Plan de Seguridad

Gestión de Seguiridad en Aplicaciones

Unidad Educativa Particular Juana de Dios

Tabla de Contenido

INTRODUCCION

El objetivo de este documento es presentar el plan de seguridad informática de la Unidad Educativa Particular Juana de Dios con respecto a los sistemas utilizados por los estudiantes y docentes de la institución.

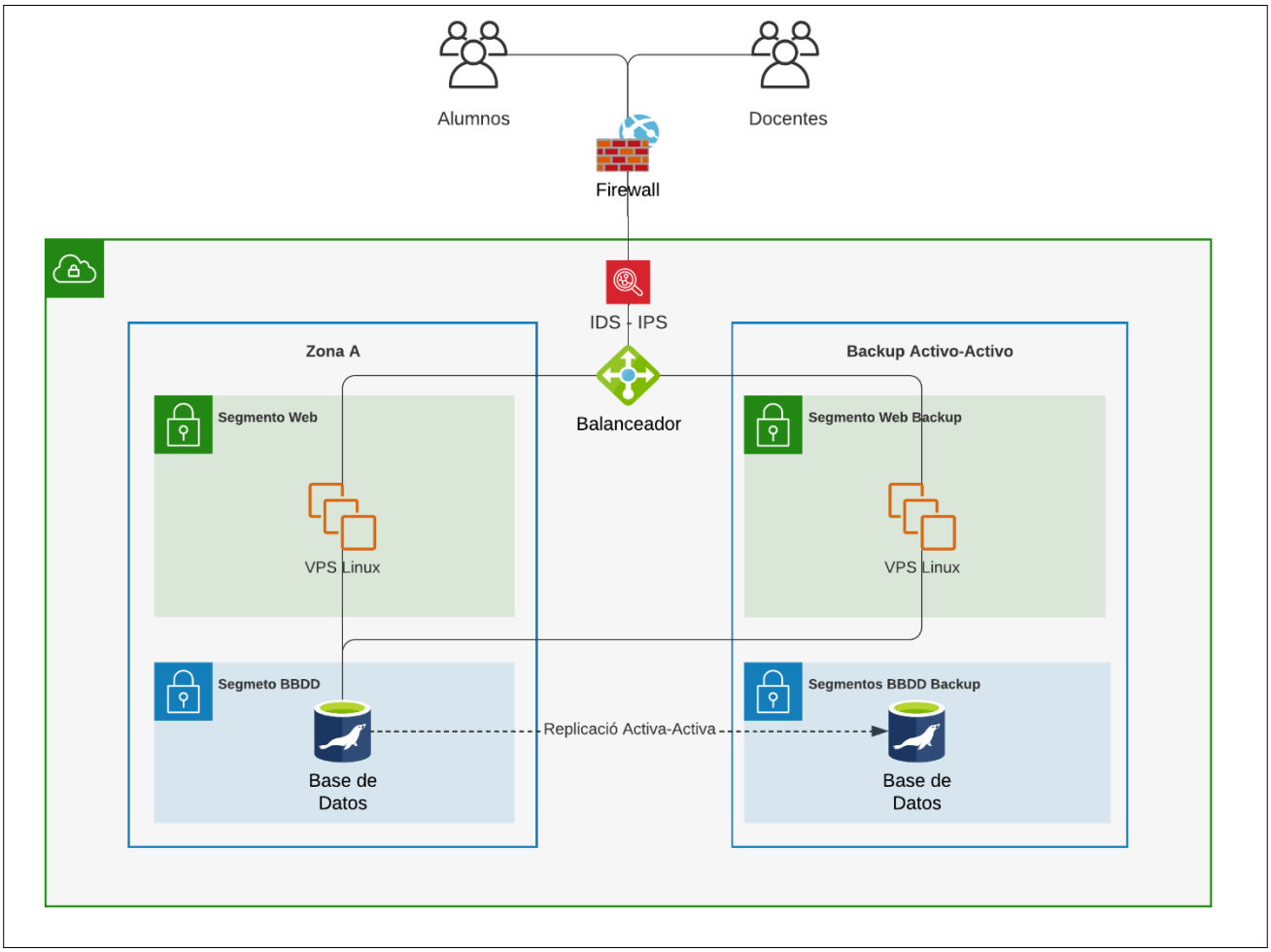
El plan de seguridad informática engloba los principios de la seguridad informática de mantener la Integridad, Disponibilidad y Confidencialidad de la información que es gestionada por nuestros sistemas. Este plan se basa en marcos de referencia NIST y controles CIS para el correcto planteamiento de los controles de seguridad aplicados en los sistemas utilizados por la institución.

Como precedente es importante mencionar que la Unidad Educativa Particular Juana de Dios cuenta con dos sistemas:

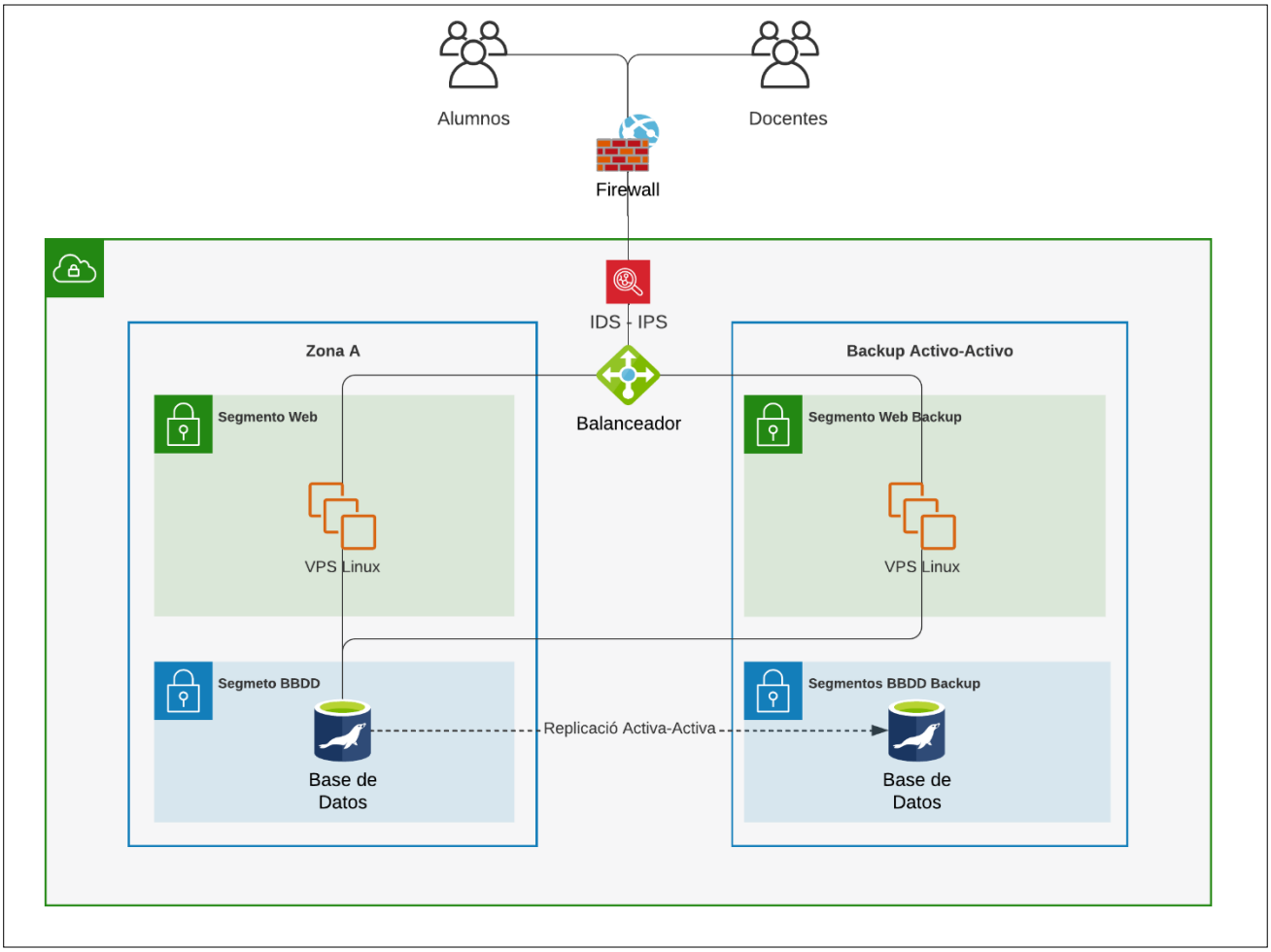
- Sinfa: Sistema académico de gestión de calificaciones
- Evajud: Plataforma de la institución

1. ARQUITECTURA DE LOS SISTEMAS

A. Arquitectura del Sistema Sinfa



B. Arquitectura del Sistema Evajud



2. GESTION DE ACCESOS

La gestión de accesos es el proceso de permitir que los usuarios hagan uso de servicios TI, datos o infraestructura. La gestión de accesos nos permite cumplir con los principios de confidencialidad, integridad y disponibilidad, ya que garantiza que solamente los usuarios que están permitidos puedan acceder a los recursos e información y modificarlos, proporcionando los mínimos privilegios posibles para el correcto desempeño de las funciones.

El objetivo de la gestión de accesos dentro de la gestión de los sistemas de la institución es: Gestionar accesos a los recursos e información, y supervisar y asegurar que los privilegios proporcionados no se están utilizados de forma inadecuada.

Actividades

Las actividades que realizan el equipo de gestión de accesos de la institución son:

- Revisar las solicitudes de acceso.
- Verificar la pertinencia de los accesos solicitados.
- Proporcionar los privilegios.
- Verificar y monitorear el estado de las identidades.
- Registrar y dar seguimiento de los accesos.
- Eliminar o restringir privilegios.

3. INTEGRIDAD Y PROTECCION DE LOS ACTIVOS

La integridad y la protección de los activos que forma parte de los dos sistemas de la institución son factores importantes dentro del plan de seguridad informática, para esto se han divido en varios controles que nos permiten brindar una capa de protección a la información de nuestros colaboradores y estudiantes.

Seguridad Física

Las barreras físicas incluyendo las puertas, entradas, garitas, etc son elementos utilizados para controlar el acceso a los equipos e información. Si bien los componentes de la infraestructura no se encuentran físicamente en la institución, el proveedor de los mismo garantiza que el acceso físico a los servidores donde se encuentra los elementos que forma parte de las aplicaciones solamente son accedidos por las personas que tiene la autorización necesaria.

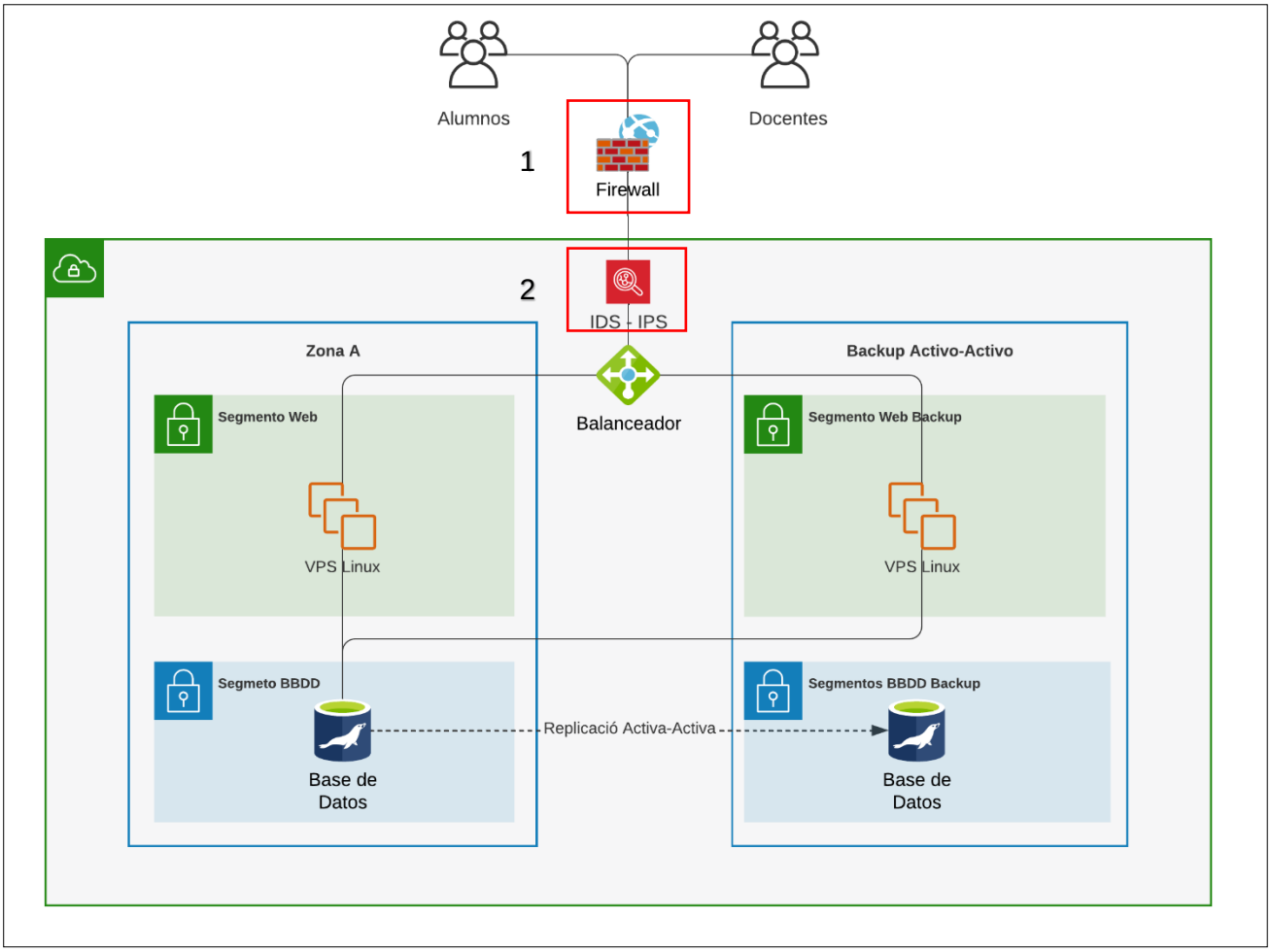
Hardening

El hardening es una medida de seguridad que es aplicada sobre los dispositivos que van a ser utilizados en los sistemas, con el objetivo de reducir la superficie de exposición, misma que es la suma de los diferentes puntos por los cuales un usuario no autorizado o maliciosos, pueda tratar de ingresar o modificar el comportamiento de los acticos.
De esta forma cuantas más funciones ejecute un sistema, mayor superficie de exposición, por consiguiente, mayor posibilidad de ser vulnerado. En contra posición, cuantas menos funciones ejecute un equipo, menor es la posibilidad de ser vulnerado.

La institución ejecuta un hardening basado en controles CIS en los sistemas operativos sobre los cuales corren los sistemas de la institución, consiguiente disminuir la superficie de exposición, sin afectar el funcionamiento de las aplicaciones. Este control es mandatorio, por lo cual podemos garantizar que los nuevos equipos que sean adicionados a la infraestructura siempre pasaran por un hardening previo.

Herramientas de Seguridad

Como se puede observar en la arquitectura a) y b) de la sección 1 de este documento, tenemos elementos de seguridad que nos permiten la protección de los activos:



1) Firewall

   El firewall es un sistema que tiene como función prevenir y proteger la infraestructura de los sistemas, de intrusiones o ataques a la red, bloqueando los intentos de accesos no autorizados. Este sistema es quien permite o restringe el tráfico entrante y saliente de la red y equipos, mediante una serie de reglas que han sido especificadas previamente.

   La institución cuenta con las reglas de firewall configuradas para la protección de los sistemas, garantizando el mínimo privilegio posible, disminuyendo la superficie de exposición para impedir que usuarios no autorizados accedan a los componentes o información.

2) IDS – IPS

   Los sistemas de detección de intrusos (IDS) y prevención de intrusos (IPS) son una capa de protección de seguridad que se encargan de vigilar el tráfico, examinando la red y los puertos analizando paquetes de datos, para detectar patrones que puedan ser sospechosos. El proveedor donde se encuentra levanta la infraestructura cuenta con IPS e IDS para proteger la infraestructura de los clientes, por lo que los sistemas Sinfa y Evajud cuentan con estas medidas de protección de seguridad informática.

4. GESTION DE VULNERABILIDADES

La gestión de las vulnerabilidades es un proceso continuo de TI en él se identifican, evalúan, gestionan e informan sobre las vulnerabilidades de seguridad en los sistemas y el software que se ejecuta sobre ellos. El proceso de gestión en la institución se evalúan los riesgos de seguridad, pero, adicionalmente, se clasifican las vulnerabilidades según el riesgo e impacto. La gestión de vulnerabilidades cuenta con 2 subprocesos:

Análisis y Pruebas de Seguridad
La institución realiza una vez al año un análisis y pruebas de seguridad sobre sinfa y evajud, con el objetivo de recolectar todas las vulnerabilidades que se puedan presentar en los sistemas y el software durante este periodo de tiempo. Estas vulnerabilidades posteriormente pasan a un proceso de gestión de vulnerabilidades para su posterior cierre.

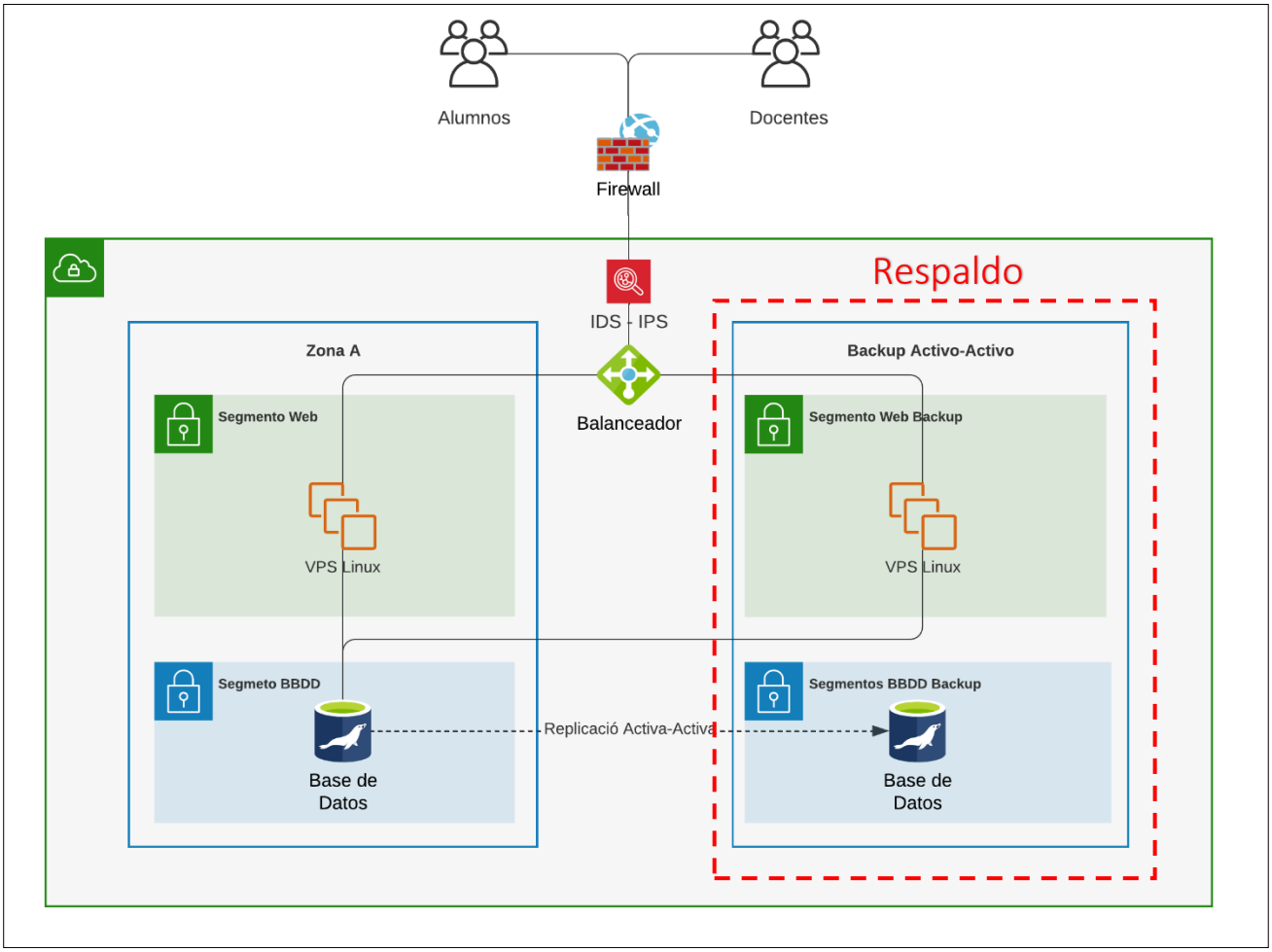
Gestión de Vulnerabilidades
En el proceso de gestión de vulnerabilidades se utiliza como input los hallazgos encontrados en los análisis y pruebas de seguridad (pentesting). El objetivo principal es generar un ciclo continuo de gestión, el mismo que toma las vulnerabilidades encontradas, las clasifica según el impacto y el riesgo que pueden presentar a los sistemas y la información. Finalmente, con esta clasificación se prioriza el cierre de estas vulnerabilidades.

La tabla de clasificación de vulnerabilidades es la siguiente:

Clasificación	Color Referencia
Alta	
Media	
Baja	

5. BACKUPS Y RESPUESTA A INCIDENTES

La institución cuenta con copias de seguridad de todos los componentes utilizados en la infraestructura.



Como se puede visualizar en la arquitectura de los sistemas, existe una réplica activo-activo de los componentes de la aplicación, es decir que, si ocurre un incidente o una caída de los servidores de aplicación y base de datos de la zona principal, en seguida empiezan a funcionar los servidores de respaldo. La mantener un esquema activo-activo, en caso de un incidente, la perdida de disponibilidad de las aplicaciones es prácticamente nula.

Christian Flores
0105500227