de verificación damos clic en continuar tal y como se muestra en la Figura 27.

Figura 27

Pestaña de verificación TXT



La adición de los registros TXT se lo hará desde el cPanel del Hosting. Por esta razón primero se debe iniciar sesión en el Panel de administración del dominio de HostGator, luego vamos a la pestaña de dominios y seleccionamos la opción de Editor de zonas tal como describe la Figura 28, en esta pestaña ejecutamos la acción de administrar y nos redirige a la Zona de Registros en donde se alojan todos los registros DNS del dominio principal, en las Figuras 29 y 30 se representa las acciones para acceder a la zona de dominio.

Figura 28

Opciones de editor de zonas

Figura 29

Panel de administración de dominios

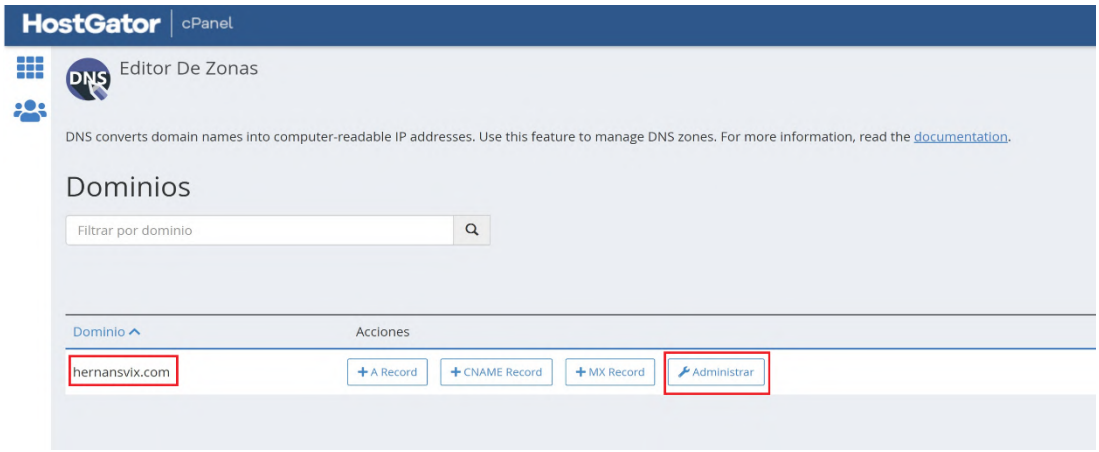
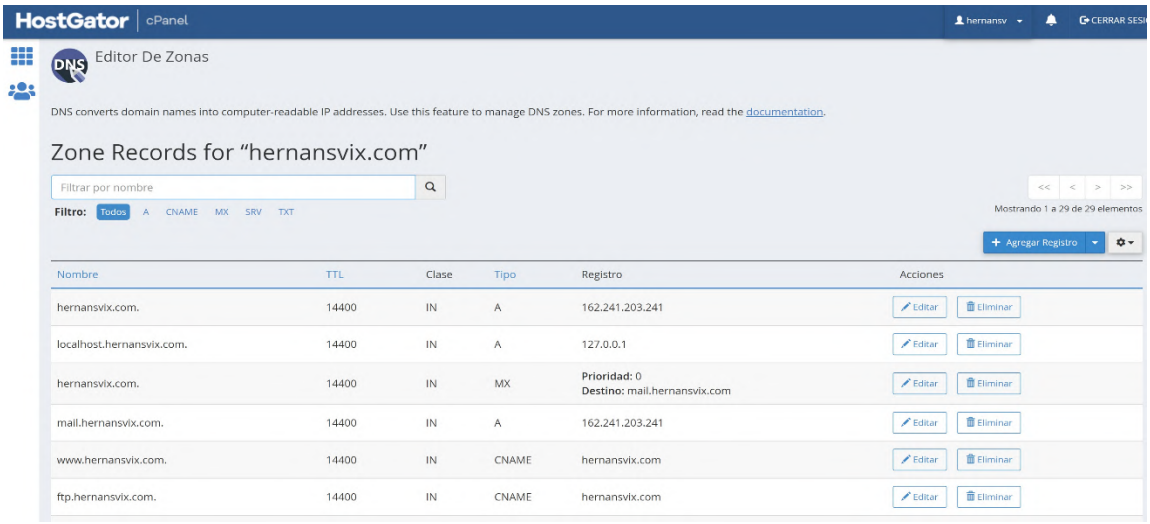


Figura 30

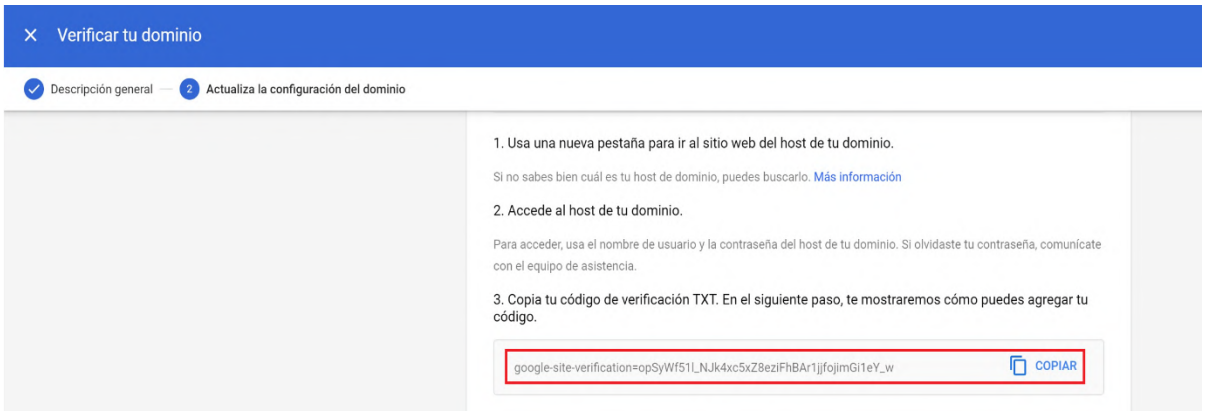
Tabla de registros DNS del Hosting



En la consola de administración de Google se observa una serie de pasos para verificar el dominio basado en el registro TXT. Se debe copiar el código de verificación que se observa en la Figura 31 para agregar a las configuraciones de zona del hosting.

Figura 31

Actualización de configuración del dominio con un registro TXT



En el cPanel seleccionamos la opción de agregar registros, en donde se especifica el tipo de registro, el código de registro y el nombre, para luego crear el nuevo registro el proceso se lo detalla de la Figura 32 a la Figura 34.

Figura 32

Agregación del registro TXT

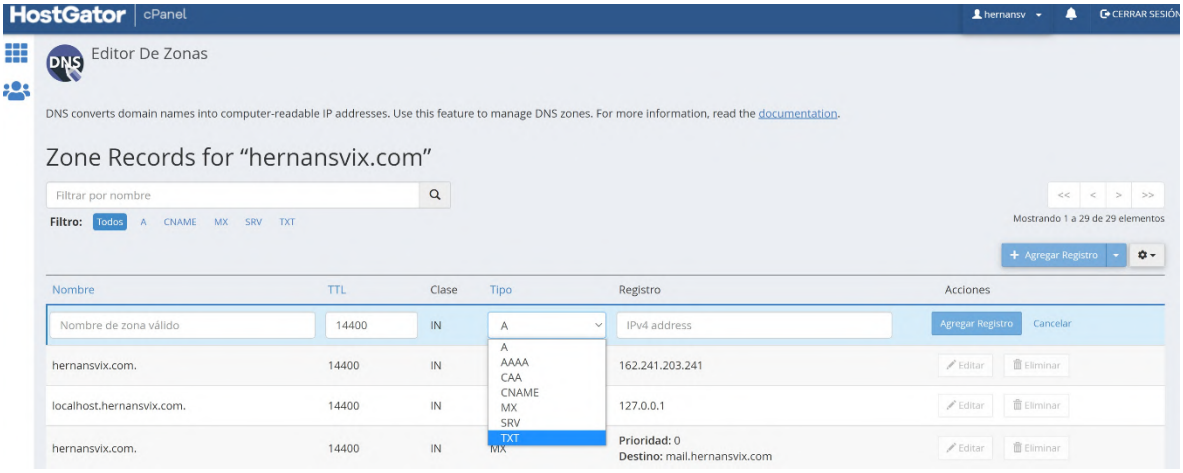


Figura 33

Modificación de los parámetros del registro TXT

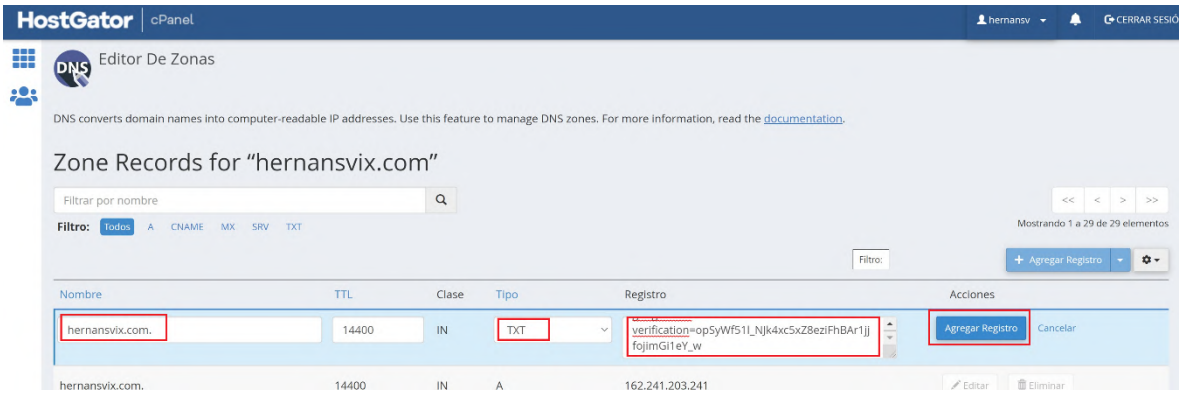
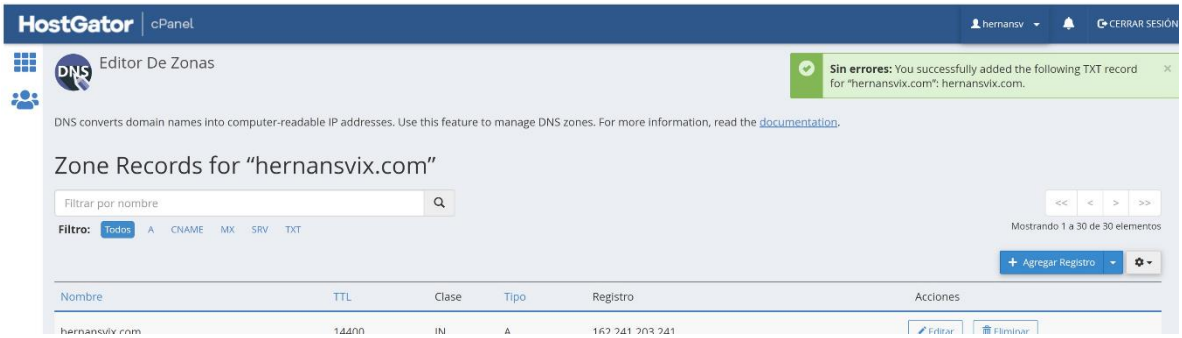


Figura 34

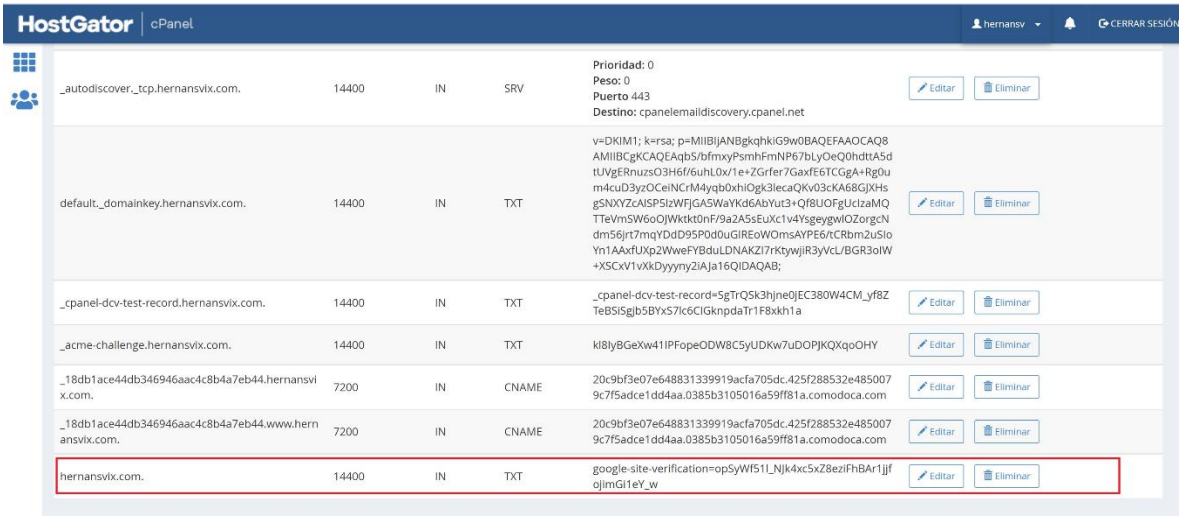
Creación del registro TXT



En la Figura 35 se visualiza el registro en la tabla de registros del Hosting.

Figura 35

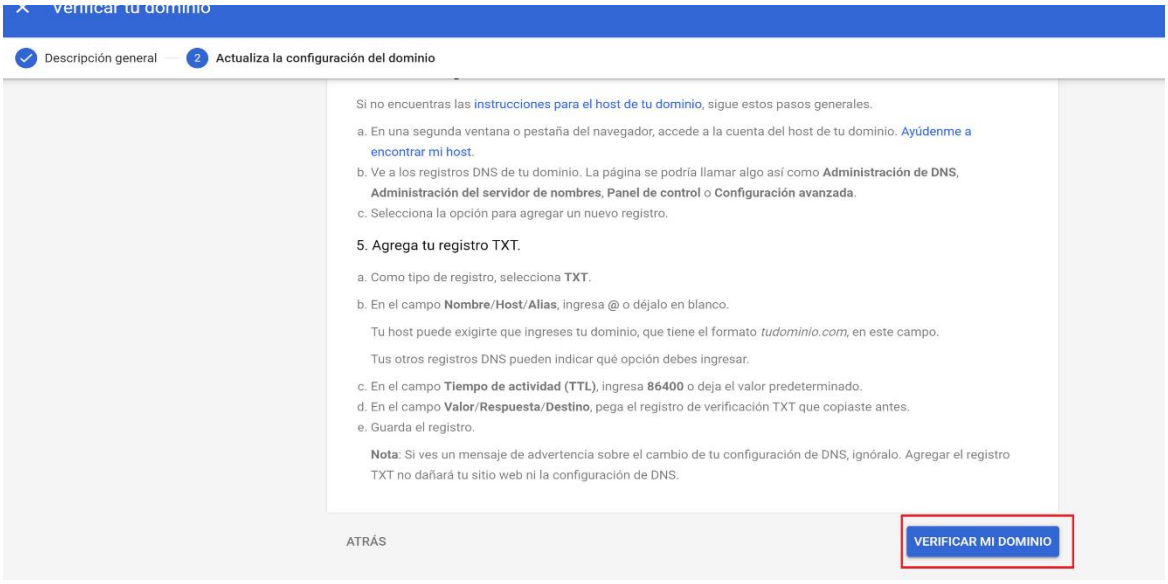
Visualización del registro TXT en la tabla de registros



Después damos clic en verificar dominio en la pestaña de verificación de Google como en la Figura 36, este proceso puede tardar entre 10 a 15 min.

Figura 36

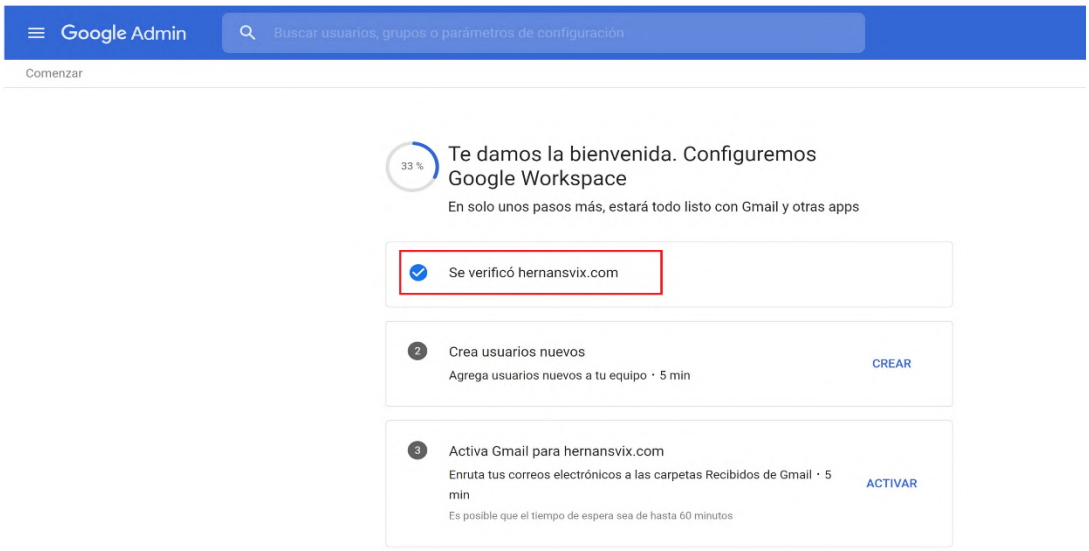
Pestaña de verificación del dominio



Hecho esto el dominio queda totalmente registrado en Google Workspace la cual se la ilustra en la Figura 37.

Figura 37

Pestaña en donde indica la verificación del dominio



Activación de Gmail en el Dominio

En esta sección inicia la fase de activación de Gmail para el dominio de *hernansvix.com*, Para activar Gmail en el dominio se debe agregar 5 registros del tipo MX, las cuales se listan en la Tabla 1.

Tabla 1

Valores de los registros MX en Google Workspace

Valor/Respuesta/Destino	Prioridad
ASPMX.L.GOOGLE.COM	1
ALT1.ASPMX.L.GOOGLE.COM	5
ALT2.ASPMX.L.GOOGLE.COM	5
ALT3.ASPMX.L.GOOGLE.COM	10
ALT3.ASPMX.L.GOOGLE.COM	10

Una vez creado todos estos registros, procedemos a verificar en el Editor de Zonas del Hosting que los registros consten en la respectiva Tabla de Zonas tal y como se detalla en la Figura 38.

Figura 38

Registros MX de Google en la tabla de Editor de Zonas del hosting

De esta manera Gmail ya estará activado para el dominio hernansvix.com que se indica en la Figura 39, se debe esperar un periodo de tiempo hasta que los cambios en la zona de DNS del hosting surtan efecto, luego nos redirige a la pestaña de confirmación de configuración de Google Workspace la misma que se ilustra en la Figura 40.

Figura 39

Pestaña que indica la activación de Gmail para hernansvix.com

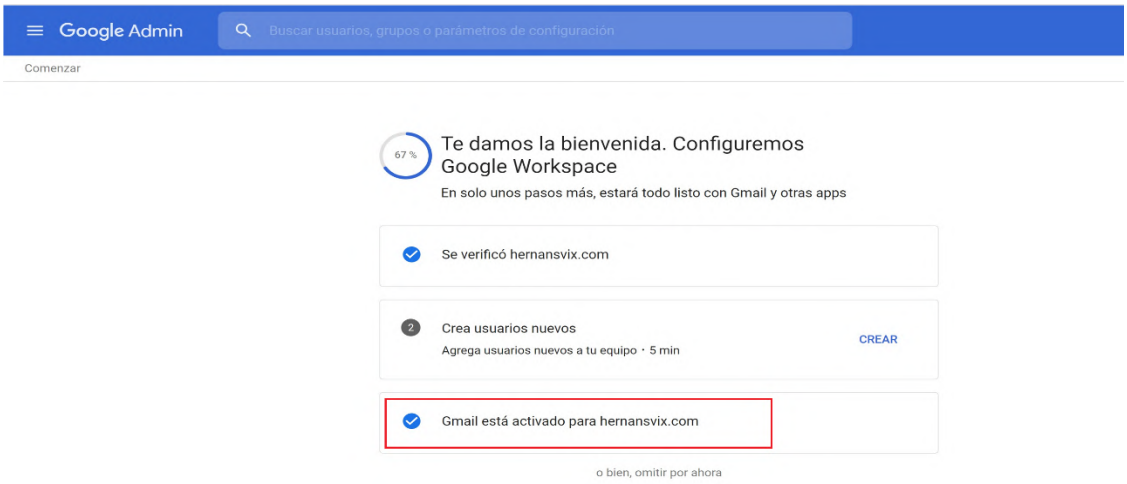
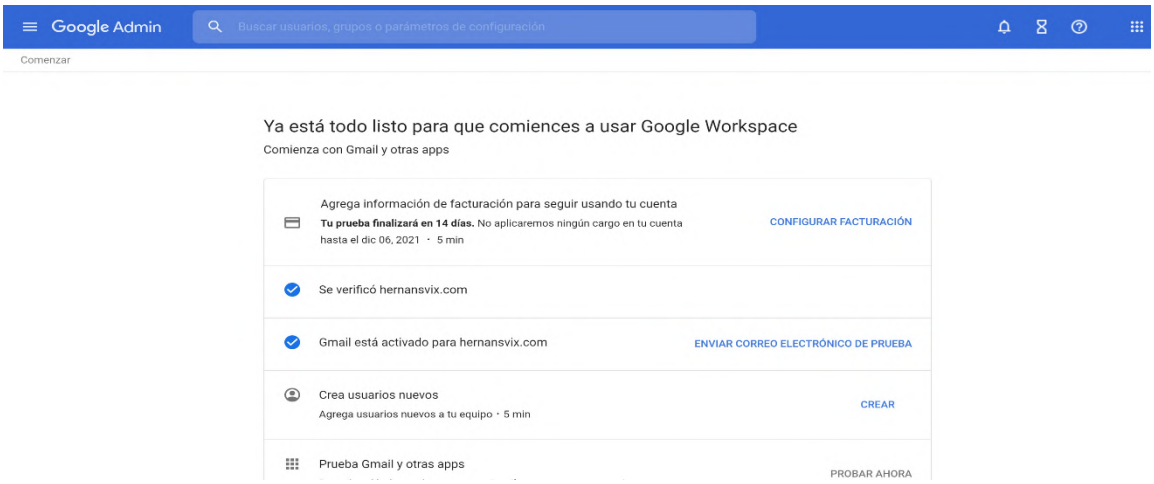


Figura 40

Pestaña de acceso a Google Workspace



Una vez que se ha agregado los registros MX de Google, se podrá recibir correos electrónicos en la bandeja de entrada de Gmail desde clientes de correo electrónico de servidores externos.

Configuración MTA-STS y TLS Reporting

Crear una política de MTA-STS

La política de MTA-STS (un archivo .txt), define los servidores de correo electrónico que utilizan MTA-STS en el dominio de recepción. Los servidores de correo admitidos se conectarán automáticamente a la web para recuperar el archivo.

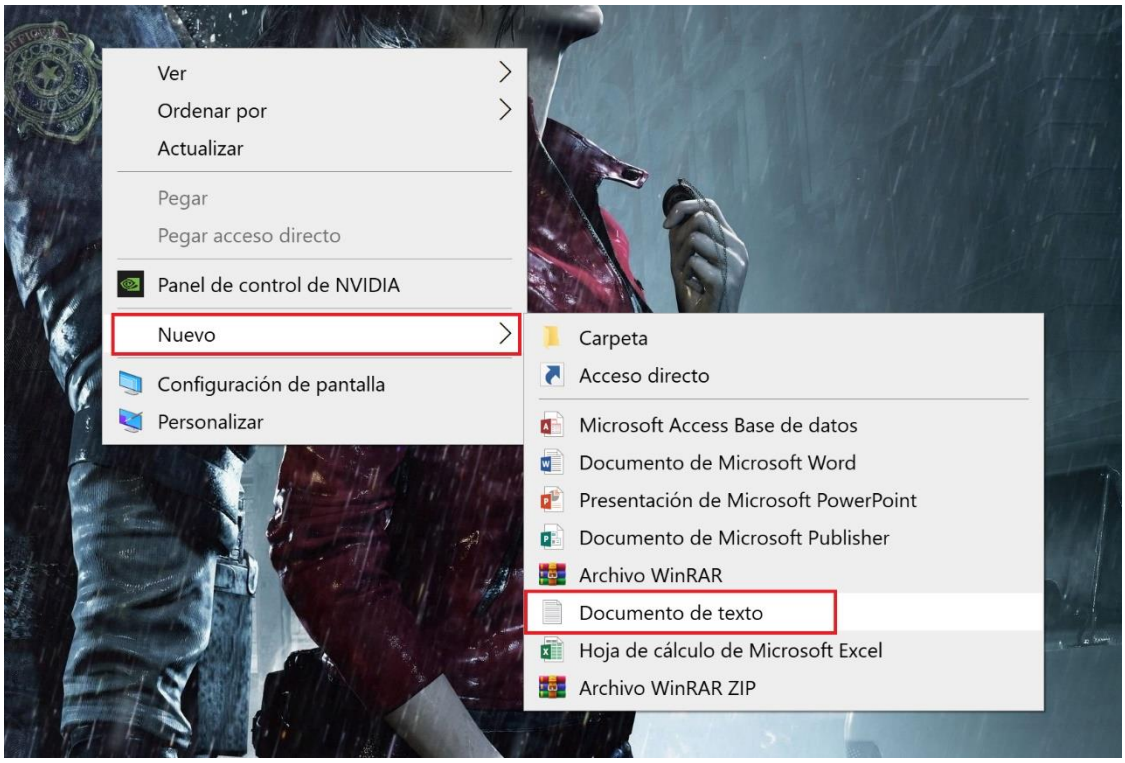
El archivo de políticas del MTA-STS es en esencia un simple archivo de texto, la cual tendrá el siguiente aspecto:

version: STSv1
mode: enforce
mx: ALT4.ASPMX.L.GOOGLE.COM
mx: ALT2.ASPMX.L.GOOGLE.COM
mx: ASPMX.L.GOOGLE.COM
mx: ALT1.ASPMX.L.GOOGLE.COM
mx: ALT3.ASPMX.L.GOOGLE.COM
max_age: 604800

Para definir el archivo de texto primero se crea un texto sin formato en el escritorio del ordenador dando clic derecho en la pantalla principal, seleccionar la opción nuevo y documento de texto tal y como se indica en la Figura 41.

Figura 41

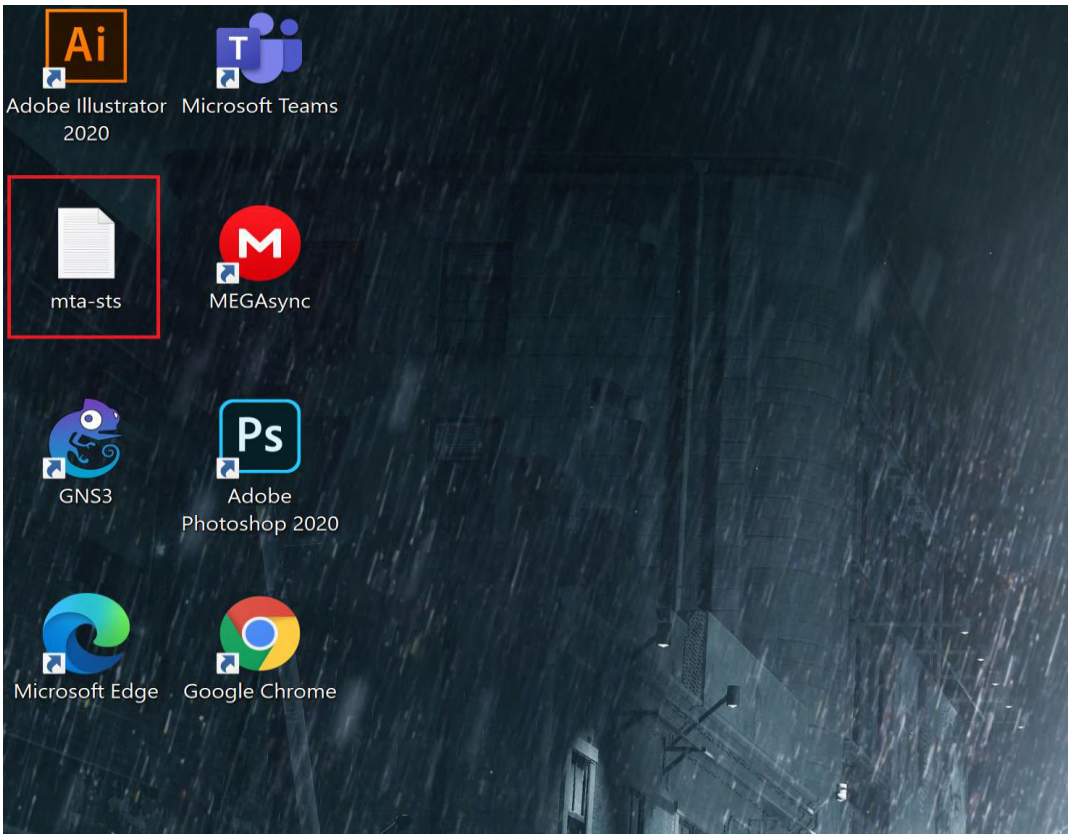
Creación de un documento de texto en el escritorio



Inmediatamente el documento de texto se ubica en el escritorio del ordenador, este archivo lo renombraremos con el nombre de *mta-sts.txt*, este documento se lo visualiza en el Figura 42.

Figura 42

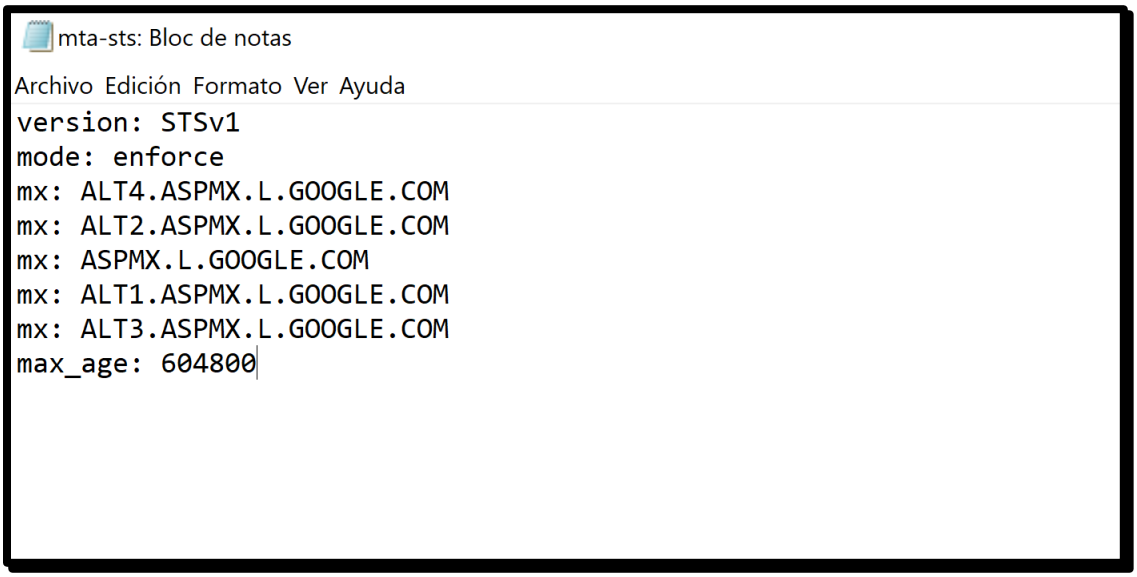
Documento de texto renombrado con el nombre mta-sts



Luego se abre el documento de texto y se escribe el contenido que será el correspondiente al cuerpo de la política MTA-STS definida anteriormente, el contenido del archivo de texto *mta-sts* se ilustra en la Figura 43. Guardamos el archivo de texto para utilizarla después.

Figura 43

Contenido del documento de texto mta-sts.txt



Con estas consideraciones se ha creado el archivo de configuración MTA-STS y se lo guardó en el escritorio. En el siguiente paso, se subirá el archivo de texto al servidor web público para que los servidores de correo externos puedan acceder a él.

Publicar la política MTA-STS en el Sitio Web

Para que el archivo de configuración del MTA-STS se pueda descubrir automáticamente por los servidores de correo externos, debe ser alojado exactamente en el camino correcto, se debe usar el subdominio sobre HTTPS y la ruta conocida; de lo contrario, la configuración no funcionará.

Para añadir una política al servidor web del dominio *hernansvix.com* hay que crear un subdominio con el nombre de *mta-sts*. Antes que nada, se debe iniciar sesión en el panel de

administración del Hosting, dirigirnos a la opción de subdominio en la función de dominio, la misma que se recalca en la Figura 44.

Figura 44

Opción subdominio del cPanel

Dentro de la opción subdominio se encuentra la función de crear un subdominio, aquí se ingresa el nombre del subdominio que será *mta-sts*, luego más abajo seleccionamos el dominio principal(*hernansvix.com*) que aloja el subdominio e inmediatamente el cuadro de texto raíz de documento muestra la URL del subdominio tal y como se expresa en la Figura 45.

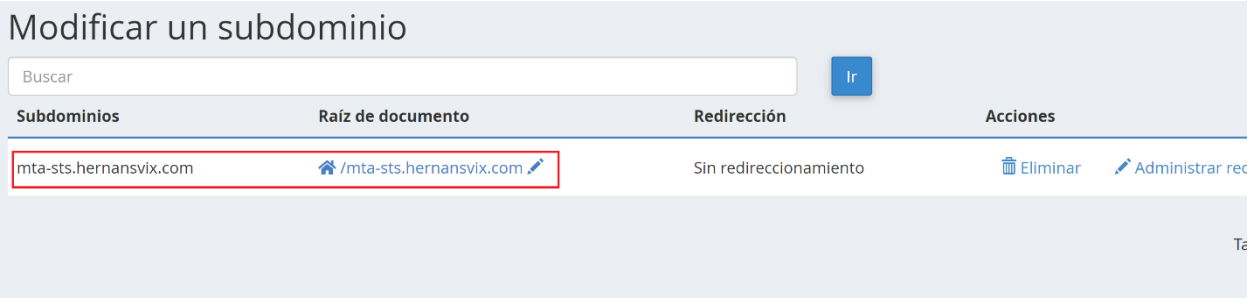
Figura 45

Parámetros para crear un subdominio

Una vez que ya se ha establecido el subdominio damos clic en crear y el subdominio ya estará visible en la parte final de la pestaña crear subdominio, en la Figura 46 se observa el subdominio ya creado.

Figura 46

Raíz de documento que contiene al subdominio



El siguiente paso es crear un directorio llamado *well-known* en el subdominio, para ello nos ubicamos en la opción de administrador de archivos en la pestaña principal del cPanel la cual es visible en la Figura 47.

Figura 47

Opción Administrador de archivos en el cPanel

Una vez dentro de la opción Administrador de archivos ubicamos la carpeta que tiene el subdominio creado, esto se visualiza en la Figura 48. Luego hacemos clic dentro de la carpeta del subdominio en donde no tiene ningún tipo de archivo alojado que haga referencia a ese subdominio, esto se lo puede ver en la Figura 49.

Figura 48

Archivos que contiene la carpeta del subdominio.

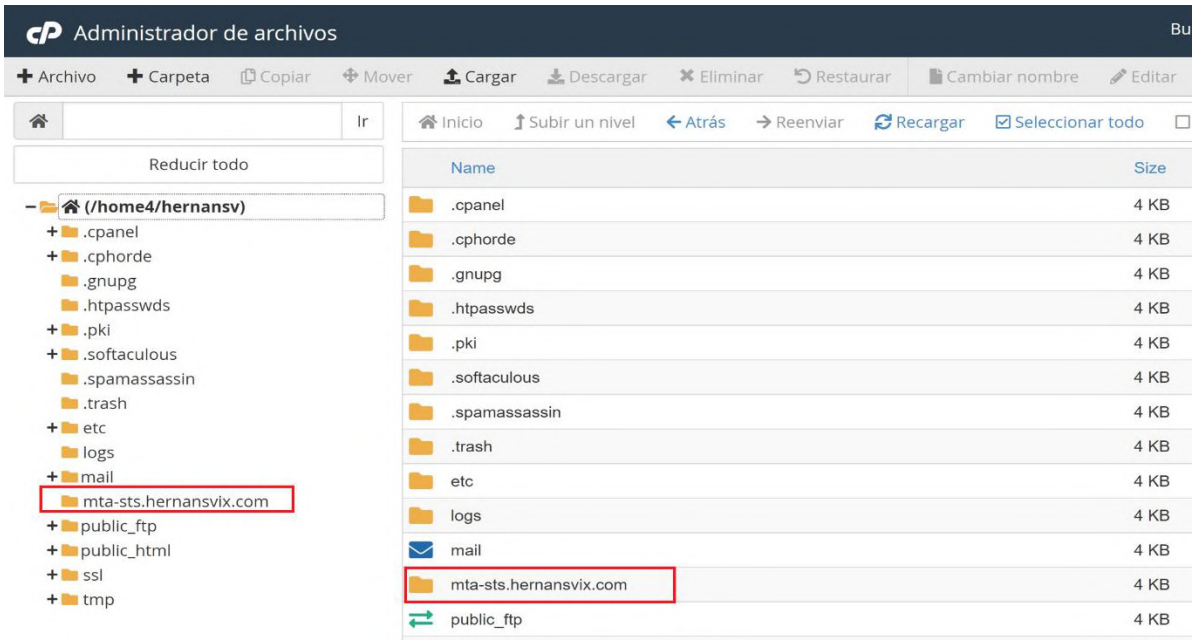
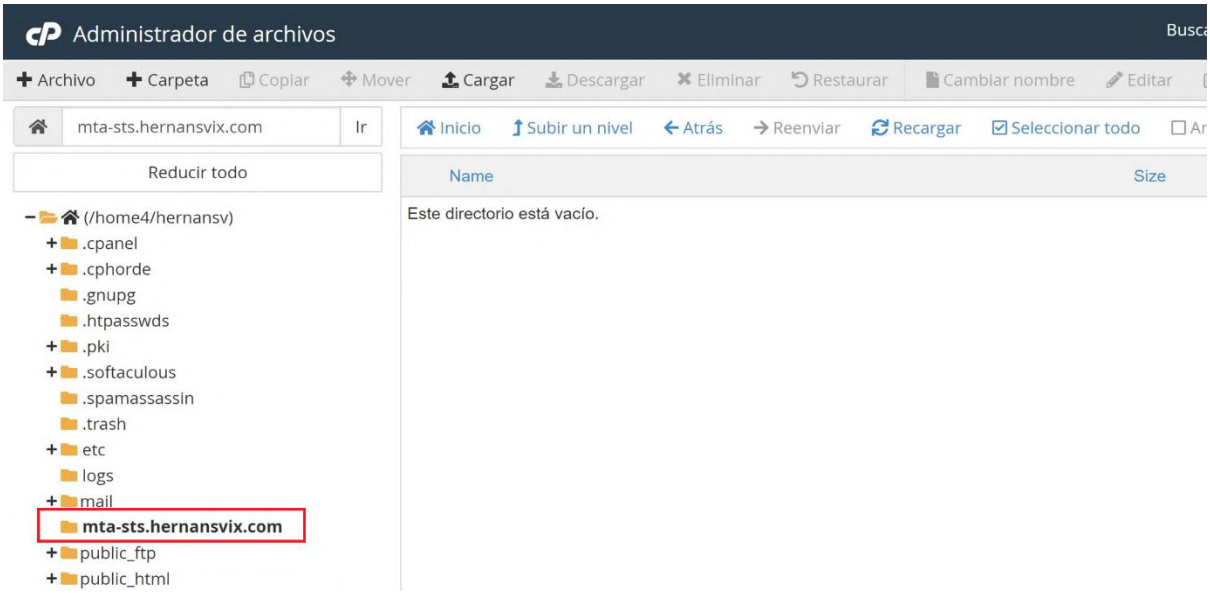


Figura 49

Contenido de la carpeta mta-sts.hernansvix.com



Dentro del directorio *mta-sts.hernansvix.com* se procede a crear un directorio, para eso se hace clic en la opción superior *Carpeta*, enseguida se despliega un cuadro de dialogo en donde se deberá especificar el nombre del directorio que debe ser *well-known* tal y como muestra la Figura 50. Enseguida dar clic en *Create New Folder* para crear la carpeta.

Figura 50

Cuadro de dialogo para crear el directorio

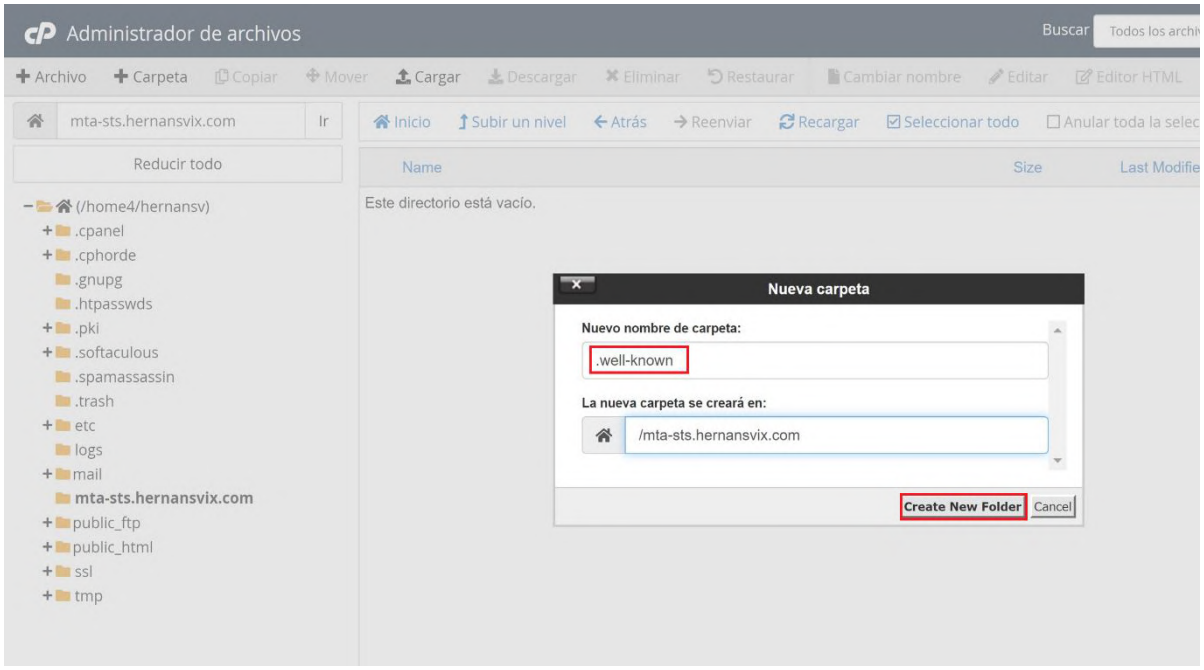
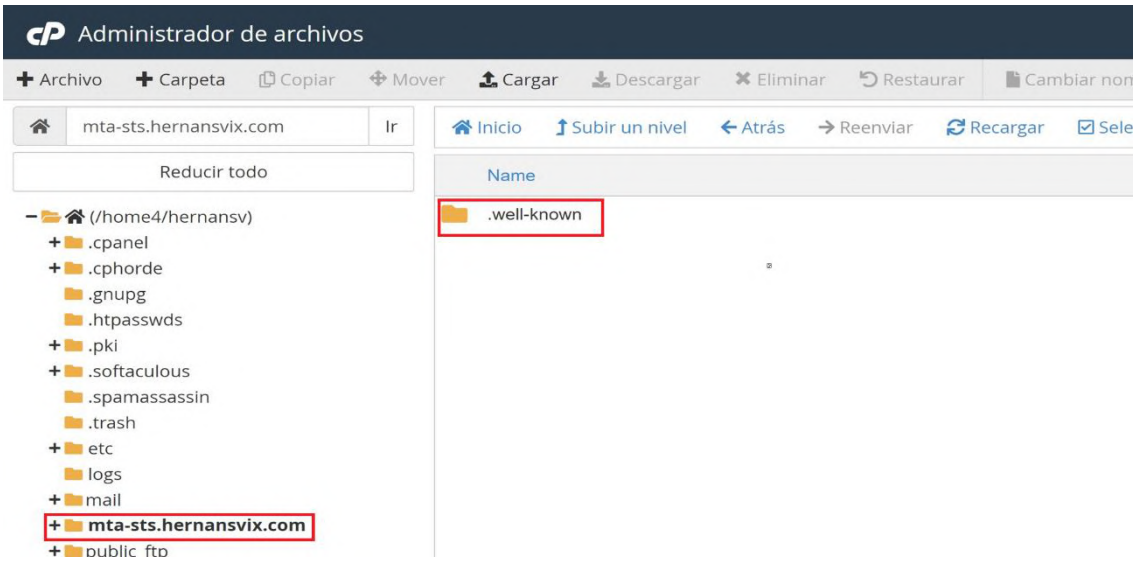


Figura 51

Directorio well-known en mta-sts.hernansvix.com



El directorio estará disponible dentro de *mta-sts.hernansvix.com,* como se ilustra en la Figura 51, ahora dentro del directorio se debe cargar el archivo de política que se creó anteriormente, para este paso dar clic en la opción *Cargar* en la parte superior del Administrador de archivos, enseguida se carga una pestaña para subir el archivo, aquí seleccionamos subir archivo y se busca el documento de texto con el nombre *mta-sts*, esto se lo representa en la Figura 52. La Figura 53 detalla cómo el documento de texto ha sido cargado totalmente en el directorio.

Figura 52

Proceso de subir el documento mta-sts.txt

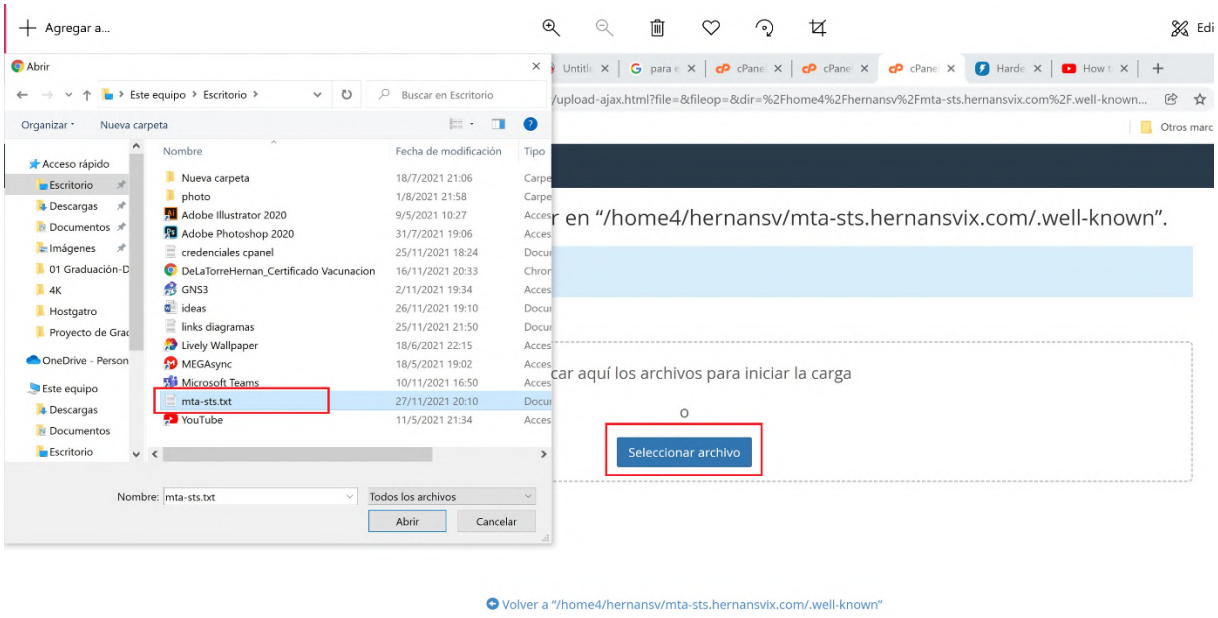
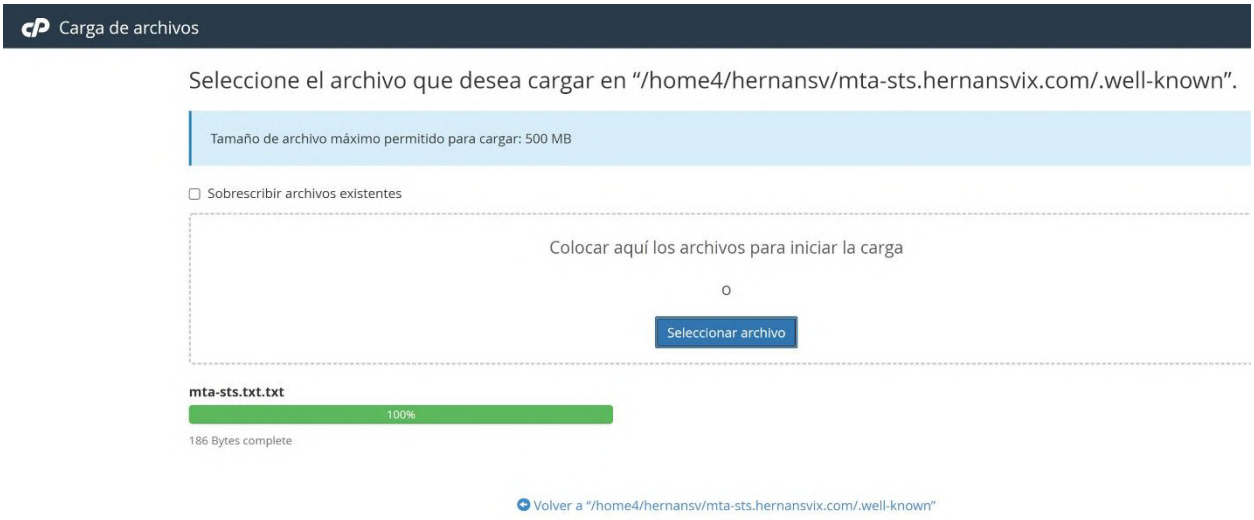


Figura 53

Documento cargado al 100%



Una vez que el archivo de texto *mta-sts* se ha cargado totalmente, éste ya estará ubicado dentro del directorio *well-known* que se observa en la Figura 54. Con todos estos ajustes hechos la URL de la política de MTA-STS correspondiente al dominio *hernansvix.com* será: *https://mta-sts.hernansvix.com/.well-known/mta-sts.txt.* Si se ingresa a éste enlace se encuentra la política publicada en la web tal y como se observa en la Figura 55.

Figura 54

Documento de texto mta-sts.txt en el directorio well-known

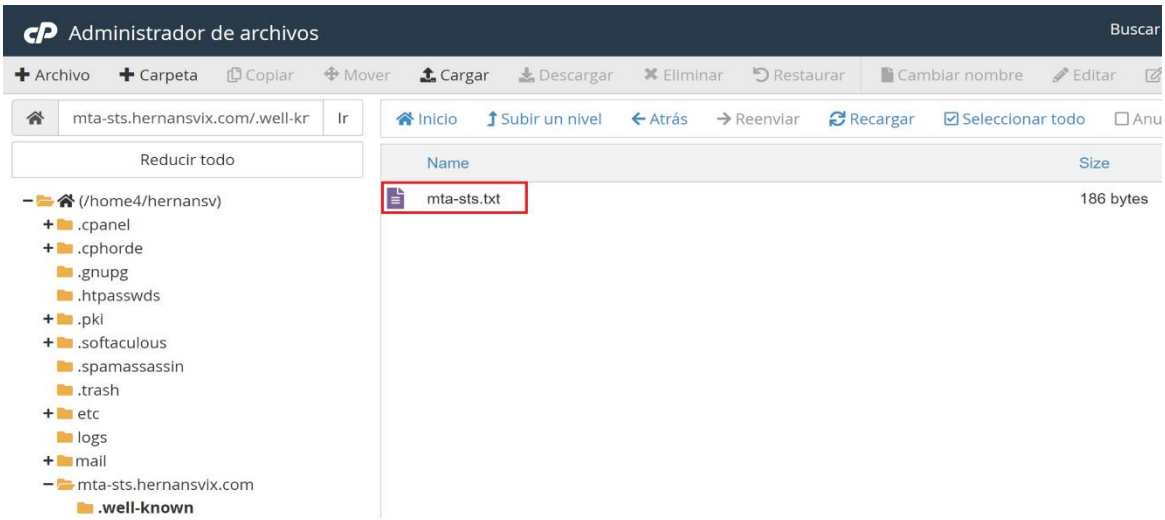
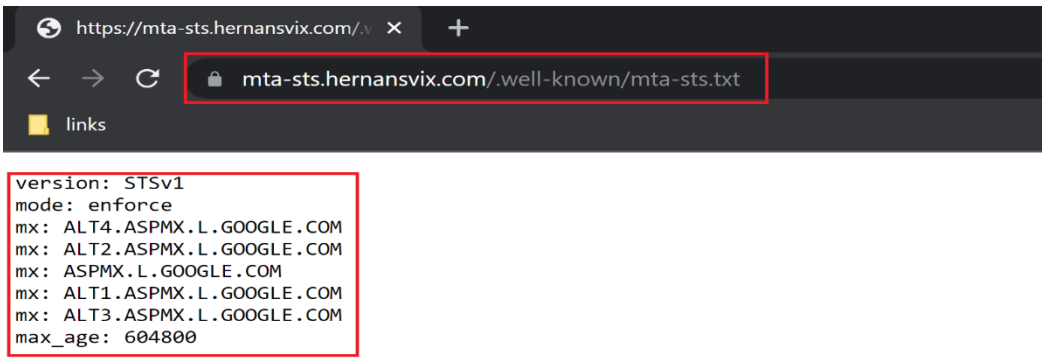


Figura 55

Política mta-sts.txt publicada en la internet



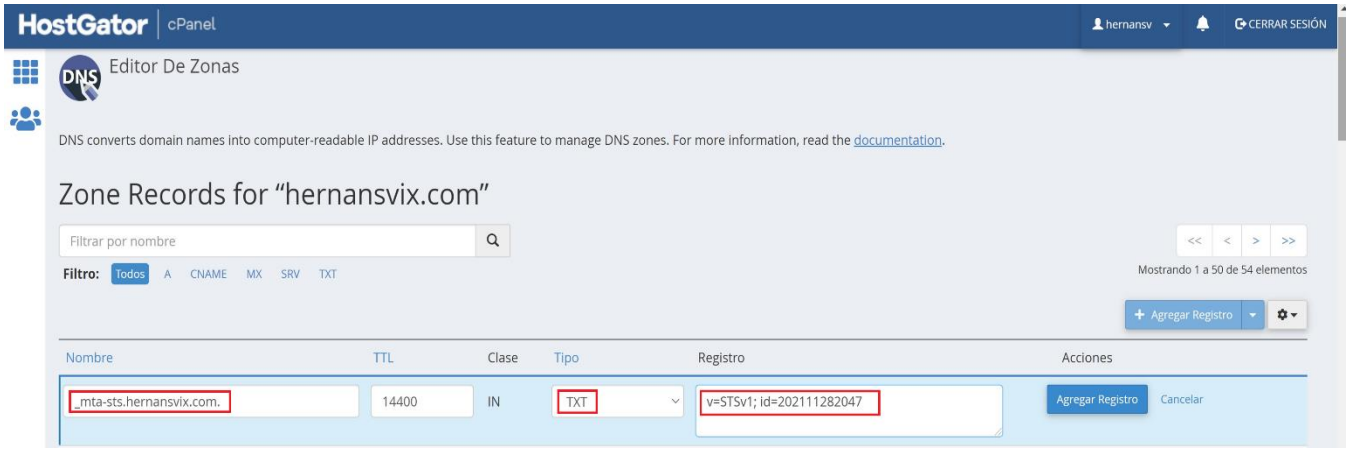
Activar MTA-STS y los Reportes TLS

Para activar el estándar MTA-STS y TLS Reporting en el dominio de recepción de correo, se debe actualizar la configuración DNS del hosting mediante dos registros TXT, las cuales son: *_mta-sts* y *_smtp. _tls* seguido del nombre de dominio. Esto posibilita que los servidores de correo externos envíen correos electrónicos al dominio cuando estén autenticados y cifrados con TLS 1.2 o superior.

Lo primero es iniciar sesión en el cPanel del hosting, en las configuraciones del editor de zonas del dominio se crea el siguiente registro: *_mta-sts.hernansvix.com*, utilizando el siguiente valor: *v=STSv1; id=202111282047;* en donde el id es un valor cualquiera de entre 1 y 32 caracteres alfanuméricos. Este proceso se la representa en la Figura 56.

Figura 56

Creación del registro _mta-sts.hernansvix.com

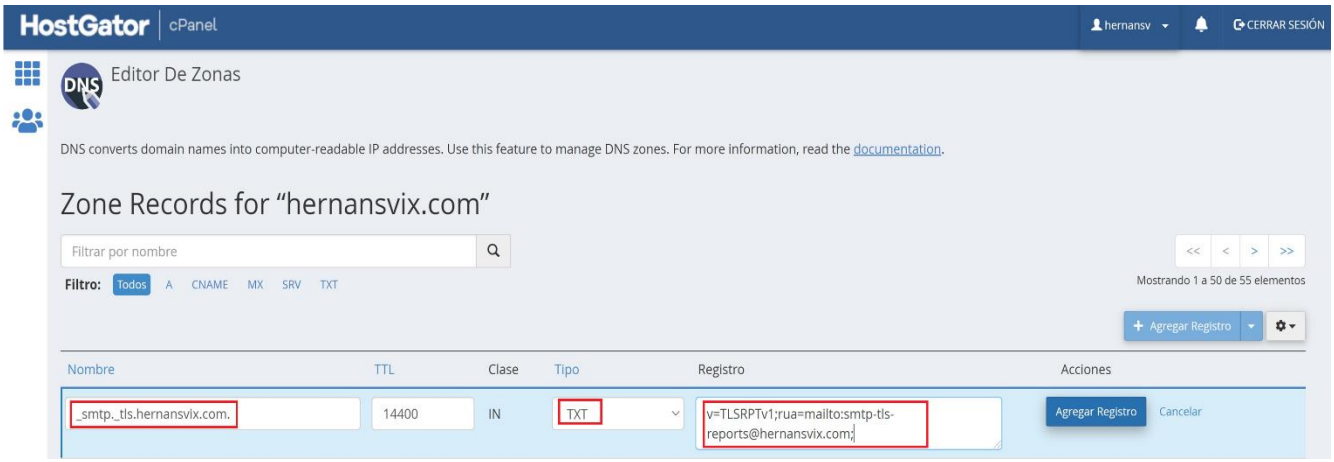


Cabe recalcar que las notificaciones se receptaran vía correo electrónico con el parámetro *mailto* a la dirección *smtp-tls-reports@hernansvix.com*, De esta forma el valor del registro es:

v=TLSRPTv1;rua=mailto:smtp-tls-reports@hernansvix.com; la creación del registro se la indica en la Figura 57.

Figura 57

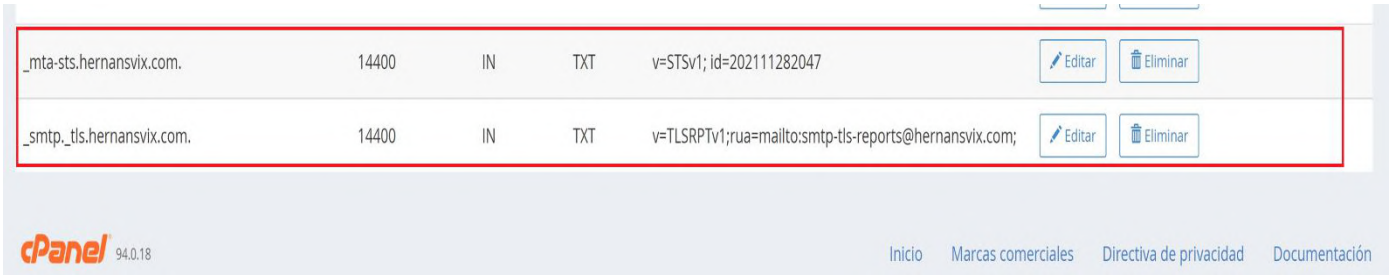
Creación del registro _smtp._tls.hernansvix.com



Una vez que se ha añadido ambos registros al hosting se debe verificar que estos registros consten en la tabla del Editor de Zonas del hosting, estos registros se visualizan en la Figura 58.

Figura 58

Registros TXT añadidos en el Edito de Zonas del hosting



Verificar el Estado de MTA-STS y TLS Reporting

Para asegurarse de que MTA-STS y TLS Reporting estén correctamente configurados se hace la verificación en la página de Estado de Seguridad de Cumplimiento de Google Admin.

Para validar las configuraciones En la Consola del administrador, se dirige a Aplicaciones > Descripción General > Google Workspace > Configuración Gmail > Cumplimiento. Aquí se podrá validar la configuración de MTA-STS y TLS Reporting.

En la Figura 59 se visualiza el Diagnostico de configuración de MTA-STS y TLS Reporting la cual es válida.

Figura 59

Diagnóstico de configuración de MTA-STS y TLS Reporting

FAQ (Frequently Asked Questions)

A continuación, se incluirá una serie de preguntas o dudas más frecuentes que pueden surgir a los usuarios que implementen el estándar MTA-STS en sus servicios de correo electrónico.

¿Para quién está orientado el uso de MTA-STS?

El estándar MTA-STS es adecuado para todos los dominios que utilizan servidores MX que admiten el comando STARTTLS. La mayoría de proveedores de correo electrónico empresarial recomiendan el uso de MTA-STS, ya que todos admiten el comando STARTTLS.

¿Qué servidores actualmente cuentan con soporte de MTA-STS y TLS Reporting?

Las políticas de MTA-STS son publicadas por aproximadamente el 0.05% de los dominios activos que protegen una gran cantidad de tráfico de correo electrónico(Dubrovin, 2020). Entre los principales proveedores que brindan soporte destacan: Google, Microsoft, Protonmail y parcialmente Yahoo!.

¿En qué modo debo configurar una política de MTA-STS al implementar el estándar por primera vez?

Siempre es recomendable activar la política en modo de prueba, Google manifiesta que lo bueno es mantener una política de prueba durante dos semanas con la finalidad de monitorear el tráfico de correo electrónico antes de cambiar a una política más agresiva de hacer cumplir. Para lo cual es indispensable utilizar la información de los Reportes TLS.

¿Qué servidores MX pongo en el archivo de política?

En el archivo de política se debe colocar todos los servidores de intercambio de correo (MX) para su dominio que lo admitan el comando STARTTLS. Estas direcciones MX están establecidos en los registros DNS del dominio.

¿Existe inconvenientes al usar MTA-STS?

Si configuró la política MTA-STS en modo *enforce*, pero su MX no entrega un certificado válido para su dominio, el correo electrónico no se entregará. Esto es, por supuesto, lo que pretende hacer MTA-STS. Por esta razón, es aconsejable configurar una política MTA-STS en modo de prueba y habilitar inicialmente los reportes TLS para el dominio.

¿Cómo puedo cambiar el modo de política de MTA-STS?

Para cambiar el modo de política de MTA-STS es necesario editar el archivo de política alojado en el servidor web y guardar los cambios. Luego se deberá editar el campo *id* del registro TXT que aloja la política de MTA-STS.

¿Realmente es necesario los Reportes TLS?

TLS Reporting permite al propietario del dominio obtener informes de las entregas de correo electrónico fallidas, por lo tanto, se puede identificar la fuente del problema y actuar en consecuencia para solucionar los problemas de entrega.

¿Cómo desactivo MTA-STS para el dominio?

Para desactivar MTA-STS se debe configurar la política en modo ninguno y después actualizar el campo *id* del registro TXT, o eliminando el registro TXT de MTA-STS.