CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"Uso Interno"**.
El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.
No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO.

Asegurar todo tipo de conexiones cifradas entre un navegador u ordenador de un usuario y un servidor o un sitio web de la infraestructura del grupo Keralty.

2. ALCANCE.

Proteger las páginas web del grupo Keralty mediante los certificados digitales para garantizar la conexión segura y transferencias de datos.

3. DEFINICIONES

SSL: Secure Sockets Layer. Es una tecnología estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web (o entre dos servidores web), protegiendo así la conexión. Esto impide que un hacker pueda ver o interceptar la información que se transmite de un punto a otro, la cual puede contener datos personales o financieros.

HTTPS: Hypertext Transfer Protocol Secure. Al principio de la dirección (URL) de un sitio web, identifica que el sitio está protegido por un certificado SSL o TLS. En la barra de direcciones del navegador muestra un candado y, al dar clic sobre ese icono, deja ver los datos del certificado, la autoridad emisora y el nombre de la empresa dueña del sitio web.

TLS: Transport Layer Security. Versión actualizada y más segura de SSL. Sin embargo, seguimos relacionado a los certificados de seguridad cómo “certificados SSL”, utilizando la tecnología TLS más moderna que entrega confianza.

Wildcard SSL: Secure Unlimited Subdomains. Un tipo universal del certificado SSL que permite asegurar todos los subdominios bajo un dominio principal.

Cifrado 256 bits. Proceso mediante el cual se cifra un documento electrónico utilizando un algoritmo cuya clave tiene una longitud de 256 bits. Cuanto más larga sea esta clave, más segura es.

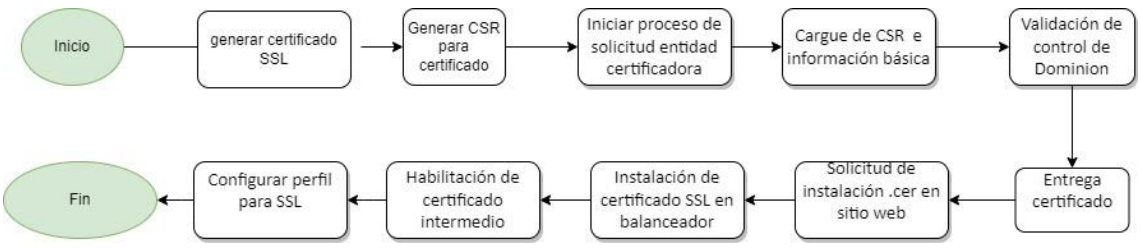
Servidor: Un **servidor** es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.

Componentes de infraestructura TI: Estos elementos incluyen el hardware, el software, los elementos de red, un sistema operativo (SO) y el almacenamiento de datos. Todos ellos se utilizan para ofrecer servicios y soluciones de **TI**.

4. CONTENIDO.

Proteger las páginas web del grupo Keralty mediante la tecnología SSL o TLS. Para asegurar la conexión de un servidor seguro, este último se autentica ante el usuario, y el navegador web cifra mediante el protocolo SSL toda la información que transmite el usuario antes de enviarla a través de Internet. De este modo, solo el sitio web que solicitó la información puede descifrarla.

5. FLUJO DEL PROCEDIMIENTO



6. DETALLE DEL PROCEDIMIENTO

Instalación de certificado: Es el proceso de instalación del certificado SSL.

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Identificación de la necesidad	Se identifica la necesidad de adquisición y/o renovación de certificado por parte de las áreas de negocio a través de las siguientes vías: a. Requerimiento de seguridad de la información. b. Herramienta de monitoreo de seguridad c. Necesidad de proyecto y/o negocio.	a y b Gerencia corporativa de seguridad de la información Otras Gerencias de VGSI	Correo electrónico
2	Solicitar certificado nuevo y/o renovación	Se solicita a la Dirección administrativa de la VGSI la adquisición y/o renovación de nuevo certificado.	Gerente corporativo de TI	Correo
3	Escalar a proveedor de Certificados la necesidad		Dirección administrativa de la VGSI	Correo
4	Generar csr	Obtener comando desde la herramienta de digicert para la generación de la llave privada como la solicitud de la firma de certificado de la por medio de openSSL	Administrador de sistemas	Generacion .key y .csr

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
5	Iniciar proceso de solicitud	Autenticarse en la página de digicert e ir a la pestaña de certificados y escoger el tipo de certificado a tramitar.	Administrador de sistemas	
6	Cargue de CSR e información básica	Cargar el texto generado en el paso 1, Asignar organización, seleccionar método de validación de control del dominio (Correo electrónico, registro DNS TXT, registro DNS CNAME o demostración práctica de http)	Administrador de sistemas	Generación número de pedido
7	Validación de control de Dominion	solicitar al proveedor de DNS la publicación del registro DNS TXT en el dominio para la confirmación por parte de digicert	Administrador de Sistemas y proveedor DNS	Generación ticket
8	Entrega y/o descarga de certificado	Una vez validada la información , el proveedor entrega vía correo o descarga de la plataforma el certificado tramitado	Digicert	habilitación de certificado
9	Solicitud de instalación .cer en sitio web	Entrega de certificado y llave privada al proveedor de plataformas de waf y balanceadores	Administrador de Sistemas	generación ticket
10	Instalación de certificado	- Inicie la GUI web F5 BIGIP. - En Tráfico local, seleccione "Certificados SSL".	Administrador de plataforma	Archivo de certificado ssl instalado

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
	SSL en balanceador	- Haga clic en el nombre que asignó al certificado en "Propiedades generales" al crear la CSR. - Busque el archivo your_domain_name.crt que recibió de DigiCert. - Haz clic en "Abrir" y luego en "Importar".		
11	Habilitación de certificado intermedio	- En la GUI web, seleccione "Tráfico local", luego "Certificados SSL" y luego "Importar". - En "Tipo de importación", elija Certificado, luego "Crear nuevo". - Ingrese "DigiCertCA" como su nombre de certificado. - Busque el archivo DigiCertCA.crt que recibió de DigiCert, haga clic en "Abrir" y luego en "Importar".	Administrador de plataforma	importación de certificado intermedio

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
12	Configurar perfil para SSL	- Cree o abra el perfil SSL que usará con este certificado. - Inicie sesión en la utilidad de configuración > Tráfico local > Perfiles > Cliente (desde el menú SSL), luego seleccione el cliente para configurar y elija "Avanzado" en el menú Configuración. - Seleccione el certificado SSL (par de clave pública/privada) que instaló al principio de estas instrucciones. - En la sección "Cadena", busque el archivo "DigiCertCA" que importó en el paso anterior, luego guarde y salga de la configuración.	Administrador de plataforma	habilitación de certificado en el sitio web

Tabla 1 Detalle del Procedimiento

7. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
01/10/2022	Creación documento	1.0
3/10/2023	Validación de Contenido	2.0
22/11/2024	El documento se revisa en el marco de la actualización del SGSI año 2024, se valida con el responsable del documento quien nos informa que a la fecha no existe ningún cambio en el contenido de este, se realiza inclusión de la sigla del país y la compañía en el código del documento	2.1

Tabla 2 Control de Cambios

8. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jairo Arley Zamudio Área/Proceso: Operaciones TI Fecha:01/10/2022	Nombre: Luisa Gineth Castaño Área/Proceso: Director Operación y Comunicaciones TI Fecha:22/11/2024	Nombre: Luisa Gineth Castaño Área/Proceso: Director Operación y Comunicaciones TI Fecha:22/11/2024

Tabla 3 Flujo de Aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.