UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE ELECTRÓNICA

Asignatura:	**Diseño de sistemas de seguridad en redes de datos**	Código:	**DSS101**
Grupos:	**01L y 02L**	Ciclo / año:	**02 - 2025**

CASO DE ESTUDIO #2

"Uso de Certificado Digital y PGP para el aseguramiento de sitios WEB y Correo Electrónico"

Condiciones de realización:

Fecha de Entrega:	**1 – 6 de septiembre 2025 (Semana 10)**
Porcentaje:	15% de la nota de laboratorio
Forma de Entrega:	Demostración de funcionamiento de la solución durante la sesión de laboratorio o por un video demostrativo.
Grupos:	4 personas

Descripción de la actividad:

De acuerdo con la figura 1, los estudiantes implementaran los sistemas de seguridad en un sitio WEB, utilizando un certificado digital generado por el servidor CA y un sistema de envío seguro de correo electrónico entre dos cuentas, se implementará las funciones de cifrado y firma digital utilizando el Protocolo PGP (Pretty Good Privacy) para la protección del mensaje por correo electrónico. En escenario podrá ser presentado en máquinas virtuales o contenedores.

Los puntos a evaluar son los siguientes:

1. Implementar una Autoridad Certificadora (CA) Raíz, sobre un Sistema Operativo Linux.
2. Implementar un Servidor Web seguro (HTTPS), donde el certificado digital utilizado por el servidor deberá ser emitido por la Autoridad Certificadora Raíz que fue creada en el numeral anterior, se realizaran pruebas desde un cliente hacia la página WEB. En este servidor se generará una solicitud de firma (CRS) para luego ser firmado por la CA.
3. Configurar el servidor de correo electrónico con cuentas de usuario, se utilizarán dos clientes con sus respectivas cuentas de usuario donde se implementarán el criptosistema basado en PGP.
4. Preguntas del instructor.

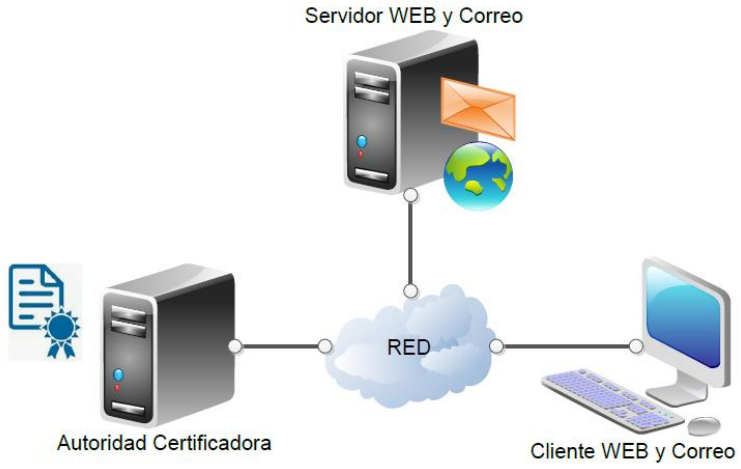

Figura 1. Escenario a implementar.

Lista de estimación:

Actividad	Criterio	Porcentaje (%)	Puntaje (0-10)
Servidor CA	Instala y configura la Autoridad Certificadora (CA).	10	
	Genera llaves y certificado del CA	10	
	Generación del certificado WEB mediante la solicitud de firma (CRS).	20	
Servidor web	Instala el certificado en el servidor WEB	10	
	Prueba desde un cliente al acceder al sitio WEB seguro desde un navegador web. Se muestran los detalles del certificado en el navegador web del cliente. Se debe evidenciar el cifrado de la información en el canal de comunicación por medio de un sniffer	15	
Servicio de correo electrónico seguro por PGP	Funcionamiento del servidor de correo, el servidor es accesible desde la red local y contiene cuentas de usuario (dos cuentas como mínimo).	10	
	Configuración de los clientes de correo electrónico con sus respectivas cuentas.	10	
	Se encriptan los correos electrónicos utilizando PGP entre cuentas de correo. (Se evidencia el intercambio de llaves públicas, cifrado, descifrado y firma digital).	15	
		Promedio	