Evaluación de vulnerabilidades de los certificados y configuración TLS de la Imprenta Nacional de Colombia

SEKINFO SAS

2026-04-07

Elaborado por

Índice

Resumen

Contexto

Se realizó un inventario de dominios, servidores y servicios web de la Imprenta Nacional de Colombia, utilizando fuentes de datos públicos, con el fin de evaluar vulnerabilidades asociadas al protocolo de conexiones seguras TLS ("Transport Layer Security").

Para mejorar la precisión de este inventario, SEKINFO requiere contrastar los datos públicos con información interna específica. Por ello, se solicita:

- El inventario completo actualizado de servidores y servicios web.
- Acceso al archivo de zona DNS (“DNS zone file”) para identificar dominios no detectados en las fuentes públicas.

Si hay diferencias significativas con la información levantada de las fuentes públicas, SEKINFO las incorporará en un informe final de evaluación de vulnerabilidades.

Metodología de Evaluación

Con base en el inventario consolidado, se ejecutaron pruebas técnicas en cada dominio para auditar:

- El estado de los certificados TLS.
- La configuración TLS, incluyendo la redirección segura, cabeceras de seguridad entre otros.

Hallazgos Principales

Indicadores básicos

- 19 dominios totales registrados en datos públicos de DNS.
- 16 dominios activos asociados a servicios expuestos a Internet.
- 8 dominios con configuraciones TLS consideradas adecuadas.

Riesgos detectados

- Certificados caducados o inválidos.
- Errores en las configuraciones de conexiones seguras TLS.
- Exposición innecesaria a Internet de servicios sensibles (ej. administración de cortafuegos y sistema DVR de cámaras de seguridad).
- Omisión de la redirección segura.
- Omisión de las cabeceras de seguridad HSTS (Véase HSTS en el glosario).
- Omisión de la configuración de la autorización de autoridades de certificados (CAA) (Véase CAA en el glosario).

Impacto Operativo

En la mayoría de los casos identificados, los usuarios finales enfrentan advertencias de seguridad en sus navegadores, viéndose obligados a añadir excepciones manuales para continuar. La aceptación de estas excepciones sin una justificación técnica válida compromete la autenticidad, integridad y confidencialidad de las comunicaciones. Esto elimina las garantías de seguridad que ofrece TLS, exponiendo a la organización a riesgos de interceptación de datos (como credenciales de acceso).

Recomendaciones Estratégicas

Se recomienda:

- **Implementación consistente de TLS**: Implementar certificados TLS válidos y vigentes en todos los servicios activos expuestos a Internet, no solo en las plataformas institucionales principales. Adoptar configuraciones TLS modernas y seguras: suites de cifrado moderno, redirección segura, HSTS y CAA.
- **Monitoreo Automatizado**: Desplegar herramientas que automaticen el seguimiento del ciclo de vida de los certificados y la configuración TLS, permitiendo una visualización en tiempo real del estado de seguridad. Debe incluir el monitoreo de los logs CT para detectar certificados sospechosos.
- **Depuración de Servicios**: Identificar y dar de baja servicios descontinuados. La exposición de servicios en desuso o parcialmente activos representa un riesgo crítico. Si no es posible su eliminación total, se deben retirar los registros DNS obsoletos y cerrar los puertos asociados.
- **Restricción de Acceso**: Analizar la exposición innecesaria de servicios internos y migrar su acceso a través de redes privadas virtuales (VPN), eliminando su exposición directa a Internet.
- **Gestión de Incidentes**: Definir criterios claros para clasificar incidentes relacionados con TLS y establecer protocolos de remediación (ej. reseteo obligatorio de contraseñas tras una transmisión no segura).
- **Actualización de Políticas**: Incorporar estas recomendaciones en las políticas y procedimientos de seguridad permanentes de la organización.

Introducción

Las conexiones seguras con sitios web, plataformas y servicios en Internet son fundamentales no solo para proteger la información transmitida, sino también para garantizar la integridad de los servidores y los dispositivos de los usuarios. El estándar tecnológico para implementar estas conexiones seguras, ya sea para páginas web, servicios de correo o acceso remoto, se denomina TLS. Su uso se identifica mediante direcciones que comienzan con https:// y por la presencia de un icono de candado en la barra del navegador.

Esta tecnología depende del uso de certificados TLS válidos y vigentes, junto con una configuración correcta. Cabe destacar que la simple adquisición de un certificado no garantiza la protección por sí sola. La generación y gestión de las llaves criptográficas asociadas, la instalación adecuada del certificado, la configuración del servidor web y otros elementos de soporte, como la automatización y el monitoreo continuo, son esenciales para lograr un nivel de seguridad óptimo.

Es importante distinguir que un certificado TLS es un mecanismo concreto de seguridad digital, muy diferente a otras certificaciones, como las certificaciones asociadas con las normas ISO. Mientras que estas últimas son documentos que acreditan el cumplimiento de estándares por parte de una entidad, un certificado TLS es un archivo digital utilizado para establecer la autenticidad de la conexión basada en el nombre de dominio y para encriptar los datos transmitidos.

Aunque existen certificados con niveles de validación adicionales (conocidos como OV y EV), estos no ofrecen una protección técnica superior frente a la opción estándar de Validación de Dominio (DV). La función esencial de cualquier certificado es doble: verificar que los datos provienen de un servicio legítimo y mantenerlos privados durante su tránsito por Internet. Para lograr esto, la Validación de Dominio (DV) es suficiente. Este mecanismo asegura que el certificado se emita únicamente a quien pueda demostrar ser el propietario real del dominio, garantizando así la seguridad requerida.

La ausencia de conexiones TLS seguras, o vulnerabilidades en su configuración (como certificados inválidos o caducados), implican riesgos significativos. Estos pueden clasificarse en tres categorías principales: interceptación de información confidencial, modificación maliciosa de datos y suplantación de identidad. En términos más generales, se habla de riesgos contra la confidencialidad, la integridad y la autenticidad. Dado que estos conceptos pueden ser demasiado abstractos, resulta útil ilustrarlos mediante ejemplos concretos de los riesgos derivados de una configuración inadecuada:

- Exposición de datos confidenciales.
- Robo de contraseñas.
- Hackeo del sistema debido a la suplantación de un administrador.
- Filtración de grabaciones de cámaras de seguridad.
- Inyección de malware (virus) en el código de las páginas web (ej. JavaScript malicioso).
- Inyección de malware en las descargas de los usuarios (ejecutables o archivos con macros).

No se puede justificar la ausencia de TLS argumentando que "los datos de la página no son importantes". Por un lado, cualquier página que solicite una contraseña es inherentemente sensible, especialmente considerando que muchos usuarios utilizan la misma contraseña para múltiples servicios. Además, cualquier formulario donde un usuario pueda ingresar información personal o privada también requiere protección. Finalmente, las páginas que ofrecen descargas deben contemplar el riesgo de que dichos archivos sean modificados maliciosamente en tránsito para introducir malware en el equipo del usuario.

En conclusión, la única postura razonable es implementar TLS en todos los servicios en Internet de manera sistemática. Existen muy pocas excepciones donde TLS podría ser innecesario o impráctico; por lo general, para cualquier servicio disponible desde Internet, el uso de TLS debe considerarse obligatorio.

Inventario y diagnóstico de certificados TLS junto con los entornos y servicios relacionados

Para caracterizar el número y tipos de entornos en operación asociados con el dominio imprenta.gov.co, se realizó un inventario de los subdominios desde datos públicos, como los registros DNS, los logs CT, registros BGP, etc.

Es importante destacar que el inventario presentado abajo no necesariamente es completo. La información pública tratada no contiene información de servidores y servicios que son completamente internos, sin ninguna conexión directa desde Internet, por ejemplo, servidores internos sin IPs públicas, servidores de nube en una red privada (VPC), servidores sin registros DNS públicos asociados, etc.

Por esto, solicitamos que se revise esta información y se compare con los registros internos de la entidad y con los registros DNS para identificar posibles omisiones debido a las limitaciones de los datos públicos utilizados.

Inventario de entornos

#	Dominios	IPs	En línea	Tipo	Organización AS	País
1	imprenta.gov.co, www.imprenta.gov.co	185.230.63.107, 34.160.37.117	SI	SaaS	Wix.com Ltd.	US
2	autodiscover.imprenta.gov.co, svremail.imprenta.gov.co	179.1.102.69	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO

#	Dominios	IPs	En línea	Tipo	Organización AS	País
3	boletines.imprenta.gov.co	185.103.10.244	SI	Desconocidc	Core-Backbone GmbH	ES
4	catalogodigital.imprenta.gov.co	159.203.122.246	SI	VPS	DigitalOcean, LLC	US
5	facturacion.imprenta.gov.co, servsgdoc.imprenta.gov.co, urnavirtual.imprenta.gov.co	179.1.102.71	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
6	gpingindc.imprenta.gov.co	179.1.102.66	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
7	jacevedo.imprenta.gov.co	179.1.102.67	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
8	portalinc.imprenta.gov.co	179.1.102.85	NO	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
9	pqrd.imprenta.gov.co	179.1.102.82	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
10	servprodoc.imprenta.gov.co	179.1.102.79	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
11	servsgint.imprenta.gov.co	179.1.102.72	NO	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
12	suscriptores.imprenta.gov.co	200.7.106.228	SI	Dedicado o virtual	HostDime.com, Inc.	US
13	svrpubindc.imprenta.gov.co	179.1.102.87	SI	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
14	svrsgdf71.imprenta.gov.co	179.1.102.86	NO	Dedicado o virtual	INTERNEXA S.A. E.S.P	CO
15	tracking.imprenta.gov.co	18.198.218.66	SI	SaaS	Amazon.com, Inc.	DE

La columna "Organización AS" representa el nombre de la organización asociada con el operador del rango de direcciones IP (ASN), que puede ser un proveedor de servicios de Internet o un operador de un datacenter.

Son 15 entornos con 17 servicios: 10 servidores dedicados o virtuales en un centro de datos nacional (InterNexa), 2 servicios SaaS (Wix, Amazon), y 3 VPS o desconocidos (Core-Backbone, DigitalOcean, HostDime).

Si se observa algún error u omisión en esta información, por favor informar a SEKINFO por correo.

Inventario de servidores web

#	Dominios	Servidor web	Necesita instalación certificado TLS	Notas
1	imprenta.gov.co, www.imprenta.gov.co	Pepyaka		Wix. No aplica la instalación. Véase la nota sobre este dominio abajo.
2	autodiscover.imprenta.gov.co, svremail.imprenta.gov.co	Microsoft-IIS/10.0	SI	Página activa de Outlook interfaz web (OWA).
3	boletines.imprenta.gov.co			¿Descontinuado? Si es así, no aplica la instalación.
4	catalogodigital.imprenta.gov.co	Apache/2.4.25 Debian		Wordpress, redirige a https://ambiegresados.com/. ¿Descontinuado?
5	facturacion.imprenta.gov.co	nginx/1.29.1	SI	Página activa en https://facturacion.imprenta.gov.co/invoice/create
6	gpingindc.imprenta.gov.co		SI	Página activa de administración del cortafuegos Palo Alto. Es inseguro exponer la interfaz de administración de un cortafuegos a Internet público. Véase la nota sobre este dominio abajo.
7	jacevedo.imprenta.gov.co	Apache/2.2.22 Win32 modjk/1.2.28		¿Descontinuado? Si es así, no aplica la instalación.

#	Dominios	Servidor web	Necesita instalación certificado TLS	Notas
8	portalinc.imprenta.gov.co			¿Descontinuado? Si es así, no aplica la instalación.
9	pqrd.imprenta.gov.co	nginx/1.29.1	SI	Página activa de PQRD.
10	servprodoc.imprenta.gov.co			Página activa de DVR HikVision. Es inseguro exponer un DVR a Internet público. Véase la nota sobre este dominio abajo.
11	servsgdoc.imprenta.gov.co	nginx/1.29.1	SI	Página activa de Orfeo.
12	servsgint.imprenta.gov.co			¿Descontinuado? Si es así, no aplica la instalación.
13	suscriptores.imprenta.gov.co	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips	SI	Página activa de Suscriptores.
14	svrpubindc.imprenta.gov.co	GlassFish Server Open Source Edition 4.1.1	SI	Página activa del Diario oficial. Raíz está en blanco, contenido está cargado en la página principal en un iframe desde https://svrpubindc.imprenta.gov.co/diario/.
15	svrsgdf71.imprenta.gov.co			¿Descontinuado? Si es así, no aplica la instalación.
16	tracking.imprenta.gov.co			¿Servicio de tracking de AWS? Si es así, no aplica la instalación.
17	urnavirtual.imprenta.gov.co	nginx/1.29.1	SI	Página activa de "Urna Virtual" (contratación).

Son 9 servicios identificados que requieren la instalación de certificados TLS, 5 servicios posiblemente descontinuados, un DVR que requiere un manejo distinto, y 2 entornos asociados con SaaS que no

requieren la instalación (Wix, Amazon). Hay múltiples servidores web en uso: Nginx, Apache, IIS y Glassfish.

Si se observa algún error u omisión en esta información, por favor informar a SEKINFO por correo.

Nota sobre www.imprenta.gov.co: Este dominio corresponde a la página institucional principal de la Imprenta. Está alojado en Wix, un servicio de "constructor de páginas" que permite la creación de páginas web sin conocimientos técnicos. Este tipo de servicio (SaaS) no permite instalar certificados TLS propios. El servicio automáticamente genera un certificado tipo DV para el dominio. Tampoco se permite cambiar la configuración TLS, pero se considera adecuada la configuración actual de los algoritmos, redirección segura y HSTS.

Nota sobre gpingindc.imprenta.gov.co: Este dominio corresponde a un cortafuegos (u otro tipo de dispositivo de seguridad) de la marca Palo Alto. Es inseguro exponer la interfaz de administración de un cortafuegos u otro dispositivo similar a Internet público. Solo los administradores de sistemas y redes deben tener acceso a esta interfaz administrativa. Exponer la página de inicio de sesión a Internet es un riesgo (vulnerabilidades de día cero, inyección de credenciales, fuerza bruta). El uso de un certificado inválido en Internet aumenta significativamente los riesgos (MiTM, suplantación). Se debe usar una VPN para las conexiones a la interfaz administrativa e instalar un certificado válido.

Nota sobre servprodoc.imprenta.gov.co: Este dominio corresponde a un DVR HikVision (grabador de camaras de seguridad). Es inseguro exponer un DVR a Internet público. Se debe usar una VPN. Se puede instalar un certificado, pero no es estrictamente requerido si se usa una VPN. Si se desea un certificado válido para este dispositivo, se recomienda ponerlo detrás de un proxy reverso como Nginx y asegurar que todas las conexiones entrantes pasen por Nginx. Así se puede instalar un certificado TLS válido en el proxy reverso, e incluso automatizar la renovación en caso de certificados DV. Aún así las ventajas de hacer esta configuración de proxy reverso para un DVR accedido por pocas personas son escasas. Se recomienda poner el DVR en una VPN, sin acceso directo desde Internet, y con esta justificación técnica, seguir usando el certificado integrado si los navegadores permiten agregar una excepción.

Diagnóstico de instalaciones de certificados TLS

#	Dominio	En línea	Tipo validación	SANs	Estado TLS	Redirección segura	HSTS
1	imprenta.gov.co	SI	DV	imprenta.gov.co, www.imprenta.gov.co	OK	SI	SI
2	autodiscover.imprenta.gov.co	SI	OV	*.imprenta.gov.co, imprenta.gov.co	ERROR: Certificado vencido	NO	NO
3	boletines.imprenta.gov.co	SI			ERROR: Fallo de negociación TLS	SI	NO

#	Dominio	En línea	Tipo validación	SANs	Estado TLS	Redirección segura	HSTS
4	catalogodigital.imprenta.gov.co	SI	DV	ambiegresados.com	ERROR: Incompatibilidad de nombre de host	NO	NO
5	facturacion.imprenta.gov.co	SI	DV	*.imprenta.gov.co, imprenta.gov.co	OK	SI	NO
6	gpingindc.imprenta.gov.co	SI	DV		ERROR: Certificado auto-firmado	SI	NO
7	jacevedo.imprenta.gov.co	SI			ERROR: Sin TLS	NO	NO
8	portalinc.imprenta.gov.co	NO					
9	pqrd.imprenta.gov.co	SI	DV	*.imprenta.gov.co, imprenta.gov.co	OK	SI	NO
10	servprodoc.imprenta.gov.co	SI	DV		ERROR: Certificado auto-firmado	NO	NO
11	servsgdoc.imprenta.gov.co	SI	DV	*.imprenta.gov.co, imprenta.gov.co	OK	SI	NO
12	servsgint.imprenta.gov.co	NO					
13	suscriptores.imprenta.gov.co	SI	DV	*.imprenta.gov.co, imprenta.gov.co	ERROR: Cadena inválida	NO	NO
14	svremail.imprenta.gov.co	SI	OV	*.imprenta.gov.co, imprenta.gov.co	ERROR: Certificado vencido	NO	NO
15	svrpubindc.imprenta.gov.co	SI	DV	svrpubindc.imprenta.gov.co	OK	NO	NO

#	Dominio	En línea	Tipo validación	SANs	Estado TLS	Redirección segura	HSTS
16	svrsgdf71.imprenta.gov.co	NO					
17	tracking.imprenta.gov.co	SI	DV	tracking.imprenta.gov.co	OK	NO	NO
18	urnavirtual.imprenta.gov.co	SI	DV	*.imprenta.gov.co, imprenta.gov.co	OK	SI	NO
19	www.imprenta.gov.co	SI	DV	imprenta.gov.co, www.imprenta.gov.co	OK	SI	SI

Se han identificado los siguientes 9 dominios para los cuales se debe instalar el nuevo certificado:

- autodiscover.imprenta.gov.co
- facturacion.imprenta.gov.co
- gpingindc.imprenta.gov.co
- pqrd.imprenta.gov.co
- servsgdoc.imprenta.gov.co
- suscriptores.imprenta.gov.co
- svremail.imprenta.gov.co
- svrpubindc.imprenta.gov.co
- urnavirtual.imprenta.gov.co

Estos 9 dominios representan 8 servicios y 6 entornos (servidores). autodiscover.imprenta.gov.co y svremail.imprenta.gov.co están asociados con el mismo servicio OWA (Outlook) en el mismo servidor. Los tres dominios de facturacion.imprenta.gov.co, servsgdoc.imprenta.gov.co y urnavirtual.imprenta.gov.co están asociados con tres servicios distintos en el mismo servidor (179.1.102.71).

De los 16 dominios observados en línea, 8 presentaban errores con los certificados o con la configuración TLS:

Dominio	Error TLS
autodiscover.imprenta.gov.co	ERROR: Certificado vencido
boletines.imprenta.gov.co	ERROR: Fallo de negociación TLS
catalogodigital.imprenta.gov.co	ERROR: Incompatibilidad de nombre de host

Dominio	Error TLS
gpingindc.imprenta.gov.co	ERROR: Certificado auto-firmado
jacevedo.imprenta.gov.co	ERROR: Sin TLS
servprodoc.imprenta.gov.co	ERROR: Certificado auto-firmado
suscriptores.imprenta.gov.co	ERROR: Cadena inválida
svremail.imprenta.gov.co	ERROR: Certificado vencido

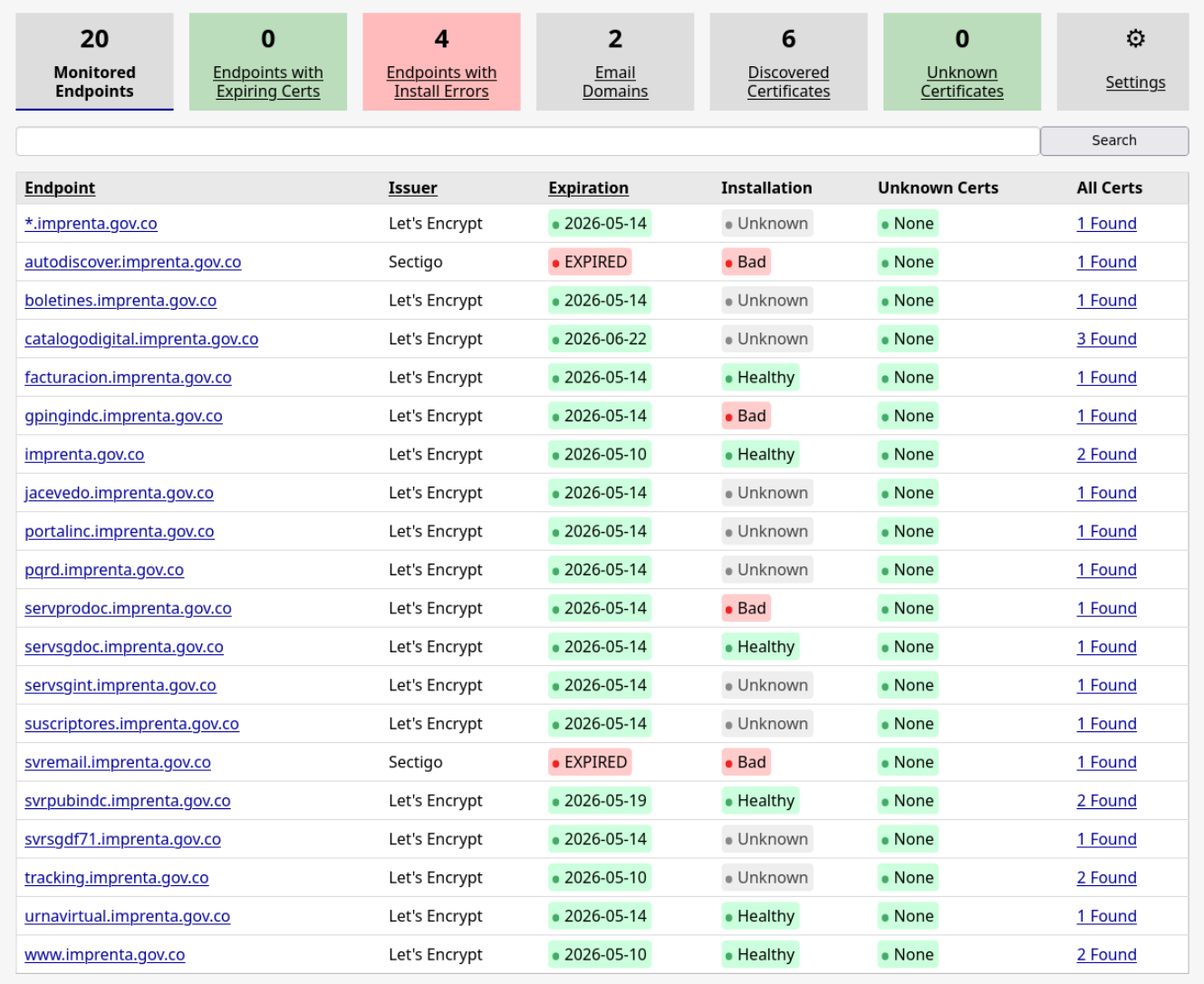
- 2 certificados vencidos
- 2 certificados auto-firmados
- 1 certificado incompatible con el nombre de host
- 1 certificado con una cadena inválida
- 1 servidor con un fallo de negociación TLS
- 1 servidor sin configuración TLS

Esta lista incluye servicios posiblemente descontinuados o inactivos, el DVR y cortafuegos, que no deben estar expuestos a Internet. Para los servicios descontinuados, se deben eliminar los registros DNS correspondientes y cerrar los puertos (80, 443, posiblemente otros).

CAA: Así mismo se debe configurar CAA en la configuración DNS que aplica al dominio y a todos los subdominios y que permite prevenir la suplantación. Actualmente CAA no está configurado.

Anexo 1: Resultado de escaneo de vulnerabilidades en la configuración TLS

A continuación se presentan los resultados detallados de realizar un escaneo de los certificados y configuración TLS.



20 Monitored Endpoints	0 Endpoints with Expiring Certs	4 Endpoints with Install Errors	2 Email Domains	6 Discovered Certificates	0 Unknown Certificates	⚙ Settings

Search

Endpoint	Issuer	Expiration	Installation	Unknown Certs	All Certs
*.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
autodiscover.imprenta.gov.co	Sectigo	EXPIRED	Bad	None	1 Found
boletines.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
catalogodigital.imprenta.gov.co	Let's Encrypt	2026-06-22	Unknown	None	3 Found
facturacion.imprenta.gov.co	Let's Encrypt	2026-05-14	Healthy	None	1 Found
gpingindc.imprenta.gov.co	Let's Encrypt	2026-05-14	Bad	None	1 Found
imprenta.gov.co	Let's Encrypt	2026-05-10	Healthy	None	2 Found
jacevedo.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
portalinc.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
pqrd.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
servprodoc.imprenta.gov.co	Let's Encrypt	2026-05-14	Bad	None	1 Found
servsgdoc.imprenta.gov.co	Let's Encrypt	2026-05-14	Healthy	None	1 Found
servsgint.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
suscriptores.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
svremail.imprenta.gov.co	Sectigo	EXPIRED	Bad	None	1 Found
svrpubindc.imprenta.gov.co	Let's Encrypt	2026-05-19	Healthy	None	2 Found
svrsgdf71.imprenta.gov.co	Let's Encrypt	2026-05-14	Unknown	None	1 Found
tracking.imprenta.gov.co	Let's Encrypt	2026-05-10	Unknown	None	2 Found
urnavirtual.imprenta.gov.co	Let's Encrypt	2026-05-14	Healthy	None	1 Found
www.imprenta.gov.co	Let's Encrypt	2026-05-10	Healthy	None	2 Found

Figura 1: Resumen de los 19 dominios encontrados. El gráfico muestra 20 debido a que hay una línea para “*.imprenta.gov.co”. Muestra 4 dominios con errores, hay otros 4 que tienen errores de otro tipo que aparecen como “Unknown” (desconocido).

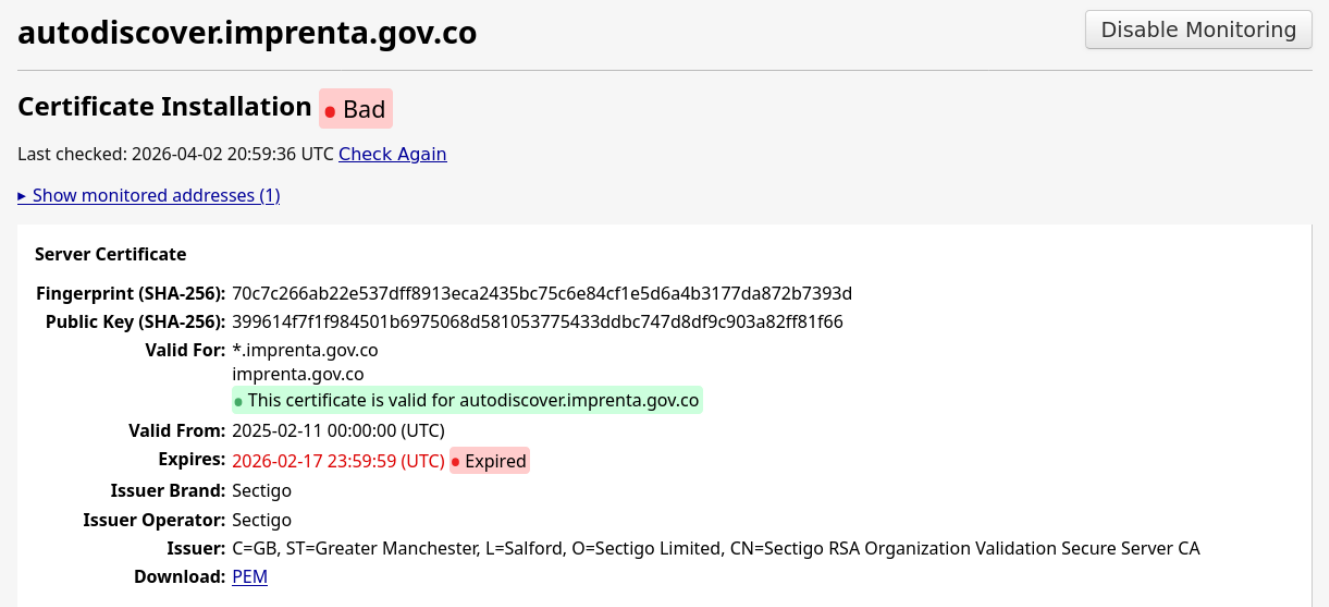


Figura 2: Detalle del error en autodiscover.imprenta.gov.co: certificado vencido

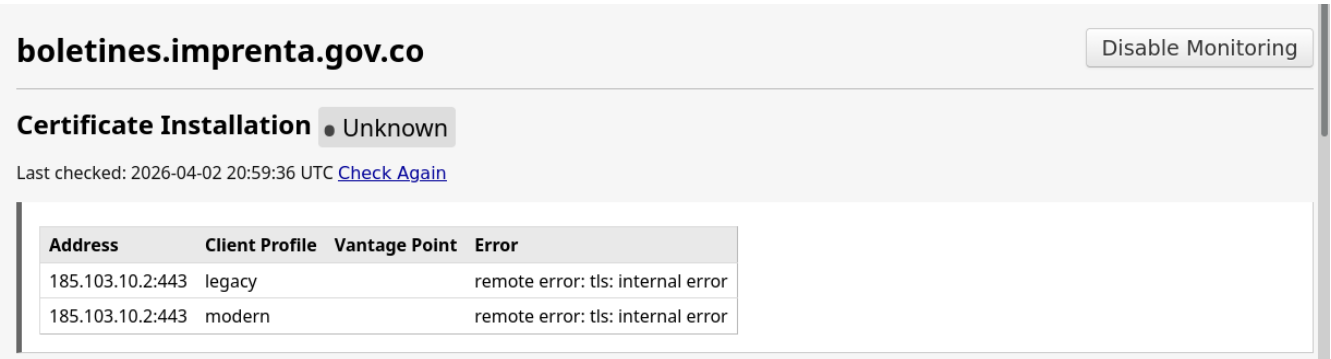


Figura 3: Detalle del error en boletines.imprenta.gov.co: “tls internal error” (fallo de negociación TLS)

Figura 4: Detalle del error en catalogodigita.imprenta.gov.co: incompatibilidad con el nombre de host, solo válido para “ambiegresados.com”.

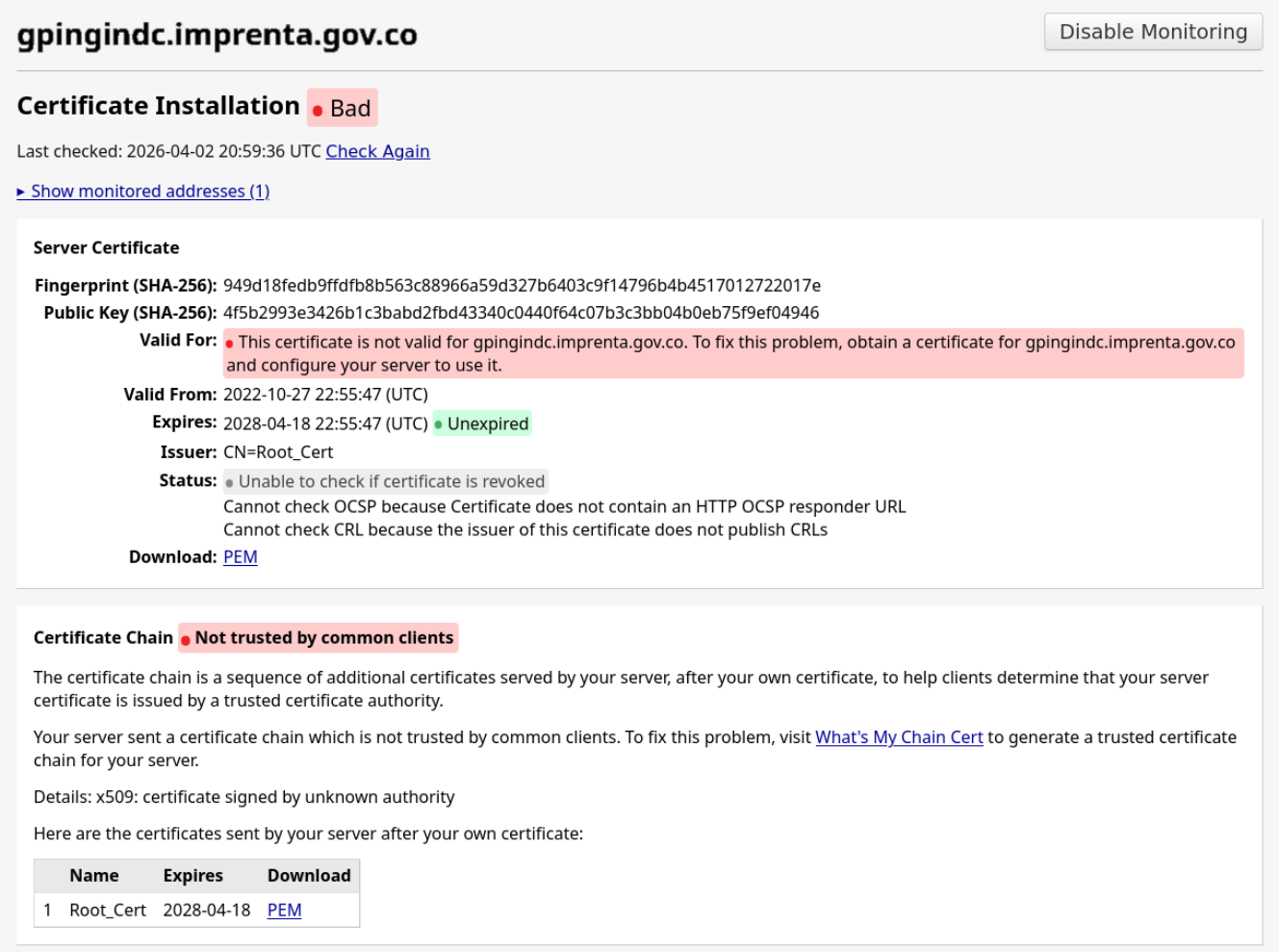


Figura 5: Detalle del error en gpingindc.imprenta.gov.co: certificado auto-firmado (cortafuegos Palo Alto)

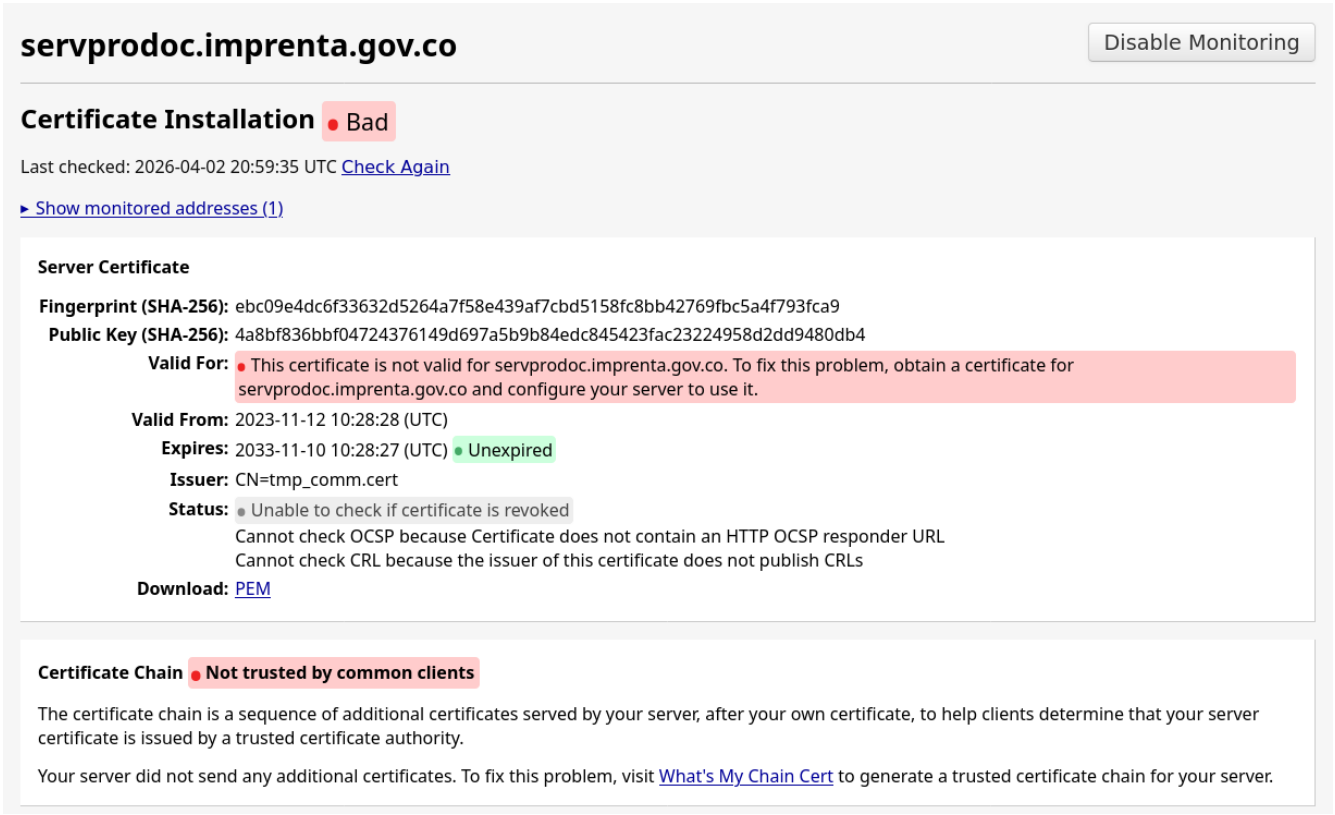


Figura 6: Detalle del error en servprodoc.imprenta.gov.co: certificado auto-firmado (DVR HikVision)

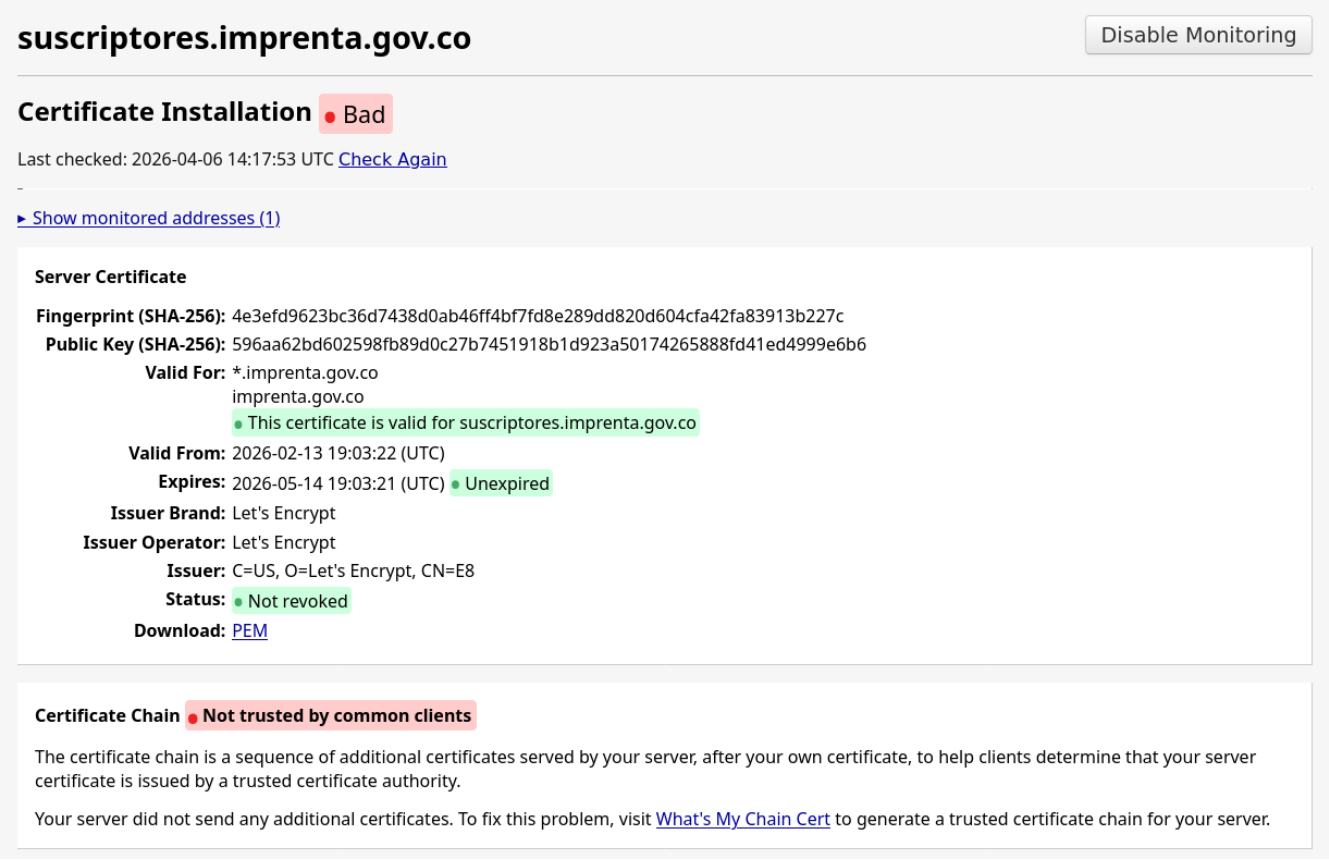


Figura 7: Detalle del error en suscriptores.imprenta.gov.co: cadena de certificados inválida

Anexo 2: Captura de pantalla de los sitios encontrados

Cómo referencia, se presentan capturas de pantalla de los sitios encontrados asociados con los dominios de imprenta.gov.co.

No fue posible visualizar los siguientes 3 dominios:

- portalinc.imprenta.gov.co
- servsgint.imprenta.gov.co
- svrsgdf71.imprenta.gov.co

Estos dominios no responden a solicitudes http:// ni https://.

Figura 8: imprenta.gov.co, www.imprenta.gov.co (ambos se refieren al entorno de Wix)

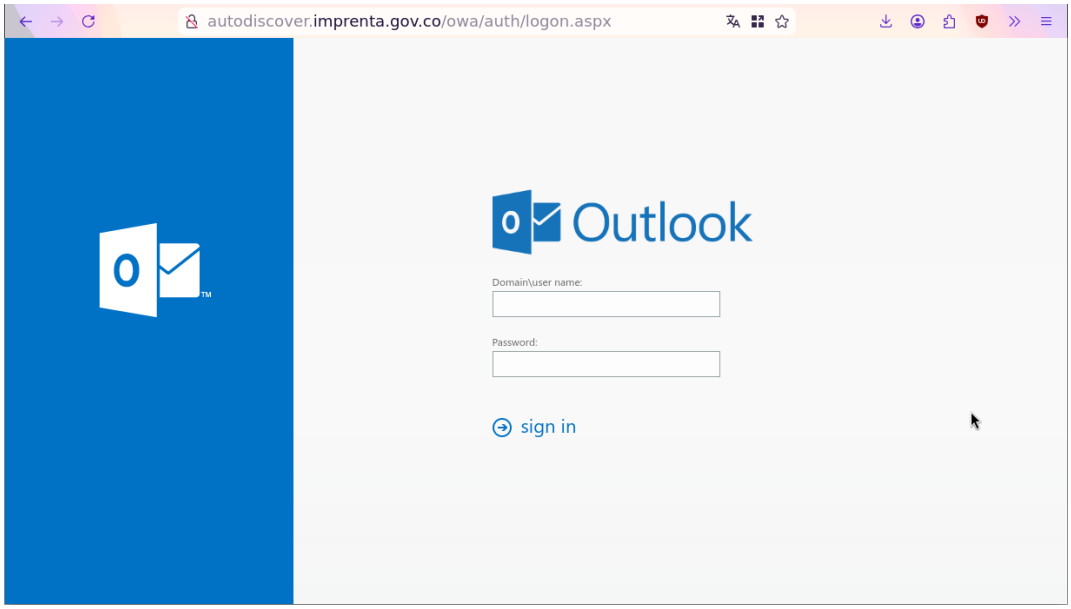


Figura 9: autodiscover.imprenta.gov.co, svremail.imprenta.gov.co (los dos dominios se refieren al mismo servicio)

Figura 10: boletines.imprenta.gov.co

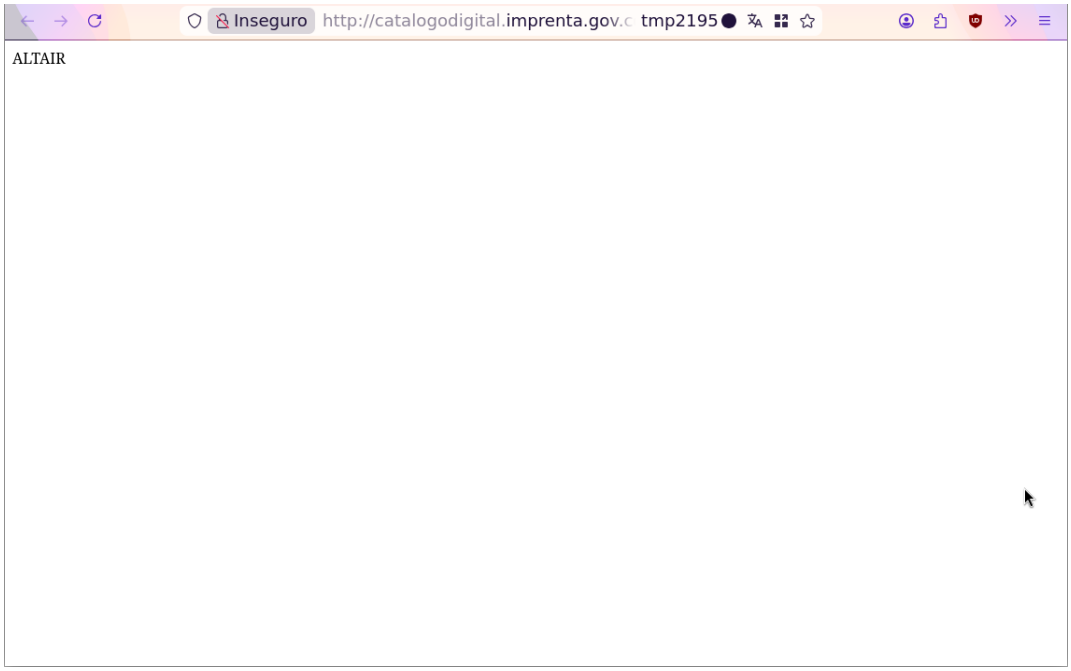


Figura 11: catalogodigital.imprenta.gov.co

Figura 12: facturacion.imprenta.gov.co

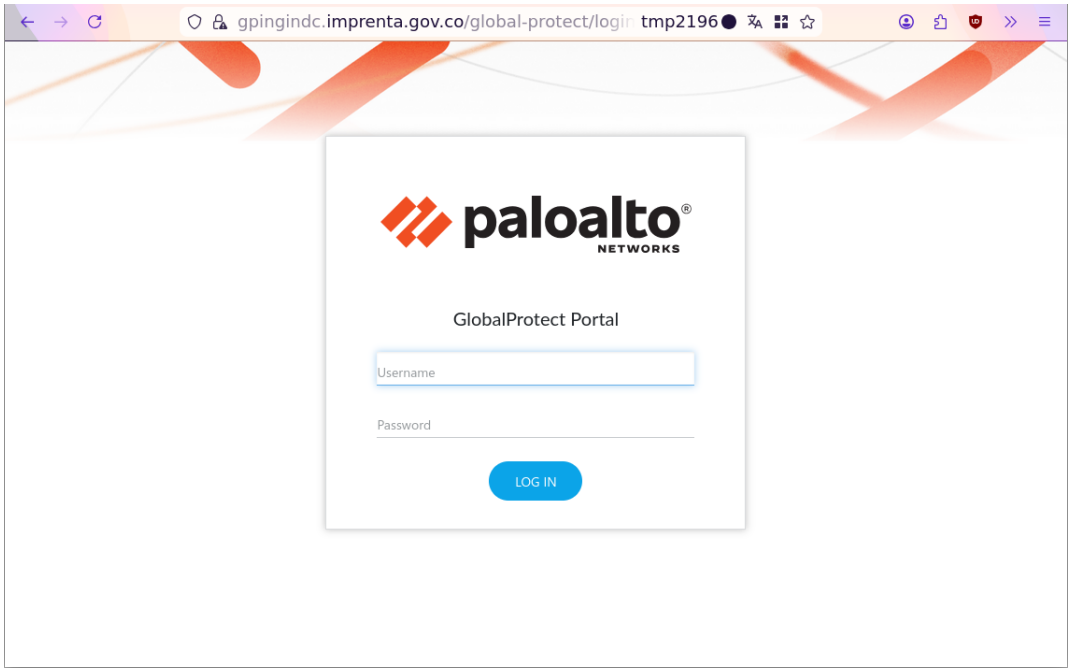


Figura 13: gpingindc.imprenta.gov.co

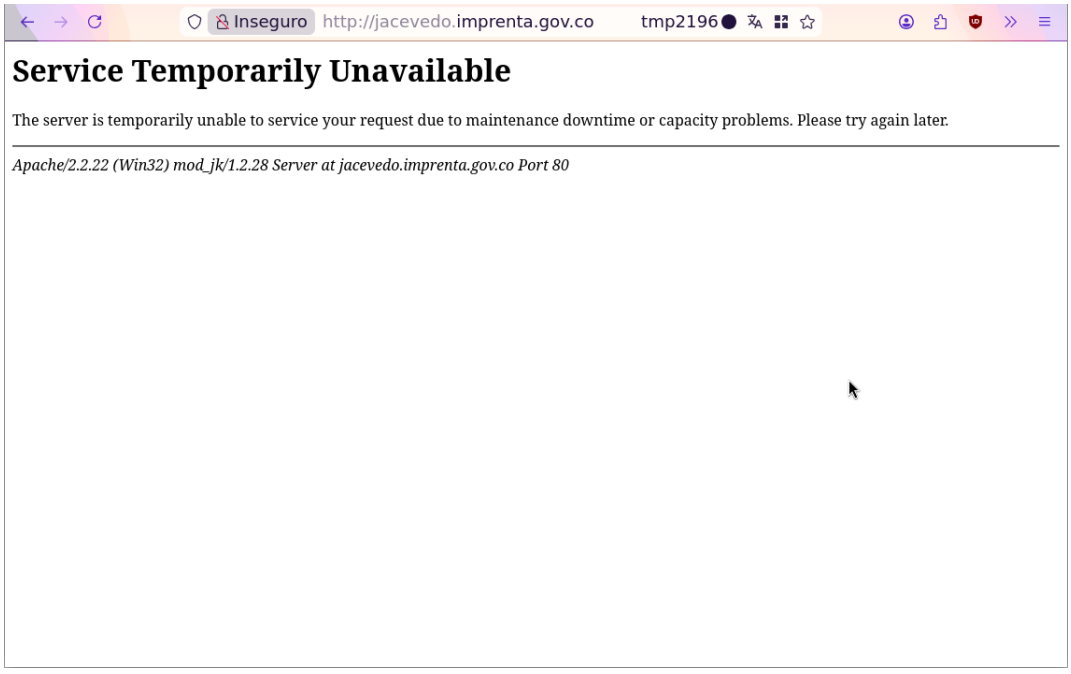


Figura 14: jacevedo.imprenta.gov.co

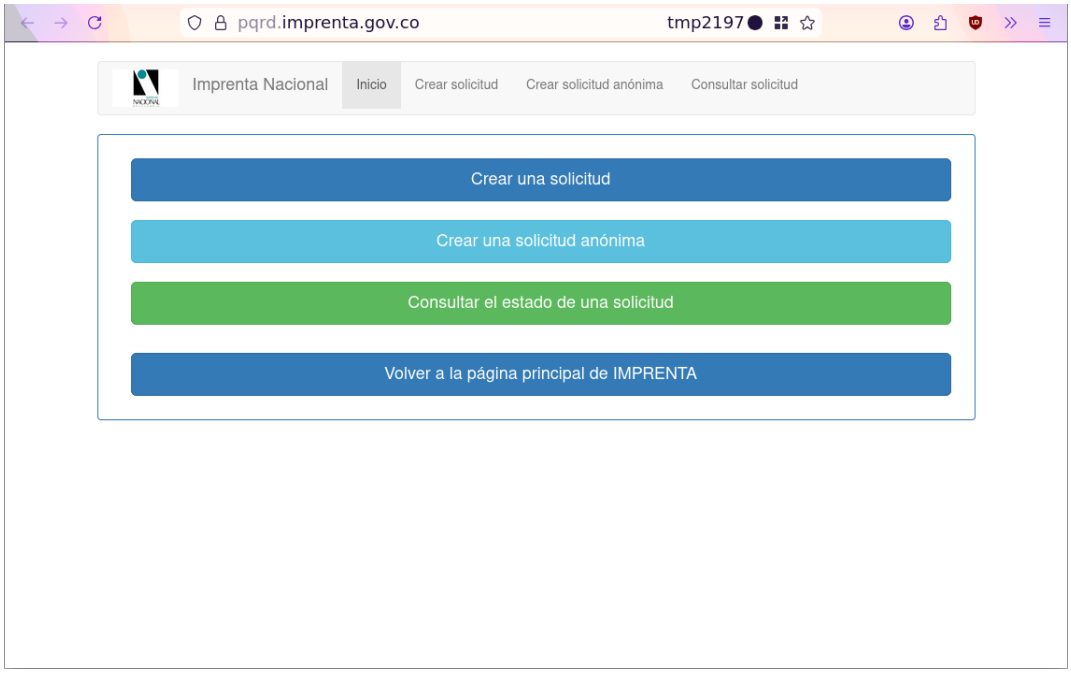


Figura 15: pqrd.imprenta.gov.co

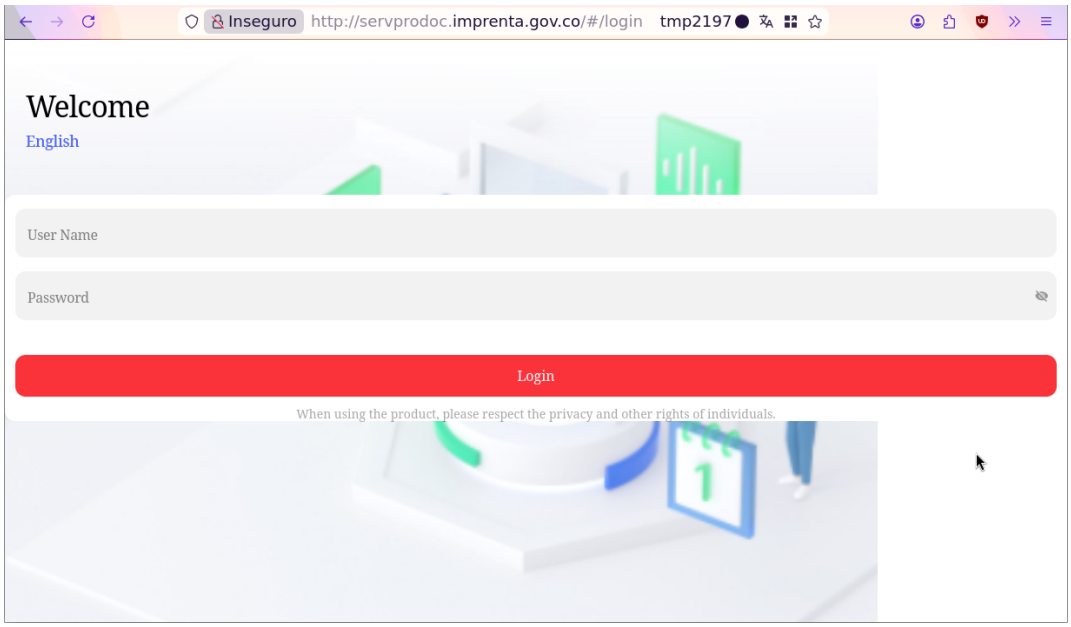


Figura 16: servprodoc.imprenta.gov.co

Figura 17: servsgdoc.imprenta.gov.co

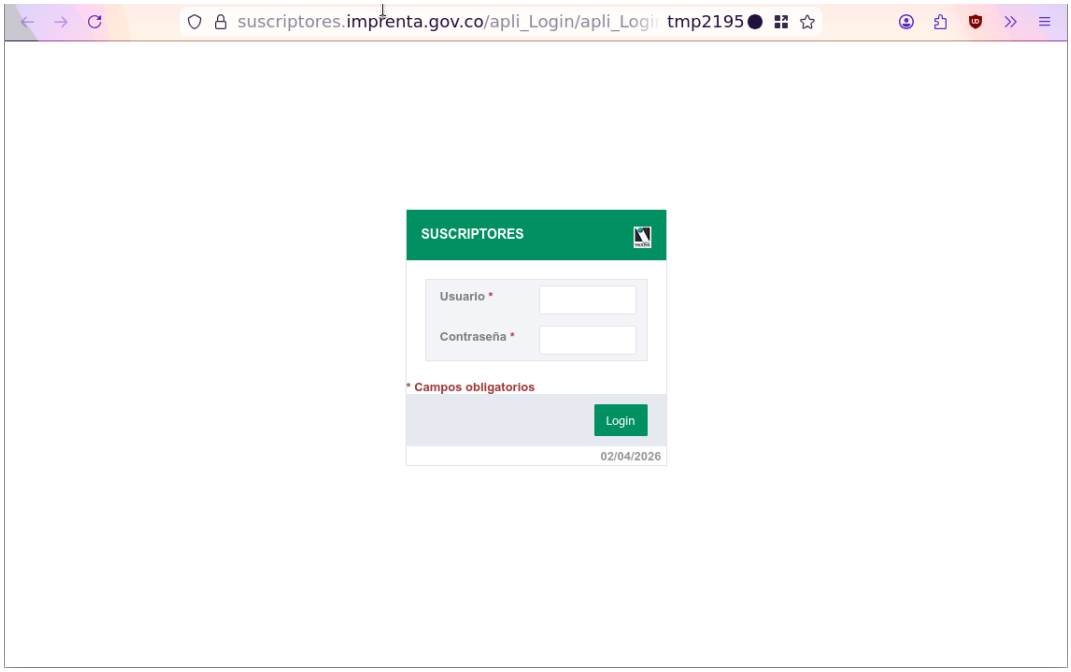


Figura 18: suscriptores.imprenta.gov.co

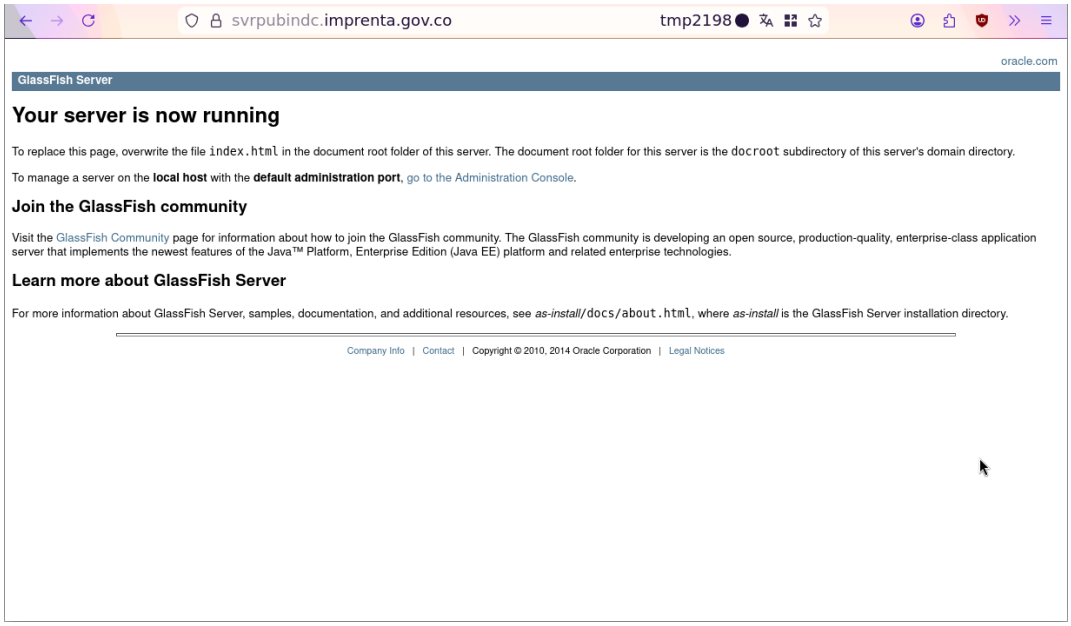


Figura 19: svrpubindc.imprenta.gov.co

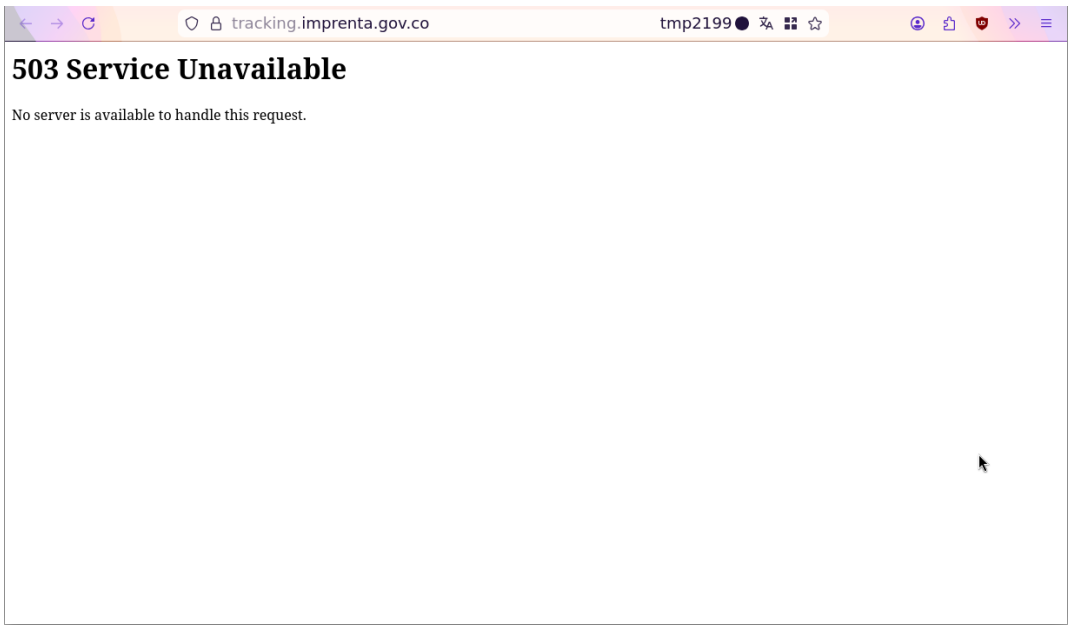


Figura 20: tracking.imprenta.gov.co

Figura 21: urnavirtual.imprenta.gov.co,

Anexo 3: Glosario

Certificados y Seguridad

- **Autenticidad:** Propiedad que verifica que los datos o la entidad son genuinos y provienen de la fuente declarada.
- **CA (Autoridad de Certificados)**: Entidad responsable de emitir y revocar certificados digitales. Verifica el control de dominio de los solicitantes y firma sus certificados para que los navegadores web los reconozcan como confiables. A nivel mundial hay alrededor de 150 CAs de nivel raíz y varios miles de nivel intermedio. Las principales CAs raíces forman parte del CA/Browser Forum, el cual define los requerimientos para la emisión de los certificados. La CA líder es Let’s Encrypt, una organización sin ánimo de lucro respaldada por la ISOC, EFF, Mozilla, Google y Amazon, que provee certificados TLS sin costo a través del protocolo de automatización ACME.
- **CA/Browser Forum:** Consorcio de nivel mundial formado por las CAs y productores de los navegadores web. Establece las “Directrices de Práctica de Certificación” (CP/CPS) que definen los estándares de seguridad, validación y requisitos técnicos que deben cumplir todas las CAs para emitir certificados reconocidos de forma segura por los navegadores modernos.
- **CAA (“Certification Authority Authorization”):** Registro DNS que especifica cuales CAs están autorizadas para emitir certificados con un dominio.
- **Certificado TLS:** Documento digital en formato X.509 que vincula una llave criptográfica con la identidad de una entidad (sitio web, servidor o servicio), permitiendo encriptar la comunicación y autenticar la identidad del servidor ante el cliente mediante el protocolo TLS.
- **Confidencialidad:** Propiedad que garantiza que la información solo sea accesible para usuarios o sistemas autorizados.
- **DV (“Domain Validation”):** Proceso de validación de certificados que verifica únicamente el control del dominio. Es el tipo de certificado estándar y más usado por las empresas más destacadas de Internet como Google y Amazon. Se puede automatizar la renovación utilizando el protocolo ACME.
- **EV (“Extended Validation”):** Proceso de validación que verifica la identidad legal de la entidad

propietaria del sitio. Significativamente más costoso que los certificados estándares sin ninguna ventaja técnica.

- **Fuerza bruta:** Tipo de ataque que intenta adivinar credenciales probando todas las combinaciones posibles.
- **Hackeo:** Acceso no autorizado a sistemas informáticos, usualmente con fines maliciosos como la ciberextorsión.
- **HSTS ("HTTP Strict Transport Security"):** Directiva de seguridad que obliga a los navegadores a usar solo conexiones HTTPS, previniendo ataques de degradación ("downgrade").
- **Integridad:** Propiedad que asegura que los datos no han sido alterados o modificados de forma no autorizada.
- **Inyección de credenciales ("credential stuffing"):** Tipo de ataque muy común que intenta obtener acceso probando credenciales robadas (nombres de usuario y contraseñas) de forma masiva. Los ataques de este tipo son posibles porque muchos usuarios reutilizan la misma combinación de nombre de usuario y contraseña en múltiples sitios.
- **Llave privada TLS:** Parte secreta del par de llaves criptográficas TLS (privada/pública) generada en el servidor. Es fundamental para descifrar los datos recibidos del cliente y firmar las solicitudes de certificado (CSR); su pérdida o robo compromete totalmente la seguridad del sitio, por lo que debe guardarse estrictamente en el servidor y nunca compartirse.
- **Llave pública:** Parte de un par de llaves criptográficas usada para encriptar datos o verificar firmas, y que puede ser compartida.
- **Logs CT ("Certificate Transparency Logs"):** Registros públicos, inmutables y de solo lectura donde todas CAs deben registrar los certificados que emiten. Su función es permitir a cualquier persona auditar la emisión de certificados para detectar emisiones no autorizadas o fraudulentas.
- **Monitoreo de logs CT:** Servicio o proceso de supervisión automatizada de los registros CT para detectar y notificar inmediatamente si se emiten certificados para dominios propios sin el conocimiento del administrador, o si aparecen certificados emitidos para dominios desconocidos, lo cual podría indicar un intento de suplantación o error por parte de una CA.
- **MitM ("Man-in-the-Middle"):** Ataque donde un tercero intercepta y posiblemente altera la comunicación entre dos partes sin que estas lo sepan.
- **OV ("Organization Validation"):** Proceso de validación sencilla que verifica la existencia legal de la organización solicitante del certificado, típicamente con una llamada telefónica. Significativamente más costoso que los certificados estándares sin ninguna ventaja técnica.
- **Renovación automática:** Proceso programado para extender la vigencia de un certificado sin intervención manual. El protocolo usado de forma estándar es ACME.
- **Suplantación de certificados:** Creación de un certificado falso para imitar a uno legítimo y engañar a los usuarios.
- **Suite de cifrado ("cipher suite"):** Conjunto de algoritmos utilizados por un protocolo (como TLS) para encriptar datos, negociar llaves y autenticar.
- **SSL**: Protocolo descontinuado de comunicaciones seguras. TLS es el reemplazo moderno para SSL. SSL fue oficialmente descontinuado por los navegadores web en los años 2014 y 2015 debido al descubrimiento de vulnerabilidades graves de seguridad. De forma coloquial muchos siguen refiriéndose a los certificados TLS como certificados SSL, siendo ambos documentos digitales del formato X.509.
- **TLS (Transport Layer Security):** Protocolo criptográfico diseñado para proporcionar comunicaciones seguras a través de las redes de datos con las propiedades de autenticación, confidencialidad y integridad. TLS es la base fundamental de las comunicaciones seguras en las redes de datos, y su uso abarca prácticamente todos los sitios web y servicios disponibles en Internet.
- **Vulnerabilidades de día cero:** Fallos de seguridad desconocidos por el proveedor y para los cuales aún no existe un arreglo. Una vez que la información sobre las vulnerabilidades de día cero empieza a circular por Internet, los actores maliciosos escanean por servidores vulnerables para identificar

objetivos de hackeo. La mejor forma de protegerse en contra de los ataques con vulnerabilidades de día cero es **"no dar papaya"**, es decir minimizar la exposición del software a atacantes en Internet en primer lugar, por ejemplo usando una VPN para el acceso a los servicios internos en lugar de disponerlos a través de una dirección pública en Internet.

- **Vigencia:** Período de tiempo durante el cual un certificado digital se considera válido. El CA/Browser Forum ha definido un proceso para reducir la vigencia máxima de los certificados paulatinamente: 200 días a partir de marzo 2026, 100 días en 2027 y 47 días en 2029. El motivo por la reducción es limitar los daños causados por la vulneración de llaves privadas y la mala emisión de certificados, también promover la automatización. Muchas organizaciones no están preparadas para estos cambios obligatorios y siguen intentando implementar procesos manuales con procesos de validación que no permiten la automatización. El resultado de esta falta de acoplarse a los nuevos requerimientos sobre la vigencia de certificados es un aumento en la frecuencia de incidentes de sitios con certificados vencidos o improvisados, más desgaste administrativo y mayores costos económicos para implementar procesos manuales para la renovación e instalación y también pagar los costos adicionales significativos de la validación OV/EV.
- **X.509:** Estándar internacional que define el formato de los certificados digitales. Especifica los campos obligatorios (como el nombre del sujeto, la autoridad emisora, la validez temporal y la firma digital) que permiten la autenticación y el cifrado en protocolos seguros como TLS, y antiguamente SSL.

Infraestructura y Redes

- **archivo de zona DNS ("DNS zone file"):** Archivo de texto que contiene los registros DNS necesarios para resolver nombres de dominio a direcciones IP. Frecuentemente se gestiona este archivo a través de un servicio DNS o en la plataforma del registrador del nombre de dominio.
- **ASN ("Autonomous System Number"):** Número único que identifica a una red o conjunto de redes en Internet. Usado para asociar un operador con una dirección IP.
- **BGP ("Border Gateway Protocol"):** Protocolo utilizado para intercambiar información de enrutamiento entre redes autónomas en Internet.
- **Cortafuegos:** Dispositivo de seguridad de red (físico o virtual) diseñado para monitorear y controlar el tráfico entrante y saliente mediante reglas de seguridad que define el administrador del dispositivo, frecuentemente con el propósito de bloquear el acceso no autorizado.
- **DNS ("Domain Name System"):** Sistema que traduce nombres de dominio legibles (ej. sekinfo.org) a direcciones IP numéricas.
- **Dirección IP ("Internet Protocol"):** Dirección numérica única asignada a cada dispositivo conectado a una red.
- **DVR ("Digital Video Recorder"):** Dispositivo electrónico que graba y almacena video digital, comúnmente usado en sistemas de cámaras de seguridad.
- **SaaS ("Software as a Service"):** Modelo de distribución de software donde las aplicaciones son alojadas por un proveedor y accesibles vía una página web.
- **VPC ("Virtual Private Cloud"):** Red virtual aislada dentro de una nube pública donde se despliegan infraestructuras como si fueran en una red privada física.
- **VPN ("Virtual Private Network"):** Software que crea una conexión segura y encriptada a través de una red menos segura (como Internet). Frecuentemente usado para dar acceso a los servicios de red internos al personal que trabaja remotamente.
- **VPS ("Virtual Private Server"):** Servidor virtual privado alojado en un servidor compartido. La virtualización garantiza una separación fuerte entre los distintos entornos y usuarios. También llamado "servidor de nube".

Sistemas Operativos y Software

- **Apache:** Servidor web de software libre.
- **CentOS:** Distribución de Linux de software libre derivada de RHEL.
- **Debian:** Distribución de Linux de software libre.
- **Entorno:** Configuración específica de servidor, software o plataforma (física, virtual o SaaS) donde se ejecuta una aplicación.
- **GlassFish:** Servidor de aplicaciones de software libre para la plataforma Java EE.
- **IIS (“Internet Information Services”):** Servidor web de Microsoft para sistemas Windows. Poco usado para servidores web en Internet en contextos profesionales, aunque es requerido para ciertos servicios de red de Microsoft como Exchange o OWA.
- **JavaScript:** Lenguaje de programación utilizado principalmente para implementar una interfaz de usuario dinámica en las páginas web.
- **Linux:** El núcleo (kernel) que sirve como la base para muchos sistemas operativos de software libre.
- **Nginx:** Servidor web de alto rendimiento y proxy reverso de software libre.
- **OWA (“Outlook Web Access”):** Interfaz web para acceder al correo y calendario de Microsoft Exchange.
- **Red Hat Enterprise Linux (RHEL):** Distribución de Linux comercial y empresarial.