Programación Segura

Adarely Lucero Cortes Santamaria

Gerardo de Jesus Lobato Zapata

Proyecto Final

13 de julio de 2020

Introducción

El proyecto final de la Experiencia Educativa Programación Segura, consiste en desarrollar una plataforma que permita la administración segura de servidores a través de tecnologías web. La plataforma permite a administradores de servidores monitorizar servidores asociados a ellos y crear conexiones remotas a los mismos, todo a partir de una interfaz Web.

Esta plataforma cuenta con dos roles que se mencionan a continuación:

ROL Administrador global:

El administrador global es capaz de administrar tanto servidores como administradores. Esto es, el puede registrar, actualizar y eliminar un servidor o un administrador. También el administrador global puede hacer asociaciones entre un administrador y servidores.

ROL Administrador de servidores:

El administrador de servidores podrá monitorizar los servidores que se hayan asociado a él, lo que puede monitorizar de cada servidor es la porcentaje de uso de memoria, porcentaje de uso de procesador y el porcentaje de uso de disco. Además de que también podrá conectar al servidor con una terminal a través de la misma interfaz web.

Requerimientos

Por parte del administrador global

El sistema web deberá de contar con un inicio de sesión, el cual cuenta con doble autenticación, y una vez que se autentica podrá tener acceso a las demás páginas. Las páginas a las que el administrador global tiene acceso son las siguientes:

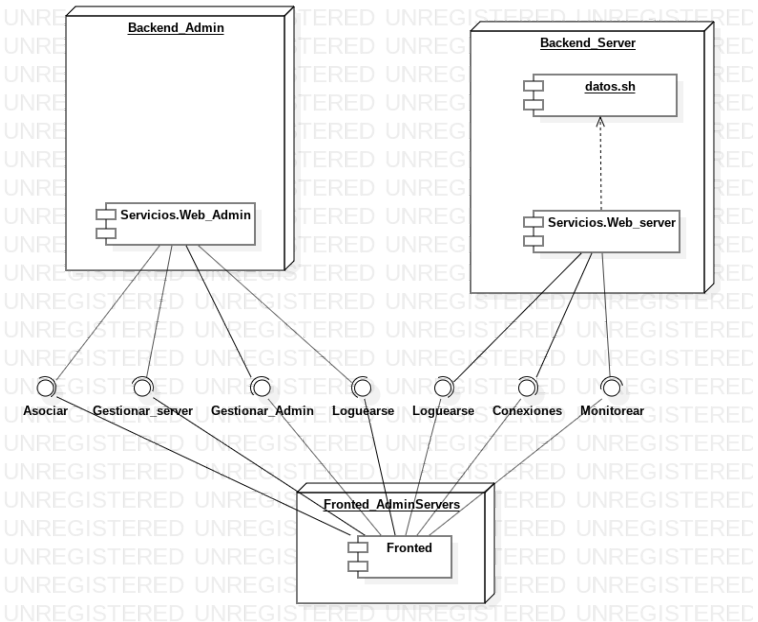
- **Página de inicio:** Esta página cuenta con cuatro botones los cuales nos manda a las páginas de registro y de listado de administradores y servidores.
- **Página de registro de administradores:** Para registrar a un administrador debemos tener el nombre de este, una password, id_chat y id_token de telegram para poder mandar un token para la doble autenticación.
- **Página de registro de servidores:** Para registrar un servidor es necesario la ip, esta debe de ser única ya que con esta se identifica y también se pedirá el usuario y password de la api.
- **Página de listado de administradores:** En esta página sólo se listan los administradores que se han registrado.
- **Página de listado de servidores:** En esta página sólo se listan los servidores que se han registrado y quien es su administrador.
- **Página de asociación:** Esta página cumple con la función de asociar un administrador con un servidor. Para la asociación es necesario el nombre del administrador el cual es único y la ip del servidor.
- **Página de borrar servidores:** Esta página borra un servidor con base a la ip que se ingresa.
- **Página de borrar administradores:** Esta página borra administrador con base a la nombre que se ingresa.

Por parte del administrador de servidores

El sistema web deberá de contar con un inicio de sesión para los administradores que es diferente al de administrador global, este cuenta con doble autenticación, y una vez que se autentica podrá tener acceso a las demás páginas. Las páginas a las que el administrador de servidores tiene acceso son las siguientes:

- Página de inicio: Esta página muestra al administrador los servidores que están asociados a él, cada servidor listado cuenta con dos botones, el primero (ttyd) nos conecta al servidor con una terminal a través de la misma interfaz web. El segundo nos manda una pagina la cual nos muestra lo que puede monitorizar de cada servidor, esto es: porcentaje de uso de memoria, porcentaje de uso de procesador y el porcentaje de uso de disco.

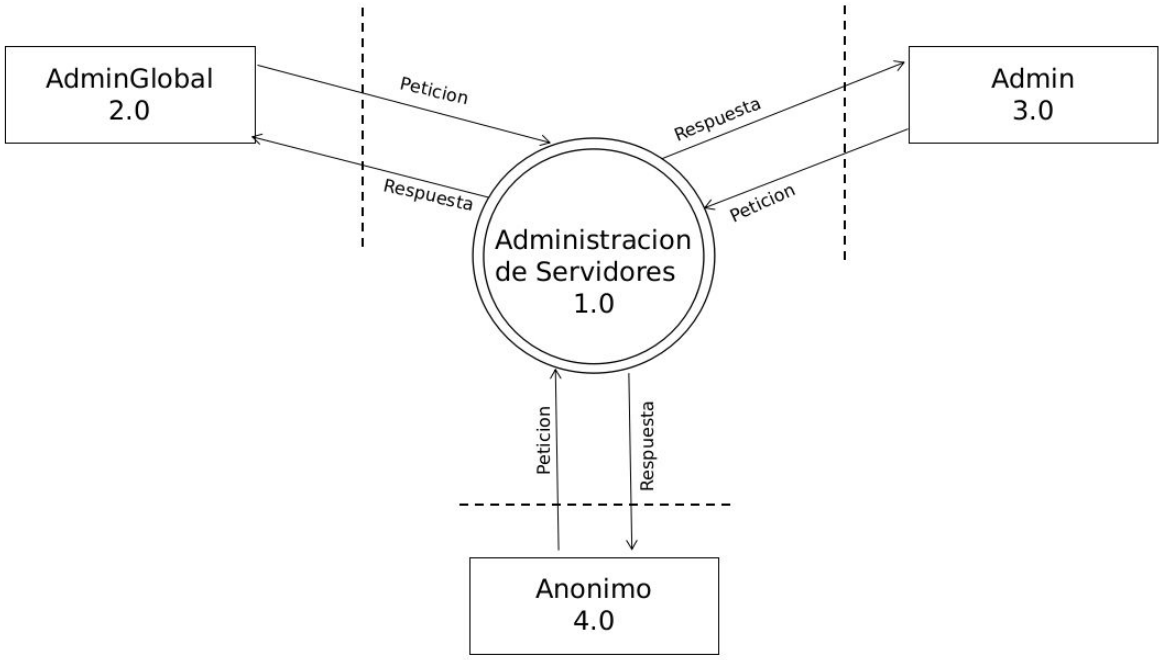
Diagrama de despliegue



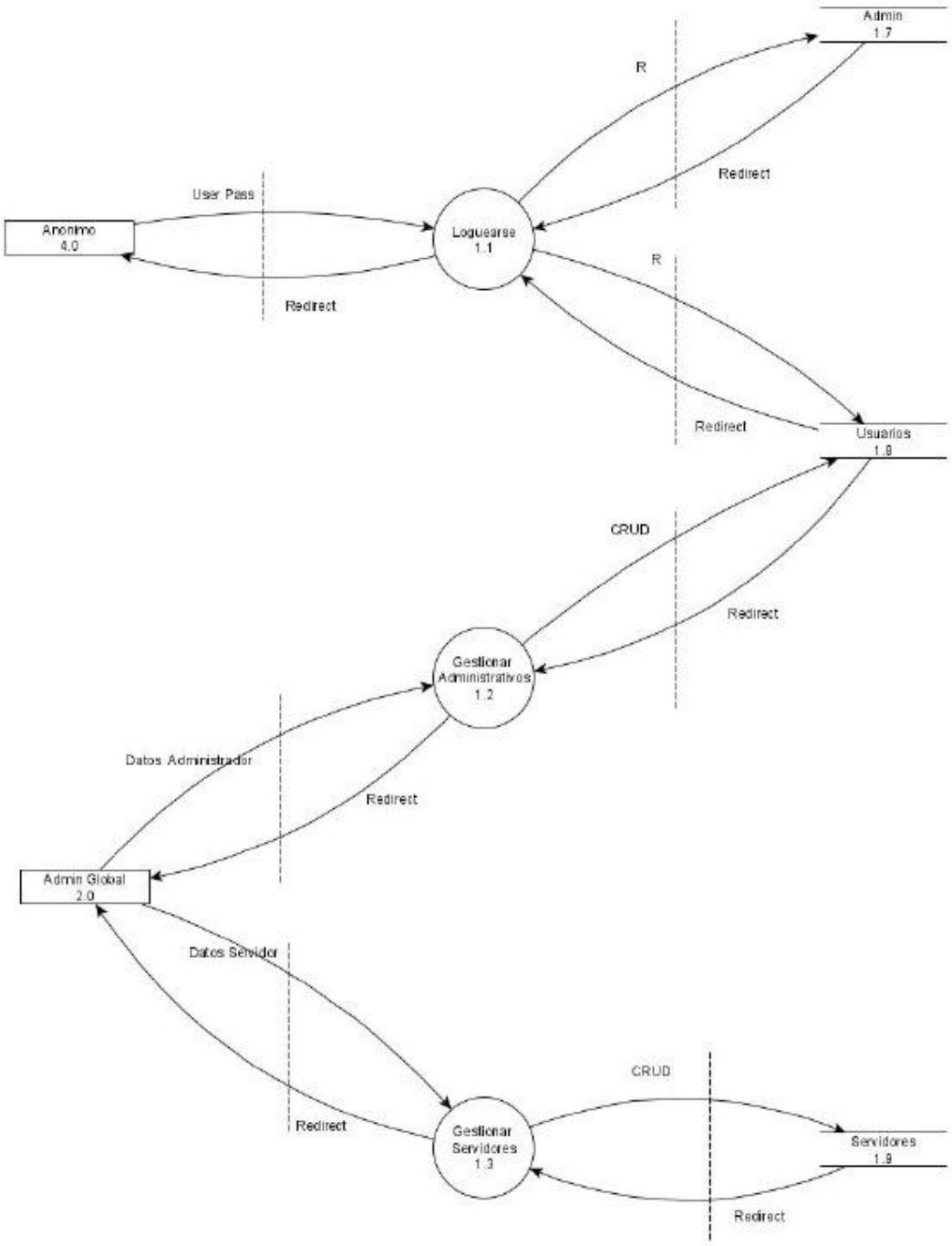
Modelado de amenazas

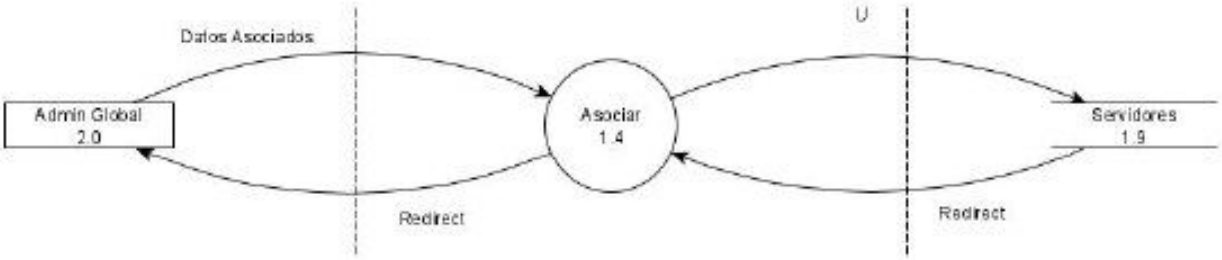
DFD nivel 0

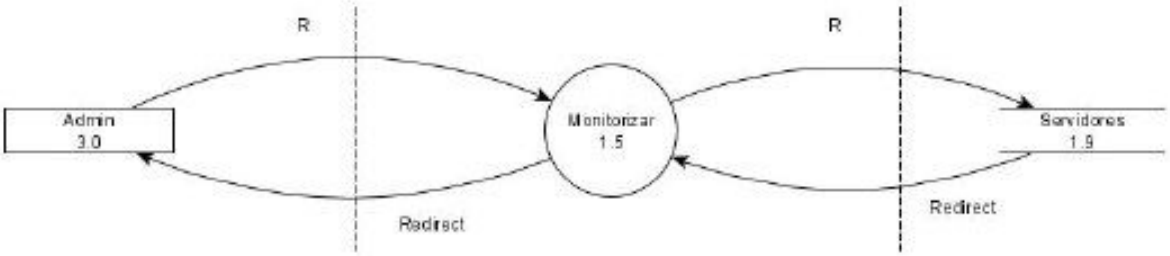
NIVEL 0

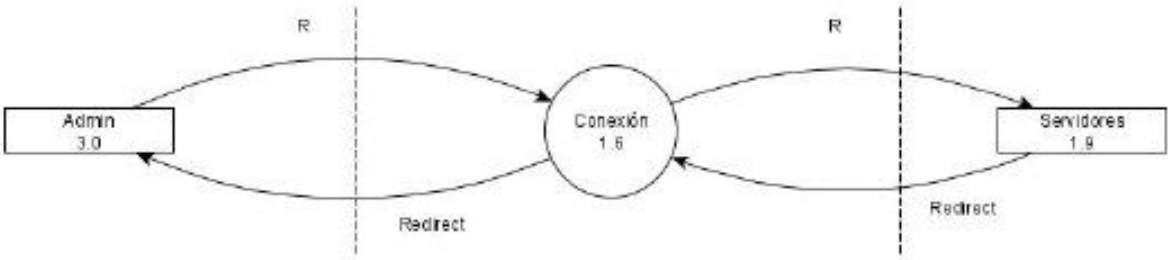


DFD nivel 1


Admin
1.7
R
Redirect
User Pass
Anonimo
4.0
Loguearse
1.1
Redirect
R
Redirect
Usuarios
1.8
CRUD
Redirect
Gestionar
Administrativos
1.2
Datos Administrador
Redirect
Admin Global
2.0
Datos Servidor
Redirect
CRUD
Gestionar
Servidores
1.3
Servidores
1.9
Redirect


Datos Asociados
U
Admin Global
2.0
Asociar
1.4
Servidores
1.9
Redirect
Redirect


R
R
Admin
3.0
Monitorizar
1.5
Servidores
1.9
Redirect
Redirect


R
R
Admin
3.0
Conexión
1.5
Servidores
1.9
Redirect
Redirect

Elementos del DFD nivel 1

Tipo elemento DFD	Numero de item
Entidades externas	AdminGlobal 2.0
	Admin 3.0
	Anonimo 4.0
Procesos	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6
Almacenes	Admin 1.7
	Usuarios 1.8
	Servidores 1.9
Flujos de datos	Usuario anonimo peticion y respuesta (4.0 -> 1.1 -> 4.0)
	Verificar datos de login admin_global (1.1 -> 1.7 -> 1.1)
	Verificar datos de login usuarios_admin (1.1 -> 1.8 -> 1.1)
	Admin Global gestiona usuarios_admin (2.0 -> 1.2 -> 2.0)
	Modificar/leer base de datos de usuarios_admin (1.2 -> 1.8 -> 1.2)
	Admin Global gestiona servidores (2.0 -> 1.3 -> 2.0)
	Modificar/leer base de datos servidores (1.3 -> 1.9 -> 1.3)
	Admin Global asocia servidores y usuarios_admin (2.0 -> 1.4 -> 2.0)
	Admin Global actualiza base de datos servidores (1.4 -> 1.9 -> 1.4)
	Usuario_admin monitorea sus servidores (3.0 -> 1.5 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.5 -> 1.9 -> 1.5)
	Usuario_admin se conecta a un servidor (3.0 -> 1.6 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.6 -> 1.9 -> 1.6)

Asociación de elementos con amenazas

Tipo de amenaza (STRIDE)	Numero Item DFD
	Entidades Externas
	AdminGlobal 2.0
	Admin 3.0
	Anonimo 4.0
	Procesos
Spoofing	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6
	Flujo de datos
	Usuario anonimo peticion y respuesta (4.0 -> 1.1 -> 4.0)
	Verificar datos de login admin_global (1.1 -> 1.7 -> 1.1)
	Verificar datos de login usuarios_admin (1.1 -> 1.8 -> 1.1)
	Admin Global gestiona usuarios_admin (2.0 -> 1.2 -> 2.0)
	Modificar/leer base de datos de usuarios_admin (1.2 -> 1.8 -> 1.2)
	Admin Global gestiona servidores (2.0 -> 1.3 -> 2.0)
	Modificar/leer base de datos servidores (1.3 -> 1.9 -> 1.3)
	Admin Global asocia servidores y usuarios_admin (2.0 -> 1.4 -> 2.0)
	Admin Global actualiza base de datos servidores (1.4 -> 1.9 -> 1.4)
	Usuario_admin monitorea sus servidores (3.0 -> 1.5 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.5 -> 1.9 -> 1.5)
Tampering	Usuario_admin se conecta a un servidor (3.0 -> 1.6 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.6 -> 1.9 -> 1.6)
	Almacenes
	Admin 1.8
	Usuarios 1.9
	Servidores 1.10
	Procesos
	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6

Repudation	Entidades Externas
	AdminGlobal 2.0
	Admin 3.0
	Anonimo 4.0
	Procesos
	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6
Information disclosure	Flujo de datos
	Usuario anonimo peticion y respuesta (4.0 -> 1.1 -> 4.0)
	Verificar datos de login admin_global (1.1 -> 1.7 -> 1.1)
	Verificar datos de login usuarios_admin (1.1 -> 1.8 -> 1.1)
	Admin Global gestiona usuarios_admin (2.0 -> 1.2 -> 2.0)
	Modificar/leer base de datos de usuarios_admin (1.2 -> 1.8 -> 1.2)
	Admin Global gestiona servidores (2.0 -> 1.3 -> 2.0)
	Modificar/leer base de datos servidores (1.3 -> 1.9 -> 1.3)
	Admin Global asocia servidores y usuarios_admin (2.0 -> 1.4 -> 2.0)
	Admin Global actualiza base de datos servidores (1.4 -> 1.9 -> 1.4)
	Usuario_admin monitorea sus servidores (3.0 -> 1.5 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.5 -> 1.9 -> 1.5)
	Usuario_admin se conecta a un servidor (3.0 -> 1.6 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.6 -> 1.9 -> 1.6)
	Almacenes
	Admin 1.8
	Usuarios 1.9
	Servidores 1.10
	Procesos
	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6

Denial of service	Flujo de datos
	Usuario anonimo peticion y respuesta (4.0 -> 1.1 -> 4.0)
	Verificar datos de login admin_global (1.1 -> 1.7 -> 1.1)
	Verificar datos de login usuarios_admin (1.1 -> 1.8 -> 1.1)
	Admin Global gestiona usuarios_admin (2.0 -> 1.2 -> 2.0)
	Modificar/leer base de datos de usuarios_admin (1.2 -> 1.8 -> 1.2)
	Admin Global gestiona servidores (2.0 -> 1.3 -> 2.0)
	Modificar/leer base de datos servidores (1.3 -> 1.9 -> 1.3)
	Admin Global asocia servidores y usuarios_admin (2.0 -> 1.4 -> 2.0)
	Admin Global actualiza base de datos servidores (1.4 -> 1.9 -> 1.4)
	Usuario_admin monitorea sus servidores (3.0 -> 1.5 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.5 -> 1.9 -> 1.5)
	Usuario_admin se conecta a un servidor (3.0 -> 1.6 -> 3.0)
	Usuario_admin lee base de datos de servidores (1.6 -> 1.9 -> 1.6)
	Almacenes
	Admin 1.8
	Usuarios 1.9
	Servidores 1.10
	Procesos
	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6
Elevation of privilages	Procesos
	Loguearse 1.1
	Gestionar Administradores 1.2
	Gestionar Servidores 1.3
	Asociar 1.4
	Monitorizar 1.5
	Conexion 1.6

Propuesta de técnica y tecnología de mitigación STRIDE

Componente	Tipo componente	Amenaza	Mitigacion
AdminGlobal 2.0	Entidad externa	S	Autenticacion de dos vias
Admin 3.0	Entidad externa	S	Autenticacion de dos vias
Anonimo 4.0	Entidad externa	R	Auditoria por medio de bitacoras
Loguearse 1.1	Proceso	SED	Limitar numero de intentos por tiempo
		R	Auditoria por medio de bitacoras
		TI	Validacion de entradas y sanitizacion
Gestionar Administradores 1.2	Proceso	R	Auditoria por medio de bitacoras
Gestionar Servidores 1.3	Proceso	R	Auditoria por medio de bitacoras
Asociar 1.4	Proceso	R	Auditoria por medio de bitacoras
Monitorizar 1.5	Proceso	SI	Token de autenticacion, Cifrado
Conexion 1.6	Proceso	IE	Sandbox, Limitar permisos
Admin 1.8	Almacen	TI	Hashing de Contraseñas , Validación de entradas
		E	Definir usuarios con privilegios especificos
Usuarios 1.9	Almacen	TI	Hashing de Contraseñas y Vaidación de entradas
		E	Definir usuarios con privilegios especificos
Servidores 1.10	Almacen	TI	Hashing de Contraseñas , Cifrado y Validación de entradas
		E	Definir usuarios con privilegios especificos
Usuario anonimo peticion y respuesta (4.0 -> 1.1 -> 4.0)	Flujos de datos	TID	Limite de intentos, Sanitización de entradas
Verificar datos de login admin_global (1.1 -> 1.7 -> 1.1)	Flujos de datos	TID	Hashing de Contraseñas, Validación de entradas y Limite de peticiones
Verificar datos de login usuarios_admin (1.1 -> 1.8 -> 1.1)	Flujos de datos	TID	Hashing de Contraseñas, Validación de entradas y Limite de peticiones
Admin Global gestiona usuarios_admin (2.0 -> 1.2 -> 2.0)	Flujos de datos	TID	HTTPS(S), Firewall
Modificar/leer base de datos de usuarios_admin (1.2 -> 1.8 -> 1.2)	Flujos de datos	TID	Hashing de Contraseñas, Validación de entradas y Limite de peticiones
Admin Global gestiona servidores (2.0 -> 1.3 -> 2.0)	Flujos de datos	TID	HTTPS(S), Firewall
Modificar/leer base de datos servidores (1.3 -> 1.9 -> 1.3)	Flujos de datos	TID	Hashing de Contraseñas, Validación de entradas y Limite de peticiones
Admin Global asocia servidores y usuarios_admin (2.0 -> 1.4 -> 2.0)	Flujos de datos	TID	HTTPS(S), Firewall
Admin Global actualiza base de datos servidores (1.4 -> 1.9 -> 1.4)	Flujos de datos	TID	Cifrado de Contraseñas, Validación de entradas y Limite de peticiones
Usuario_admin monitorea sus servidores (3.0 -> 1.5 -> 3.0)	Flujos de datos	TID	HTTPS(S), Firewall
Usuario_admin lee base de datos de servidores (1.5 -> 1.9 -> 1.5)	Flujos de datos	TID	Cifrado de Contraseñas, Validación de entradas y Limite de peticiones
Usuario_admin se conecta a un servidor (3.0 -> 1.6 -> 3.0)	Flujos de datos	TID	HTTPS(S), Firewall
Usuario_admin lee base de datos de servidores (1.6 -> 1.9 -> 1.6)	Flujos de datos	D	Limite de peticiones

Conclusiones

En años recientes la web ha presentado una rápida evolución, desde el diseño de páginas o sitios web, mismos que han sido pilares para el crecimiento y proyección de la vida moderna y negocios de las organizaciones.

En el transcurso del curso se revisaron diversos temas relacionados con la seguridad en los sistemas web, vulnerabilidades, modelado de amenazas, consejos para programación, cifrado, password hashing entre otros. También se hizo uso de diferentes herramientas como django, peticiones (GET y POST), back-end y front-end , métodos de request, controlador de versiones, herramienta de revisión estática de código, dockers, por mencionar algunos.

El objetivo del proyecto era que como estudiantes y futuros profesionistas desarrolláramos una plataforma web que ofreciera una implementación funcional en tiempo real de una solución para administrar tanto servidores como administradores y monitorizar servidores asociados a los administradores registrados, haciendo uso de los aprendizajes que se obtuvieron de la materia.