ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN SISTEMAS

BUENAS PRÁCTICAS DE DISPONIBILIDAD DE INFORMACIÓN EN EL SUBSISTEMA SÍLABOS 1.0.0 DE LA DIRECCIÓN DE DESARROLLO ACADÉMICO EN LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Trabajo de integración curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN SISTEMAS INFORMÁTICOS

AUTOR: RODRIGO LENIN RAMOS AVEROS

DIRECTOR: Ing. JORGE ARIEL MENÉNDEZ VERDECIA

Riobamba – Ecuador

2021

Yo, Rodrigo Lenin Ramos Averos, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 10 de mayo de 2021

Rodrigo Lenin Ramos Averos

020214805-2

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN SISTEMAS

El Tribunal del Trabajo de Integración Curricular certifica que: El trabajo de integración curricular; tipo: Proyecto Técnico **BUENAS PRÁCTICAS DE DISPONIBILIDAD DE INFORMACIÓN EN EL SUBSISTEMA SÍLABOS 1.0.0 DE LA DIRECCIÓN DE DESARROLLO ACADÉMICO EN LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**, realizado por el señor: **RODRIGO LENIN RAMOS AVEROS**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	FECHA
Ing. Raúl Rosero **PRESIDENTE DEL TRIBUNAL**	RAUL HERNAN ROSERO MIRANDA	2021-05-10
Ing. Jorge Menéndez **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**	Firmado electrónicamente por: JORGE ARIEL MENENDEZ VERDECIA	2021-05-10
Dra. Narcisa Salazar **MIEMBRO DEL TRIBUNAL**	NARCISA DE JESUS SALAZAR ALVAREZ Firmado digitalmente por NARCISA DE JESUS SALAZAR ALVAREZ Fecha: 2021.05.11 18:36:57 -05'00'	2021-05-10

DEDICATORIA

Dedico este Trabajo de Integración Curricular a Dios, quien cuida cada paso que doy. A mi padre y mi madre por ser mi eterna inspiración.

Rodrigo.

AGRADECIMIENTO

Agradezco a Dios por no dejar que se apague la llama en mi interior, a mi padre y mi madre por su apoyo e incansable esfuerzo para que yo logre todas mis metas. A mis maestros, especialmente al Ing. Jorge Menéndez tutor de mi Trabajo de Integración Curricular, a la Dra. Narcisa Salazar, por brindarme sus conocimientos. A mí ESPOCH por darme la oportunidad de formarme en sus aulas.

Rodrigo.

TABLA DE CONTENIDO

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo del trabajo de investigación fue aplicar buenas prácticas de disponibilidad en el subsistema Sílabos 1.0.0 de la Dirección de Desarrollo Académico en la Escuela Superior Politécnica de Chimborazo; dado que la Institución tiene la necesidad de tener un subsistema con alta disponibilidad para prevenir interrupciones no autorizadas, ya que el actual tiene un 27,03% de disponibilidad, se procedió a la investigación de buenas prácticas de alta disponibilidad, entre ellas, la utilización de clúster de servidores utilizando contenedores (Docker), balanceador de carga y proxy inverso (Traefik), así como herramientas para su administración (Portainer, Visualizer), clúster de base de datos (Postgres) y copias de seguridad automáticas (Rsnapshot), se realizó el mantenimiento mediante el uso de la metodología ágil SCRUM combinada con el estándar IEEE 1219, para aplicar las buenas prácticas investigadas en el subsistema Sílabos 1.0.0, dando como resultado la versión 1.1.0. Donde al realizar las pruebas se obtuvo un 81.08% de disponibilidad. Los resultados obtenidos permitieron determinar que se logró mejorar la disponibilidad en un 54,05 %. Se concluye que las buenas prácticas de disponibilidad influyen positivamente en prevenir interrupciones no autorizadas. Se recomienda realizar un estudio de alta disponibilidad con respecto a proxies inversos, para evitar conflictos con el servidor de nombres de dominio (DNS).

Palabras clave: <INFORMÁTICA>, <SOFTWARE>, <ALTA DISPONIBILIDAD>**,** <CLÚSTER>**,** <DOCKER (SOFTWARE)>**,** <ESTÁNDAR IEEE 1219>, <METODOLOGÍA DE DESARROLLO ÁGIL (SCRUM)>

ABSTRACT

The objective of the work research was to apply good practice of availability in the syllabus system 1.0.0 of the Direction of Academic Development in the Escuela Superior Politécnica de Chimborazo because the institution possesses the capacity to have a subsystem which has a high availability to prevent unauthorized interruptions due to the current system has a 27,03% of availability. We did a research about good practice of high availability, for instance: the use of server cluster utilizing containers (Docker), load balancer and inverse proxy (Traefik), as well as tools for its management (Portainer, Visualizer), database cluster (Postgres) and automatic back-up copies (Rsnapshot). We did a maintenance using the methodology SCRUM along with IEEE 1219 to apply the good research practice in the syllabus system 1.0.0. resulting in the 1.1.0 version. The results showed 81.08% of availability and they allowed to determine that the availability was improved in 54,05%. We conclude that the good practice of availability influences positively on preventing unauthorized interruptions. It is recommended to do a study of high availability regarding reverse proxies to avoid conflicts with the Domain Name System (DNS).

Keywords: <COMPUTING>, <SOFTWARE>, <HIGH AVAILABILITY>, <CLUSTER>, <DOCKER (SOFTWARE)>, <IEEE 1219>, <AGILE SOFTWARE DEVELOPMENT METHODOLOGY (SCRUM)>

INTRODUCCIÓN

Las aplicaciones web, facilitan considerablemente el acceso a la información, esto proporciona una ventaja notable frente a las aplicaciones de escritorio, ya que no permiten a los usuarios ser accedidas desde cualquier lugar, sin embargo, las aplicaciones web al estar funcionando en internet existen aspectos importantes a considerar, entre ellos se encuentra la seguridad, lo cual evita que el activo más importante de las entidades se vea comprometido. Para ello existen una serie de nomas que proporcionan una base para la gestión de la seguridad, entre ellos se encuentra la norma ISO/IEC 27001, esta norma menciona tres principios fundamentales de la seguridad informática, donde se destaca la disponibilidad (ISO, 2013). En el artículo "Un enfoque cualitativo de la disponibilidad de la información", se menciona a la disponibilidad como "la prevención de la retención no autorizada de información o recursos" (Tryfonas et al., 2000, p. 38). Sin embargo, según el Departamento de Seguridad de la Universidad Nacional de Luján la disponibilidad "implica que debe protegerse la información de forma tal que se pueda disponer de ella para su gestión en el tiempo y la forma requeridos por el usuario" (Universidad de Luján, 2017). Es decir, la disponibilidad se vincula estrechamente con prevenir interrupciones no autorizadas, con el fin de que el sistema proporcione la información al usuario final cuando este lo requiera.

El objetivo de este estudio es dar mantenimiento al subsistema Sílabos 1.0.0 por medio de la metodología SCRUM junto con el estándar IEEE 1219 para aplicar buenas prácticas de disponibilidad con el fin de lograr proporcionar la información cuando el usuario la requiera sin interrupciones no autorizadas.

El Trabajo de Integración Curricular está organizado en cuatro capítulos, donde cada uno tiene un alto grado de importancia, motivo por el cual se describe una visión general de los mismos:

Capítulo I, denominado Diagnóstico del problema, el cual contiene los antecedentes, formulación y sistematización del problema, justificación teórica, justificación aplicativa, objetivo general y objetivos específicos, identificando así la necesidad de tener un subsistema con alta disponibilidad para acceder a la información cuando esta sea requerida, por ello se propone la aplicación de buenas prácticas.

Capítulo II denominado Revisión de la Literatura o Fundamentos Teóricos, consiste en la investigación teórica que será de utilidad para el desarrollo del presente trabajo, en el cual se encuentra información ordenada desde lo correspondiente a lo que es un Sílabo, una aplicación web, arquitectura, seguridad, disponibilidad, buenas prácticas, entre ellas; clústeres con docker, balanceador de carga, replicación de base de datos, copias de seguridad automáticas, entre otras.

Capítulo III denominado Marco Metodológico, se describen los pasos considerados para poder realizar el mantenimiento por medio de la metodología ágil SCRUM junto con el estándar IEEE 1219, con el fin de aplicar las buenas prácticas de disponibilidad, así como las pruebas para la obtención de datos necesarios para el posterior análisis de los mismos.

Capítulo IV denominado Resultados, en el cual se realiza un análisis estadístico de los resultados obtenidos, para con ellos emitir las conclusiones con un margen de error del 5% y un nivel de confianza del 95%.

Posterior a los capítulos descritos anteriormente se encuentran las conclusiones, recomendaciones, bibliografía y finalmente los anexos donde se detalla minuciosamente las actividades realizadas en el transcurso del desarrollo del presente Trabajo de Integración Curricular para una mayor comprensión del mismo.

CAPITULO I

1. DIAGNÓSTICO DEL PROBLEMA

1.1 Antecedentes

La Escuela Superior Politécnica de Chimborazo, en el mes de julio del 2003 aprobó mediante resolución de Consejo Politécnico la reestructuración orgánica funcional de la institución, misma que involucró a las diferentes dependencias administrativas y académicas con la finalidad de lograr una administración moderna y eficiente en sus diferentes ámbitos. Este cambio determinó que las tareas académicas encargadas al Departamento de Cómputo y Sistemas se vinculen directamente a las diferentes facultades y las funciones técnicas de asesoría, desarrollo de soluciones tecnológicas en el área informática se integren en la Dirección de Tecnologías de la Información y Comunicación (DTIC) mismas que se encontraban divididas en el comité Informático y el Departamento de Cómputo y Sistema (ESPOCH, 2017). Entre las funciones del DTIC se encuentra desarrollar y mantener los sistemas informáticos administrativos, académicos y de la organización, uno de ellos es el subsistema Sílabos, el cual se encarga de la gestión de los Sílabos Institucionales que se encuentra registrado en el Reglamento para la distribución y cumplimiento de la jornada laboral del personal académico de la ESPOCH (resolución 116.CP.2014), Artículo 7. Actividades de Docencia. En su actividad No. 3 “Diseño y elaboración de material didáctico, guías docentes, syllabus o programa de estudio de asignatura (PEA)”.

En reuniones efectuadas con el personal del DTIC, manifestaron algunos de los efectos adversos tales como pérdidas económicas debido a hurto y modificación de la información, así como el incumplimiento de la norma de contraloría No. 410-10 Seguridad de tecnología de información, específicamente en la medida No. 5 “Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados” (Contraloría General del Estado, 2009, p. 79), además de la norma No. 410-12 Administración de soporte de tecnología de información, “La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen”

(Contraloría General del Estado, 2009, p. 80), también el incumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública, en el artículo 10 Custodia de la información, artículo 13 Falta de claridad en la información y artículo 18 Protección de la Información Reservada (SEPS, 2019, p. 6). Donde claramente en las normas y artículos mencionados se hace referencia a la confidencialidad, integridad y disponibilidad de información, considerados principios fundamentales de la seguridad informática. Esto originado por vulnerabilidades en los sistemas informáticos de la ESPOCH, donde el problema principal es la falta de disponibilidad de información en dichos sistemas, los cuales al necesitar conexión a la red de internet, ocasiona como causa ataques informáticos, además otro de los problemas es la falta de personal destinado a realizar pruebas de vulnerabilidades y desarrollar medidas de seguridad para la protección del activo elite de la institución como es la información, del mismo modo el no aplicar buenas prácticas de disponibilidad de información.

Razón por la cual, el presente Trabajo de Integración Curricular tiene como objetivo la aplicación de buenas prácticas de disponibilidad de información en el subsistema Sílabos 1.0.0 el cual actualmente se encuentra implantado en los servidores del DTIC de la ESPOCH, dicho subsistema pertenece al aplicativo Instrumentos Pedagógicos de la Dirección de Desarrollo Académico (DDA).

Cabe recalcar, la existencia de registros de trabajos afines, tales como "PROPUESTA DE MEJORES PRÁCTICAS DE SEGURIDAD PARA EL DESARROLLO DE APLICACIONES MÓVILES" (Cevallos Muñoz y Siguenza Plaza, 2016), el cual propone resolver inconvenientes de seguridad por medio del desarrollo de una aplicación móvil segura. "ELABORAR UNA METODOLOGÍA APLICANDO LA NORMA ISO IEC 27001 EN LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL DESITEL DE LA ESPOCH" (Gavilánes Pilco, 2012), lo cual consiste en la creación de una metodología para la gestión de seguridad basada en la norma ISO IEC 27001. "GUÍA DE BUENAS PRÁCTICAS DE DESARROLLO DE APLICACIONES WEB SEGURAS APLICADO AL SISTEMA CONTROL DE NUEVOS ASPIRANTES EMPRESA GRUPO LAAR" (Yánez Romero, 2014), se enfoca en el desarrollo de aplicaciones web por medio de la aplicación de medidas de seguridad. "IMPLEMENTACIÓN DE LA NORMA ISO 27 PARA GESTIÓN EN SEGURIDAD DE INFORMACIÓN, CASO PRÁCTICO: DESITEL" (Guevara Espinoza, 2013), donde se aborda la creación de una aplicación que permite la gestión de seguridad en base a la norma ISO 27. Para el desarrollo del presente Trabajo de Integración Curricular existe como punto de partida, "BUENAS PRÁCTICAS DE SEGURIDAD EN EL SISTEMA DE ESTAFETAS DE LA DIRECCIÓN DE DESARROLLO ACADÉMICO EN LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO" (Ordoñez y Chimbo, 2019), consiste en la

aplicación de un manual de buenas prácticas de seguridad en una aplicación web, cabe mencionar que dichas prácticas de seguridad se aplicarán en el presente Trabajo de Integración Curricular. De igual forma "TÉCNICAS DE PROGRAMACIÓN SEGURA PARA MITIGAR VULNERABILIDADES EN APLICACIONES WEB" (Monar, Pastor, Arcos, y Oñate, 2018), servirá para el desarrollo de la aplicación utilizando técnicas de programación seguras para mitigar vulnerabilidades.

1.2 Formulación del problema

¿Aplicar buenas prácticas de disponibilidad de información en el mantenimiento del subsistema Sílabos 1.0.0 prevendrá interrupciones no autorizadas?

1.3 Sistematización del problema

¿Cuál es el nivel de disponibilidad de información que posee el subsistema Sílabos 1.0.0 actualmente?

¿Cuáles son las buenas prácticas de disponibilidad de información en una aplicación web?

¿Es posible aplicar el manual de buenas prácticas de seguridad sugeridas en el trabajo de Ordoñez Sandra y Chimbo Kevin en el mantenimiento del subsistema Sílabos 1.0.0?

¿Es posible aplicar buenas prácticas de disponibilidad de información en el mantenimiento del subsistema Sílabos 1.0.0?

¿Cuál es el nivel de disponibilidad de información del subsistema Sílabos 1.0.0 después de haber realizado el mantenimiento?

1.4 Justificación

1.4.1 Justificación teórica

Actualmente, la seguridad es uno de los factores más importantes en el desarrollo de sistemas informáticos ya que la información es el activo más importante de las entidades, es necesario resaltar, para que la seguridad funcione, se requiere significativamente que el personal de la organización esté dispuesto a cumplir medidas establecidas, de nada sirve si no se cumplen las medidas de seguridad en el transcurso del desarrollo de los sistemas, según Costas en su libro sobre Seguridad y Alta Disponibilidad afirma que "la seguridad depende de la suma de la tecnología más la organización" (Costas Santos, 2014, p. 22).

Existes algunos estándares que proporcionan una base para la gestión de la seguridad, es así el caso de la familia de normas ISO 27000, entre ellas se encuentran "la ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 27007 y la ISO/IEC 27799:2008" (ISO, 2018). Además, de otras como "la ISO 15408, que permite que diferentes aplicaciones puedan ser probadas e integradas de forma segura" (ISO, 2009). También "el RFC 2196 publicado por el Internet Engineering Task Force para políticas y procedimientos de seguridad" (Fraser, 1997).

Es por ello que al revisar dichos estándares, el que se va a tomar como referencia en el presente Trabajo de Integración Curricular es la norma ISO/IEC 27001, ya que dentro de la misma se habla de los tres principios fundamentales de la seguridad informática, entre ellos destaca la disponibilidad (ISO, 2013) donde se investigará buenas prácticas de dicho pilar para aplicarlas en el subsistema Sílabos 1.0.0.

Es indispensable, disponer de una idea clara acerca de disponibilidad, así para Tryfonas et al. en su artículo científico Un Enfoque Cualitativo de la Disponibilidad de la Información mencionan "la disponibilidad como la prevención de la retención no autorizada de información o recursos." (Tryfonas et al., 2000, p. 38). Sin embargo, según el Departamento de Seguridad de la Universidad Nacional de Luján la disponibilidad es "uno de los tres principios básicos de la implementación de la seguridad de la información. La disponibilidad implica que debe protegerse la información de forma tal que se pueda disponer de ella para su gestión en el tiempo y la forma requeridos por el usuario" (Universidad de Luján, 2017). Por lo tanto, la disponibilidad se vincula estrechamente con prevenir interrupciones no autorizadas, es decir que el sistema proporcione la información al usuario final cuando este lo requiera.

Por lo tanto garantizar que haya disponibilidad de información es indispensable. Es por ello que debemos aplicar buenas prácticas al desarrollar aplicaciones. Ya que estos problemas no pueden ser tratados aisladamente, un punto débil compromete en la totalidad, una analogía clara es cuando por ejemplo existe máxima seguridad en la puerta principal de una casa, pero de nada sirve aquello si las ventanas no tienen protección (Costas Santos, 2014, p. 22).

Aplicar buenas prácticas de disponibilidad de información disminuye los riesgos de pérdidas cuantiosas, como información sensible, de igual forma permite solucionar problemas a futuro, sin embargo, según Roa en su libro Seguridad Informática expresa "es dura la tarea del responsable de seguridad informática en una empresa: hay mucha información que proteger y múltiples puertas por donde sufrir intrusiones. Nuestra sociedad actual se basa en información procesada digitalmente, hay que protegerla, la información es poder" (Roa Buendía, 2013, p. 21).

Por supuesto la utilización de buenas prácticas de disponibilidad desde el inicio es vital, se suele considerar la información como el factor más vulnerable, el hardware se puede volver a comprar o restaurar, pero la información dañada no siempre es recuperable, lo que pude ocasionar daños sobre la economía y la imagen de la organización, ahí es donde los principios de la seguridad se deben cumplir, fundamentalmente el de disponibilidad de información ya que una aplicación web debe estar funcionando en todo momento que los usuarios la requieran.

El mantenimiento de un sistema permite aplicar dichas prácticas de disponibilidad de información, sin embargo para lograrlo según López en su libro Seguridad Informática es necesario conocer:

> *Cuáles son los elementos que componen el sistema. Cuáles son los peligros que afectan al sistema, accidentales o provocados, se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas de intrusión o muestreos sobre el mismo. Finalmente cuáles con las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales.* (López, 2010, p. 9)

Es por esto, que el presente Trabajo de Integración Curricular se realiza con el fin de aplicar buenas prácticas de disponibilidad de información en el subsistema Sílabos 1.0.0, ya que el mismo será una herramienta que ayudará sustancialmente en la automatización de la gestión de los Sílabos Institucionales, además se contribuirá al desarrollo de futuros sistemas en la Dirección de Tecnologías de la Información y Comunicación gracias al Manual de Buenas Prácticas de Disponibilidad que se desarrollará.

1.4.2 Justificación aplicativa

Las aplicaciones web en la actualidad han evolucionado a gran escala, con un nivel creciente de utilización, convirtiéndose en herramientas fundamentales en la automatización de procesos. Razón por la cual la Dirección de Desarrollo Académico de la ESPOCH para cumplir con mayor facilidad sus funciones entre ellas la gestión de los sílabos institucionales es indispensable la utilización de una aplicación web, por ello se cuenta con el subsistema Sílabos 1.0.0, sin embargo el subsistema al encontrarse en Internet se manifiestan ciertas desventajas, entre lo más controversial el tema de inseguridad, ya que la información que se maneja dentro de la aplicación web puede ser accedida por personas con intenciones maliciosas y verse comprometida, por ello es necesario aplicar buenas prácticas de disponibilidad de información, en cada uno de sus módulos.

El subsistema Sílabos cuenta con los siguientes módulos:

Módulo de Administrador

Módulo Gestión Sílabo: El cual se encarga de la gestión de aspectos concernientes a la Estructura y Desarrollo del Sílabo, donde se establece las estrategias metodológicas, recursos, actividades de aprendizaje en el aula y las actividades de aprendizaje autónomas. Además permite gestionar los escenarios de aprendizaje reales, áulicos y virtuales.

Módulo Gestión de Roles: Correspondiente a la asignación de los roles que puedan disponer los usuarios dentro del sistema.

Módulo Gestión de Usuarios: Correspondiente a ingresar, modificar y eliminar los usuarios dentro del sistema.

Módulo de Opciones: Permite la gestión de lo que pueden realizar los distintos roles dentro del sistema.

Módulo Parámetros del Sílabo: Permite ingresar, modificar y eliminar parámetros tales como lugar y fecha de presentación en lo referente al sílabo.

Módulo Gestión del Sílabo

Módulo de Datos Generales: Muestra los datos del sílabo tales como la Facultad, Escuela, Carrera, Sede, Modalidad, Sílabo, Semestre, Período Académico, Campo de Formación, Código, Número de Créditos, Número de Horas, Prerrequisitos y Correquisitos.

Módulo Estructura y Desarrollo: Permite gestionar las unidades correspondientes al sílabo, dentro del cual se puede identificar la información de la unidad, es decir temas, subtemas. También se puede agregar, modificar y eliminar los objetivos de la unidad, recursos, estrategias metodológicas, actividades de aprendizaje en el aula, actividades de aprendizaje autónomas y los logros de aprendizaje. Además permite gestionar las unidades, así como crear nuevas, modificarlas y eliminarlas.

Módulo de Escenarios de Aprendizaje: Correspondiente a seleccionar los escenarios de aprendizaje real, áulico y virtual.

Módulo de Criterios de Evaluación: Permite gestionar los valores que serán considerados en los distintos parámetros de evaluación de la asignatura, dentro de los tres parciales, examen principal y de suspenso.

Módulo de Bibliografías: Permite gestionar la bibliografía del sílabo, tanto básica como complementaria, en donde se puede elegir dos tipos de bibliografía tanto web como libros.

Módulo Datos del Profesor: Correspondiente a la información del docente tales como nombres, correo electrónico, teléfono, títulos académicos de tercer nivel y títulos académicos de posgrado.

Módulo de Revisión: Permite revisar cada una de las secciones y subsecciones del sílabo que gestiona el docente, así como también permite la gestión de observaciones en cada una de las secciones del sílabo para poder emitir correcciones en cada una de las mismas y que el docente pueda verificar si debe realizar correcciones o no.

Módulo de Reportes

Permite generar los reportes en formato PDF del Sílabo, además cuenta con reportes de bibliografías básicas, criterios de evaluación, recursos, logros de aprendizaje, así como también reportes estadísticos y reportes del estado de los sílabos.

Ayuda

Correspondiente a mensajes que facilitan la utilización del subsistema.

Con la finalidad de mejorar el proceso de gestión de los sílabos, se realizará el mantenimiento del subsistema Sílabos, donde se aplicará buenas prácticas de disponibilidad de información, para lo cual se llevará a cabo una investigación de buenas prácticas de disponibilidad de información y se recabará el nivel de disponibilidad que posee actualmente el subsistema.

El subsistema contribuirá a la Escuela Superior Politécnica de Chimborazo con la automatización del proceso de gestión de los sílabos, proporcionando la generación del documento por medio del subsistema, así como los respectivos reportes, para un manejo más detallado de la información, además se garantizará la disponibilidad de información gracias a las buenas prácticas que se aplicarán en el presente Trabajo de Integración Curricular y de esta manera aportar con el Plan Nacional de Desarrollo según el objetivo cinco el mismo que consiste en impulsar la productividad y competitividad para el crecimiento económico sostenible de manera Redistribuida y solidaria (Plan Nacional de Desarrollo 2017 – 2021 Toda una Vida, 2017, p. 80), de igual forma se vincula con la líneas de investigación 2018 – 2022 de la ESPOCH Tecnologías de la Información y Comunicación, finalmente se relaciona con la línea de investigación de Ingeniería de Software y Seguridad de la gestión de la información de la escuela de Ingeniería en Sistemas de la Escuela Superior Politécnica de Chimborazo.

1.5 Objetivos

1.5.1 Objetivo general

Aplicar buenas prácticas de disponibilidad de información en el mantenimiento del subsistema Sílabos 1.0.0 de la Dirección de Desarrollo Académico en la Escuela Superior Politécnica de Chimborazo para prevenir interrupciones no autorizadas.

1.5.2 Objetivos específicos

- Determinar el nivel de disponibilidad de información del subsistema Sílabos 1.0.0 a través de pruebas de intrusión para obtener el estado actual.
- Investigar buenas prácticas de disponibilidad de información de aplicaciones web para generar un manual.
- Aplicar el manual de buenas prácticas de seguridad sugeridas en el trabajo de Ordoñez Sandra y Chimbo Kevin en el mantenimiento del subsistema Sílabos 1.0.0.
- Aplicar buenas prácticas de disponibilidad de información en el mantenimiento del subsistema Sílabos 1.0.0 mediante el uso del estándar IEEE 1219.
- Determinar el nivel de disponibilidad de información del subsistema Sílabos 1.0.0 a través de pruebas de intrusión para obtener el estado una vez realizado el mantenimiento.

CAPÍTULO II

2. FUNDAMENTOS TEÓRICOS

En el presente capítulo se abordará la información necesaria y suficiente de los conceptos y definiciones que se utilizarán en este Trabajo de Integración Curricular.

2.1 Sílabo

Según la Universidad del Pacífico un sílabo "es una herramienta de planificación del curso que organiza los contenidos y el trabajo que se realizará en el semestre académico para lograr el aprendizaje que se propone en el curso" (Sánchez y Araujo, 2019).

En el modelo académico de las Carreras de la Escuela Superior Politécnica de Chimborazo, consta de los datos generales y específicos de la asignatura, estructura y desarrollo de la asignatura, escenarios de aprendizaje (Reales, Virtuales, Áulicos), Criterios normativos para la evaluación de la asignatura, bibliografía básica y complementaria, perfil del profesor que imparte la asignatura (ESPOCH, 2019). Esto aporta a que los estudiantes puedan tener información de lo que se presentará en el transcurso del semestre.

2.2 Aplicación web

Hoy en día las aplicaciones web han evolucionado de manera extraordinaria, mismas que se utilizan alrededor del mundo, por lo tanto, es necesario conocer en qué consisten:

> *Una aplicación Web consiste en un software basado en Internet, en el cual una población extensa de usuarios, por medio del navegador, hacen peticiones remotas y esperan una respuesta que puede implicar una mezcla de publicación impresa y desarrollo de software, de mercadeo e informática, de comunicaciones internas y relaciones externas, y de arte y tecnología.* (Mendoza y Barrios, 2004, p. 90)

En lo que respecta a lo que Mendoza y Barrios mencionan, se resalta que una aplicación consiste en un software basado en internet, sin embargo, se cuestiona que estas aplicaciones estén destinadas a una población extensa, ya que muchas de las veces dichas aplicaciones están destinadas para una cierta cantidad de usuarios, según el objetivo de la misma. Desde otra

perspectiva. Según Shklar y Rosen en su libro Principios, Protocolos y Prácticas de la Arquitectura de Aplicación Web mencionan que una aplicación web:

> *Es algo más que solo un sitio web, es aquella que utiliza un navegador web como programa cliente, y permite transformar un servicio interactivo conectándose con servidores a través de Internet (o Intranet).Un sitio web simplemente entrega contenido desde files estático. Una aplicación Web presenta un contenido adaptado dinámicamente basado en parámetros de solicitud, comportamientos de seguimiento de los usuarios y consideraciones de seguridad.* (Shklar y Rosen, 2003, p. 5)

En cuanto a la concepción de aplicación web por parte de Shklar y Rosen se resalta que una aplicación web permite transformar un servicio interactivo por medio de servidores en el internet. Sin embargo, en lo que respecta a consideraciones de seguridad, muchas de las aplicaciones no disponen de seguridad robusta, por ello el presente trabajo propone aplicar buenas prácticas de disponibilidad que fortalezcan a la seguridad. Además, según Gao y Miao en su artículo científico sobre la reconfiguración dinámica de la aplicación Web utilizando la verificación de compatibilidad en dos fases afirman que "una aplicación web es una parte esencial de nuestra vida diaria. Se considera el paradigma informático más prometedor para crear aplicaciones que permitan resolver problemas sofisticados en el ámbito del comercio electrónico y la investigación científica" (Gao y Miao, 2013, p. 2265). Respecto a lo que Gao y Miao plantean es interesante que una aplicación web sea considerada un paradigma informático más prometedor para crear aplicaciones, y que las mismas puedan ser utilizadas en varios ámbitos.

Otra de las consideraciones de lo que es una aplicación web según Pressman en su libro Ingeniería de Software un enfoque para el practicionista afirma que una aplicación web:

> *Llamadas "WebApps", esta categoría de software centrada en la red abarca una amplia gama de aplicaciones. En su forma más simple, las WebApps pueden ser poco más que un conjunto de archivos de hipertexto enlazados que presentan información utilizando texto y gráficos limitados. Sin embargo, a medida que surge la Web 2.0, las aplicaciones Web evolucionan hacia entornos informáticos sofisticados que no sólo proporcionan funciones informáticas y contenidos independientes al usuario final, sino que también se integran con las bases de datos corporativas y las aplicaciones empresariales.* (Pressman, 2005: p. 8)

Mientras más sofisticada sea una aplicación web mayores recursos conlleva, especialmente el recurso económico. Según Sampath et al. (2007) en su artículo científico Aplicación del análisis de conceptos a las pruebas basadas en sesiones de usuario de aplicaciones Web mencionan que una aplicación web:

> *Consiste en un conjunto de Páginas Web y componentes que forman un sistema que se ejecuta utilizando servidores Web, red, HTTP y navegador(s) en los cuales la entrada del usuario (navegación y entrada de datos) afecta el estado del sistema. Una página Web puede ser estática en cuyo caso, el contenido es el mismo para todos los usuarios o dinámica, de modo que su contenido puede depender de la entrada del usuario.* (Sampath et al., 2007, p. 644)

De acuerdo a Sampath las aplicaciones web utilizan el protocolo HTTP lo cual tiene sus ventajas, y al ser ejecutadas en un navegador web estás son muy accesibles para el usuario, sin embargo, una aplicación web no puede ser solo estática o solo dinámica, la unión entre estática y dinámica resulta en una aplicación web donde está gestione y procese información que permita resolver problemas a los usuarios.

En resumen, una aplicación web es un software basado en internet que utiliza servidores web, red, el protocolo HTTP, para poder ser ejecutadas en un navegador web el cual es independiente del sistema operativo lo cual permite que sean muy accesibles para los usuarios, que a su vez realizan peticiones para resolver un problema en varios ámbitos ya sea empresarial, educativo, tecnológico, etc. Gracias a la combinación de páginas estáticas, dinámicas y demás elementos se puede alcanzar un nivel de sofisticación muy alto permitiendo resolver problemas muy complejos. Debido a todo esto su utilización se encuentra en el punto cumbre.

2.2.1 Componentes

Una aplicación web está conformada por varios componentes que trabajan en conjunto, la agrupación de los mismos se denomina aplicación web, ya que un componente por sí solo no cumple con las funciones para las que están destinadas hoy en día, por ello, en la Figura 1-1, se puede observar el flujo de datos entre los componentes.

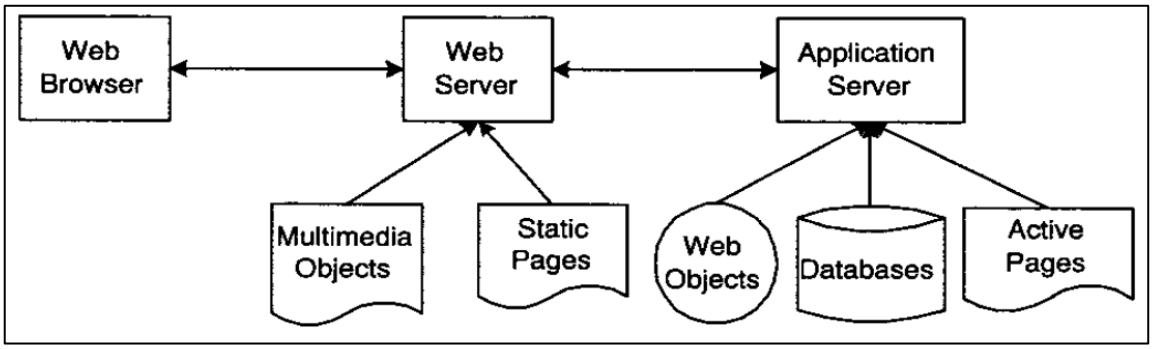

Figura 1-2. Flujo de datos entre los componentes de una aplicación Web
Fuente: (Hassan y Holt, 2002, p. 350)

En la figura 1-2 se puede ver el flujo donde el usuario interactúa con el navegador el cual realiza peticiones al servidor web este identifica si puede realizar la petición directamente o debe invocar al servidor de la aplicación para poder cumplir con las peticiones que realiza el usuario. Es importante, tener claro en que consiste cada uno de los componentes, según Hassan y Holt en su artículo científico Recuperación de la Arquitectura de Aplicaciones Web mencionan la descripción de cada uno de los componentes:

> *Páginas estáticas, contienen HTML y son ejecutables en un navegador web. Páginas activas, contienen una mezcla entre etiquetas HTML y código ejecutable integra datos de diversos recursos como objetos web o bases de datos. Objetos Web, piezas de código compilado que proporcionan un servicio al resto del sistema software a través de una interfaz definida. Objetos Multimedia, como imágenes y videos. Base de Datos, se utilizan para almacenar datos y ser compartidos por los demás componentes.* (Hassan y Holt, 2002, pp. 350-351)

Según Hernández et al. afirman que "la mayoría de aplicaciones Web trabajan con base de datos, interactúan con un Sistema Gestor de Base de Datos. No es necesario tenerlo físicamente en el servidor de la aplicación, para mejorar el rendimiento es aconsejable separarlo del servidor" (Hernández Diaz et al., 2012, p. 9). Esto es importante al momento de desarrollar una aplicación web ya que esto puede determinar que el funcionamiento sea correcto o no, de acuerdo a la función que la misma esté destinada a cumplir.

Existen distintas nociones sobre los componentes de una aplicación web, por ello según Ordax y Ocaña (Ordax y Ocaña, 2012, pp. 6-7) proponen los siguientes:

- **Componentes cliente:** son aplicaciones Java SE (AWT/Swing, Applets) o un navegador web (Firefox, Chrome, IExplorer…). Se despliegan en la capa cliente.
- **Componentes web:** son Java Servlets, JavaServer Pages (JSP) o JavaServer Faces (JSF). Se despliegan en la capa web.
- **Componentes de negocio:** Enterprise JavaBeans (EJB). Se despliegan en la capa de negocio.

Estos componentes son esenciales para que una aplicación web funcione correctamente, sin embargo, dichos componentes difieren según la aplicación web que se desee desarrollar. Pero esto no significa que se debe desatender a ciertos componentes, uno que no funcione implica que haya errores al momento de ejecutar la misma. Entre los más importantes, los componentes cliente; es decir navegadores. Componentes web; páginas jsp, java, etc. Componentes de negocio; donde se encontrará el acceso a datos para la gestión de la información proveniente de servicios y base de datos de la aplicación.

2.2.2 Ventajas

Existe una cantidad innumerable de ventajas que proporcionan las aplicaciones web, por ello se describen algunas de ellas a continuación:

- Se pueden utilizar en distintos ámbitos científico, cultural, académico, empresarial entre otros, y esto es debido a las múltiples ventajas que el usuario tiene respecto a los programas de escritorio. (Molina Ríos et al., 2018, p. 4)
- Otra de las ventajas, es el sistema operativo multiplataforma. Es decir, pueden ser ejecutadas por cualquier dispositivo el cual disponga de una conexión a internet. (Molina Ríos et al., 2018, p. 4)
- Para poder usarlas solo se necesita un navegador web, esto evita que se tenga que instalar en el dispositivo que se requiera utilizar dicha aplicación web. (Molina Ríos et al., 2018, p. 4)
- Una de las grandes ventajas es que la información que se gestiona puede ser compartida por varios usuarios al mismo tiempo. Los datos son almacenados en un servidor lo cual facilita el uso. (Molina Ríos et al., 2018, p. 4)
- Otra de las ventajas es que el problema de gestionar el código en el cliente se reduce drásticamente. No solo se reduce el tiempo de actualización, además no hay que desplazarse de un puesto de trabajo a otro. (Luján-Mora, 2002, p. 54)
- Si la empresa ya dispone de internet no se necesitan incurrir a comprar o instalar herramientas para los clientes. (Luján-Mora, 2002, p. 54)
- Otra ventaja, es que de cara al usuario, los servidores externos (Internet) e internos (intranet) aparecen integrados, lo que facilita el aprendizaje y uso. (Luján-Mora, 2002, p. 54)

2.2.3 Desventajas

Las aplicaciones web también tienen ciertas desventajas, no todo puede ser positivo, por ello se describen algunas a continuación:

- Una de las principales desventajas es que al necesitar de conexión a internet puede verse afectada por ataques los cuales pueden dañar o hurtar la información que se gestiona en dichas aplicaciones web.
- La utilización está limitada a disponer de internet, en caso de que no haya dicha conexión no se puede hacer uso.
- Si no se dispone de una infraestructura para poder desplegar una aplicación web, se necesita incurrir en gastos de servidores, o arriendos de los mismos.
- Los datos que se manejan dentro de las aplicaciones web pueden ser utilizados indebidamente si las aplicaciones no cuentan con un buen nivel de seguridad.

2.3 Arquitectura

La arquitectura de una aplicación es un punto muy importante a tratar "el modelo de aplicaciones Java para servicios como aplicaciones multicapa que aseguren escalabilidad, accesibilidad necesarias en un ámbito empresarial. El modelo divide en dos partes, lógica de presentación y de negocio a implementar por el desarrollador y los servicios estándar" (Ordax y Ocaña, 2012, p. 5). Esto es importante ya que se separa la lógica de negocios de la interfaz, facilitando entre muchos aspectos la funcionalidad de la aplicación, así como el mantenimiento de la misma.

Además, la aplicación web del presente trabajo se encuentra desarrollada en n capas, es decir "la lógica de la aplicación se divide en distintos componentes dependiendo de su funcionalidad, y estos son desplegados en las distintas capas dependiendo de a cuál pertenecen" (Ordax y Ocaña, 2012, p. 5). En la cual se considera distintas capas cada una con distintas funciones a cumplir. Se detallan a continuación las capas involucradas:

- **Capa Cliente:** donde el cliente interactúa con la aplicación web.
- **Capa Web:** como función principal la administración de la aplicación, a veces se encarga de interactuar con el cliente.
- **Capa de Negocio:** se encarga de la parte lógica.
- **Capa de Datos:** se encarga de la persistencia, así como transacciones y manejo de los mismos.

A continuación, se muestra en la Figura 2-2, el diagrama de despliegue donde se detalla la arquitectura de la aplicación web en la que se va a centrar la aplicación de las buenas prácticas de disponibilidad.

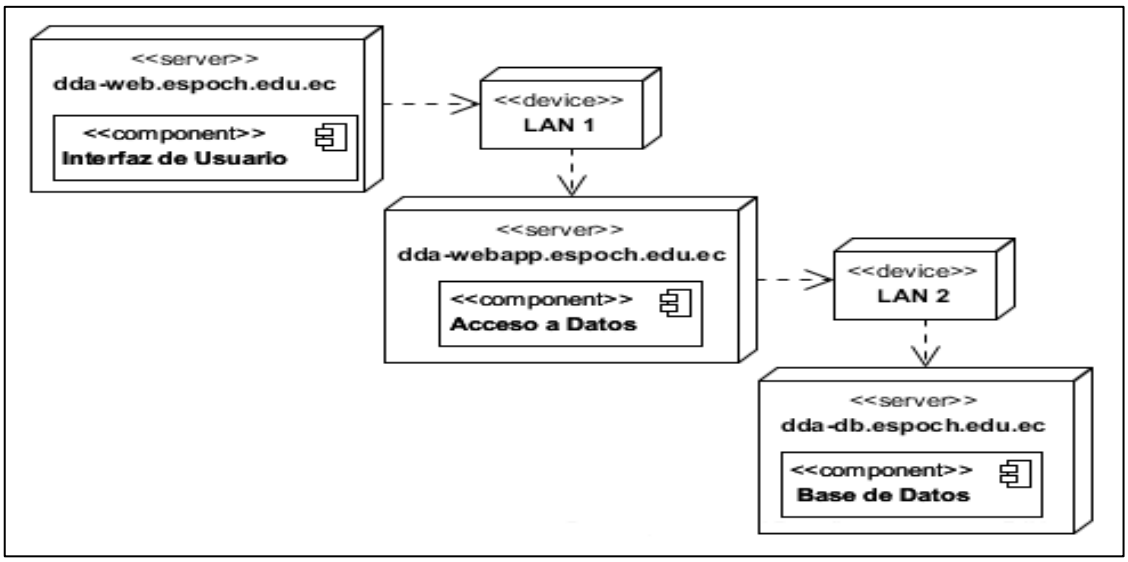

Figura 2-2. Diagrama de Despliegue

Fuente: (Veloz y Menéndez, 2016)

Este diseño, toma en cuenta la necesidad de integrar los módulos o subsistemas, a parte de su fácil implementación, es decir es escalable, donde la comunicación entre los módulos y subsistemas se los realiza por medio de los Servicios Web SOAP. Esta arquitectura pretende responder al requisito funcional planteado por la Dirección de Desarrollo Académico (DDA), de que el sistema permite introducir cambios o adaptarse a nuevas regulaciones existentes en la institución. Es decir que la aplicación se una aplicación en n-capas (Veloz y Menéndez, 2016). Está arquitectura en n-capas, aunque disminuye el desempeño por la cantidad de componentes por los que tiene que pasar una petición, facilita las actividades de mantenimiento, lo cual es un punto a favor para el desarrollo del presente Trabajo de Integración Curricular, además, la arquitectura propuesta facilita la rápida adaptación a un aumento inesperado de peticiones.

La descomposición modular propuesta, toma en cuenta la máxima cohesión posible, o sea están enfocados a un requisito funcional básico, simplificando la realización de cambios necesarios. Esto con el objetivo de disminuir el acoplamiento entre las capas del sistema, implementa los Servicios Web SOAP que encapsulen, o sea oculten los detalles de implementación de la lógica del negocio, facilitando la modificación de la aplicación con impactos mínimos en otras capas dependientes, además de aumentar la reutilización de partes de la aplicación en otros.

2.4 Patrón de diseño modelo vista controlador

El patrón modelo vista controlador en lo que respecta al desarrollo de aplicaciones Web es uno de los más utilizados. Según Leff y Rayfield respecto a MVC mencionan:

> *En MVC, la Vista muestra información al usuario y, junto con el Controlador que procesa la interacción del usuario, comprende la cara de usuario de la aplicación. El Modelo es la parte de la aplicación que contiene tanto la información representada por la Vista como la lógica que cambia esta información en respuesta a la interacción del usuario. El uso del patrón de diseño MVC facilita el desarrollo y mantenimiento de una aplicación ya que: el "look" de la aplicación puede cambiarse drásticamente sin cambiar las estructuras de datos y la lógica de negocio.* (Leff y Rayfield, 2001, p. 118)

Por lo tanto, una de las grandes ventajas como mencionan Leff y Rayfield es la facilidad de mantenimiento que proporciona, así como la escalabilidad, lo fácil que es cambiar la estructura de datos, lógica de negocios, inclusive la interfaz, esto facilita aplicar las buenas prácticas de disponibilidad en el subsistema Sílabos ya que se encuentra desarrollada utilizando este patrón. Mientras que según Abran et al. En su publicación Arquitectura Orientada a Patrones para Aplicaciones Web mencionan:

> *El patrón MVC se utiliza comúnmente para estructurar aplicaciones web que tienen requisitos de procesamiento significativos. Esto hace que sean más fáciles de codificar y mantener. MVC se utiliza aquí para describir los componentes principales de la arquitectura de las aplicaciones Web, mientras que MVC se considera una arquitectura de 3 niveles que a menudo es utilizada por los diseñadores de aplicaciones Web para mantener múltiples vistas de los mismos datos.* (Abran et al., 2007, p. 2)

Utilizar MVC implica que permite a la aplicación web alcanzar un nivel sofisticado, y resolver problemas complejos. Concretamente, según Kristaly et al. "El objetivo del patrón de diseño MVC es separar el objeto de la aplicación (modelo) de la forma en que se representa al usuario (vista) de la forma en que el usuario lo controla (controlador)" (Kristaly et al., 2005, p. 2). Para mayor comprensión de MVC se detalla a continuación en que consiste el modelo, la vista y el controlador:

- **Modelo:** A breves rasgos, es el encargado de actualizar datos (Abran et al., 2007, p. 2). Incluye la lógica de negocio de la aplicación, esto permite probar y depurar la aplicación fácilmente, esto consiste en que el modelo no tenga que lidiar con el mundo exterior, el modelo recibe las entradas y calcula las salidas, la reutilización de código es máxima, el código escrito para este componente resuelve el problema. Permite acceder a los datos y se los gestiona independientemente de la IU (Kristaly et al., 2005, p. 3). Es decir, facilita el modificar el procesamiento de datos permite hacerlo de forma independiente sin que se afecte el funcionamiento de la aplicación.
- **Vista:** Permite al usuario visualizar la información (Abran et al., 2007, p. 2). Consiste en la presentación de la aplicación, es la forma en cómo se presenta los datos al usuario. Al separar la vista del modelo es posible crear interfaces de usuario diferentes, sin la necesidad de cambiar la forma de procesar los datos. Es decir se muestra la información que requiere el usuario (Kristaly et al., 2005, p. 3). Permite al usuario interactuar con la aplicación y facilita el modificar el procesamiento de datos.
- **Controlador:** Se encarga de la gestión de eventos que afectan tanto al modelo como a la vista (Abran et al., 2007, p. 2). Es aquel que recibe los eventos y determina las acciones de acuerdo a cada situación, en concreto se puede decir que es el centro de envío de eventos, cumple diversas tareas, en el aspecto de seguridad es responsable de autenticación de los usuarios, identificación del evento, así como identificar el evento sugerido, preparación del modelo, procesamiento de eventos, es decir lanza, según un mapa de eventos. Además, se encarga del tratamiento de errores, envío de la respuesta, etc. (Kristaly et al., 2005, pp. 3-4). Funciona como un enrutador, es decir indica los eventos y lo que la aplicación debe hacer en cada situación según lo que el usuario requiera.

Del patrón de diseño MVC, se resalta que es un patrón que permite el fácil mantenimiento de una aplicación web, de igual forma realizar cambios se convierte en una actividad sencilla, la presente aplicación web a implementar las buenas prácticas de disponibilidad está desarrollada por medio de este patrón, como se muestra en la Figura 3-1, donde se detalla un diagrama de despliegue con la utilización de MVC.

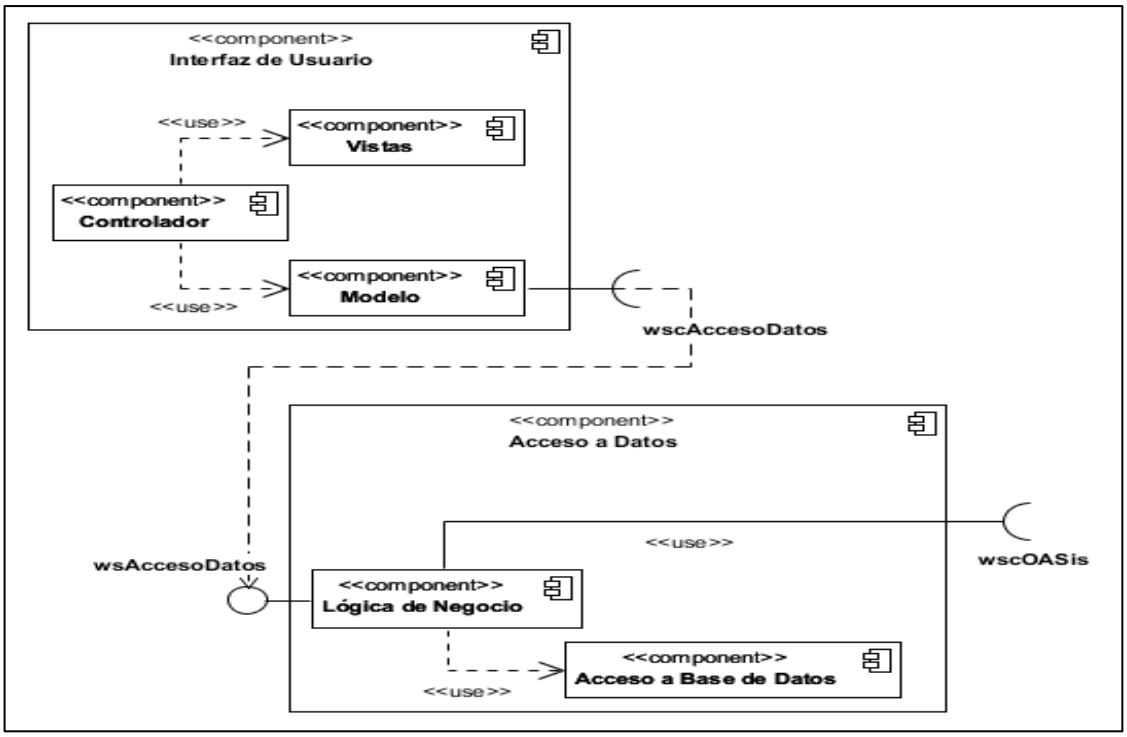

Figura 3-2. Diagrama de Componentes

Fuente: (Veloz y Menéndez, 2016)

En la Figura 3-2 se puede observar el Diagrama de componentes del Subsistema Sílabos donde cuenta con un componente de interfaz de usuario que facilitará la comunicación entre los usuarios y el sistema informático, gestionando la información por medio del componente de Acceso a Datos. El componente interfaz de usuario tendrá el patrón de arquitectura de software Modelo Vista Controlador (MVC) lo que permitiré que el subsistema sea robusto y se potencie la facilidad de mantenimiento, reutilización del código y separación de conceptos (Veloz y Menéndez, 2016). Lo cual contribuye a la aplicación de las buenas prácticas en el subsistema haciendo posible el desarrollo del presente Trabajo de Integración Curricular. Por otra parte, en el componente de Acceso a Datos se implementará toda la Lógica de Negocio (componente Lógica de Negocio) apoyándose para la obtención de información en el componente de Acceso a Datos y de otros Clientes de Servicios Web provisto por otras aplicaciones.

2.5 Seguridad informática

La seguridad informática es un punto clave, según Roa en su libro Seguridad Informática afirma que "la seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital. Controla conexiones a la red de la empresa. Ahora las redes necesitan estar más abiertas al exterior, estarán más expuestas a ataques desde cualquier parte del mundo" (Roa Buendía, 2013, p. 8). Esto implica que cualquier persona con conocimientos y una conexión a internet pueden adquirir información y utilizarla para perjudicar a los usuarios de la aplicación web.

Además, según Dussan en su artículo científico Políticas de Seguridad menciona que "ofrecer productos o servicios a través de Internet sin considerar la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación y afectar los ciclos del negocio" (Dussan Clavijo, 2006, p. 87). La falta de seguridad en una aplicación web es una irresponsabilidad, implica que los usuarios pueden perder información muy importante para ellos. Según Pressman en su libro Ingeniería de Software un Enfoque para el Practicionista menciona:

> *Las aplicaciones Web se han integrado en gran medida con las bases de datos corporativos y gubernamentales más importantes. Las aplicaciones de comercio electrónico extraen y almacenan información sensible del cliente. Por estas y muchas otras razones, la seguridad de WebApp es punto cumbre en muchas situaciones. La medida clave de la seguridad es la capacidad de la WebApp y su entorno de servidor para rechazar el acceso no autorizado y/o frustrar un ataque totalmente malintencionado.* (Pressman, 2005, p. 375)

Es decir, por medio de la seguridad informática se evita que las aplicaciones web sean atacadas al estar en el internet, la información que se manejan en las mismas tendrán mayor protección lo cual es sustancial, ya que a pérdida de información denota grandes pérdidas, así como la evidencia de la falta de responsabilidad al lanzar aplicaciones no seguras.

Según Kizza en su libro Seguridad de las redes informáticas considera que en un sistema informático:

> *Su seguridad implica la seguridad de todos sus recursos tales como sus componentes físicos de hardware tales como lectores, impresoras, la CPU, los monitores, y otros. Además de sus recursos físicos, también almacena recursos no físicos como datos e información que necesitan ser protegidos. Por lo tanto, la seguridad significa prevenir el acceso no autorizado, el uso, la alteración y el robo o daño físico a estos recursos.* (Kizza, 2005: p. 49)

Mientras que otro autor como Vacca, en su libro Prácticas de Seguridad en Internet afirma "la verdadera seguridad sólo puede lograrse cuando la información está aislada, encerrada en caja fuerte, rodeada de guardias, perros, cercas, y se hace inaccesible. Algunos argumentarían que, incluso en ese caso, no existe una seguridad absoluta. Simplemente no es posible" (Vacca, 2007: p. 27). Sin embargo, para Kalman en su libro Guía de Campo de Seguridad Web la seguridad es "herramientas y técnicas que evitan que personas o procesos no autorizados hagan algo con o para sus datos, computadoras o periféricos" (Kalman, 2003: p. 50). Independientemente si se logra la máxima seguridad o no es muy importante la implementación de medidas de seguridad en el desarrollo una aplicación web.

Así según Media Planet en su libro Fundamentos de la Ciberseguridad afirma que "los profesionales de la Ciberseguridad son muy solicitados y necesitamos asegurarnos de que estamos reponiendo el talento y enseñando a la próxima generación" (Media Planet, 2016, p. 15). Esto invita a que es necesario la preparación en ámbitos concernientes a la utilización de medidas de seguridad para el desarrollo de aplicaciones mucho más robustas, que generen confianza en los usuarios finales.

La seguridad es toda herramienta, técnica y medida que permita a un sistema informático preservar su confidencialidad, integridad y disponibilidad, esto con el fin de que la información del usuario no se vea afectada, ni utilizada por otras personas de manera incorrecta.

2.5.1 Principios

Según Guamán al hablar de aplicaciones Web se está haciendo directamente referencia a seguridad lógica, y para ello es necesario garantizar los principios de la seguridad informática, como lo menciona Guamán en su Tesis sobre Seguridad en entornos web para sistemas de gestión académica (Guamán Quinche, 2011, p. 509):

- **Confidencialidad:** los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello. Asegura el secreto de las comunicaciones contenidas en los mensajes.
- **Integridad:** los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada. Hace referencia al hecho de que la información no pueda ser manipulada en el proceso de envío.
- **Disponibilidad:** los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

Sin embargo, para Kizza en su libro Seguridad de las redes informáticas (Kizza, 2005, p. 49) los principios de seguridad los considera de la siguiente manera:

- **Confidencialidad:** para evitar la divulgación no autorizada de información a terceros. Esto incluye la divulgación de información sobre los recursos.
- **Integridad:** para evitar la modificación no autorizada de los recursos y mantener el statusquo. Incluye la integridad de los recursos del sistema, la información y el personal. La alteración de recursos como la información puede ser causada por un deseo de beneficio personal o por la necesidad de venganza.
- **Disponibilidad:** para evitar la retención no autorizada de recursos del sistema a quienes los necesitan cuando los necesitan.

En base a lo anterior, el principio de confidencialidad, consiste en que los elementos de un sistema no puedan ser accedidos por personas ajenas a la propietaria. Con respecto a la integridad, no permitir modificaciones dentro del sistema. Disponibilidad, garantizar que un sistema funcione en los tiempos establecidos y permitidos, evitando interrupciones no autorizadas.

2.6 Estándares para la gestión de la seguridad

Actualmente, existen varios estándares que proporcionan un marco para la gestión de la seguridad, entre ellos se encuentran la familia de las normas ISO 27000, según Mentor "contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener" (Mentor, 2018). Por ello se detalla a continuación, en la tabla 1-2 las normas que se encuentran dentro de la ISO 27000:

Tabla 1-2: Familia de Normas ISO 27000

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.
ISO/IEC 27002	Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.

Continua

Continua

ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información.
ISO/IEC 27006	Esta norma específica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

Fuente: Mentor, 2018

Realizado por: Ramos Averos, Rodrigo, 2020.

En la tabla se detalla en que consiste cada una de las normas que se encuentran dentro de la familia de Normas ISO 27000. Además, la ISO 15408, permite que diferentes aplicaciones puedan ser probadas e integradas de forma segura (ISO, 2009, p. 8). También, el RFC 2196 para políticas y procedimientos de seguridad" (Fraser, 1997, p. 3). Sin embargo, para el presente trabajo la norma ISO/IEC 27001 proporciona un enfoque relacionado con la disponibilidad.

2.7 Norma ISO/IEC 27001

Se puede considerar que la norma ISO 27001 "es un conjunto de estándares desarrollados en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), proporcionan un marco de gestión de seguridad de información utilizable por cualquier organización, pública o privada, grande o pequeña" (ISO27000, 2019).

Mientras que Serrano en su publicación ISO 27001 Seguridad de la Información menciona "la ISO 27001 o más exactamente ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Requisitos de un Sistema de Gestión de Seguridad de la Información es un estándar reconocido internacionalmente" (Serrano, 2015).

Dentro de la ISO fundamentalmente el objetivo es la seguridad de la información, enfocada en garantizar la confidencialidad, integridad y disponibilidad, garantizando confianza dentro de la empresa donde se la utilice.

El presente trabajo se enfoca en aplicar buenas prácticas de disponibilidad de información, según la Norma ISO/IEC 27001 (ISO, 2013), la cual se basa en la preservación de su confidencialidad, integridad y disponibilidad, por ello se los detalla a continuación:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

2.7.1 Modelo de pirámide

Este modelo de pirámide "en el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001" (ISO27000, 2019) de la siguiente forma:

Figura 4-2. Modelo Pirámide ISO 27001
Fuente: (ISO27000, 2019)

Donde, el manual de seguridad; se refiere a un documento que se expone alcance, responsabilidades, políticas, objetivos y directrices principales. Procedimientos; documentos a nivel operativo donde se controla la planificación, operación y control. Instrucciones, Cheklists y Formularios; documentos que se refieren a tareas que tienen que ver con la seguridad. Registros; documentos que contienen la evidencia (ISO 27001 - Software ISO 27001 de Sistemas de Gestión, 2019).

2.7.2 Beneficios

Existen varios beneficios que otorga la norma ISO 27001 (2019, p. 8) entre los más importantes se menciona:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Descubrir los riesgos de seguridad no controlados.
- Iniciar la protección activa y eficaz de los riesgos.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001L).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.

2.7.3 Novedades

Algunas de las novedades que fueron añadidas a la Norma 27001 (ISO 27001 - Software ISO 27001 de Sistemas de Gestión, 2019, p. 12) son las siguientes:

- No aparece la sección "Enfoque a procesos" con su respectiva metodología basada en el ciclo PHVA, ahora ofrece mayor flexibilidad.
- Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad.
- Se han revisado los requisitos y controles.
- Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación.

2.8 OWASP

A continuación se detalla, en que consiste OWASP, directamente de la página oficial donde se encuentra mucha información respecto a la misma:

> *El Open Web Application Security Project (OWASP) es una organización benéfica mundial sin fines de lucro enfocada en mejorar la seguridad del software. OWASP se encuentra en una posición única para proporcionar información imparcial y práctica sobre AppSec a*

> *individuos, corporaciones, universidades, agencias gubernamentales y otras organizaciones en todo el mundo. Operando como una comunidad de profesionales con ideas afines, OWASP emite herramientas de software y documentación basada en el conocimiento sobre seguridad de aplicaciones.* (OWASP, 2019)

Además, todos son libres de participar en OWASP los materiales están disponibles bajo una licencia de software libre y abierto. Encontrará todo sobre OWASP aquí o en nuestro wiki e información actual en nuestro Blog de OWASP. OWASP no respalda ni recomienda productos o servicios comerciales, permite que la comunidad permanezca neutral con la sabiduría colectiva de las mejores mentes en seguridad de software en todo el mundo (OWASP, 2019). Cabe recalcar que dentro de dicha comunidad se puede encontrar mucha información que permite mejorar la seguridad de las aplicaciones, además de disponer de contenido gratuito, con buenas soluciones aportadas por personas de todo el mundo, lo que permite desarrollar nuestro conocimiento en el aspecto de seguridad.

2.9 Disponibilidad

Existen algunos conceptos de varios autores entre los más destacados, se encuentra Magerit que define:

> *La disponibilidad como grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Se produce cuando se puede acceder a un sistema de información en un período de tiempo considerado aceptable. Asociada a la fiabilidad técnica de los componentes del sistema de información.* (PAe - MAGERIT, 2012, p. 39)

Según Roa en su libro Seguridad Informática "la disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido. Para ello se invierte en sobredimensionar los recursos" (Roa Buendía, 2013, p. 15). Sin embargo, para Dussan en su artículo científico acerca de Políticas de Seguridad informática afirma que "una vez que nos aseguramos que la información correcta llegue a los usuarios correctos, debemos garantizar es que llegue en el momento oportuno, y precisamente de esto trata el tercer principio: la disponibilidad. Para que una información se pueda utilizar, deberá estar disponible" (Dussan Clavijo, 2006, p. 88). La disponibilidad se puede simplificar en garantizar que un sistema sea utilizado por los usuarios en el momento que ellos desean sin que haya interrupciones de ningún tipo.

Ahora bien, cabe recalcar acerca de alta disponibilidad según Costas en su Libro sobre Seguridad y Alta Disponibilidad se refiere a la disponibilidad como "la capacidad de que aplicaciones y

datos se encuentren operativos para los usuarios autorizados en todo momento, debido a su carácter crítico" (Costas Santos, 2014, p. 186).

Mientras otros autores como Offutt en su publicación Atributos de Calidad de las Aplicaciones Web menciona:

> *Disponibilidad significa algo más que estar en funcionamiento 24 horas al día, 7 días a la semana, 365 días al año. El software debe estar disponible cuando se accede a él a través de diversos navegadores. Las aparentemente interminables guerras de navegadores de los últimos años han significado que los vendedores de software utilicen funciones que sólo están disponibles para un navegador. Para estar disponibles en este sentido, los sitios web deben adaptar sus presentaciones para que funcionen con todos los navegadores, lo que requiere un conocimiento y una experiencia mucho mayor, esfuerzo por parte de los desarrolladores.* (Offutt, 2002, pp. 5-6)

Una de las buenas prácticas como lo dice Offutt es que la aplicación web funcione igual en todos los navegadores, de esta forma garantizar que la aplicación se presente de igual forma y esté disponible. Según Pressman en su libro Ingeniería de Software un Enfoque para el Practicionista menciona:

> *Aunque la expectativa de una disponibilidad del 100 por ciento no es razonable, los usuarios de las aplicaciones Web más populares a menudo exigen acceso las 24 horas del día, los 7 días de la semana, los 365 días del año. Incluso la mejor WebApp no satisfará las necesidades de los usuarios si no está disponible. En un sentido técnico, la disponibilidad es la medida del porcentaje de tiempo que una aplicación Web está disponible para su uso. Cualquier otra cosa se considera inaceptable.* (Pressman, 2005, p. 7)

La disponibilidad consiste en la capacidad que dispone una aplicación web para encontrarse operativa en cualquier momento que los usuarios requieran utilizarla, sin embargo, la disponibilidad no solo tiene que ver con el tiempo, sino, también que la aplicación web haga lo que tenga que hacer de la misma forma independientemente de las condiciones en que el usuario la ejecute, en el momento preciso.

2.10 Amenazas

Existen amenazas que pueden comprometer la disponibilidad de información según Costas en su libro sobre Seguridad y Alta Disponibilidad afirma:

> *Las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Las amenazas pueden ser provocadas por: personas, condiciones físicas-ambientales y software, o lógicas.* (Costas Santos, 2014, p. 24)

Además, según Weik en su publicación Diccionario de Informática y Comunicaciones menciona que una amenaza es "una violación potencial de la seguridad del sistema, como el procesamiento automático de datos, las comunicaciones, la computadora, la información o la seguridad del sistema de control" (Weik, 2001, p. 398). Mientras que según Herrmann y Bucksch afirman que una amenaza simplemente es "exposición a un peligro" (Herrmann y Bucksch, 2014, p. 1390). Sin embargo, según Brauch en su libro Hacer frente al cambio ambiental mundial, los desastres y las amenazas a la seguridad, los desafíos, las vulnerabilidades y los riesgos menciona que una amenza es la posibilidad de que suceda un riesgo el cual puede ocasionar la destrucción del objetivo (Brauch, 2011, p. 62).

Una amenaza consiste en toda acción que afecte considerablemente un objeto en cuestión, así como la vulneración de la seguridad, un riesgo potencial que puede causar pérdidas cuantiosas e irreparables.

2.10.1 Tipos

Según el Departamento de Seguridad de la Universidad de Luján (2017) algunas de las amenazas más destacadas son las que se detallan a continuación:

- Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
- No intencionales, en donde se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).

2.11 Ataques

Anteriormente, se detalló información acerca de una amenaza pero también es importante conocer sobre que es un ataque, se considera un intento organizado e intencionado causada por una o más

personas para causar daño o problemas a un sistema informático o red (EcuRed, 2018). Además, un ataque puede ocasionar un sinnúmero de inconvenientes en los sistemas informáticos según Media Planet en su libro sobre Fundamentos de la Ciberseguridad "los sofisticados ataques que vimos hace sólo unos años entre Estados-nación están siendo utilizados ahora por delincuentes comunes contra todos los sectores de la economía" (Media Planet, 2016, p. 2). Motivos por el cual es conveniente tomar medidas de seguridad.

Según Weik en su publicación Diccionario de Informática y Comunicaciones menciona que un ataque "en seguridad del sistema, como procesamiento automático de datos, comunicaciones, información o seguridad del sistema de control, un intento de violar la seguridad del sistema, por ejemplo, mediante uso de escuchas clandestinas, lógica maliciosa o escuchas telefónicas" (Weik, 2001). Sin embargo según Mientras que según Sokol et al. en su publicación Definición de Ataque en Contexto de Interacción de Alto Nivel Honeypots menciona al ataque como "un intento de destruir, exponer, alterar, desactivar, robar u obtener acceso no autorizado (por ejemplo, escanear los puertos)" (Sokol et al., 2015, p. 163). Mientras que en el Diccionario de la Lengua Española define un ataque como "acción de acometer o emprender una ofensiva, perjudicar o destruir" (ASALE y RAE, 2019).

En resumen, un ataque consiste en todo intento de perjudicar, dañar y destruir un objetivo, violando la seguridad y obteniendo acceso no autorizado, con el fin de causar efectos adversos en el afectado.

2.11.1 Denegación de Servicio (DoS)

Es un ataque dirigido a la disponibilidad de aplicaciones, cuya finalidad no es robar información, sino ralentizar o destruir una aplicación web, en ocasiones las intenciones de los atacantes es por beneficio económico. Este ataque agota los recursos informáticos, impidiendo que los usuarios autorizados accedan a dicha aplicación web. (RADWARE, 2019a)

Estos ataques afectan a empresas en muchos sectores, muchas de las veces atacan a la capa de red y hasta la capa de aplicación (RADWARE, 2019a). En el ataque DoS los recursos o servicios no están disponibles para usuarios legítimos y se niegan o degradan para realizar una funcionalidad normal con el sistema. Se lo lleva a cabo con una petición superflua, lo cual causa una sobrecarga del sistema, lo que ocasiona que no responda inclusive se den fallos (Hack2Secure, 2019, p. 2).

Según Piqueras en su publicación Ataques de seguridad contra la disponibilidad de las redes LTEMobility: Descripción general y direcciones de investigación menciona que la atención se

centra sobre todo en los ataques locales, es decir, los atascos, así como en las amenazas contra la RAM que podrían ser aprovechadas por un solo atacante (Piqueras, 2013, p. 4). Además "es un tipo de ataque a un servidor de red con un gran número de peticiones de servicio que no puede manejar. Puede causar que el servidor se bloquee y los usuarios legítimos se vean privados del servicio" (OmniSecu, 2019, p. 3).

Sin embargo, cuándo ocurre este ataque, según el Departamento de Seguridad de Homeland:

> *Ocurre cuando los usuarios legítimos no pueden acceder a los sistemas de información, dispositivos u otros recursos de la red debido a las acciones de un actor de amenazas cibernéticas maliciosas. Los servicios afectados pueden incluir correo electrónico, sitios web, cuentas en línea (por ejemplo, banca) u otros servicios que dependen de la computadora o red afectada. Los ataques DoS pueden costar a una organización tiempo y dinero, mientras que sus recursos y servicios son inaccesibles.* (Departamento de Seguridad Homeland, 2009)

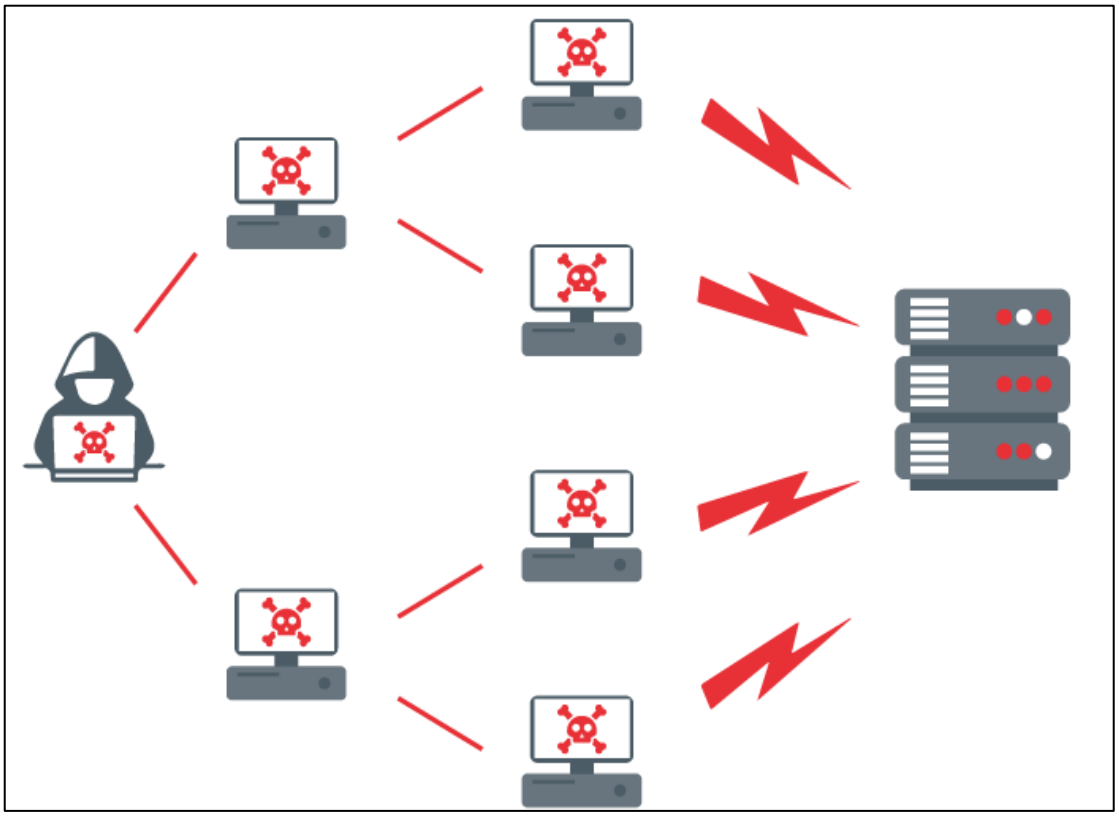

Figura 5-2. Denegación de Servicios (DoS)

Fuente: (Instituto Nacional de Ciberseguridad, 2019)

Un ataque de Denegación de Servicios consiste en dejar una aplicación web inutilizable, el cual se logra a través de una sobrecarga a los recursos de la aplicación. Este ataque ocurre muchas de las veces por beneficios económicos, más no por robar información.

2.11.1.1 ICMP Ping Flood

En el ataque ICMP Ping Flood, al equipo víctima se le envía muchos paquetes ICMP falsos (OmniSecu, 2019, p. 4). Consiste en el "envío anormalmente grande de paquetes ICMP de cualquier tipo (paquetes "ping" pruebas de latencia de red) abruma al servidor de destino que intenta procesar cada petición ICMP entrante, y puede resultar en una denegación de servicio para el servidor destino" (RADWARE, 2019b). Donde al quedar inutilizado el servidor la aplicación queda inaccesible para los usuarios. En la **Figura 6-2** se puede ver como es el proceso de este ataque para afectar a la víctima.

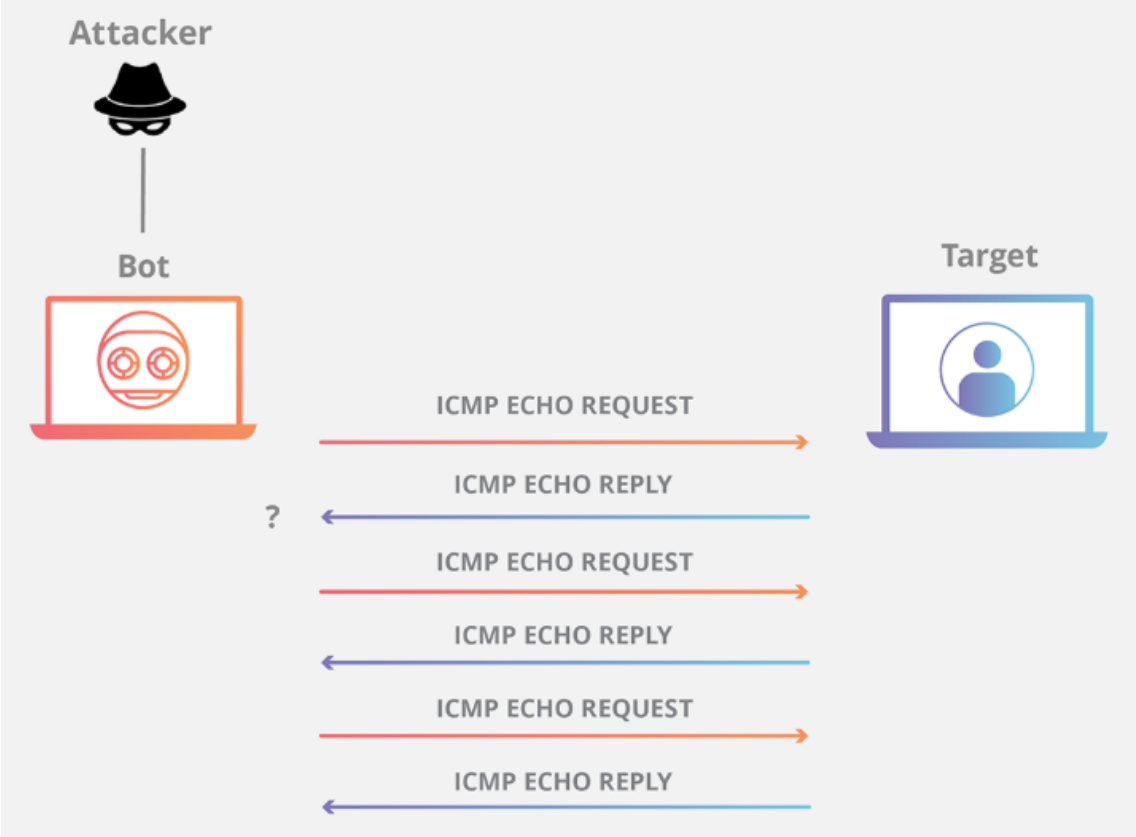

Figura 6-2. Ataque ICMP Ping Flood

Fuente: (Cloudflare, 2019)

2.11.1.2 Smurf Attack

Este ataque consiste en "enviar un gran número de peticiones echo (ICMP) a direcciones de Broadcast usando una IP de origen falsa. Esto provoca que la IP de origen sea inundada con multitud de respuestas" (Blasco, 2007, p. 7). Según el Departamento de Seguridad de Homeland menciona que "el atacante envía paquetes difusión del Protocolo de mensajes de control Internet a varios hosts con dirección IP origen falso perteneciente al equipo destino. Los destinatarios de

estos paquetes falsificados responderán, el anfitrión objetivo será inundado con esas respuestas" (Departamento de Seguridad Homeland, 2009). Además, según Cloudflare:

> *Puede ser considerado metafóricamente como un bromista llamando a un gerente de oficina y fingiendo ser el CEO de la compañía. El bromista le pide al gerente que le diga a cada empleado que vuelva a llamar al ejecutivo a su número privado y que le informe de cómo le va. El bromista da el número de devolución de llamada de una víctima objetivo, que luego recibe tantas llamadas telefónicas no deseadas como personas hay en la oficina.* (Cloudflare, 2019)

Este ataque, puede dejar la aplicación no disponible, es recomendable, revisar la configuración del router, con respecto a los paquetes enviados a sus direcciones de difusión por defecto. En la **Figura 7-2** se puede observar cómo funciona este ataque.

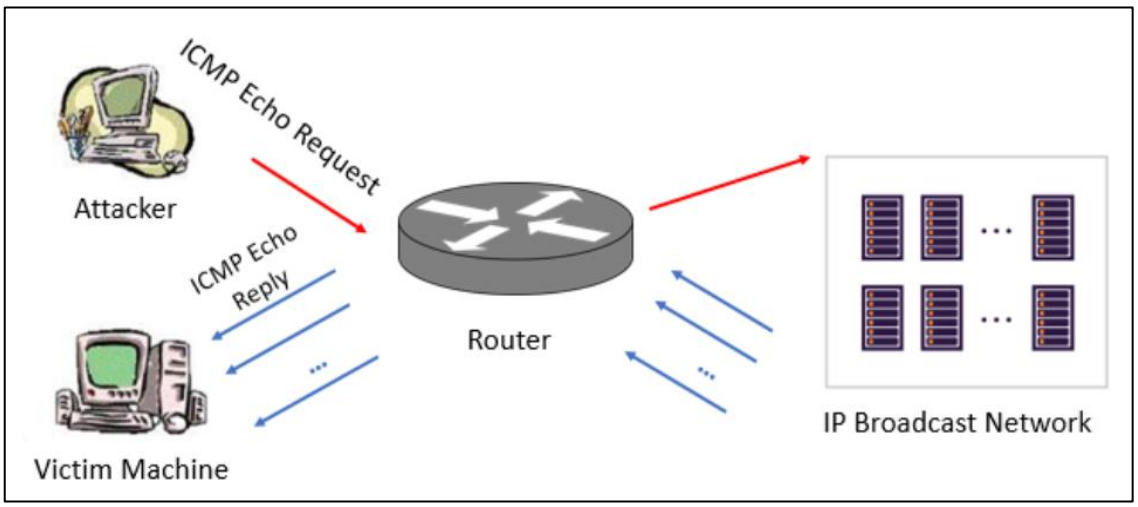

Figura 7-2. Smurf Attack

Fuente: (Hack2Secure, 2019, p. 4)

2.11.1.3 Fraggle Attack

Este ataque implica el envío enorme de tráfico UDP falsificado a la dirección de difusión de un enrutador dentro de una red. Similar a un Smurf Attack, que utiliza tráfico ICMP falso en lugar de tráfico UDP para lograr el mismo objetivo. Aunque a partir de 1999 las redes ya no reenvían paquetes dirigidos a sus direcciones de transmisión, dichas redes son inmunes. Sin embargo, se debe tener la precaución adecuada para evitar este ataque (RADWARE, 2019c). Además, consiste en "inundar dirección de difusión UDP con paquetes con dirección IP falsa donde cada paquete sea enviado a cada servidor de red (cliente). El enrutador se convierte en generador de tráfico basura, ocasiona sobrecarga de red. Este ataque es bastante raro" (DDoS-GUARD, 2019). Sin embargo es aconsejable, revisar la configuración del router con respecto al tráfico en dirección de transmisión. En la **Figura 8-2** se puede observar el proceso al ejecutar este ataque.

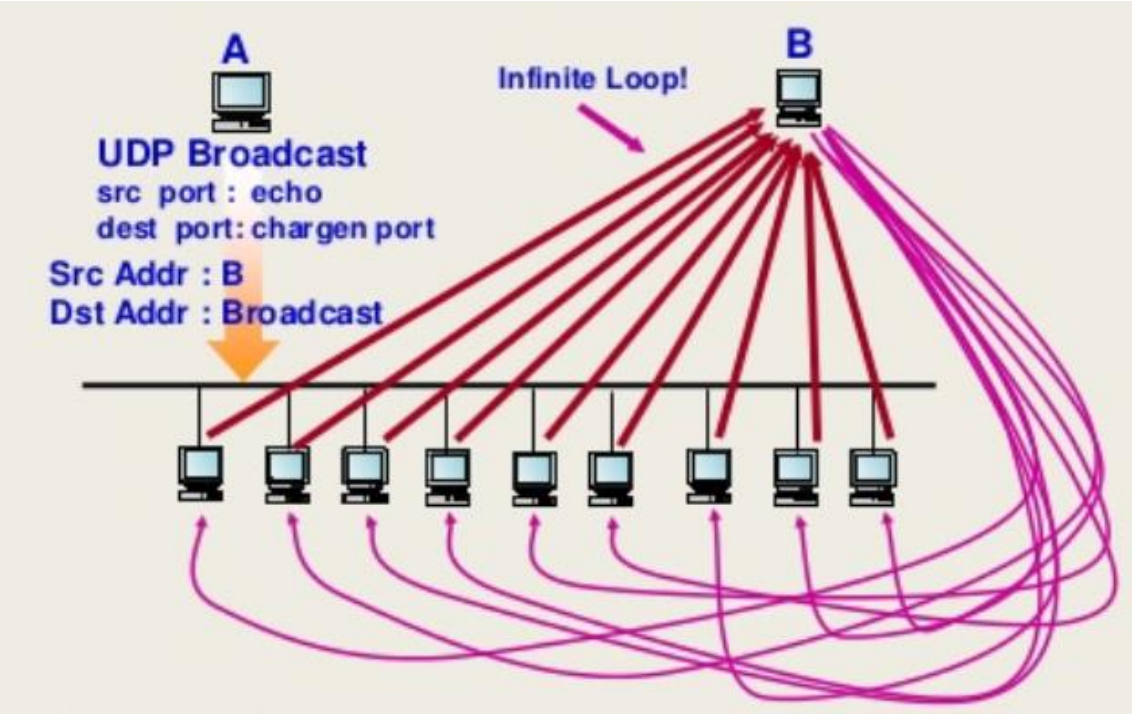

Figura 8-2. Fraggle Attack

Fuente: (Shrestha, 2017, p. 25)

2.11.1.4 SYN Flood Attack

Este ataque consiste en "el atacante envía muchos paquetes TCPSYN para iniciar un TCP conectado, pero nunca devuelve un paquete SYN-ACK" (OmniSecu, 2019, p. 4). Trayendo como consecuencia que "el servidor espere las respuestas que nunca llegan, provocando un consumo elevado de recursos que afectan al rendimiento del servidor" (Blasco, 2007, p. 8). Según el Departamento de Seguridad de Homeland:

> *Ocurre cuando un atacante envía una solicitud para conectarse al servidor de destino pero no completa la conexión a través de lo que se conoce como un apretón de manos de tres vías, un método utilizado en una red de Protocolo de Control de Transmisión (TCP)/IP para crear una conexión entre un host/cliente local y el servidor. El handshake incompleto deja el puerto conectado en un estado ocupado y no disponible para más peticiones. Un atacante continuará enviando peticiones, saturando todos los puertos abiertos, para que los usuarios legítimos no puedan conectarse.* (Departamento de Seguridad Homeland, 2009)

Además, "una inundación SYN supera la máquina objetivo enviando miles de solicitudes conexión con IP falsificadas. Los atacantes añaden información legítima en las solicitudes, número de secuencia, puerto origen 0, aumenta uso del CPU servidor y causa congestión en red" (RADWARE, 2019d). En la Figura 9-2 se puede observar cómo se efectúa este tipo de ataque.

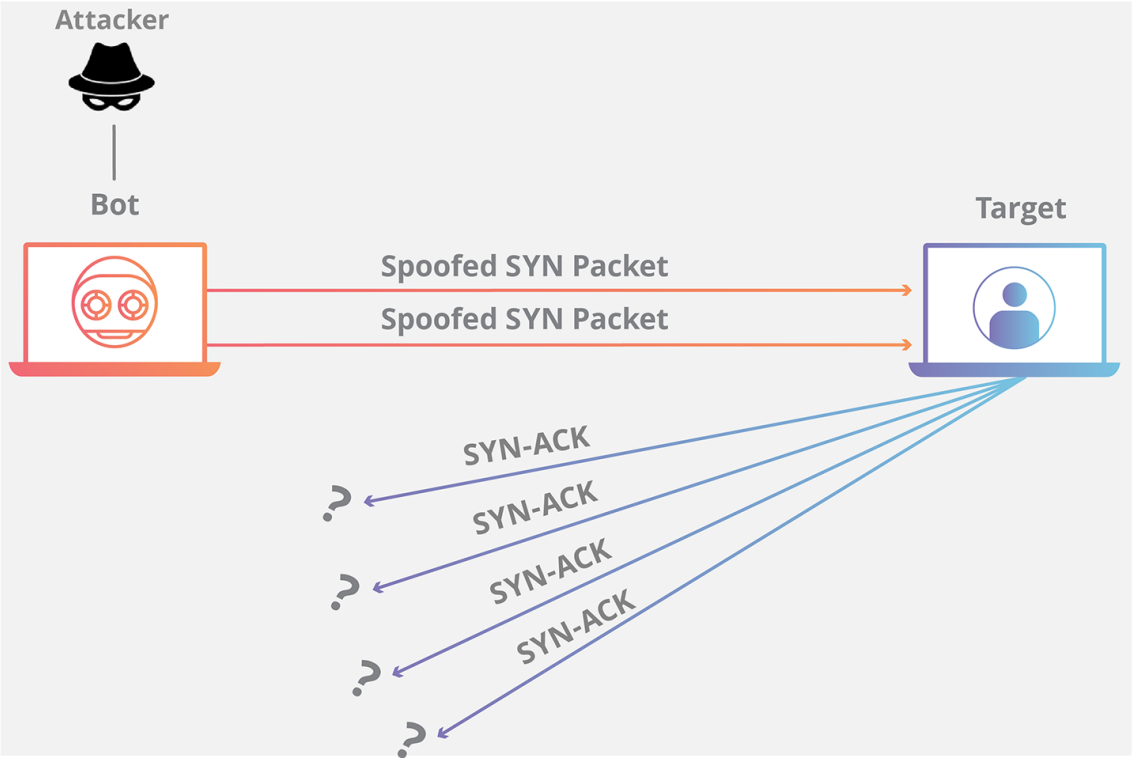

Figura 9-2. Ataque SYN Flood

Fuente: (Cloudflare, 2019)

2.11.2 Denegación de Servicio Distribuido (DDoS)

Este ataque es una variación del ataque de Denegación de Servicios, según Blasco en la conferencia OWASP menciona que es un tipo especial de ataque DoS, donde utilizar varios equipos para poder realizar un ataque coordinada hacia una máquina, utiliza máquinas zombi que se controla mediante un malware, a estas máquinas se las denomina BotNets (Blasco, 2007, p. 9). Es decir que mientras más máquinas se logren controlar mayor efecto va a tener el ataque sobre la víctima.

Este tipo de ataque afecta directamente a la disponibilidad de la aplicación, el cual "es un tipo de ataque que se origina en muchos equipos atacantes de diferentes regiones geográficas" (OmniSecu, 2019). No requiere que el atacante se encuentre cerca de la víctima para causar daños. El funcionamiento de este ataque es tan peculiar:

> *Los múltiples sistemas inundan simultáneamente los recursos o el ancho de banda de la víctima. Aquí los atacantes atacan a varios usuarios e inyectan agentes de ataque indetectables (caballo de Troya, por ejemplo) en sus sistemas. Los sistemas atacados actúan como zombi. El agente de ataque no influye en la funcionalidad normal del sistema; por lo tanto, su presencia permanece inconsciente para los usuarios.* (Hack2Secure, 2019)

Debido a esto las aplicaciones no pueden detectar los ataques rápidamente para poder ejecutar medidas de protección. Según Open Data Security "un ataque DDoS apunta a servicios y sitios web en línea con el objetivo de dejarlos inoperativos. Implica un proceso por el cual una víctima dispone del tráfico web mayor que la capacidad de un servidor o red, dejándolo inaccesible" (Open Data Security, 2019). Sin embargo, cuando ocurre este ataque según el Departamento de Seguridad de Homeland:

> *Este ataque ocurre cuando varias máquinas están operando juntas para atacar a un objetivo. Los atacantes DDoS a menudo aprovechan el uso de una BotNets, un grupo de dispositivos secuestrados conectados a Internet, para llevar a cabo ataques a gran escala. Los atacantes aprovechan vulnerabilidades de seguridad para controlar numerosos dispositivos utilizando software de comando y control. Una vez en control, un atacante puede ordenar a su red de bots que realice DDoS en un objetivo. En este caso, los dispositivos infectados también son víctimas del ataque.* (Departamento de Seguridad Homeland, 2009)

Además, este ataque hace uso de redes BotNets o redes zombis para lanzar el ataque, por lo tanto el ataque es ejecutado desde ubicaciones distintas y distribuidas (González, 2019). Esta red de zombis es potente, está bien coordinada y puede contar con millones de ordenadores. El anonimato del atacante se mantiene seguro ya que se origina en las IPs de los robots. En ataques ideológicos estos ataques pueden estar compuestos por hackers/hacktivistas reclutados por grandes campañas (Operación Blackout, Operación Payback, etc.) por ello es difícil encontrar el atacante (RADWARE, 2019e). Mitigar este tipo de ataque puede llegar a ser complejo por la cantidad de equipos que atacan al objetivo, además estos mantienen oculto al que origina el ataque.

Este ataque es de los más comunes que afectan a la disponibilidad de una aplicación, tanto es el impacto que en el año 2000 sitios web muy grandes como son Amazon, CNN y Yahoo se convirtieron en el blanco de este ataque (Yu, 2014, p. 2).

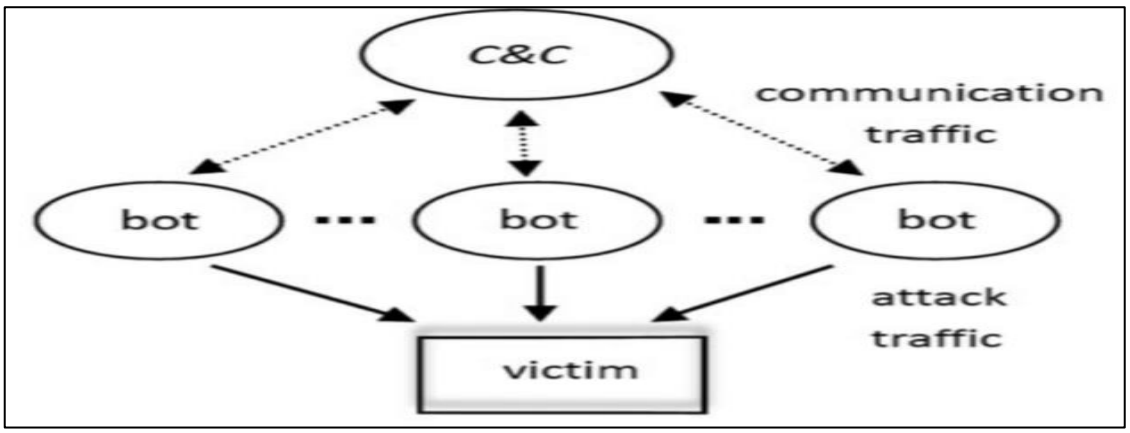

Figura 10-2. Ataque Denegación de Servicios Distribuido (DDoS)

Fuente: (Yu, 2014, p. 4)

Un ataque de Denegación de Servicios Distribuido es una variante del ataque de denegación de servicios, pero este se diferencia principalmente por utilizar otros equipos que actúan como bots a voluntad del atacante, los cuales pueden ser miles mismos que contribuyen atacar al objetivo, por esto es muy difícil detectar al que ocasiona el ataque, ya que dicho ataque se origina en las IPs de los bots, otro punto que dificulta mitigar este ataque es que al ser distribuido los ataques se efectúan de diversos puntos geográficos, este ataque tiene como objetivo dejar inaccesible una aplicación para los usuarios autorizados.

2.11.2.1 Ping of Death

Este tipo de ataque consiste en que "el atacante intenta interrumpir el objetivo enviando un paquete mayor que tamaño máximo permitido, provoca que el equipo objetivo se congele o bloquee. El ataque original es menos común hoy en día. Un ataque de inundación ICMP es más frecuente" (Cloudflare, 2019). Se da cuando se produce un desbordamiento de buffer, lo que provoca inestabilidad, colapso o reinicio de equipo destino (RADWARE, 2019f). Donde, según Yu en su publicación Denegación de Servicio Distribuido Ataque y Defensa, menciona que este ataque puede "causar que algunos sistemas operativos se bloqueen, congelen o reinicien. Esta forma de DDoS puede ser derrotada mediante la aplicación de parches en las vulnerabilidades del sistema" (Yu, 2014, p. 3). En la **Figura 11-2** se puede observar cómo se lleva a cabo este tipo de ataque.

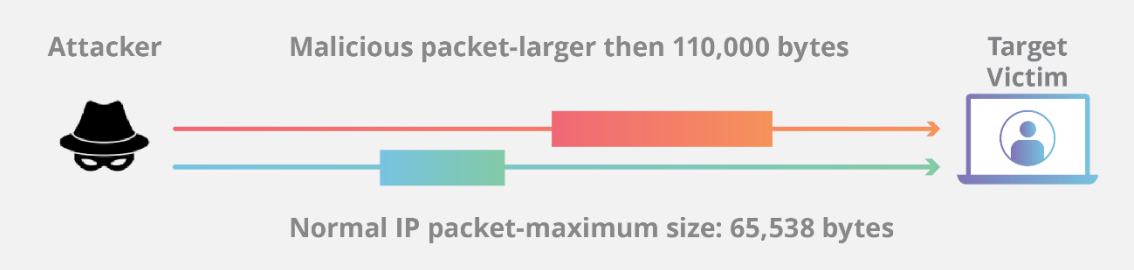

Figura 11-2. Ping of Death

Fuente: (Cloudflare, 2019)

2.11.2.2 Buffer Overflow

Según Blasco en una conferencia de OWASP menciona "este tipo de ataques se producen cuando se escriben datos en un buffer que sobrescriben otros adyacentes, se suelen producir al copiar cadenas de caracteres de un buffer a otro. Estos desbordamientos de buffer pueden provocar muchas veces ataques de denegación de servicio contra la aplicación" (Blasco, 2007). Es decir, que este ataque "ocurre cuando los datos de entrada exceden el espacio reservado. Si el sistema no lo trunca, los datos excedidos sobrescribirán los trozos de memoria adyacentes. Esta circunstancia causa el compromiso de disponibilidad al poner el programa en bucle interminable" (Hack2Secure,

2019). Además, "cuando se produce un desbordamiento de búfer, se bloquea o se vuelve inestable. Los proveedores de software a menudo emplean contramedidas para evitar ataques de desbordamiento de búfer; particularmente, asignación al azar de la pila de llamadas y memoria virtual" (RADWARE, 2019g). En la **Figura 12-2** se puede observar cómo funciona este tipo de ataque.

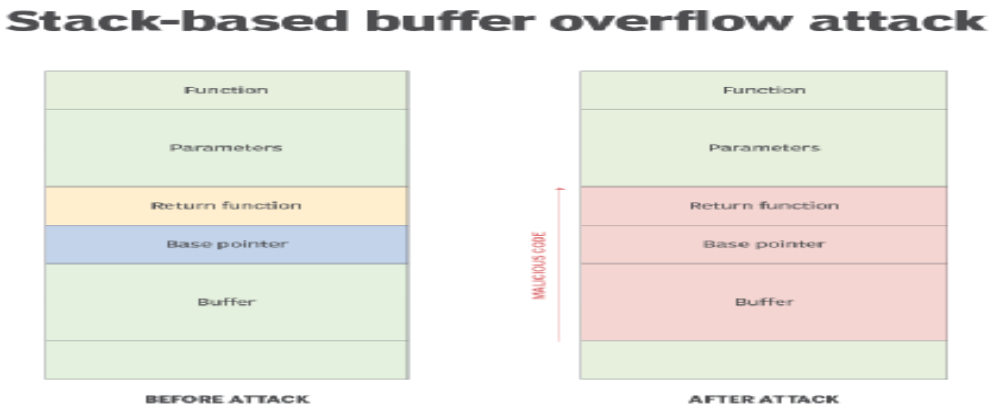

Figura 12-2. Comportamiento del ataque Buffer Overflow

Fuente: (Posey y Bacon, 2018, p. 3)

2.12 Buenas Prácticas de Disponibilidad

En cuanto a las soluciones adoptadas en sistemas de alta disponibilidad, para sistemas en los que es necesario un mayor nivel de seguridad se debe utilizar lo que se denominan como buenas prácticas, por ello se profundizará en que consiste, "una buena práctica es una intervención que se ha implementado con resultados positivos, siendo eficaz y útil en un contexto concreto, contribuyendo al afrontamiento, regulación, mejora o solución de problemas y/o dificultades que se presenten en el objetivo a mejorar" (Comunidad de Prácticas en APS, 2018). Según la Universidad Internacional de Valencia desde un contexto generalista menciona "el concepto de buenas prácticas hace referencia a todas aquellas experiencias que se guían por principios, objetivos y procedimientos apropiados o por pautas aconsejables que se adecuan a una normativa determinada o a una serie de parámetros consensuados" (Universidad Internacional de Valencia, 2018).

Mientras, que según el Instituto Nacional de Ciberseguridad menciona que las buenas prácticas de seguridad se las realiza con el fin de conocer cómo tratar los riesgos, así como desarrollar la capacidad de resistir ante incidentes graves de seguridad una recuperación ante desastres (Instituto Nacional de Ciberseguridad, 2016). Además, según Mieres Analista de Seguridad de ESET para Latinoamérica menciona que "es necesario que los usuarios incorporen buenas prácticas para proteger la información, y prevenir la posibilidad de formar parte del conjunto que engloba a potenciales y eventuales víctimas de cualquiera de las amenazas, que buscan sacar provecho de las debilidades" (Mieres, 2009, p. 3).

En fin, las buenas prácticas dentro del ámbito informático, son todas aquellas intervenciones que se realizan en una aplicación con el fin de mejorarlas, corregir ciertos errores e inconvenientes, proporcionando una mayor robustez, con el objetivo de evitar problemas a futuro, tales como incidentes de seguridad y otros aspectos que influyan en la pérdida de información sensible para una organización. Por ello, se propone ciertas prácticas de disponibilidad que ayuden en el mejoramiento del subsistema Sílabos 1.0.0.

2.12.1 Clústeres

Se conoce como un clúster de alta disponibilidad como un conjunto de servidores que soportan aplicaciones de servidor con una cantidad mínima de tiempo de inactividad cuando cualquier nodo del servidor falla, algunas de las razones para tener un clúster es por el equilibrio de carga, servidores de conmutación por error y sistema de copias de seguridad (ACCU Web Hosting, 2019). Además, los servidores están configurados de forma idéntica de tal forma que proporcionen un mismo tipo de servicio, pero con un componente de puerta frontal que los hace parecer un mismo servidor, consiste en que solo un servidor proporciona un servicio y si falla el servidor secundario toma el control. La solución basada en software normalmente se basa en la configuración de servidores físicos, mientras que la solución basada en hardware se basa en un servidor individual para que aparezca como múltiples servidores (Micro Focus, 2018).

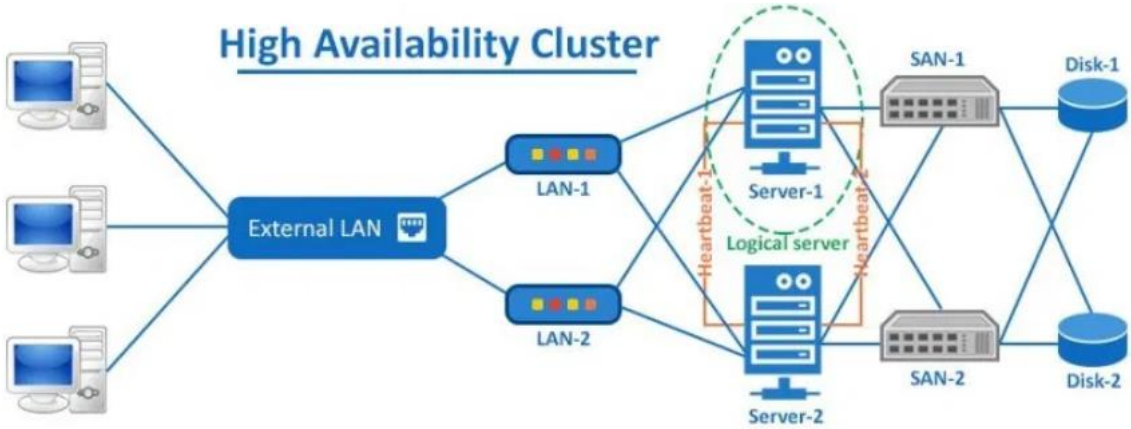

Figura 13-2. Alta Disponibilidad Clústeres

Fuente: (ACCU Web Hosting, 2019)

2.12.1.1 Docker Swarm

Docker Swarm permite administrar de forma nativa un grupo de motores Docker llamados Swarm, es decir permite la orquestación de clústeres integrados en Docker Engine los cuales se crean mediante Swarmkit, una de las ventajas clave de los servicios de enjambre sobre los

contenedores independientes es que puede modificar la configuración de un servicio, incluidas las redes y los volúmenes a los que está conectado, sin la necesidad de reiniciar manualmente el servicio. “Docker actualizará la configuración, detendrá las tareas de servicio con la configuración desactualizada y creará otras nuevas que coincidan con la configuración deseada” (Docker, 2020).

Características

Según la documentación oficial de Docker Swarm (Docker, 2020) permite muchas características entre ellas se encuentran:

- **Gestión de clústeres integrada con Docker Engine:** permite crear un enjambre de Docker Engines donde pueda implementar servicios de aplicaciones. No necesita software de orquestación adicional para crear o administrar un enjambre.
- **Diseño descentralizado:** maneja cualquier especialización en tiempo de ejecución. Puede implementar ambos tipos de nodos, administradores y trabajadores. Esto significa que puede crear un enjambre completo a partir de una sola imagen de disco.
- **Modelo de servicio declarativo:** puede describir una aplicación compuesta por un servicio web front-end con servicios de cola de mensajes y un back-end de base de datos.
- **Escalado:** para cada servicio, puede declarar la cantidad de tareas que desea ejecutar. Cuando escala hacia arriba o hacia abajo, el administrador de enjambres se adapta automáticamente agregando o eliminando tareas para mantener el estado deseado.
- **Conciliación del estado deseado:** el nodo del administrador de enjambres monitorea constantemente el estado del clúster y concilia cualquier diferencia entre el estado real y el estado deseado expresado.
- **Red de múltiples hosts:** puede especificar una red superpuesta para sus servicios.
- **Descubrimiento de servicios:** los nodos del administrador de enjambres asignan a cada servicio en el enjambre un nombre DNS único y equilibran la carga que ejecutan los contenedores.
- **Equilibrio de carga:** puede exponer los puertos para servicios a un equilibrador de carga externo. Internamente, el enjambre le permite especificar cómo distribuir contenedores de servicios entre nodos.
- **Seguro de forma predeterminada:** cada nodo del enjambre aplica la autenticación mutua y el cifrado TLS para proteger las comunicaciones entre él y todos los demás nodos.
- **Actualizaciones continuas:** en el momento del lanzamiento, puede aplicar actualizaciones de servicio a los nodos de forma incremental.

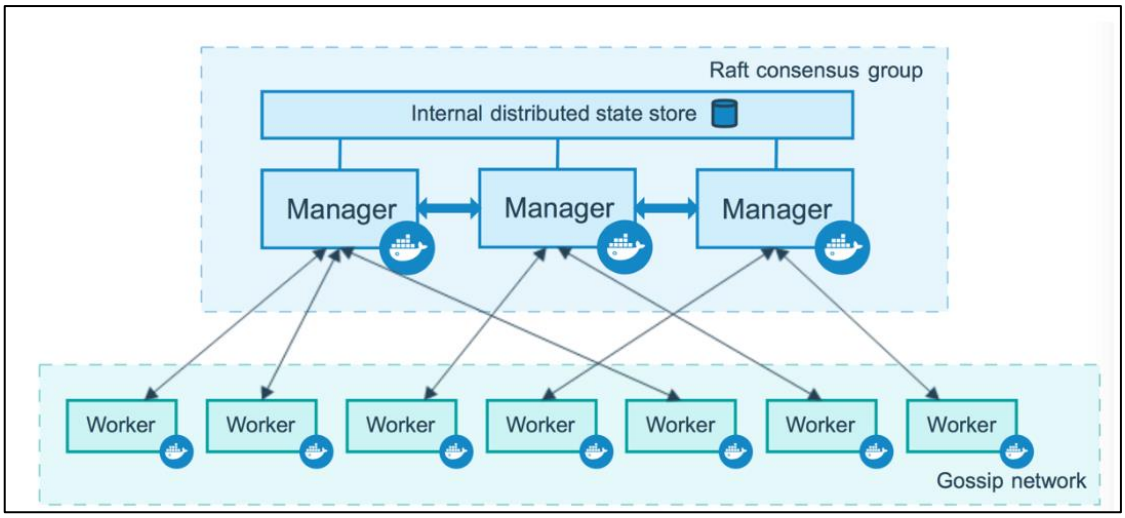

Figura 14-2. Ejemplo de un escenario con la utilización de Docker Swarm

Fuente: (Docker, 2020)

2.12.2 Balanceador de Carga

Se considera una buena práctica de disponibilidad "al proceso de distribuir el tráfico web entrante a través de un grupo de servidores de forma eficiente y sin intervención se denomina Balanceo de Carga" (ACCU Web Hosting, 2019). También, "se utiliza para distribuir las cargas de usuarios finales de forma uniforme entre varios servidores. Las tecnologías inteligentes monitorean y entienden la cantidad de recursos que utilizan y dirigen automáticamente a usuarios al servidor con tasa de utilización más baja" (Micro Focus, 2018).

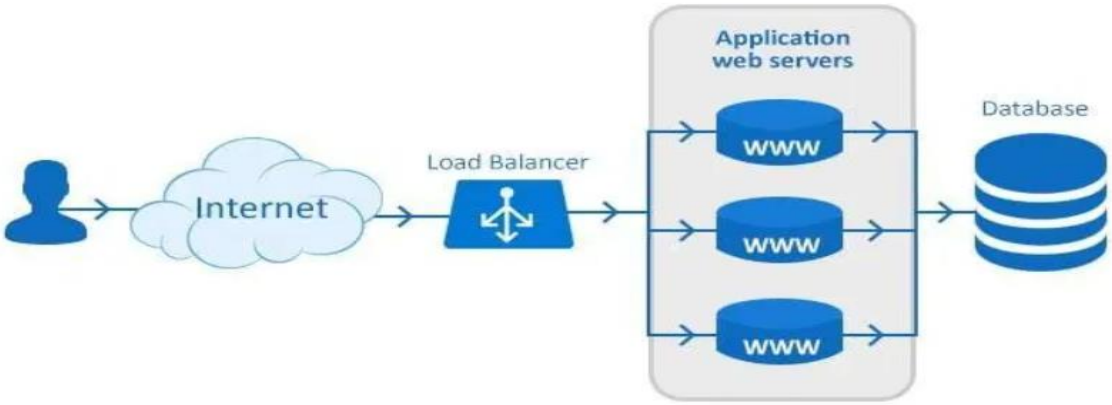

Figura 15-2. Balanceador de Carga

Fuente: (ACCU Web Hosting, 2019)

2.12.2.1 Traefik

Traefik es un Edge Router de código abierto que hace que la publicación de sus servicios sea una experiencia divertida y fácil. Recibe solicitudes en nombre de su sistema y descubre qué componentes son responsables de manejarlas. Lo cual hace que el equilibrio de carga sea un proceso sencillo:

> *Lo que distingue a Traefik, además de sus muchas características, es que descubre automáticamente la configuración correcta para sus servicios. La magia ocurre cuando Traefik inspecciona su infraestructura, donde encuentra información relevante y descubre qué servicio atiende qué solicitud. Traefik es compatible de forma nativa con todas las principales tecnologías de clúster, como Kubernetes, Docker, Docker Swarm, AWS, Mesos, Marathon, y la lista continúa; y puede manejar muchos al mismo tiempo. (Incluso funciona para software heredado que se ejecuta en bare metal).* (Traefik, 2020)

Por medio de Traefik no se debe preocupar del correcto equilibrio de carga ni mucho menos del DNS donde se va a desplegar el servicio.

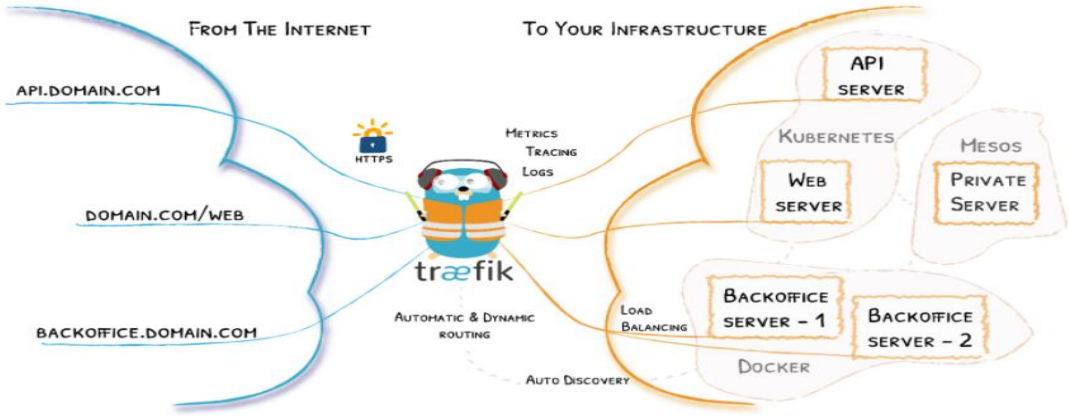

Figura 16-2. Funcionamiento de Traefik

Fuente: (Traefik, 2020)

2.12.3 Failover Solutions

Esta solución consiste en "cambiar instantáneamente a un servidor de reserva o red cuando se produce errores al servidor/red principal. Cuando el host principal cae o necesita mantenimiento, la carga de trabajo cambia automáticamente a un host secundario. Con usuarios inconscientes de lo sucedido" (ACCU Web Hosting, 2019). Mientras que Imperva menciona que "es el proceso operativo de conmutación entre sistemas primarios y secundarios o componentes del sistema (servidor, procesador, red o una base de datos) caso de tiempo de inactividad. Esta inactividad puede ser mantenimiento programado, fallo imprevisto del sistema, o componentes" (IMPERVA, 2019).

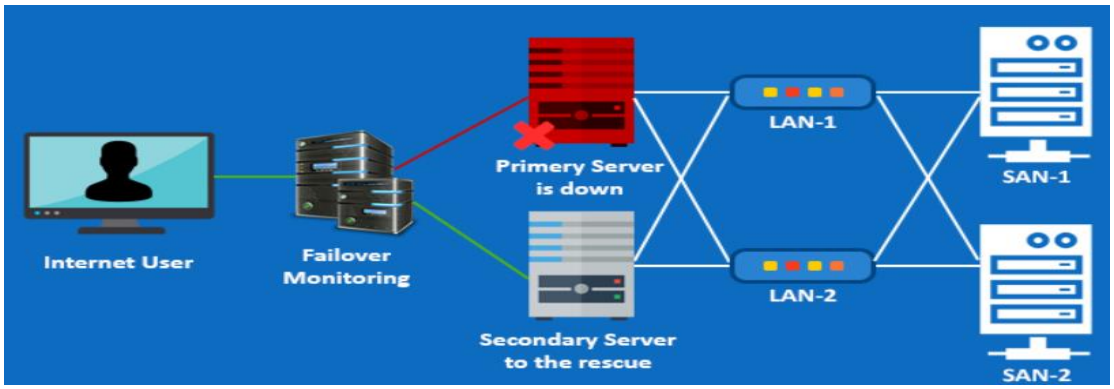

Figura 17-2. Failover Solutions

Fuente: (ACCU Web Hosting, 2019)

2.12.3.1 Portainer

Portainer nos proporciona una GUI web desde la que administrar un clúster de Docker Swarm: "operatividad de contenedores parada, reinicio, etc. Gestión de stacks, servicios, plantillas de imágenes, volúmenes para persistencia de datos" (Array, 2019). Es decir a través, de Portainer se puede monitorear por medio de una interfaz gráfica el funcionamiento del clúster, de esta forma prevenir que alguno de los nodos se caiga, o se pierda alguno de los servicios, evitando así la pérdida de información.

2.12.3.2 Visualizer

Herramienta que permite observar el funcionamiento de un clúster por medio de una interfaz gráfica la cual es de acceso fácil, y de interpretación sencilla de lo que se ve en pantalla, muestra los nodos activos, así como los servicios que se encuentran ejecutándose en cada nodo. De esta forma permite monitorear el clúster y evitar que alguno de los nodos falle.

2.12.4 Replicación Base de Datos

La replicación de base de datos es una buena práctica muy útil para garantizar la disponibilidad de aplicaciones web, según Charron-Bost et al. En su libro Replicación: Teoría y Práctica mencionan:

> *La replicación es la creación de múltiples copias de un objeto posiblemente mutante (archivo, sistema de archivos, base de datos, etc.) con el objetivo de proporcionar alta disponibilidad, alta integridad, alto rendimiento o cualquier combinación de los mismos. Para una alta disponibilidad e integridad, las réplicas deben ser diversas, por lo que los fallos son suficientemente independientes. Para un alto rendimiento, sólo se necesita un*

número suficiente de réplicas a fin de satisfacer la carga impuesta sobre el objeto replicado. (Charron-Bost et al., 2010, p. 19)

Sin embargo, según Muñoz-Escoí y Decker en su publicación Enfoques de Replicación de Base de Datos mencionan que "la gestión de réplicas no es tan fácil de lograr cuando se fusionan los controles de concurrencia y réplica, los protocolos de control de réplicas para asegurar la consistencia tiene que ser aceptado por control concurrencia que se está utilizando" (Muñoz-Escoí y Decker, 2007, p. 3).

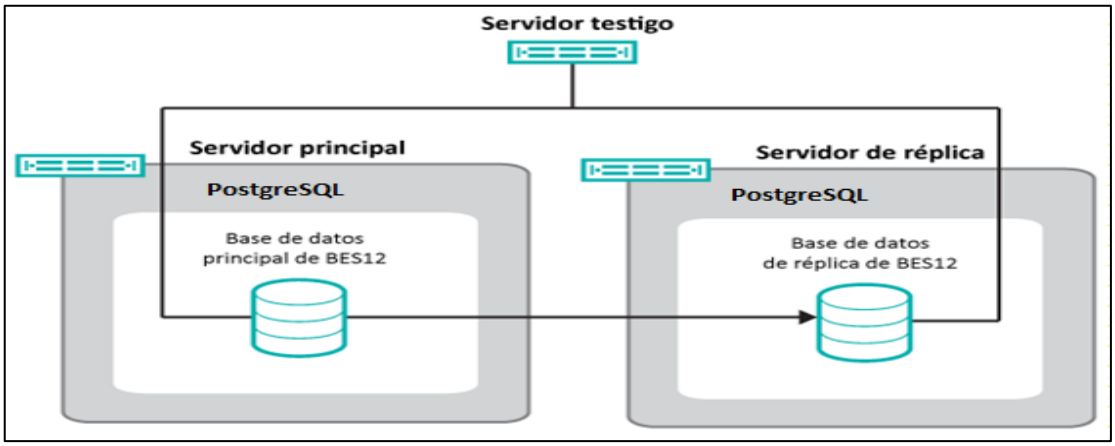

Figura 18-2. Replicación de una base de datos

Fuente: (Díaz, 2016)

2.12.5 Copias de seguridad

Realizar copias de seguridad es una de las prácticas que nos ayudan a recuperar nuestra información y aplicaciones en caso de un ataque o amenazas imprevistas, según GADAE "simplemente se trata de un sistema de réplica de ficheros o archivos que guardas en ordenador o cualquier parte. Puedes copiar tus datos fácilmente, así como también aplicaciones, y tenerlas a salvo en un dispositivo externo, o en la nube" (GADAE, 2019). Mientras que según el Instituto Nacional de Ciberseguridad "una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos" (Instituto Nacional de Ciberseguridad, 2018, p. 3). Además, se considera "la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe. Es fundamental para un plan de recuperación de desastres exitoso" (Search Data Center, 2018).

2.12.5.1 Rsnapshot

Realiza copias de seguridad (Backup) incrementales y automáticas por medio de rsync, utiliza enlaces duros para las copias incrementales con lo que las copias de seguridad ocupan poco espacio en el disco.

Básicamente, “realiza una primera copia y en posteriores copias, copia los archivos nuevos y modificados, creando enlaces duros a los archivos que ya existían. Así que las copias sucesivas solo ocupan los archivos nuevos” (Alba, 2013). Por lo tanto, “no hay cintas que cambiar, por lo que una vez que está configurado, sus copias de seguridad pueden ocurrir automáticamente sin que las manos humanas las toquen esto hace que el espacio en disco utilizado no aumentará continuamente” (Rsnapshot, 2020). Dependiendo de su configuración, es muy posible configurarlo en solo unos minutos. Los archivos pueden ser restaurados por los usuarios que los poseen, sin que el usuario root se involucre.

2.12.6 Firewall

La utilización de un firewall ayuda a mantener una aplicación web libre de ataques que comprometan la disponibilidad, según Altalef un firewall “es aquel que lleva un control de las conexiones establecidas, de manera que puede determinar si un paquete pertenece o no a una conexión. Si determina que pertenece a una conexión, se acepta sin necesidad de validarlo contra las reglas” (Altalef, 2007). Según Pandini en su publicación sobre Firewall en Alta Disponibilidad “es una solución unificada para la prevención de amenazas virtuales, incluyendo módulos de seguridad perimetral, acceso remoto seguro y gestión de contenido, como objetivo traer seguridad donde se haya implantado” (Pandini, 2017). Según Brodbeck “el costo con alta disponibilidad de firewalls ha sido reducido a lo largo del tiempo, tanto términos de inversiones hardware, como formatos de licenciamiento. La cuenta es simple y generalmente la inversión se devuelve rápidamente ya en la primera indisponibilidad” (Brodbeck, 2017, p. 3). Además, contribuye analizando paquetes de información que se encuentren bajo las condiciones establecidas, para poder evitar que lleguen a realizar peticiones a una aplicación y causar fallas en la misma.

2.13 Mantenimiento

A pesar, que el mantenimiento se encuentra en las últimas en el ciclo de vida del software, las actividades de mantenimiento no es la menos importante. Según el estándar IEEE 1219, el mantenimiento del software es: “la modificación de un producto software después de su entrega al cliente o usuario para corregir defectos, para mejorar el rendimiento u otras propiedades deseables, o para adaptarlo a un cambio de entorno” (IEEE Standards Association, 2019).

Además, mantenimiento también se considera como “modificación del código y de la documentación asociada debido a un problema o la necesidad de mejorar. El objetivo es modificar

el producto de software existente, preservando al mismo tiempo su integridad" (ISO/IEC 12207, 2017; citado en Pigoski, 2001). Sin embargo, según la norma ISO/IEC 14764:

> *El proceso del ciclo de vida del mantenimiento del software comienza con la implementación del proceso que se planifica el mantenimiento y termina con la retirada del producto software. Incluye la modificación del código y la documentación debido a un problema o necesidad de mejora. El objetivo del Proceso de Mantenimiento es modificar un archivo al mismo tiempo que se preserva su integridad.* (ISO/IEC 14764, 2006, p. 6)

Según SWEBOK, la cual es una guía para el mantenimiento de software donde su principal objetivo es que los esfuerzos que se hace durante el desarrollo de software resulten en la satisfacción de los requerimientos por parte del cliente, por ello SWEBOK menciona:

> *El mantenimiento de software se define como el conjunto de actividades necesarias para proporcionar un soporte rentable al software. Las actividades se realizan durante la etapa anterior a la entrega así como durante la etapa posterior a la entrega. Las actividades previas a la entrega incluyen la planificación de las operaciones posteriores a la entrega, la capacidad de mantenimiento y la determinación logística para las actividades de transición. Las actividades posteriores a la entrega incluyen la modificación del software, la capacitación y la operación o interfaz con un centro de ayuda*. (SWEBOK, 2019)

De esta forma en cada uno de los estándares el mantenimiento del software se puede decir que es un factor primordial el cual se ha convertido en la principal actividad que influye a los recursos y costes dentro del desarrollo de software.

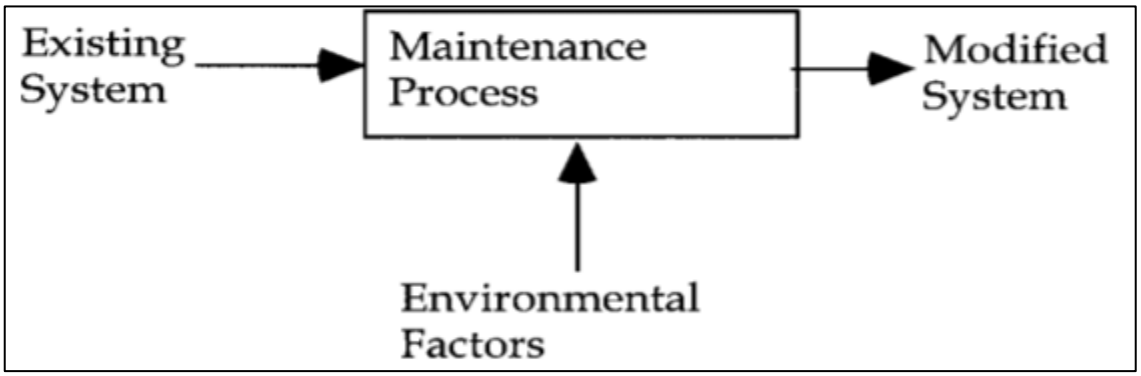

Figura 19-2. Modelo conceptual del proceso de mantenimiento.
Fuente: (Banker et al., 2002: p. 27)

En la Figura 19-2 se muestra el modelo conceptual del proceso de mantenimiento donde se toma en cuenta la existencia de un sistema, además de los factores ambientales, donde se determina los posibles cambios para que ocurra el mantenimiento, una vez hecho esto se realiza el

mantenimiento, produciendo como salida el sistema modificado con las respectivas mejoras que se haya hecho.

Razón por la cual, en el presente trabajo se resalta el estándar IEEE 1219, para realizar el mantenimiento del subsistema Sílabos, debido a que dicho estándar nos brinda flexibilidad, con un proceso que conlleva fases que hacen del mantenimiento de software sea muy completo. A más de ello lo podemos combinar con la metodología SCRUM, la cual es una metodología ágil que conjuntamente con el estándar permitirá un desarrollo rápido y eficiente del mantenimiento, de esta forma poder aplicar las buenas prácticas de disponibilidad.

2.14 Metodología híbrida SCRUM e IEEE 1219

SCRUM es una metodología ágil para proyectos de desarrollo de software, pero por medio de las prácticas propuestas por el estándar IEEE 1219 se pretende utilizar SCRUM para llevar a cabo el proceso de mantenimiento (Alfonzo et al., 2012, p. 5).

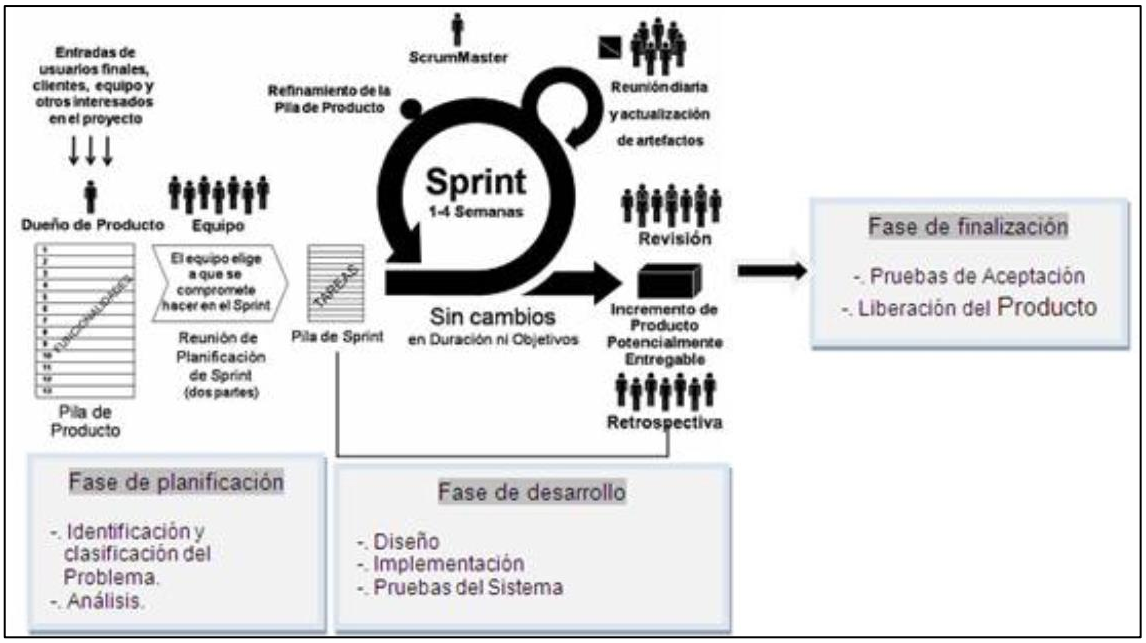

Figura 20-2. Metodología híbrida SCRUM e IEEE 1219

Fuente: (Alfonzo et al., 2012, p. 5)

Dentro de esta combinación entre SCRUM e IEEE 1219 se pueden resaltar que se inicia con la fase de planificación, donde se define el equipo de trabajo, solicitudes de modificación del software, esto se registra en el Product Backlog y en función a los requerimientos se seleccionan las peticiones de modificación a incluir en el Sprint. Donde se realiza las estimaciones y el alcance de las mismas. Se definen roles como; cliente, equipo de desarrollo, responsable de mantenimiento (SrumMaster). En la fase de desarrollo se realizan una serie de reuniones para

verificar el normal avance, así como para la revisión, validación y verificación del producto con el cliente. Dentro de cada Sprint se aborda fases propuestas por el Estándar IEEE 1219 como es el diseño, implementación y pruebas del sistema. Depende del mantenimiento la duración del Sprint mismo que puede ser de 1 a 4 semanas, según la decisión del equipo (Alfonzo et al., 2012, p. 4-6). Una vez realizado el proceso anterior se procede a la fase de finalización, realizando las actividades que se muestran en la **Tabla 2-2**.

Tabla 2-2: Fases y actividades de la metodología SCRUM - IEEE 1219

Estándar IEEE 1219		**SCRUM**
Fases	**Tareas**	Fase de Planificación
Identificación y Clasificación del Problema o de la Modificación.	• Identificar el problema • Clasificar el problema por tipo de mantenimiento • Asignar prioridad • Obtener aprobación de la solicitud de modificación y las tareas a llevar a cabo. • Estimar inicialmente los recursos necesarios para modificar el sistema existente.	
Análisis.	• Evaluar el impacto • Evaluar los costos • Estudia la viabilidad y el alcance de las modificaciones • Desarrollar un plan preliminar de diseño, implementación, pruebas y liberación del software. • Desarrollar estrategia de pruebas	
Diseño	• Determinar objetos a modificar • Generar los casos de pruebas • Obtener lista de modificaciones revisada. • Generar guía básica del diseño actualizado. • Obtener planes de pruebas actualizados. • Obtener análisis detallado actualizado, requisitos verificados y plan de implementación revisado.	Fase de Desarrollo

Continua

Continua

	• Generar lista de restricciones y riesgos documentados.	
Implementación	• Desarrollar y probar las modificaciones realizadas • Codificar y generar pruebas unitarias. • Integrar el software modificado con el sistema existente. • Analizar el riesgo. • Revisar la preparación para las pruebas.	
Pruebas del Sistema	• Realizar pruebas sobre el sistema modificado • Revisar integridad. • Obtener aprobación.	
Pruebas de Aceptación	• Realizar pruebas sobre el sistema completamente integrado	Fase de Finalización
Liberación del Producto	• Desarrollar un plan. • Notificar a los usuarios. • Realizar una copia de seguridad de la versión del sistema. • Realizar la instalación y capacitar a los usuarios.	

Fuente: (Alfonzo et al., 2012, pp. 6-7)

Realizado por: Ramos Averos, Rodrigo, 2020.

CAPÍTULO III

3. MARCO METODOLÓGICO

En el presente capítulo se aborda todo lo concerniente al desarrollo del Trabajo de Integración Curricular, es decir, la identificación del tipo de estudio, métodos y técnicas, posterior a ello, la identificación de la población, planteamiento de la hipótesis, realización del proceso de pruebas, identificando dos experimentos, el primero sin aplicar las buenas prácticas de disponibilidad y el segundo con la aplicación de las buenas prácticas de disponibilidad.

3.1 Tipo de estudio

El tipo de estudio para el desarrollo de este trabajo es la investigación aplicativa e investigación descriptiva, la razón de ser una investigación aplicativa se debe a que se establecerán nuevos procesos que aportarán a la mejora de las buenas prácticas de disponibilidad de información, al mismo tiempo se considera una investigación descriptiva dado que se describen los procesos que son llevados a cabo para el desarrollo del presente Trabajo de Integración Curricular.

3.2 Métodos y técnicas

Métodos

Los métodos a utilizarse en este trabajo son las que se detallan a continuación:

- Para la identificación de las buenas prácticas de disponibilidad de información, con respecto al desarrollo de una aplicación web segura se utilizará el método analítico.
- Con el objetivo de integrar las prácticas de disponibilidad de información investigadas al subsistema Sílabos se utilizará el método sintético.
- Para el análisis de los resultados se toma en cuenta el total de las pruebas, razón por lo que no es necesario utilizar un método estadístico inferencial.

Técnicas

Las técnicas a utilizarse en este trabajo son las que se detallan a continuación:

- Entrevistas utilizadas con el personal de DTIC para identificar falencias de seguridad en las aplicaciones web.

- Revisión de documentos utilizados durante todo el desarrollo de este Trabajo de Integración Curricular, para sustentar la información y verificar su originalidad.
- Técnicas de estadística descriptiva utilizada para evaluar los resultados.

3.3 Población

La población se obtiene a partir de todos los escenarios posibles en base a la configuración de alta disponibilidad que se propone en el presente trabajo, se determinó un total de 37 escenarios, debido a la cantidad de escenarios determinados, se los tomará como población total, esto se visualiza a mayor detalle en la **Tabla 2-3**.

3.4 Planteamiento de la hipótesis

H0: El uso de buenas prácticas de disponibilidad, NO influye en las interrupciones no autorizadas en el subsistema Sílabos 1.0.0.

H1: El uso de buenas prácticas de disponibilidad, influye en las interrupciones no autorizadas en el subsistema Sílabos 1.0.0.

3.4.1 Operacionalización de la Hipótesis

De acuerdo con la hipótesis planteada se ha determinado dos variables, las cuales se detallan a continuación:

Independiente: Buenas prácticas de disponibilidad.

Dependiente: Interrupciones no autorizadas en el subsistema Sílabos 1.0.0.

Tabla 1-3: Operacionalización de la hipótesis

Hipótesis	Variable	Indicadores	Instrumentos
El uso de buenas prácticas de disponibilidad, influye en las interrupciones no autorizadas en el subsistema Sílabos 1.0.0.	Buenas prácticas de disponibilidad	Técnicas aplicadas	Lista de verificación
	Interrupciones no autorizadas en el subsistema Sílabos 1.0.0.	Número de pruebas fallidas	Pruebas

Realizado por: Ramos Averos, Rodrigo, 2020.

3.5 Proceso de pruebas

La **Figura 1-3** muestra el escenario inicial donde se encuentra desplegado el subsistema Sílabos 1.0.0. Es decir, en dicho escenario no están aplicadas las buenas prácticas de disponibilidad.

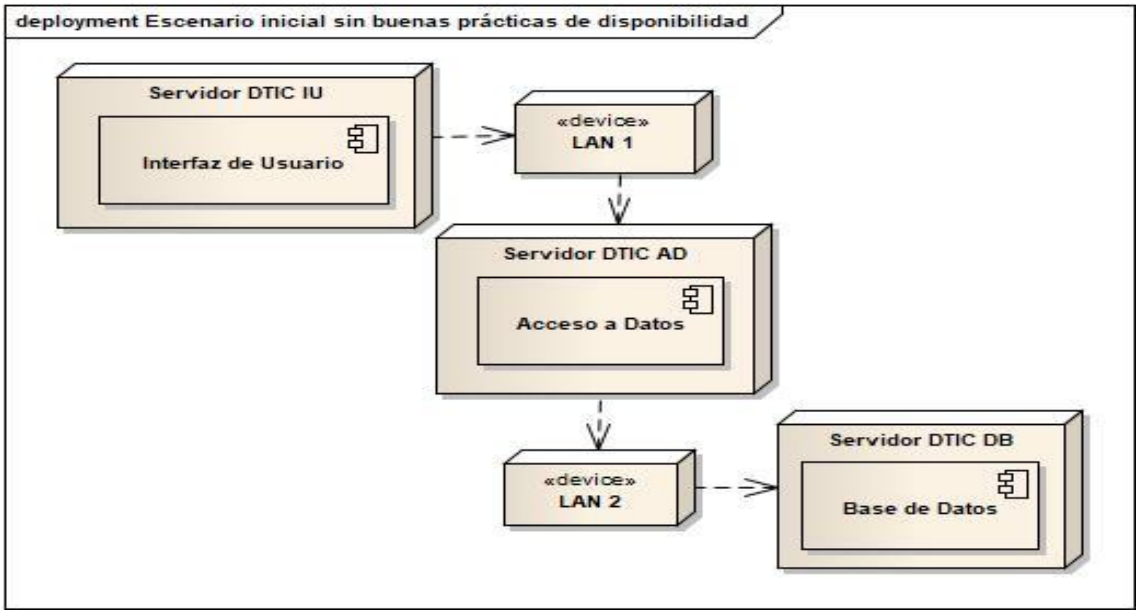

Figura 1-3. Escenario inicial sin buenas prácticas de disponibilidad

Realizado por: Ramos, R. 2020

La **Figura 2-3** muestra el escenario final con la aplicación de las buenas prácticas de disponibilidad.

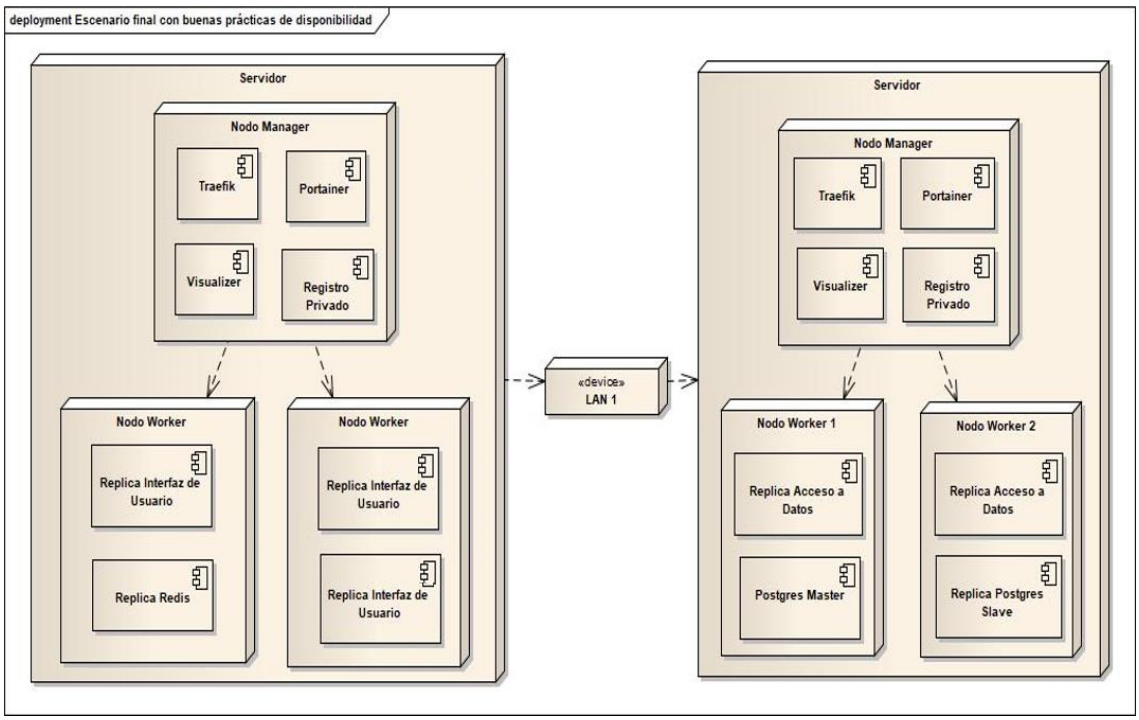

Figura 2-3. Escenario final con buenas prácticas de disponibilidad

Realizado por: Ramos, R. 2020

3.5.1 Etapa 1: Planificación de las pruebas

Dentro de la planificación de las pruebas se determina los escenarios que permiten obtener el resultado acerca de la disponibilidad que brinda las buenas prácticas planteadas en el presente trabajo, un mayor detalle se presenta en la **Tabla 2-3.**

Tabla 2-3: Escenarios para las pruebas de las buenas prácticas de disponibilidad

Categoría	Escenario
Disponibilidad	1. Todos los nodos del servidor 1 activos
	2. Un solo nodo del servidor 1 activo
	3. Un nodo manager cero nodos worker activos en el servidor 1
	4. Un nodo manager un nodo worker activos en el servidor 1
	5. Cero nodos manager un nodo worker activo en el servidor 1
	6. Cero nodos manager dos nodos worker activos en el servidor 1
	7. Fallo de un nodo con réplicas Redis en el servidor 1
	8. Fallo de dos nodos con réplicas Redis en el servidor 1
	9. Fallo de tres nodos con réplicas Redis en el servidor 1
	10. Fallo de un nodo con réplicas Payara para la interfaz de usuario en el servidor 1
	11. Fallo de dos nodos con réplicas Payara para la interfaz de usuario en el servidor 1
	12. Fallo de tres nodos con réplicas Payara para la interfaz de usuario en el servidor 1
	13. Fallo nodo manager con Traefik proxy inverso en el servidor 1
	14. Fallo de un nodo manager con Portainer la cual es una herramienta para administrar clúster Swarm mediante interfaz gráfica en el servidor 1
	15. Fallo nodo con Visualizer en el servidor 1
	16. Fallo de un nodo con el Registro Privado en el servidor 1
	17. Fallo de dos nodos con el Registro Privado en el servidor 1
	18. Fallo de tres nodos con el Registro Privado en el servidor 1
	19. Todos los nodos del servidor 2 activos
	20. Un solo nodo del servidor 2 activo
	21. Un nodo manager cero nodos worker activos en el servidor 2
	22. Un nodo manager un nodo worker activos en el servidor 2
	23. Cero nodos manager un nodo worker activo en el servidor 2
	24. Cero nodos manager dos nodos worker activos en el servidor 2
	25. Fallo de un nodo con Postgres Master en el servidor 2
	26. Fallo de un nodo con réplicas Postgres Slave en el servidor 2
	27. Fallo de dos nodos con réplicas Postgres Slave en el servidor 2
	28. Fallo de tres nodos con réplicas Postgres Slave en el servidor 2
	29. Fallo de un nodo con réplicas Payara para el acceso a datos en el servidor 2
	30. Fallo de dos nodos con réplicas Payara para el acceso a datos en el servidor 2
	31. Fallo de tres nodos con réplicas Payara para el acceso a datos en el servidor 2
	32. Fallo nodo manager con Traefik proxy inverso en el servidor 2
	33. Fallo de un nodo manager con Portainer herramienta para administrar clúster Swarm mediante interfaz gráfica en el servidor 2
	34. Fallo nodo con Visualizer en el servidor 2
	35. Fallo nodo con el Registro Privado en el servidor 2
	36. Fallo dos nodos con el Registro Privado en el servidor 2
	37. Fallo tres nodos con el Registro Privado en el servidor 2

Realizado por: Ramos Averos, Rodrigo, 2020.

En la **Tabla 2-3** se muestra el plan para el antes y después de aplicar la buenas prácticas de disponibilidad, la documentación se encuentra en (Plan de Pruebas, 2020, pp. 5-9)**.**

3.5.2 Etapa 2: Diseño de pruebas

Para cada uno de los escenarios se diseña un formato para poder realizar la documentación de las mismas, con el fin de obtener un resultado antes y después de aplicar las buenas prácticas de disponibilidad, en la **Tabla 3-3** se muestra el detalle de la información a tomar en cuenta.

Tabla 3-3: Diseño de la prueba todos los nodos del servidor 1 activos

Caso de Prueba PPSS-1: Todos los nodos del servidor 1 activos		
Autor:	Rodrigo Ramos	
Resumen: Caso de prueba correspondiente a verificar el resultado de tener activo toda la infraestructura donde se encuentra desplegado el subsistema Sílabos 1.0.0		
Precondiciones: - Tener desplegado el subsistema Sílabos 1.0.0.		
N°:	**Pasos:**	**Resultados Esperados:**
1.	Acceder al subsistema Sílabos en un navegador web	Interfaz de usuario cargada en el navegador
2.	Autenticarse en el subsistema	Autenticación satisfactoria en el subsistema
3.	Verificar el correcto funcionamiento del subsistema	Funcionamiento correcto del subsistema
Tipo de ejecución:	Manual	
Duración estimada de la ejec. (min):	15	
Importancia:	Alta	
Requisitos:	Ninguno	
Keywords:	Ninguno	

Realizado por: Ramos Averos, Rodrigo, 2020.

En la **Tabla 3-3,** se puede observar todos los campos que tiene cada una de las pruebas, con el fin de proporcionar un detalle completo y así poder obtener los resultados una vez ejecutadas las pruebas, la información completa de las pruebas se encuentran en el (Plan de Pruebas, 2020, p. 10-30)**.**

3.5.3 Etapa 3: Ejecución de pruebas

Para la ejecución de las pruebas se toma en cuenta cada uno de los escenarios propuestos en la etapa de planificación, donde se considera que la prueba es exitosa, cuando al ejecutarla el subsistema responde correctamente sin ninguna interrupción en su funcionamiento, mientras que se declara como fallida, cuando al ejecutar una prueba el subsistema deja de funcionar correctamente, es decir se interrumpe el funcionamiento totalmente o parcialmente. En la **Tabla 4-3** se puede observar el diseño de las pruebas para la documentación de la ejecución de las pruebas donde la diferencia con el diseño mostrado en la etapa 2 radica en los campos adicionales como son; la versión, el tester, el resultado de la ejecución, modo ejecución y la duración de la ejecución.

Tabla 4-3: Diseño de la prueba para la documentación de la ejecución

Caso de Prueba PPSS-1: Todos los nodos del servidor 1 activos		
Autor:	Rodrigo Ramos	
Resumen: Caso de prueba correspondiente a verificar el resultado de tener activo toda la infraestructura donde se encuentra desplegado el subsistema Sílabos 1.0.0		
Precondiciones: - Tener desplegado el subsistema Sílabos 1.0.0.		
N°:	**Pasos:**	**Resultados Esperados:**
1.	Acceder al subsistema Sílabos en un navegador web	Interfaz de usuario cargada en el navegador
2.	Autenticarse en el subsistema	Autenticación satisfactoria en el subsistema
3.	Verificar el correcto funcionamiento del subsistema	Funcionamiento correcto del subsistema
Tipo de ejecución:	Manual	
Duración estimada de la ejec. (min):	15	
Importancia:	Alta	
Requisitos:	Ninguno	
Keywords:	Ninguno	
Detalles Ejecución:		
Versión:	1	
Tester:	Rodrigo Ramos	
Resultado de la Ejecución:	Pasada	
Modo Ejecución:	Manual	
Duración Ejecución (min):	7	

Realizado por: Ramos Averos, Rodrigo, 2020.

La información detallada de la ejecución de las pruebas antes y después de aplicar las buenas prácticas de disponibilidad se encuentra en el (Plan de Pruebas, 2020, p. 31).

3.5.4 Etapa 4: Resultados

Para el cálculo de los resultados se realiza en base a los principios básicos que propone la norma ISO 27001, tomando en cuenta el principio de la disponibilidad.

Para el cálculo de los porcentajes de vulnerabilidad del subsistema se aplicará la siguiente fórmula.

$$\%\ vulnerabilidad\ = \frac{\sum_{l=1}^{n} x}{\mathrm{n}}$$

Donde,

n = número de pruebas realizadas

x = valor de vulnerabilidad (0% = no vulnerable, 100% = vulnerable)

3.6 Metodología de mantenimiento al subsistema

En la actualidad, elegir una metodología es algo complejo, esto conlleva realizar un análisis de aquella que se adapte más al trabajo que se esté realizando, por ello en el presente Trabajo de Integración Curricular se hará uso de SCRUM, al ser una metodología ágil, permite reducir la dificultad del desarrollo de un proyecto, según Schwaber en su artículo científico SCRUM Development Process menciona:

> *SCRUM es una metodología de gestión, mejora y mantenimiento para un sistema existente o un prototipo de producción. Asume el diseño y el código existente, lo cual es prácticamente siempre el caso en el desarrollo orientado a objetos debido a la presencia de librerías de clases. SCRUM abordará los esfuerzos de desarrollo de sistemas heredados totalmente nuevos o Rediseñados en una fecha posterior.* (Schwaber, 1997, p. 118)

Es por ello, la metodología SCRUM en el presente Trabajo de Integración Curricular está enfocada en el mantenimiento del Subsistema Sílabos 1.0.0, gracias a que SCRUM es más flexible a la hora de obtener un software nuevo.

3.6.1 Análisis

Estimaciones

Las estimación es uno de los puntos de partida, con ello se puede obtener el tiempo en que se podría realizar determinada tarea, por ello se eligió el método de la camiseta o T-shirt. Como se muestra en la **Tabla 5-3**.

Tabla 5-3: Estimaciones por el método T-Shirt

Talla	Puntos estimados	Horas de Trabajo
S	20	20
M	60	60
L	120	120
XL	240	240

Realizado por: Ramos Averos, Rodrigo, 2020.

Equipo de trabajo

En la **Tabla 6-3**, se detalla el equipo de trabajo involucrado en el desarrollo del presente trabajo.

Tabla 6-3: Equipo de trabajo

Persona	Rol
ESPOCH	Product Owner
Ing. Jorge Menéndez	Scrum Master
Rodrigo Ramos	Development Team

Realizado por: Ramos Averos, Rodrigo, 2020.

Estudio de factibilidad

Realizar este estudio es fundamental debido al resultado que ofrece, es decir, permite determinar el éxito o fracaso de realizar el presente trabajo, con el fin de tomar la decisión de proceder o no con el desarrollo.

- *Factibilidad técnica*

Por medio de este estudio se determina los recursos de hardware y software necesario para el desarrollo del trabajo, permitiendo responder a la pregunta de si se dispone de los equipos y herramientas para llevarlo a cabo (Manual Técnico, 2020, p. 26).

- *Factibilidad operativa*

Dentro de este estudio se determina el personal involucrado en el uso del subsistema, es decir, identificar los roles que deben tener los usuarios a los cuales va destinando el subsistema. Donde cada uno de estos tendrá distintas funcionalidades dependiendo el rol de cada uno (Manual Técnico, 2020, p. 27).

- *Factibilidad económica*

Al realizar este estudio se obtiene todos los costos requeridos en el transcurso del mantenimiento del subsistema, en el cual se toma en cuenta: costo de personal, instalación, operación, materiales y suministros. Es de vital importancia la información completa con respecto a la factibilidad económica, pues en este punto se toma en cuenta los costos mencionados anteriormente, por ello después del cálculo respectivo el costo es de $ 3.681,00. Ya que este tipo de recurso es el más

difícil de conseguir por lo tanto es indispensable conocerlo, de esta forma se puede evitar la interrupción del trabajo (Manual Técnico, 2020, pp. 28-29).

La realización de estos estudios anteriormente mencionados permitió concluir que el presente Trabajo de Integración Curricular propuesto es factible.

Riesgos

Conocer los posibles riesgos que pueden surgir en el transcurso de la realización del trabajo, es clave para de esta forma estar prevenidos ante algún problema que interrumpa las actividades necesarias para culminar el trabajo, por ello, se debe documentar los riesgos a través de la identificación, análisis, priorización y gestión, de esta forma estar preparados para cualquier eventualidad.

- *Identificación de riesgos*

A través de esta etapa, se conoce e inspecciona los riesgos, es decir, se asegura el reconocimiento de las causas y procedencia del riesgo que puedan afectar a los objetivos. Como resultado se obtuvo 7 riesgos, los cuales han sido clasificados de la siguiente manera: 6 Riesgos del Proyecto, 1 Riesgo Técnico. Al tener diferentes tipos de riesgos, también tendrán un impacto de nivel variable para el desarrollo de la solución del problema. Mayor información se encuentra en el (Manual Técnico, 2020, p. 30).

- *Análisis de riesgos*

El análisis de riesgos se estableció una probabilidad a cada riesgo, esto permite que el análisis que se le haga a cada uno tenga un valor con el cual se pueda clasificar, también su exposición y tomando como referencia los valores anteriores se pueda medir el impacto que este tendrá en el desarrollo de la solución del problema. Mayor información se encuentra en el (Manual Técnico, 2020, pp. 31-32).

- *Priorización de riesgos*

La priorización de los riesgos permite tener una referencia de cada riesgo y saber cuál es el que posee un nivel alto y por ende van a ser los primeros en presentarse por lo cual las soluciones a estos tipos de riesgos deben estar en las primeras opciones, por ello se ha tomado valores para clasificar los riesgos: Impacto bajo, color verde: 1 – 3, Impacto medio, color naranja/amarillo: 4 – 8, Impacto Alto, color rojo: 9 – 12. Estos valores han sido tomados aleatoriamente para clasificar los riesgos y su impacto en el desarrollo de la solución del problema. Mayor información, se encuentra en el (Manual Técnico, 2020, p. 33).

- *Gestión de riesgos*

La gestión de riesgos se determina los aspectos para desarrollar lo siguiente: disminuir, supervisar o evitar la presencia de riesgos que afecten en el desarrollo de la solución del problema, esto implicaría problemas a nivel general. Por esta razón se define la reducción, supervisión, gestión y evaluación del estado en todas las etapas del mantenimiento del sistema, mediante una hoja de gestión. Mayor información, se encuentra en el (Manual Técnico, 2020, pp. 34-40).

3.6.2 Fase de Planificación

Esta fase permite tener una idea del tiempo que tomará llevar a cabo las actividades necesarias para cumplir con el presente trabajo, permite realizar estimaciones de los recursos y costos. Dentro de esta fase se determinó las funcionalidades que requieren una actualización dando un total de 21, además, se tomó en cuenta la aplicación de las buenas prácticas de disponibilidad como requerimiento no funcional.

Product backlog

El Product backlog consiste un listado de requerimientos los cuales son establecidos por el cliente, admite priorizar y estimar los mismos según las necesidades del negocio. La herramienta que usa el product backlog es la historia de usuario la cual está documentada con lenguaje tradicional del cliente. En la **Tabla 7-3** se muestra las historias de usuario y el tipo de mantenimiento.

Tabla 7-3: Product backlog

HU	Tarea	Tipo	Estimación
HU_47	Mantenimiento a la funcionalidad Estrategias Metodológicas	Correctivo	30
HU_48	Mantenimiento a la funcionalidad Datos Generales del Sílabo	Correctivo	30
HU_49	Mantenimiento a las Ayudas de las Secciones del Sílabo	Correctivo	30
HU_50	Mantenimiento a la funcionalidad información de unidad	Perfectivo	30
HU_51	Mantenimiento a la funcionalidad objetivos de unidad	Perfectivo	30
HU_52	Mantenimiento a la funcionalidad actividades de aprendizaje en el aula	Perfectivo	30
HU_53	Mantenimiento a la funcionalidad actividades de aprendizaje autónomas	Perfectivo	30
HU_54	Mantenimiento a la funcionalidad logros de aprendizaje	Perfectivo	30
HU_55	Mantenimiento a la funcionalidad gestión de unidades	Perfectivo	30
HU_56	Mantenimiento a la funcionalidad bibliografía	Perfectivo	30
HU_57	Mantenimiento a la funcionalidad títulos académicos	Perfectivo	30
HU_58	Mantenimiento a la funcionalidad observaciones	Perfectivo	30
HU_59	Mantenimiento a la funcionalidad estrategias metodológicas administración Silabo	Perfectivo	30
HU_60	Mantenimiento a la funcionalidad recursos administración Silabo	Perfectivo	30
HU_61	Mantenimiento a la funcionalidad actividades de aprendizaje en el aula administración Silabo	Perfectivo	30
HU_62	Mantenimiento a la funcionalidad actividades de aprendizaje autónomas administración Silabo	Perfectivo	30
HU_63	Mantenimiento a la funcionalidad escenarios de aprendizaje reales administración Silabo	Perfectivo	30
HU_64	Mantenimiento a la funcionalidad escenarios de aprendizaje áulicos administración Silabo	Perfectivo	30
HU_65	Mantenimiento a la funcionalidad escenarios de aprendizaje virtuales administración Silabo	Perfectivo	30
HU_66	Mantenimiento a la funcionalidad modificar opciones	Perfectivo	30
HU_67	Mantenimiento a la funcionalidad modificar parámetros del sílabo	Perfectivo	30
HT_14	Estudio del subsistema Sílabos 1.0.0		30
HT_15	Estudio de Docker		60
HT_16	Estudio de Docker Swarm		60
HT_17	Estudio de la creación de servicios en un clúster Swarm		30
HT_18	Estudio de la herramienta Traefik		60
HT_19	Estudio de la herramienta Portainer		30
HT_20	Estudio de la configuración de Postgres como master y Slave en un clúster Swarm		60
HT_21	Estudio de la herramienta Rsnapshot		60
HT_22	Cambiar preparet statements del acceso a datos		60
HT_23	Seguridad en contra de los ataques CSRF		30
HT_24	Instalar el subsistema en la infraestructura de alta disponibilidad		60
HT_25	Revisión final del subsistema		30
HT_26	Documentación final		30

Realizado por: Ramos Averos, Rodrigo, 2020.

Las historias de usuario son utilizadas por las metodologías ágiles, con el fin de especificar y detallar de una forma concreta las necesidades del cliente y de esta manera tener claro lo que se debe incluir en el desarrollo del sistema, en cada historia de usuario se evidencia las discusiones y acuerdos que se tienen con el cliente y así también las pruebas de aceptación, esto se realiza por cada requerimiento determinado.

En la historia de usuario se detalla lo que se va a realizar en el sistema y está estructurada así: un número, el nombre de la HU, el usuario del sistema que cuenta con el menor nivel de acceso al mismo, a continuación tenemos el campo "Iteración" donde colocamos el número correspondiente a la misma, en la cual se va a desarrollar esta historia de usuario, además posee una prioridad en el negocio que es determinada como alta, media, baja dependiendo de la necesidad del usuario, en el riesgo del desarrollo se va determinar cómo alto, medio, bajo analizando la complejidad del mismo, una descripción de lo que el usuario requiere del sistema y su beneficio a obtener. En cuanto a las observaciones deben ir de acuerdo con las especificaciones y detalles importantes a tomar en cuenta en el desarrollo del requerimiento. Además, cada una tiene pruebas de aceptación que permitirán al cliente y al desarrollador verificar si ha satisfecho o no la funcionalidad especificada. Cómo se muestra en la **Tabla 8-3**.

A continuación, se muestra un modelo de historia de usuario, las demás historias de usuario que hacen referencia a cada uno de los requerimientos se encuentran en el (Manual Técnico, 2020, pp. 41-107)**.**

Tabla 8-3: Historia de usuario

HISTORIA DE USUARIO	
Número: HU_50	**Nombre de la Historia:** Mantenimiento a la funcionalidad información de unidad
Modificación de historia de usuario:	
Usuario: Docente	**Sprint Asignada:** 4
Prioridad en el Negocio: Media	**Puntos Estimados:** 30
Riesgo en el Desarrollo: Media	**Puntos Reales:** 30
Descripción: Se desarrollará para dar mantenimiento a la información de unidad, tomando en cuenta temas y subtemas, con el fin de mejorar la seguridad en cuanto al ingreso de caracteres o scripts no deseados.	
Observaciones: • Se controlará que no se permita ingresar caracteres especiales en los input de temas y subtemas correspondientes a información de la unidad	

Realizado por: Ramos Averos, Rodrigo, 2020.

Tabla 9-3: Pruebas de Aceptación

Historia de Usuario (Reverso) Pruebas de Aceptación
• Verificar que el usuario no ingrese caracteres especiales en los campos • Verificar la conexión a la base de datos

Realizado por: Ramos Averos, Rodrigo, 2020.

Sprint backlog

Sprint o iteración es la unidad básica de trabajo para un equipo dentro de la metodología SCRUM, esta es la característica principal que marca la diferencia entre SCRUM y otros modelos para el desarrollo ágil.

Para alcanzar la solución al problema de este Trabajo de Integración Curricular, se establecieron 10 Sprints haciendo referencia cada uno de ellos a los módulos del subsistema contemplados. La ejecución de los Sprints se realizó con un total de 1230 puntos de esfuerzo, dichos Sprints se detallan en la **Tabla 10-3**.

Tabla 10-3: Sprint backlog

ID	Fecha inicial	Fecha final	Esfuerzo	Responsable
SPRINT 1	**09/03/2020**	**26/03/2020**	**150**	
HT_14	09/03/2020	12/03/2020	30	Rodrigo Ramos
HT_15	13/03/2020	19/03/2020	60	Rodrigo Ramos
HT_16	20/03/2020	26/03/2020	60	Rodrigo Ramos
SPRINT 2	**27/03/2020**	**09/04/2020**	**120**	
HT_17	27/03/2020	31/03/2020	30	Rodrigo Ramos
HT_18	01/04/2020	06/04/2020	60	Rodrigo Ramos
HT_19	07/04/2020	09/04/2020	30	Rodrigo Ramos
SPRINT 3	**10/04/2020**	**30/04/2020**	**120**	
HT_20	10/04/2020	21/04/2020	60	Rodrigo Ramos
HT_21	22/04/2020	30/04/2020	60	Rodrigo Ramos
SPRINT 4	**01/05/2020**	**21/05/2020**	**120**	
HU_46	01/05/2020	06/05/2020	30	Rodrigo Ramos
HU_48	07/05/2020	12/05/2020	30	Rodrigo Ramos
HU_49	13/05/2020	18/05/2020	30	Rodrigo Ramos
HU_50	19/05/2020	21/05/2020	30	Rodrigo Ramos
SPRINT 5	**22/05/2020**	**11/06/2020**	**120**	
HU_51	22/05/2020	27/05/2020	30	Rodrigo Ramos
HU_52	28/05/2020	02/06/2020	30	Rodrigo Ramos
HU_53	03/06/2020	08/06/2020	30	Rodrigo Ramos
HU_54	09/06/2020	11/06/2020	30	Rodrigo Ramos
SPRINT 6	**12/06/2020**	**02/07/2020**	**120**	
HU_55	12/06/2020	17/06/2020	30	Rodrigo Ramos
HU_56	18/06/2020	23/06/2020	30	Rodrigo Ramos
HU_57	24/06/2020	26/06/2020	30	Rodrigo Ramos
HU_58	29/06/2020	02/07/2020	30	Rodrigo Ramos
SPRINT 7	**03/07/2020**	**23/07/2020**	**120**	
HU_59	03/07/2020	08/07/2020	30	Rodrigo Ramos
HU_60	09/07/2020	14/07/2020	30	Rodrigo Ramos
HU_61	15/07/2020	20/07/2020	30	Rodrigo Ramos
HU_62	21/07/2020	23/07/2020	30	Rodrigo Ramos
SPRINT 8	**24/07/2020**	**13/08/2020**	**150**	
HU_63	24/07/2020	28/07/2020	30	Rodrigo Ramos
HU_64	29/07/2020	31/07/2020	30	Rodrigo Ramos
HU_65	03/08/2020	05/08/2020	30	Rodrigo Ramos
HU_66	06/08/2020	10/08/2020	30	Rodrigo Ramos
HU_67	11/08/2020	13/08/2020	30	Rodrigo Ramos

Continua

Continua

SPRINT 9	**14/08/2020**	**27/08/2020**	**90**	
HT_22	14/08/2020	24/08/2020	60	Rodrigo Ramos
HT_23	25/08/2020	27/08/2020	30	Rodrigo Ramos
SPRINT 10	**28/08/2020**	**17/09/2020**	**120**	
HT_24	28/08/2020	03/09/2020	60	Rodrigo Ramos
HT_25	04/09/2020	10/09/2020	30	Rodrigo Ramos
HT_26	11/09/2020	17/09/2020	30	Rodrigo Ramos

Realizado por: Ramos Averos, Rodrigo, 2020.

3.6.3 Fase de Desarrollo

Dentro de esta fase, se realiza el mantenimiento del subsistema, en el cual se respeta los estándares, interfaz de usuario, base de datos establecidos por los anteriores involucrados en el proyecto, el enfoque está dirigido a implementar buenas prácticas de disponibilidad a través del mantenimiento, por lo que las se garantizará mejorar la versión actual del subsistema sin afectar el funcionamiento del mismo.

Análisis de la arquitectura del subsistema.

Para el análisis del subsistema se utiliza UML, tomando en cuenta para ello, el diagrama de componentes (Manual Técnico, 2020, p. 107) y el diagrama de despliegue (Manual Técnico, 2020, p. 108), los cuales contribuyeron en la comprensión del subsistema Silabos 1.0.0 para tener claro el desarrollo de las buenas prácticas de disponibilidad y el mantenimiento al subsistema.

Implementación

En esta etapa se realiza la aplicación de las buenas prácticas de disponibilidad de información en base a los diagramas de despliegue y componentes mencionados anteriormente. Además, para conocer la estructura del subsistema y posteriormente identificar las clases en donde realizar el mantenimiento, se desarrolló el diagrama de Clases (Manual Técnico, 2020, p. 109) y el Diagrama de Objetos (Manual Técnico, 2020, p. 110). Con el fin de implementar las buenas prácticas de seguridad del manual del Trabajo de Integración Curricular de Kevin Chimbo y Sandra Ordoñez en el subsistema.

Posterior a ello, se realizó el mantenimiento para aplicar las buenas prácticas de disponbilidad en el Subsistema Sílabos Institucionales obteniéndose la versión 1.1.0, Mismas que se encuentran documentadas en las historias técnicas e historias de usuario, un mayor detalle se muestra en el (Manual Técnico, 2020, pp. 41-106)**.**

Pruebas del subsistema

Una vez finalizado el mantenimiento se realizó el proceso de pruebas, en base al Plan de Pruebas desarrollado. Los resultados de las pruebas mencionadas se encuentran en el documento (Plan de Pruebas, pp. 31-146).

3.6.4 Fase de Finalización

En base a la metodología aplicada se realiza pruebas al subsistema una vez subido a los servidores tomando en cuenta las buenas prácticas de disponibilidad investigadas, con el fin de verificar el correcto funcionamiento, además, los respectivos documentos y versiones del subsistema se encuentran cargados en un repositorio GitHub. Para la utilización del subsistema se debe capacitar a los usuarios para que tengan una idea clara de cómo utilizarlo, como ayuda para que esta tarea sea más sencilla se encuentra también un manual de usuario.

Seguimiento del riesgo

De los riesgos que se determinaron no tuvieron impacto en el desarrollo del presente trabajo, ya que se los planificó correctamente y las medidas de mitigación ayudaron a que no representen amenaza alguna.

Reuniones

Reuniones diarias, están se efectuaron con el fin de tener una idea clara de cómo iba avanzando el trabajo, donde se definieron las buenas prácticas de disponibilidad así como las pruebas a realizar.

Reuniones de planificación, estás se efectuaron semanalmente con el grupo de desarrollo encargado del proyecto, donde se generaron las siguientes actividades:

- Determinar las buenas prácticas de disponibilidad a investigar.
- Generar los casos de pruebas.
- Ejecutar las pruebas antes de las buenas prácticas.
- Obtener resultados de las pruebas antes de las buenas prácticas.
- Aplicar las buenas prácticas investigadas.
- Ejecutar las pruebas después de las buenas prácticas.

- Obtener resultados de las pruebas después de las buenas prácticas.
- Generar guía de las buenas prácticas de disponibilidad.
- Aplicar buenas prácticas de seguridad
- Realizar las modificaciones al subsistema.
- Documentar el proceso.

Reuniones de entrega, se las realiza una vez por cada Sprint, donde se hace conocer al cliente los cambios realizados. En cada reunión se realizó las siguientes actividades.

- Revisar el avance.
- Obtener aprobación.
- Generar nuevas tareas a realizar.

Reuniones de retroalimentación, se realizaron después de cada Sprint donde se revisó posibles soluciones a errores e inconvenientes encontrados en el transcurso del Sprint.

En el **Anexo A** se lista el cumplimiento de las buenas prácticas de disponibilidad.

CAPÍTULO IV

4. RESULTADOS

El presente capítulo se realiza un análisis estadístico de los resultados obtenidos antes y después de haber aplicado buenas prácticas, además de un comparativo de la disponibilidad del subsistema.

4.1 Análisis de resultados del subsistema Sílabos 1.0.0

Los valores obtenidos en la ejecución de las pruebas realizadas al Subsistema Sílabos 1.0.0 antes de aplicar las buenas prácticas de disponibilidad, se muestran en la **Tabla 1-4**, donde se puede identificar un indicador, el cual muestra lo que se está evaluando, los escenarios considerados para las pruebas, el resultado ejecución fallida y exitosa, marcado con una X de acuerdo con el resultado obtenido. La información detallada se encuentra en el (Plan de Pruebas, 2020, pp. 31-88)**.**

Tabla 1-4: Resultado de las pruebas antes de aplicar las buenas prácticas de disponibilidad

Indicador	Escenarios de las Pruebas	Resultado Ejecución Fallida	Resultado Ejecución Exitosa
Disponibilidad	Todos los nodos del servidor 1 activos		X
	Un solo nodo del servidor 1 activo		X
	Un nodo manager cero nodos worker activos en el servidor 1	X	
	Un nodo manager un nodo worker activos en el servidor 1	X	
	Cero nodos manager un nodo worker activo en el servidor 1	X	
	Cero nodos manager dos nodos worker activos en el servidor 1	X	
	Fallo de un nodo con réplicas Redis en el servidor 1	X	
	Fallo de dos nodos con réplicas Redis en el servidor 1	X	
	Fallo de tres nodos con réplicas Redis en el servidor 1	X	
	Fallo de un nodo con réplicas Payara para la interfaz de usuario en el servidor 1	X	
	Fallo de dos nodos con réplicas Payara para la interfaz de usuario en el servidor 1	X	

Continua

Continua

	Fallo de tres nodos con réplicas Payara para la interfaz de usuario en el servidor 1	X	
	Fallo nodo manager con Traefik proxy inverso en el servidor 1		X
	Fallo de un nodo manager con Portainer la cual es una herramienta para administrar clúster Swarm mediante interfaz gráfica en el servidor 1		X
	Fallo nodo con Visualizer en el servidor 1		X
	Fallo de un nodo con el Registro Privado en el servidor 1	X	
	Fallo de dos nodos con el Registro Privado en el servidor 1	X	
	Fallo de tres nodos con el Registro Privado en el servidor 1	X	
	Todos los nodos del servidor 2 activos		X
	Un solo nodo del servidor 2 activo		X
	Un nodo manager cero nodos worker activos en el servidor 2	X	
	Un nodo manager un nodo worker activos en el servidor 2	X	
	Cero nodos manager un nodo worker activo en el servidor 2	X	
	Cero nodos manager dos nodos worker activos en el servidor 2	X	
	Fallo de un nodo con Postgres Master en el servidor 2	X	
	Fallo de un nodo con réplicas Postgres Slave en el servidor 2	X	
	Fallo de dos nodos con réplicas Postgres Slave en el servidor 2	X	
	Fallo de tres nodos con réplicas Postgres Slave en el servidor 2	X	
	Fallo de un nodo con réplicas Payara para el acceso a datos en el servidor 2	X	
	Fallo de dos nodos con réplicas Payara para el acceso a datos en el servidor 2	X	
	Fallo de tres nodos con réplicas Payara para el acceso a datos en el servidor 2	X	
	Fallo nodo manager con Traefik proxy inverso en el servidor 2		X
	Fallo de un nodo manager con Portainer herramienta para administrar clúster Swarm mediante interfaz gráfica en el servidor 2		X
	Fallo nodo con Visualizer en el servidor 2		X
	Fallo nodo con el Registro Privado en el servidor 2	X	
	Fallo dos nodos con el Registro Privado en el servidor 2	X	
	Fallo tres nodos con el Registro Privado en el servidor 2	X	
	TOTAL	27	10

Realizado por: Ramos Averos, Rodrigo, 2020.

Con el objetivo de analizar los resultados se hizo un análisis del porcentaje de pruebas exitosas vs las fallidas como se observan en el **Gráfico 1-4**.

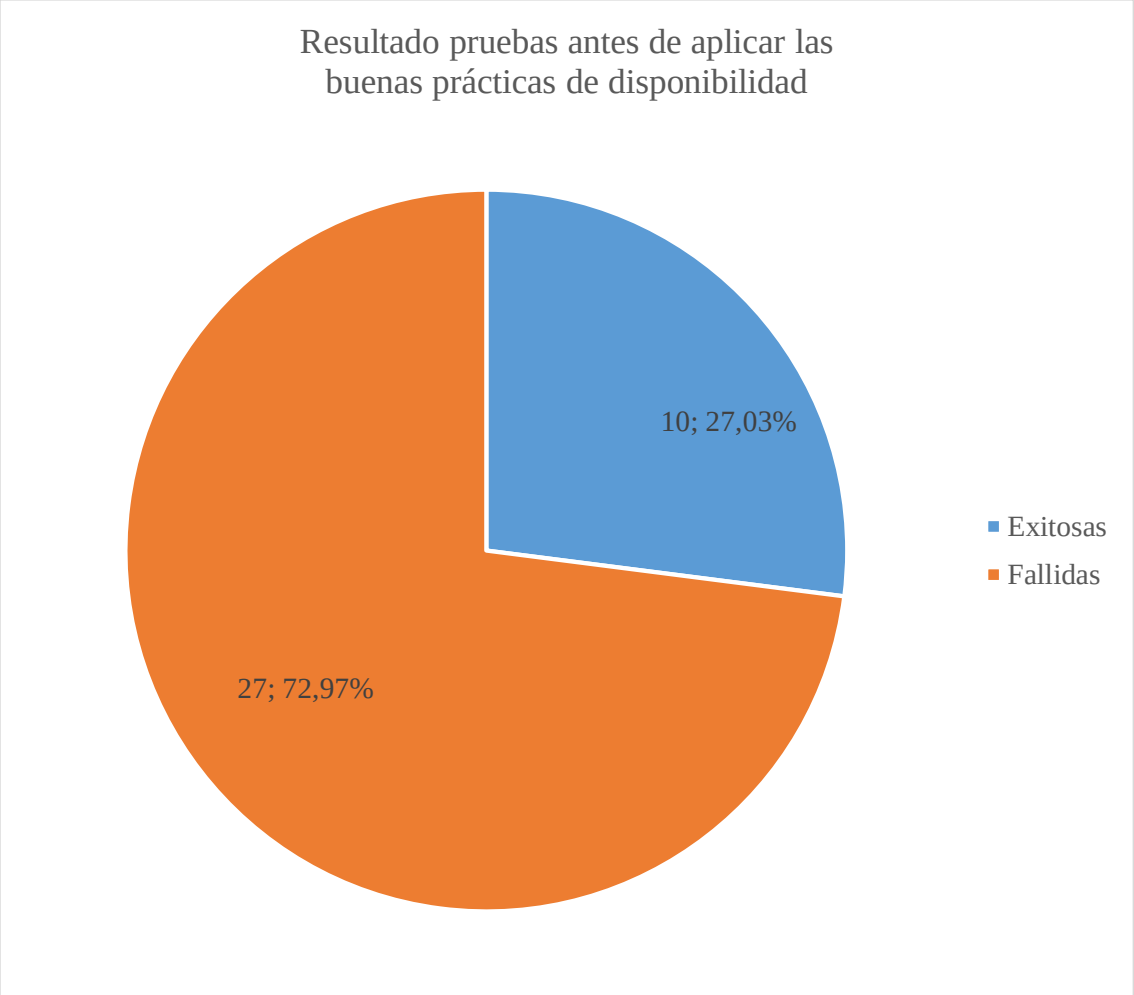

Gráfico 1-4. Resultados de las pruebas realizadas antes de aplicar las buenas prácticas de disponibilidad

Realizado por: Ramos R. 2020

De los resultados anteriores se evidencia que solo el 27,03 % de las pruebas fueron exitosas demostrando que es necesario investigar y aplicar buenas prácticas para lograr alta disponibilidad.

El valor de tantas pruebas fallidas se debe a que la infraestructura donde se encuentra desplegado el subsistema no cuenta con una configuración de alta disponibilidad, es decir, no existe redundancia en los nodos, la falta de un clúster de nodos hace que al tener un solo nodo si este nodo cae falla la disponibilidad, además, hay fallas en cuando a memoria cache, base de datos, replicación de servicios. También, no hay una configuración para copias de seguridad automáticas, ni herramientas que permitan monitorear el funcionamiento de la infraestructura.

4.2 Análisis de resultados del subsistema Sílabos 1.1.0

Los valores obtenidos en la ejecución de las pruebas realizadas al Subsistema Sílabos 1.1.0 después de aplicar las buenas prácticas de disponibilidad, se muestran en la **Tabla 2-4**, donde se puede identificar un indicador, el cual muestra lo que se está evaluando, los escenarios considerados para las pruebas, el resultado ejecución fallida y exitosa, marcado con una X de acuerdo con el resultado obtenido. La información detallada se encuentra en el (Plan de Pruebas, 2020, pp. 89-146).

Tabla 2-4: Resultado de las pruebas después de aplicar las buenas prácticas de disponibilidad

Indicador	Escenarios de las Pruebas	Resultado Ejecución Fallida	Resultado Ejecución Pasada
Disponibilidad	Todos los nodos del servidor 1 activos		X
	Un solo nodo del servidor 1 activo		X
	Un nodo manager cero nodos worker activos en el servidor 1		X
	Un nodo manager un nodo worker activos en el servidor 1		X
	Cero nodos manager un nodo worker activo en el servidor 1		X
	Cero nodos manager dos nodos worker activos en el servidor 1		X
	Fallo de un nodo con réplicas Redis en el servidor 1		X
	Fallo de dos nodos con réplicas Redis en el servidor 1		X
	Fallo de tres nodos con réplicas Redis en el servidor 1	X	
	Fallo de un nodo con réplicas Payara para la interfaz de usuario en el servidor 1		X
	Fallo de dos nodos con réplicas Payara para la interfaz de usuario en el servidor 1		X
	Fallo de tres nodos con réplicas Payara para la interfaz de usuario en el servidor 1	X	
	Fallo nodo manager con Traefik proxy inverso en el servidor 1	X	
	Fallo de un nodo manager con Portainer la cual es una herramienta para administrar clúster Swarm mediante interfaz gráfica en el servidor 1		X
	Fallo nodo con Visualizer en el servidor 1		X
	Fallo de un nodo con el Registro Privado en el servidor 1		X
	Fallo de dos nodos con el Registro Privado en el servidor 1		X
	Fallo de tres nodos con el Registro Privado en el servidor 1		X
	Todos los nodos del servidor 2 activos		X

Continua

Continua

	Un solo nodo del servidor 2 activo		X
	Un nodo manager cero nodos worker activos en el servidor 2		X
	Un nodo manager un nodo worker activos en el servidor 2		X
	Cero nodos manager un nodo worker activo en el servidor 2		X
	Cero nodos manager dos nodos worker activos en el servidor 2		X
	Fallo de un nodo con Postgres Master en el servidor 2	X	
	Fallo de un nodo con réplicas Postgres Slave en el servidor 2		X
	Fallo de dos nodos con réplicas Postgres Slave en el servidor 2		X
	Fallo de tres nodos con réplicas Postgres Slave en el servidor 2	X	
	Fallo de un nodo con réplicas Payara para el acceso a datos en el servidor 2		X
	Fallo de dos nodos con réplicas Payara para el acceso a datos en el servidor 2		X
	Fallo de tres nodos con réplicas Payara para el acceso a datos en el servidor 2	X	
	Fallo nodo manager con Traefik proxy inverso en el servidor 2	X	
	Fallo de un nodo manager con Portainer herramienta para administrar clúster Swarm mediante interfaz gráfica en el servidor 2		X
	Fallo nodo con Visualizer en el servidor 2		X
	Fallo nodo con el Registro Privado en el servidor 2		X
	Fallo dos nodos con el Registro Privado en el servidor 2		X
	Fallo tres nodos con el Registro Privado en el servidor 2		X
	TOTAL	7	30

Realizado por: Ramos, Rodrigo, 2020.

Con el objetivo de analizar los resultados se hizo un análisis del porcentaje de pruebas exitosas vs las fallidas como se observan en el **Gráfico 2-4**.

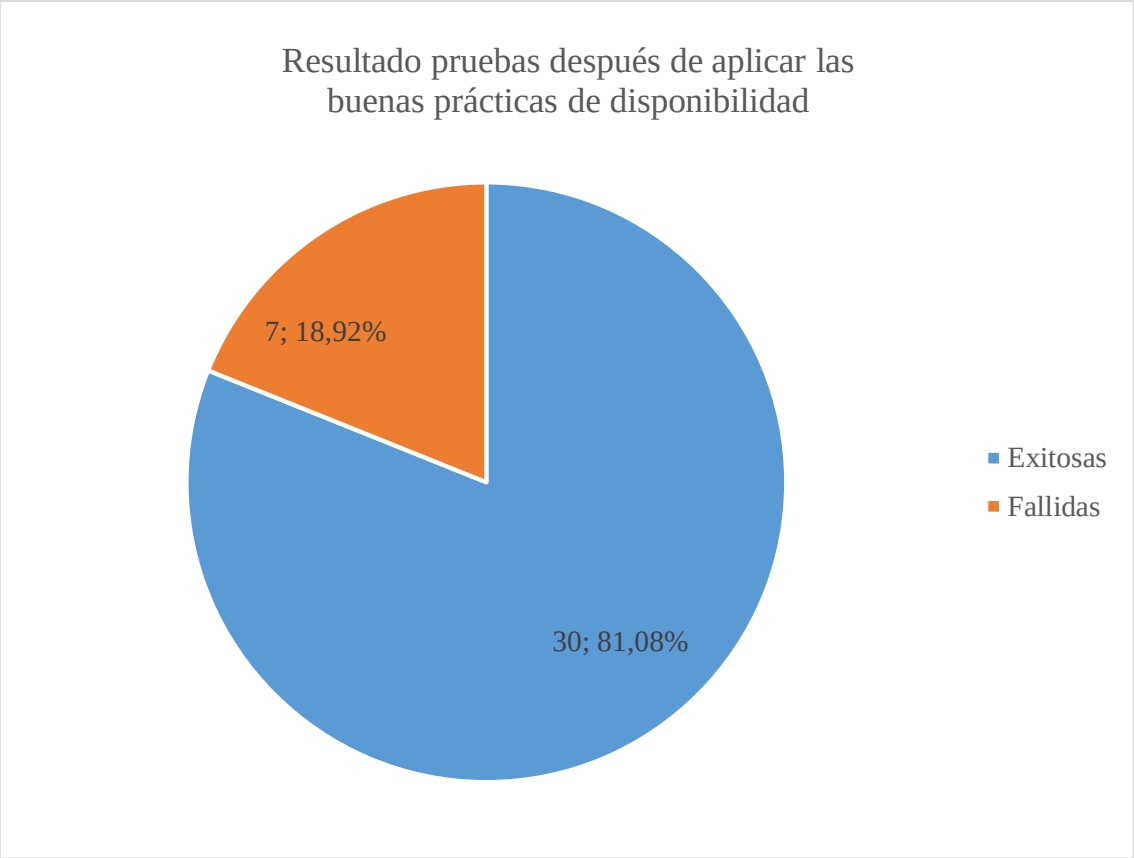

Gráfico 2-4. Resultados de las pruebas realizadas después de aplicar las buenas prácticas de disponibilidad

Realizado por: Ramos R. 2020

De los resultados anteriores se evidencia que el 81,08 % de las pruebas fueron exitosas demostrando que el subsistema una vez aplicada las buenas prácticas de disponibilidad se disminuye las interrupciones no autorizadas.

El incremento del valor en cuanto a pruebas pasadas con un porcentaje del 81,08% se debe a las fortalezas que brinda la solución propuesta, ya que permite que el subsistema Sílabos 1.1.0 se encuentre desplegado en un clúster de Docker Swarm, las ventajas que esto proporciona son muchas. Entre ellas, la replicación de servicios, al estar la aplicación en un contenedor permite que si un nodo cae, el contenedor se despliegue automáticamente en otro, lo cual impide que el funcionamiento sea interrumpido, además, esto proporciona seguridad ya que la aplicación se encuentra aislada y respaldada en un contenedor, facilita la portabilidad, así como la restauración de la aplicación en caso de una falla. Además, se cuenta con un proxy reverso (Traefik), el cual permite dirigir el tráfico del subsistema a un DNS en específico, también aporta la generación de certificados SSL automáticamente, así como el balanceo de carga. También, se dispone de un clúster de base de datos el cual falla sólo si se caen todos los nodos esclavos o master, lo mismo sucede con los nodos para caché de memoria, así como para la aplicación, todo esto monitorizado

por medio de dos herramientas Portainer y Visualizer. Adicionalmente, existe una configuración de copias de seguridad automáticas por medio de la herramienta Rsnapshot, Finalmente se cuenta con la activación del firewall para evitar tráfico indebido, esta solución permite garantizar la disponibilidad del subsistema Sílabos 1.1.0 por más tiempo.

Sin embargo, existen un 18,92% de pruebas fallidas esto se debe a que aun aplicando las buenas prácticas de disponibilidad, existen aspectos en los que falla tales como; la herramienta de proxy inverso (Traefik) el cual al tener un solo nodo en el cual funcionar existe un punto de falla, ya que se perdería el vínculo entre los servicios que ofrece el Subsistema Sílabos con el DNS. Otro de los inconvenientes es en cuanto al clúster Postgres ya que la configuración actual permite tener un solo nodo master y en caso de que falle, se pierde la capacidad de que el subsistema realice registros y modificaciones. Finalmente, otro de los aspectos a tomar en cuenta es el caso de que todos los nodos fallen.

4.3 Comparativo de la disponibilidad del subsistema Sílabos

Para analizar la disponibilidad se tomó en cuenta los resultados de las pruebas en los dos escenarios, es decir, antes y después de aplicar las buenas prácticas de disponibilidad, como se muestra en la **Tabla 3-4**.

Tabla 3-4: Resumen de resultados

Indicador	Disponibilidad del Subsistema (%)	
	Sin Buenas Prácticas	Con Buenas Prácticas
Disponibilidad	27,03	81,08
Mejora	0	54,05

Realizado por: Ramos Averos, Rodrigo, 2020.

La mejora de la disponibilidad en un 54,05 % se debe a las buenas prácticas de disponibilidad donde se tiene; clústeres administrado por Docker Swarm, lo cual permite escalabilidad, replicación de servicios de forma rápida y sencilla. Balanceador de carga, proxy reverso y vinculación de los servicios a un DNS por medio de Traefik. Failover Solutions por medio de herramientas de administración y monitoreo de clúster como Portainer y Visualizer con el fin de verificar que no haya fallas en los nodos y los servicios que estos proporcionan. Replicación de base de datos por medio de la configuración de clúster Postgres con nodo manager y nodos esclavos para poder aumentar la disponibilidad en la base de datos. Copias de seguridad automáticas de la información del Subsistema por medio de Rsnapshot para tener un respaldo de la información de manera periódica evitando pérdidas en caso de fallos y finalmente la activación de un firewall para evitar el tráfico no deseado, todo esto contribuye a una configuración de alta

disponibilidad para el subsistema Sílabos 1.1.0 garantizando que el mismo funcione por más tiempo evitando de esta forma interrupciones no autorizadas.

Sin embargo, existe un porcentaje que falta mejorar para llegar a un 100 % de disponibilidad, esto debido a los inconvenientes que se mencionó anteriormente como es el caso de la herramienta Traefik que sirve como proxy reverso, por lo tanto se recomienda analizar la opción de añadir más nodos manager donde pueda funcionar la herramienta Traefik o investigar la utilización de otros proxies que brinden funcionalidades similares. En cuando a la configuración del clúster de Postgres, se debe analizar la posibilidad de montar un clúster de alta disponibilidad para una base de datos Postgres SQL replicada, es decir, pensar en la posibilidad de alta disponibilidad del nodo master, donde haya dos clúster replicándose entre sí, master con master, esclavos con esclavos y luego un sistema de alta disponibilidad entre las parejas de nodos master y esclavos, de tal forma que si cae uno, el otro se levante aparte de ya haberse replicado. Finalmente, se toma en cuenta el escenario donde se dé la caída total de los nodos, por lo tanto, se recomienda analizar la probabilidad de que esto ocurra, y posteriormente la factibilidad económica de incorporar más nodos, para el análisis del costo / beneficio de aumentar nodos, con el objetivo de ver si es factible o no desde el punto de vista económico.

CONCLUSIONES

- La aplicación de las buenas prácticas de disponibilidad establecidas en el Manual de Buenas Prácticas de Disponibilidad desarrollado, permitió mejorar la disponibilidad en un 54,05 %.
- Se determinó que el nivel de disponibilidad del subsistema Sílabos 1.0.0 es de 27,03 %, mediante la ejecución de las pruebas antes de las buenas prácticas de disponibilidad.
- Se investigó un total de 6 buenas prácticas: Clúster por medio de la utilización de contenedores, Balanceador de Carga, Failover Solutions, Replicación Base de Datos, Copias de Seguridad, Firewall y se generó un Manual de Buenas Prácticas de Disponibilidad, el mismo que contiene los pasos para la configuración de alta disponibilidad.
- Se dio mantenimiento al subsistema Sílabos 1.0.0, donde se aplicó las buenas prácticas de seguridad propuestas en el Trabajo de Integración Curricular de Kevin Chimbo y Sandra Ordoñez, además de las buenas prácticas de disponibilidad, obteniendo la versión 1.1.0.
- Se determinó el nivel de disponibilidad del subsistema Sílabos 1.1.0 donde se obtuvo un valor correspondiente a 81,08 %.

RECOMENDACIONES

- Evitar el uso de caracteres especiales en la configuración de los archivos docker-compose.yml para la configuración de los servicios en el clúster de Docker Swarm, debido a que se produce errores y no se puede desplegar los servicios.
- Realizar un estudio de alta disponibilidad con respecto a proxies inversos, para evitar conflictos con el DNS.
- Investigar sobre clúster de alta disponibilidad con Postgres para solucionar el problema de disponer un solo servicio con Postgres Master.
- Realizar el análisis de la factibilidad económica de agregar más nodos a los clústeres.
- Actualizar cada dos años el Manual de Buenas Prácticas de Disponibilidad para incorporar las técnicas publicadas en nuevas investigaciones.

BIBLIOGRAFÍA

ABRAN, A., SEFFAH, A. y TALEB, M. "Pattern-Oriented Architecture for Web Applications". [en línea], 2007, [Consulta: 19 junio 2020]. Disponible en: https://www.academia.edu/16763709/Pattern-Oriented_Architecture_for_Web_Applications.

ACCU WEB HOSTING. *Top 5 High Availability Dedicated Server Solutions | Windows VPS Hosting Blog - AccuWeb Hosting* [blog], 2019. [Consulta: 17 julio 2020]. Disponible en: https://www.accuwebhosting.com/blog/top-5-high-availability-dedicated-server-solutions/.

ALBA, I. "Rsnapshot Tutorial de Utilización". *Aplicaciones y Sistemas* [en línea], 2013. [Consulta: 7 septiembre 2020]. Disponible en: https://aplicacionesysistemas.com/rsnapshot-backups-en-gnulinux-1/.

ALFONZO, P.L., MARIÑO, S.I. y GODOY, M.V. "Propuesta de aplicación de SCRUM para gestionar el proceso de mantenimiento del software: estudio preliminar". *Técnica administrativa*, vol. 11, nº 49 (2012), pp. 4. ISSN 1666-1680. DOI 10.1109/ICSM.2004.1357864.

ALTALEF, N. *Firewall en Alta Disponibilidad* [en línea], 2007. S.l.: RedKlee. Disponible en: http://www.bvs.hn/cu-2007/ponencias/SWL/SWL23.pdf.

ARRAY. *Administración de Docker Swarm con Portainer – El array de Jota* [blog]. 2019. [Consulta: 7 septiembre 2020]. Disponible en: https://www.elarraydejota.com/administracion-de-docker-swarm-con-portainer/.

ASALE, R., & RAE. Ataque | Diccionario de la Lengua Española. *«Diccionario de la lengua española» - Edición del Tricentenario* [en línea], 2019. [Consulta: 2 julio 2020]. Disponible en: https://dle.rae.es/ataque.

BANKER, R.D., DATAR, S.M., KEMERER, C.F., & ZWEIG, D. "Software Errors and Software Maintenance Management". *Information Technology and Management*, vol. 3, nº 1 (2002), pp. 25-41. ISSN 1573-7667. DOI 10.1023/A:1013156608583.

BLASCO, J. "Ataques DoS en aplicaciones Web". *OWASP, Ataques DoS en aplicaciones Web*. S.l.: s.n., 2007, pp. 39.

BRAUCH, H.G.; et al. "Concepts of Security Threats, Challenges, Vulnerabilities and Risks". *Coping with Global Environmental Change, Disasters and Security: Threats, Challenges, Vulnerabilities and Risks* [en línea], 2011, Berlin, Heidelberg: Springer, Hexagon Series on

Human and Environmental Security and Peace, pp. 61-106. [Consulta: 2 julio 2020]. ISBN 978-3-642-17776-7. Disponible en: https://doi.org/10.1007/978-3-642-17776-7_2.

BRODBECK, C. *La importancia de alta disponibilidad en firewalls para las organizaciones OSTEC Blog* [blog], 2017. [Consulta: 17 julio 2020]. Disponible en: https://ostec.blog/es/seguridad-perimetral/alta-disponibilidad-firewalls.

CEVALLOS MUÑOZ, Fausto Danilo, & SIGUENZA PLAZA, Ángel Javier. Propuesta de Mejores Prácticas de Seguridad para el Desarrollo de Aplicaciones Móviles [en línea] (Trabajo de Titulación). (Ingeniería) Escuela Superior Politécnica de Chimborazo, Facultas Informática y Electrónica, Escuela de Ingeniería en Sistemas. Riobamba, Ecuador. 2016. [Consulta: 14 abril 2020]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/4762.

CHARRON-BOST, B., PEDONE, F. & SCHIPER, A. *Replication: Theory and Practice.* [en línea]. Berlin Heidelberg: Springer-Verlag, 2010. [Consulta: 7 julio 2020]. Theoretical Computer Science and General Issues, Lect.Notes ComputerState-of-the-Art Surveys. ISBN 978-3-642-11293-5. Disponible en: https://www.springer.com/la/book/9783642112935.

CLOUDFLARE. *DoS y DDoS Attack | Cloudflare* [en línea]. 2019. [Consulta: 17 julio 2020]. Disponible en: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/.

COMUNIDAD DE PRÁCTICAS EN APS. *¿Qué es una Buena Práctica?* [en línea], 2018. [Consulta: 17 julio 2020]. Disponible en: http://buenaspracticasaps.cl/que-es-una-buena-practica/.

CONTRALORÍA GENERAL DEL ESTADO ECUADOR. *Portal Web Oficial de la Contraloría General del Estado del Ecuador* [en línea]. 2009. [Consulta: 14 abril 2020]. Disponible en: https://www.contraloria.gob.ec/Normatividad/BaseLegal.

COSTAS SANTOS, J. *Seguridad y alta disponibilidad* [en línea]. Madrid, SPAIN: RA-MA Editorial, 2014. [Consulta: 25 junio 2020]. ISBN 978-84-9964-345-8. Disponible en: http://ebookcentral.proquest.com/lib/espochsp/detail.action?docID=3228975.

DDOS-GUARD. *DoS y DDoS Attacks Tipos de Ataques* [en línea]. 2019. [Consulta: 17 julio 2020]. Disponible en: https://ddos-guard.net/en/terminology/attack_type/fraggle-attack-broadcast-udp-packets-attack.

DEPARTAMENTO DE SEGURIDAD HOMELAND. "Understanding Denial-of-Service Attacks | CISA". *CISA Cyber-Infraestructure* [en línea], 2009. [Consulta: 6 julio 2020]. Disponible en: https://www.us-cert.gov/ncas/tips/ST04-015.

DÍAZ, G. *Réplica Base de Datos Tópicos de Bases de Datos* [en línea], 2016. [Consulta: 17 julio 2020]. Disponible en: https://topicdb.wordpress.com/4-1-2-replica-4/.

DOCKER. "Swarm mode overview". *Docker Documentation* [en línea], 2020. [Consulta: 7 septiembre 2020]. Disponible en: https://docs.docker.com/engine/swarm/.

DUSSAN CLAVIJO, C.A. *Políticas de Seguridad Informática* [en línea]. 2006. [Consulta: 20 abril 2020]. Disponible en: https://www.redalyc.org/pdf/2654/265420388008.pdf.

ECURED. *Ataque informático* [en línea]. 2018. [Consulta: 4 mayo 2020]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico.

ESPOCH. *Dirección de Desarrollo Académico. Escuela Superior Politécnica de Chimborazo* [en línea]. 2019. [Consulta: 14 abril 2020]. Disponible en: https://www.espoch.edu.ec/index.php/u-des-acad-y-educ-dist.html#publicaciones

ESPOCH. *Dirección de Tecnologías de la Información y Comunicación. Escuela Superior Politécnica de Chimborazo* [en línea]. 2006. [Consulta: 14 abril 2020]. Disponible en: https://www.espoch.edu.ec/index.php/direccion-de-tecnologias-de-la-informacion-y-comunicacion.html.

FRASER, B.Y. *Site Security Handbook* [en línea]. 1997. [Consulta: 8 mayo 2020]. Disponible en: https://tools.ietf.org/html/rfc2196?fbclid=IwAR1WeoTP0oL9Rd0dzsncLnSuZGxkWcxDXLCeVQHaGW4gyea9ccqejnC7I2s.

GADAE. *Copias de seguridad: ¿para qué sirven? Informática para empresas* [en línea]. 2019. [Consulta: 17 julio 2020]. Disponible en: http://www.gadae.com/blog/para-que-sirven-las-copias-de-seguridad/.

GAO, H. y MIAO, H. "Research on the dynamic reconfiguration of Web application using two-phase compatibility verification". *International Journal of Computer Mathematics*, vol. 90, nº 11 (2013), pp. 2265-2278. ISSN 0020-7160. DOI 10.1080/00207160.2013.782398.

GAVILÁNES PILCO, Verónica Isabel. Elaborar una Metodología Aplicando la Norma ISO IEC 27001 en la Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en EL DESITEL de la ESPOCH [en línea] (Trabajo de Titulación). (Ingeniería) Escuela Superior Politécnica de Chimborazo, Facultad Informática y Electrónica, Escuela de Ingeniería en Sistemas. Riobamba, Ecuador. 2012. [Consulta: 14 abril 2020]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/1533.

GONZÁLEZ, C. *Ataques DOS y DDOS | Guía Emagister. Ataques DoS y DDoS* [blog]. 2019. [Consulta: 17 julio 2020]. Disponible en: https://www.emagister.com/blog/ataques-dos-ddos/.

GUAMÁN QUINCHE, E.R. S*eguridad en entornos web para sistemas de gestión académica* [en línea]. 2011. [Consulta: 15 abril 2020]. Disponible en: http://repositorio.educacionsuperior.gob.ec/handle/28000/120.

GUEVARA ESPINOZA, Lucia Verónica. Implementación de la norma ISO 27 para gestión en seguridad de información, caso práctico: DESITEL [en línea] (Trabajo de Titulación). (Ingeniería) Escuela Superior Politécnica de Chimborazo, Facultad Informática y Electrónica, Escuela de Ingeniería en Sistemas. Riobamba, Ecuador. 2013. [Consulta: 14 abril 2020]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/2541.

HACK2SECURE. *Common Attacks Against Availability* [en línea]. 2019. [Consulta: 6 julio 2020]. Disponible en: https://www.hack2secure.com/blogs/common-attacks-against-availability.

HASSAN, A.E. & HOLT, R.C. "Architecture Recovery of Web Applications". En: event-place: Orlando, Florida, *Proceedings of the 24th International Conference on Software Engineering* [en línea], 2002, New York, NY, USA: ACM, pp. 349–359. [Consulta: 18 junio 2020]. ISBN 978-1-58113-472-8. DOI 10.1145/581339.581383. Disponible en: http://doi.acm.org/10.1145/581339.581383.

HERNÁNDEZ DIAZ, L.R., ANDRÉ AMPUERO, M. & MARTÍNEZ PRIETO, J.P. *Un modelo para la implementación de la seguridad de una aplicación Web con el uso de la programación orientada a aspectos* [en línea]. La Habana, CUBA: D - Instituto Superior Politécnico José Antonio Echeverría. CUJAE, 2012. [Consulta: 18 junio 2020]. Disponible en: http://ebookcentral.proquest.com/lib/espochsp/detail.action?docID=3203748.

HERRMANN, H. & BUCKSCH, H. *Dictionary Geotechnical Engineering/Wörterbuch GeoTechnik* [en línea]. Berlin, Heidelberg: Springer, 2014. [Consulta: 2 julio 2020]. ISBN 978-3-642-41714-6. Disponible en: https://doi.org/10.1007/978-3-642-41714-6_200986.

IEEE STANDARDS ASSOCIATION. I*EEE 1219-1992 - IEEE Standard for Software Maintenance* [en línea]. 2019. [Consulta: 12 mayo 2020]. Disponible en: https://standards.ieee.org/standard/1219-1992.html.

IMPERVA. *Instant Failover | Auto-Detection and Disaster Recovery | Imperva* [en línea]. 2019. [Consulta: 17 julio 2020]. Disponible en: https://www.imperva.com/learn/availability/instant-failover/.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. "Buenas prácticas en el área de informática". *INCIBE* [en línea], 2016. [Consulta: 17 julio 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/buenas-practicas-area-informatica.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. *Copias de Seguridad* [en línea]. 2018. S.l.: s.n. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. "Medidas de prevención contra ataques de denegación de servicio". *INCIBE* [en línea], 2019. [Consulta: 6 julio 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio.

ISO/IEC 15408-1. *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*.

ISO/IEC 27001. *Information technology — Security techniques — Information security management systems — Requirements.*

ISO/IEC 27000. *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

ISO 27001. *Software ISO 27001 de Sistemas de Gestión. ISOTools*.

ISO27000. *El portal de ISO 27001 en español. Gestión de Seguridad de la Información*.

ISO/IEC 14764. *Information technology — Software maintenance ISO/IEC 14764*.

KALMAN, S. *Security Field Guide* [en línea]. S.l.: Cisco Press, 2003. [Consulta: 25 junio 2020]. ISBN 978-1-58705-092-3. Disponible en: https://books.google.com/books/about/Web_Security_Field_Guide.html?hl=es&id=uQTBwAEACAAJ.

KIZZA, J.M. *Understanding Network Security* [en línea]. Boston, MA: Springer US, 2005. [Consulta: 25 junio 2020]. ISBN 978-0-387-25228-5. Disponible en: https://doi.org/10.1007/0-387-25228-2_2.

KRISTALY, D., CRACIUN, A. & PELCZ, A. "MVC Architecture in Web Applications Development". [en línea], 2005. [Consulta: 19 junio 2020]. Disponible en: https://www.academia.edu/26399640/MVC_Architecture_in_Web_Applications_Development.

LEFF, A. & RAYFIELD, J.T. "Web-application development using the Model/View/Controller design pattern". *Proceedings Fifth IEEE International Enterprise Distributed Object Computing Conference*. S.l.: s.n. (2001), pp. 118-127. DOI 10.1109/EDOC.2001.950428.

LÓPEZ, P.A. *Seguridad informática*. S.l.: Editex, 2010. ISBN 978-84-9771-761-8.

LUJÁN-MORA, S. *Programación de aplicaciones web: historia, principios básicos y clientes web* [en línea]. S.l.: Editorial Club Universitario, 2002. [Consulta: 25 junio 2020]. ISBN 978-84-8454-206-3. Disponible en: http://rua.ua.es/dspace/handle/10045/16995.

MANUAL DE INSTALACIÓN. 2020.

MANUAL TÉCNICO. 2020.

MEDIA PLANET. "Cybersecurity Fundamentals - Risks, Procedures, & Integration", *Mediaplanet: Future of Business and Tech eGuide* [en línea], 2016. [Consulta: 12 mayo 2020]. Disponible en: https://cyberdefensemagazine.tradepub.com/free-offer/cybersecurity-fundamentals--risks-procedures-and-integration/w_medc02?sr=hicat&_t=hicat:1091.

MENDOZA, M. & BARRIOS, J. "Propuestas metodológicas para el desarrollo de aplicaciones Web: una evaluación según la ingeniería de métodos". *Revista Ciencia e Ingeniería. 25(2)*. [en línea], 2004. [Consulta: 10 julio 2020]. Disponible en: http://ebookcentral.proquest.com/lib/espochsp/detail.action?docID=3207767.

MENTOR. *Normas ISO sobre gestión de seguridad de la información | Seguridad Informática.* [en línea]. 2018. [Consulta: 8 mayo 2020]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestion_de_seguridad_de_la_informacin.html.

MICRO FOCUS. *Architecting a High Availability Solution - Operations Center Server Installation Guide* [en línea]. 2018. [Consulta: 17 julio 2020]. Disponible en: https://www.netiq.com/documentation/operations-center-57/server_installation/data/bmg3ki8.html.

MIERES, J. *Buenas prácticas en seguridad informática | ESET* [en línea]. 2009. S.l.: s.n. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf.

MOLINA RÍOS, J.R., ZEA ORDÓÑEZ, M.P., CONTENTO SEGARRA, M.J. & GARCÍA ZERDA, F.G. "Comparación de Metodologías en Aplicaciones Web". *3C Tecnología_Glosas de*

innovación aplicadas a la pyme, vol. 7, nº 1 (2018), pp. 1-19. ISSN 22544143. DOI 10.17993/3ctecno.2018.v7n1e25.1-19.

MONAR, J.S., PASTOR RAMIREZ, D.M., ARCOS MEDINA, G. de L. & OÑATE ANDINO, M.A.O. "Técnicas de programación segura para mitigar vulnerabilidades en aplicaciones web". *Congreso de Ciencia y Tecnología ESPE* [en línea], 2018, vol. 13, nº 1. [Consulta: 14 abril 2020]. ISSN 1390-4663. DOI 10.24133/cctespe.v13i1.753. Disponible en: https://journal.espe.edu.ec/ojs/index.php/cienciaytecnologia/article/view/753.

MUÑOZ-ESCOÍ, F.D. y DECKER, H. *Database Replication Approaches* [en línea], 2007. [Consulta: 9 julio 2020]. Disponible en: https://www.academia.edu/2253842/Database_Replication_Approaches.

OFFUTT, J. "Quality attributes of Web software applications". *Software IEEE*, 2002, vol. 19, pp. 25-32. DOI 10.1109/52.991329.

OMNISECU.COM. *Types of Network Attacks against Confidentiality, Integrity and Avilability* [en línea]. 2019. [Consulta: 6 julio 2020]. Disponible en: http://www.omnisecu.com/ccna-security/types-of-network-attacks.php.

OPEN DATA SECURITY. *Ataques DDoS: guía detallada sobre protección ante DDoS. ODS | Seguridad Informática* [en línea]. 2019. [Consulta: 15 julio 2020]. Disponible en: https://opendatasecurity.io/es/ataques-ddos-guia-detallada/.

ORDAX CASSÁ, J.M. y OCAÑA DÍAZ-UFANO, P.A. *Programación web en java* [en línea]. Madrid, SPAIN: Ministerio de Educación de España, 2012. [Consulta: 19 junio 2020]. ISBN 978-84-369-5430-2. Disponible en: http://ebookcentral.proquest.com/lib/espochsp/detail.action?docID=3214540.

ORDOÑEZ GRANIZO, Sandra Johanna, & CHIMBO ORTIZ, Kevin David. Buenas prácticas de seguridad en el sistema de estafetas de la Dirección de Desarrollo Académico en la Escuela Superior Politécnica de Chimborazo [en línea] (Trabajo de Titulación). (Ingeniería) Escuela Superior Politécnica de Chimborazo, Facultad Informática y Electrónica, Escuela de Ingeniería en Sistemas. Riobamba, Ecuador. 2019. [Consulta: 14 abril 2020]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/12294.

OWASP. *Medidas de Seguridad* [en línea], 2019. [Consulta: 1 julio 2020]. Disponible en: https://www.owasp.org/index.php/Main_Page.

PAe - MAGERIT v.3. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Criterios de Seguridad, Normalización y Conservación* [en línea], 2012. [Consulta: 1 mayo 2020]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XWyHlnu21PY.

PANDINI, W. *Entiende lo que es alta disponibilidad de firewall UTM y sus posibilidades de aplicación. OSTEC Blog* [blog]. 2017. [Consulta: 17 julio 2020]. Disponible en: https://ostec.blog/es/generico/entiende-alta-disponibilidad-firewall-utm.

PIGOSKI, T. *Software Maintenance* [en línea], 2001. [Consulta: 2 julio 2020]. Disponible en: https://www.academia.edu/6036220/CHAPTER_6_SOFTWARE_MAINTENANCE.

PIQUERAS JOVER, R. "Security attacks against the availability of LTE mobility networks: Overview and research directions". *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*. S.l.: s.n. (2013), pp. 1-9.

PLAN DE PRUEBAS. 2020.

POSEY, B. y BACON, M. "How do buffer overflow attacks work?" *SearchSecurity* [en línea], 2018. [Consulta: 21 julio 2020]. Disponible en: https://searchsecurity.techtarget.com/tip/1048483/Buffer-overflow-attacks-How-do-they-work.

PRESSMAN, R.S. *Software Engineering: A Practitioner's Approach*. Séptima. 2005. S.l.: Palgrave Macmillan. ISBN 978-0-07-301933-8.

RADWARE. *DoS Attack: What is a Denial-of-Service Attack? | DDoSPedia.* [en línea]. 2019a. [Consulta: 6 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/dos-attack/.

RADWARE. *ICMP Flood Attack | Radware Security* [en línea]. 2019b. [Consulta: 15 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/icmp-flood/.

RADWARE. *What Is a Fraggle Attack? | Radware — DDoSPedia* [en línea]. 2019c. [Consulta: 15 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/fraggle-attack/.

RADWARE. *What Is a Syn Flood? | Radware — DDoSPedia* [en línea]. 2019d. [Consulta: 15 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/syn-flood/.

RADWARE. *DDoS Attacks (Distributed Denial-of-Service Attacks) | DDoSPedia* [en línea]. 2019e. [Consulta: 15 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/ddos-attack/.

RADWARE. *What Is the Ping of Death? | Radware — DDoSPedia* [en línea]. 2019f. [Consulta: 15 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/ping-of-death/.

RADWARE. *Buffer Overflow Attacks - Definitions & Consequences* [en línea]. 2019g. [Consulta: 21 julio 2020]. Disponible en: https://security.radware.com/ddos-knowledge-center/ddospedia/buffer-overflow-attack/.

ROA BUENDÍA, J.F. *Seguridad informática* [en línea]. Madrid, SPAIN: McGraw-Hill España, 2013. [Consulta: 25 junio 2020]. ISBN 978-84-481-8569-5. Disponible en: http://ebookcentral.proquest.com/lib/espochsp/detail.action?docID=3211239.

RSNAPSHOT. *Rsnapshot Documentación Oficial. Rsnapshot ORG* [en línea]. 2020. [Consulta: 7 septiembre 2020]. Disponible en: https://rsnapshot.org/.

SAMPATH, S., SPRENKLE, S., GIBSON, E., POLLOCK, L. & SOUTER GREENWALD, A. "Applying Concept Analysis to User-Session-Based Testing of Web Applications". *IEEE Transactions on Software Engineering*, vol. 33, nº 10 (2007), pp. 643-658. ISSN 0098-5589, 1939-3520, 2326-3881. DOI 10.1109/TSE.2007.70723.

SÁNCHEZ, E. & ARAUJO, R. *Psicomentarios - ¿Qué es el sílabo?* [blog]. Universidad del Pacífico, 2019. [Consulta: 2 julio 2020]. Disponible en: http://blogs.up.edu.pe/psicomentarios/que-es-el-silabo/.

SCHWABER, K. SCRUM Development Process. *Business Object Design and Implementation*. London: Springer, 1997, pp. 117-134. ISBN 978-1-4471-0947-1. DOI 10.1007/978-1-4471-0947-1_11.

SEARCH DATA CENTER. *¿Qué es Copia de seguridad o respaldo?* [en línea]. 2018. [Consulta: 21 julio 2020]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Copia-de-seguridad-o-respaldo.

SECRETARÍA TÉCNICA PLANIFICA ECUADOR. *Plan Nacional de Desarrollo 2017 – 2021 Toda una Vida* [en línea], 2017. [Consulta: 1 mayo 2020]. Disponible en: https://www.planificacion.gob.ec/plan-nacional-de-desarrollo-2017-2021-toda-una-vida/.

SEPS. *Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)* [en línea]. 2019. [Consulta: 14 abril 2020]. Disponible en: https://www.seps.gob.ec/interna-npe?775.

SERRANO, J. "ISO 27001 Seguridad de la Información". *Food Defense Soluciones* [en línea], 2015. [Consulta: 1 julio 2020]. Disponible en: https://www.fooddefense-soluciones.com/es/iso-27001-seguridad-de-la-informacion.

SHKLAR, L. & ROSEN, R. *Web Application* [en línea], 2003. [Consulta: 12 junio 2020]. Disponible en: https://www.academia.edu/35670207/Web_Application.

SHRESTHA, S. *DDoS - Distributed Denial of Service* [en línea]. 2017. [Consulta: 15 julio 2020]. Disponible en: https://www.slideshare.net/ErShivaKShrestha/ddos-distributed-denial-of-service.

SOKOL, P., ZUZČÁK, M. & SOCHOR, T. "Definition of Attack in Context of High Level Interaction Honeypots". *Software Engineering in Intelligent Systems*. Cham: Springer International Publishing, pp. 155-164. ISBN 978-3-319-18473-9. DOI 10.1007/978-3-319-18473-9_16.

SWEBOK. *Software Maintenance* [en línea]. 2019. [Consulta: 3 julio 2020]. Disponible en: http://swebokwiki.org/Chapter_5:_Software_Maintenance.

TRAEFIK. *Traefik documentación* [en línea], 2020. [Consulta: 7 septiembre 2020]. Disponible en: https://docs.traefik.io/.

TRYFONAS, T., GRITZALIS, D. y KOKOLAKIS, S. "A Qualitative Approach to Information Availability". *Information Security for Global Information Infrastructures* [en línea]. Boston, MA: Springer US, pp. 37-47. [Consulta: 8 mayo 2020]. ISBN 978-1-4757-5479-7. Disponible en: http://link.springer.com/10.1007/978-0-387-35515-3_5.

UNIVERSIDAD DE LUJÁN. D*isponibilidad | Departamento de Seguridad Informática* [en línea]. 2017. [Consulta: 8 mayo 2020]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/2.

UNIVERSIDAD INTERNACIONAL DE VALENCIA. *Concepto y utilidad de las buenas prácticas en la enseñanza | VIU* [en línea]. 2018. [Consulta: 21 julio 2020]. Disponible en: https://www.universidadviu.com/concepto-y-utilidad-de-las-buenas-practicas-en-la-ensenanza/.

VACCA, J.R. *Practical Internet Security* [en línea]. Boston, MA: Springer US, 2007. [Consulta: 30 junio 2020]. ISBN 978-0-387-40533-9. Disponible en: http://link.springer.com/10.1007/978-0-387-29844-3.

VELOZ, G. & MENÉNDEZ, J. *Diagrama de Despliegue y Componentes*. 2016.

WEIK, M.H. *Computer Science and Communications Dictionary* [en línea]. Boston, MA: Springer US. [Consulta: 1 julio 2020]. ISBN 978-1-4020-0613-5. Disponible en: https://doi.org/10.1007/1-4020-0613-6_19544.

YÁNEZ ROMERO, E.N. G*uía de buenas prácticas de desarrollo de aplicaciones web seguras aplicado al sistema control de nuevos aspirantes Empresa Grupo LAAR.* [en línea], [Consulta: 15 abril 2020]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/3560.

YU, S. *Distributed Denial of Service Attack and Defense* [en línea]. New York: Springer-Verlag. [Consulta: 15 julio 2020]. SpringerBriefs in Computer Science. ISBN 978-1-4614-9490-4. Disponible en: https://www.springer.com/la/book/9781461494904.

ANEXOS

ANEXO A: LISTA DE VERIFICACIÓN DE BUENAS PRÁCTICAS DE DISPONIBILIDAD

N°	Buena Práctica	Descripción	Cumple
1.	Clúster por medio de la utilización de contenedores (Docker Swarm)	La configuración de clúster por medio de Docker Swarm, permite tener alta disponibilidad, ya que si falla un nodo, el clúster administrado por Docker Swarm se encarga de hacer funcionar las aplicaciones de dicho nodo en otro de forma automática, evitando interrupciones en el funcionamiento de las aplicaciones. Esta configuración se muestra en (Manual de Instalación, pp. 18-39)	Sí
2.	Balanceador de Carga (Traefik)	Esta configuración permite que el tráfico web entrante sea distribuido de forma eficiente y sin intervención, esto ofrece la herramienta denominada Traefik, la cual monitorea la cantidad de recursos que utiliza cada aplicación y los dirige al nodo con más recursos que tenga desplegada la aplicación, la configuración se muestra en (Manual de Instalación, pp. 39-46)	Sí
3.	Failover Solutions (Portainer, Visualizer)	Las herramienta Visualizer, permiten el monitoreo del clúster de de forma gráfica y rápida, muestra en que nodo se encuentra desplegado un contenedor Docker, esto permite tomar decisiones cuando ocurra un fallo. Además, Portainer permite aministrar el cluster de forma gráfica, haciendo que encontrar soluciones a fallas en el clúster sea un trabajo sencillo, permitiendo que la conmutación entre nodos master y esclavos sea muy fácil, la configuración se muestra en (Manual de Instalación, pp. 60-64)	Sí
4.	Replicación Base de Datos (Clúster Postgres)	Muy útil para proporcionar disponibilidad ya que permite satisfacer la carga impuesta sobre la base de datos, permitiendo que la aplicación realice peticiones sin interrupción alguna, la configuración se muestra en (Manual de Instalación, pp. 67-76)	Sí
5.	Copias de Seguridad (Rsnapshot)	Tener copias de seguridad es altamente importante al momento de proporcionar disponibilidad, ya que en caso de una falla, se puede restaurar la información evitando pérdidas e interrupciones. Por medio de Rsnapshot se puede configurar copias de seguridad automáticas como se muestra en (Manual de Instalación, pp. 76-85)	Sí
6.	Firewall	Al instalar el sistema operativo (CentOS 7) para el Servidor, se configura el firewall, de tal manera que no permita tráfico no deseado, de esta forma se evita ataques al servidor, como se muestra en (Manual de Instalación, pp. 15-17)	Sí

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 07 / 04 / 2021

INFORMACIÓN DEL AUTOR
Nombres – Apellidos: RODRIGO LENIN RAMOS AVEROS
INFORMACIÓN INSTITUCIONAL
Facultad: INFORMÁTICA Y ELECTRÓNICA
Carrera: INGENIERÍA EN SISTEMAS INFORMÁTICOS
Título a optar: INGENIERO EN SISTEMAS INFORMÁTICOS
f. Analista de Biblioteca responsable: Firmado electrónicamente por: ELIZABETH FERNANDA AREVALO MEDINA