ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD:

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

CIBERSEGURIDAD Y SU APLICACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ

AUTORAS:

NERINA VICTORIA AVELLÁN ZAMBRANO

MARÍA FERNANDA ZAMBRANO BRAVO

TUTORA:

ING. JESSICA MORALES CARRILLO, Mg.

COTUTOR:

ING. BEQUER BRIONES VELIZ, MG.

CALCETA, MAYO 2019

DERECHOS DE AUTORÍA

NERINA VICTORIA AVELLÁN ZAMBRANO y MARÍA FERNANDA ZAMBRANO BRAVO, declaramos bajo juramento que el trabajo aquí escrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

_____ _____

NERINA V. AVELLÁN ZAMBRANO **MARÍA F. ZAMBRANO BRAVO**

CERTIFICACIÓN DE TUTORA

ING. JESSICA MORALES CARRILLO, Mg certifica haber tutelado el trabajo de titulación **CIBERSEGURIDAD Y SU APLICACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ,** que ha sido desarrollada por **NERINA VICTORIA AVELLÁN ZAMBRANO** y **MARÍA FERNANDA ZAMBRANO BRAVO**, previo a la obtención del título de Magister en Tecnología de la Información mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TRABAJO DE TITULACIÓN DE LA UNIDAD DE TITULACIÓN** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____

ING. JESSICA MORALES CARRILLO, MG.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **CIBERSEGURIDAD Y SU APLICACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ**, que ha sido propuesto, desarrollado por **NERINA VICTORIA AVELLÁN ZAMBRANO** y **MARÍA FERNANDA ZAMBRANO BRAVO**, previa la obtención de título de Magister en Tecnología de la Información mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TRABAJO DE TITULACIÓN** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

ING. GUSTAVO MOLINA GARZÓN MG.
MIEMBRO

ING. SERGIO INTRIAGO BRIONES, MG.
MIEMBRO

DR. INF. MARLON NAVIA MENDOZA
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Feliz López, que nos dio la oportunidad de una educación superior de calidad y en la cual hemos forjado conocimientos profesionales día a día;

A los docentes por las enseñanzas compartidas durante estos 5 años, las cuales fueron necesarias para nuestra formación,

A nuestra tutora Ing. Jessica Morales Carrillo, Mg y a nuestro cotutor Ing. Bécquer Briones Véliz, Mg por los conocimientos y guía proporcionada, durante el proceso de ejecución del proyecto de titulación.

A las instituciones de educación superior públicas de Manabí: Universidad Técnica de Manabí (UTM), Universidad Laica Eloy Alfaro (ULEAM), Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM MFL) y Universidad Estatal del Sur de Manabí (UNESUM), por abrirnos las puertas otorgándonos el permiso para el levantamiento de información y de esta manera ejecutar nuestro trabajo de titulación,

LAS AUTORAS

DEDICATORIA

El presente trabajo de titulación significa la culminación de una de las etapas más importantes de nuestras vidas como profesionales, por lo tanto, consideramos importante dedicar este logro:

A Dios, que nos dio fortaleza y sabiduría para cumplir esta meta trazada que fue alcanzada con satisfacción y dedicación.

A nuestros padres que han sido nuestro apoyo incondicional en nuestro proceso de formación contínua,

A nuestros amigos que nos ayudaron y aportaron con un granito de arena para conseguir nuestra meta anhelada.

Dios los bendiga siempre.

LAS AUTORAS

CONTENIDO GENERAL

CONTENIDO DE TABLAS Y GRÁFICOS

RESUMEN

El presente trabajo de titulación denominado Ciberseguridad y su aplicación en las Instituciones de Educación Superior Públicas de Manabí, tuvo el propósito de determinar el nivel de Ciberseguridad utilizando la norma ISO 27032-2012 con el fin de conocer los riesgos, amenazas y vulnerabilidades de los sistemas distribuidos. Mediante la metodología Análisis Modal de Fallos y Efectos (AMFE), se identificó y evaluó el nivel de riesgos en cada dominio de seguridad (Información, Redes, Aplicación), lo que permitió plantear otras medidas o soluciones sugeridas de mejora ya sea a corto o largo plazo en aspectos de integridad, disponibilidad y confiabilidad de la información. Para complementar el objetivo, se aplicaron las herramientas de escaneo de vulnerabilidades Shodan, Nessus y Acunetix en los sistemas distribuidos de las IES Públicas, mostrando como resultado reportes de las diferentes categorías de vulnerabilidades que tenían dichos sistemas, y estos a su vez brindaron recomendaciones para mitigar las inseguridades en el Ciberespacio. Todo esto conlleva a un mejor refuerzo de los niveles de seguridad en los portales, sistemas o servicios web, de los cuales son formas de acceso a la información, y que deben ser monitoreadas o analizadas continuamente para su adecuada protección de los datos. Como medida de solución las autoras desarrollaron un plan de acción que le permitió a cada institución objeto de estudio, tomar acciones para salvaguardar la integridad de su información.

PALABRAS CLAVES

Ciberseguridad, AMFE, seguridad informática, riesgos en ciberespacio.

ABSTRACT

The present investigation, called Cybersecurity and its application in the Institutions of Public Higher Education of Manabí, had the purpose of determining the level of Cybersecurity using the ISO 27032-2012 standard in order to know the risks, threats and vulnerabilities of the systems distributed. Using the Modal Analysis of Faults and Effects (AMFE) methodology, the level of risks in each security domain was identified and evaluated (Information, Networks, Application), which allowed us to propose other measures or suggested solutions for improvement, either short or long term in aspects of integrity, availability and reliability of the information. To complement the objective, the vulnerability scanning tools Shodan, Nessus and Acunetix were applied in the distributed systems of the Public IES, showing as a result reports of the different vulnerability categories that these systems had, and these in turn provided recommendations for mitigate the insecurities in Cyberspace. All this leads to a better reinforcement of the levels of security in the portals, systems or web services, of which are forms of access to information, and which must be continuously monitored or analyzed for adequate protection of the data. As a solution measure, the authors developed an action plan that allowed each institution under study to take actions to safeguard the integrity of its information.

KEYWORDS

Cybersecurity, AMFE, computer security, risks in cyberspace.

CAPÍTULO I. ANTECEDENTES

1.1. DESCRIPCIÓN DEL PROBLEMA

En las últimas décadas, las nuevas tecnologías, los servicios electrónicos y redes de comunicación se han visto cada vez más integradas en el quehacer diario; las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las tecnologías de la información y comunicaciones (TICs) y de la operación de las Infraestructuras Críticas de Información (ICIs); el transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y servicios públicos se sustentan en la disponibilidad, integridad y confidencialidad de la información que fluye a través de estas infraestructuras (Anchundia, 2017).

En el Ecuador no se ha desarrollado aún una estrategia nacional de ciberseguridad, que permita establecer los lineamientos, objetivos y plan de acción para proteger los servicios, la información, las infraestructuras críticas y a los ciudadanos frente a ciber amenazas en el ciberespacio. Sin embargo, diferentes instituciones públicas han realizado actividades de manera independiente y están contribuyendo a mejorar la ciberseguridad a nivel nacional (Gómez, 2017).

Según lo que ha reportado el Consejo Nacional Electoral (CNE) del Ecuador, un caso de Ciberataque fue, la página web del organismo comicial, que recibió ochocientos mil (800.000) intentos no permitidos de instrucción o penetración informática durante los comicios presidenciales (AVN, 2013 citado por Rodríguez y Acacio, 2014) De esta manera se puede expresar que, el ciberespacio está vinculado prácticamente a todos los sectores de la economía donde impregna un sistema, redes, datos, y que, en algunos casos, se sufren ataques solo a través de direcciones IP (Rosenzweig, 2013 citado por Rodríguez y Acacio, 2014).

La Constitución de la República del Ecuador, dentro del título II, capitulo segundo, sección tercera, establece que todas las personas tienen derecho al acceso universal a las tecnologías de información y comunicación. En el título VII, capitulo primero, sección novena, que trata de la gestión de riesgo, el Estado se compromete a proteger a las personas, entidades públicas y entidades privadas frente a amenazas existentes y potenciales, ya sea internas o externas, que afecten al territorio ecuatoriano, fortalecer las capacidades de los ciudadanos y de sus empresas para combatir y prevenir los riesgos, y finalmente coordinar acciones para reducir las vulnerabilidades (CE, 2008).

Por otra parte indica Flores (2017), que en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del año 2017, dentro de los marcos normativos definido por el Ecuador, que incluye normas sobre la Ciberseguridad del país; por ejemplo condena y multa a toda persona que destruya de forma maliciosa documentos, programas, bases de datos o información vital para el estado, o la empresa privada, también a las personas que alteren documentación con el fin de agraviar a una tercera y que viole la privacidad de otro mediante ciberespionaje.

Según Gómez (2017), la norma ISO/IEC 27032:2012 refiere que la "Tecnología de la información, Técnicas de seguridad, Directrices para la Ciberseguridad" (publicada en julio del 2012) proporciona un marco de orientación para mejorar el estado de la Ciberseguridad, usando para ello los aspectos estratégicos y técnicos relevantes para esa actividad, y sus dependencias con otros dominios de seguridad, en particular: Seguridad de la información (considerando que la información es el activo más relevante de cualquier organización).

El conocimiento de Ciberseguridad en las empresas, como lo manifiesta Information Security Breach Survey (2015), todos los usuarios deben conocer los riesgos principales y cómo notificar incidentes, es decir la capacidad de una organización de prevenir un incidente y recuperar la normalidad lo antes posible es esencial después de un evento de seguridad de la información. Dado que la ISO 27032 aporta un marco metodológico y de buenas prácticas en la

implementación de la Ciberseguridad, dentro de controles relacionados al Ciberespacio, que permite enfocarse en la seguridad, adicionando este factor al sistema de Gestión de Seguridad de la Información, que proveen directrices para la ejecución de un marco seguro, confiable, eficaz y eficiente de intercambio de información y respuesta a incidentes cibernéticos (Gómez, 2017).

Todos estos criterios que brindan las buenas prácticas, deben tomarse en cuenta en todos los sectores y sobre todo públicos, ya que existen diversos sitios gubernamentales que son vulnerablemente constantes de amenazas o ataques cibernéticos y por lo tanto estas directrices ayudarán a mejorar a nivel global, la gestión de la seguridad de la información (Borghello y Temperini, 2013).

Como caso de ciberseguridad aplicada a las Instituciones de Educación Superior Públicas, según Medranda (2017), se encuentra la Universidad de las Américas, en donde se estableció un sistema de ciberdefensa adjunto a la infraestructura del DataCenter académico en sus enlaces internos como externos, con el fin de mitigar la mayoría de ataques informáticos que puedan provenir de miembros propios y extraños a la red, para así controlar los aspectos de vulnerabilidad de las redes en sentido de integridad, privacidad, disponibilidad y legalidad; y evitar los ataques informáticos del ciberespacio, puesto que el contar con una solución multiplataforma evita en un caso hipotético tener un acceso no autorizado al *Core* del negocio y por ende a información flexible que en las manos incorrectas podría afectar los planes de la empresa a largo plazo.

1.2. JUSTIFICACIÓN

Con respecto a las universidades públicas de Manabí, no se han realizado estudios de ciberseguridad como tal, pero si se han aplicado otros tipos de seguridades en la información, seguridad de redes y en sistemas de aplicaciones basados en la Norma de Contraloría General del Estado Ecuatoriano y otros estándares de buenas prácticas para el análisis de las vulnerabilidades y amenazas de los sistemas de información con el fin de disminuir los riesgos mediante políticas de seguridad y planes de contingencia.

Por este motivo las autoras determinan que, la presente investigación permitió la vinculación de las entidades públicas y privadas en la concienciación de la ciberseguridad, favoreciendo económicamente y socialmente a las organizaciones que manejan TI mediante la mitigación de riesgos.

Además como es de conocimiento, la tecnología no es la solución para todos los riesgos, pero es imprescindible prevenirlos mediante el apoyo de la alta gerencia; un marco referencial para la implementación de la ciberseguridad; la evaluación y mitigación de riesgos; las medidas de protección; capacitación y concienciación, que coadyuven a salvaguardar la integridad de los datos de los usuarios que usan TI, por tal razón este trabajo aporta con un plan de mejora en ciberseguridad para las instituciones de educación superior públicas, con el fin de determinar los riesgos, amenazas y vulnerabilidades en los sistemas distribuidos.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Determinar el nivel de la Ciberseguridad mediante la aplicación de la norma ISO 27032-2012 con el fin de conocer los riesgos, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones de Educación Superior Públicas de Manabí.

1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.
- Identificar los riesgos de ciberseguridad mediante la metodología AMFE (Análisis Modal de Fallos y Efectos).
- Elaborar un plan de mejora para mitigar los riesgos a la ciberseguridad en las instituciones de educación superior públicas.

1.4. IDEA A DEFENDER

La propuesta de un plan de mejora de Ciberseguridad aplicando la norma ISO 27032-2012 permitirá disminuir los riesgos, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones de educación superior públicas en Manabí.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1. CIBERSEGURIDAD EN ÁMBITOS GENERALES

Los sistemas de información, como lo menciona Mayol (2018), son todo aquello que integran personas, procesos, datos y tecnología, y van más allá de los umbrales de la organización, para colaborar de formas más eficientes con proveedores, distribuidores y clientes, para una adecuada gestión y la toma de decisiones. Para Torres (2015), dicha estructura tiene la finalidad de administrar los procesos operativos y disponibles permanentemente en la red para los usuarios, por medio de planeación, análisis de eventos en la red y la aplicación de controles de seguridad.

Los riesgos que tienen estos sistemas de información, no sólo son un gran problema, puesto que hoy en día, conforman un tema prioritario, debido a que los sistemas informáticos están dispersos e interconectados en toda la Organización (Ardita, 2018); que no sólo trata dentro de la información, sino a grandes volúmenes de datos, que tienen a ser más receptivos y tratar de evitar posibles riesgos de IT (Lloyd's, 2018). Toda vez que un Sistema de Gestión, mantenga la finalidad de poder optimizar la inversión en seguridad y priorizar la implementación de controles o salvaguardar la información ante algún inconveniente (Gómez, 2017).

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones (Diaz, 2013). Debido a que las vulnerabilidades son una puerta abierta para los atacantes, es tan importante tenerlas en cuenta, ya que estas en cualquier momento pueden ser aprovechadas para posibles ataques que se dan en los sistemas de información. Entre las diferentes categorías de vulnerabilidades está: en caso crítico, el propagar un gusano de Internet sin la acción del usuario; en caso importante, pone en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o

disponibilidad de los recursos de procesamiento; en caso moderada, el impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad; y en caso baja, muy difícil de aprovechar o cuyo impacto es mínimo (Permalink, 2013).

Por otro lado, dentro del entorno de un sistema de información, también existe la oportunidad de una amenaza que puede dar lugar a una violación de la seguridad en confidencialidad, integridad, disponibilidad o uso legítimo de los datos (Diaz, 2013). Un gran número de amenazas son los atacantes en el ciberespacio conocidos como: Hackers, Crackers, Phreakers, Sniffers, Lammers, Newbie, Ciberterrorista, Programadores de virus, Carders (Permalink, 2013).

Tabla 2. 1 Tipos de atacantes de Sistemas de Información

Nombre de los atacantes	Definición
Hackers	Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas pero sin motivación económica o dañina.
Crackers	Un hacker que, cuando rompe la seguridad de un sistema, lo hace con intención maliciosa, bien para dañarlo o para obtener un beneficio económico.
Phreakers	Crackers telefónicos, que sabotean las redes de telefonía para conseguir llamadas gratuitas.
Sniffers	Expertos en redes que analizan el tráfico para obtener información extrayéndola de los paquetes que se transmiten por la red.
Lammers	Chicos jóvenes sin grandes conocimientos de informática pero que se consideran a sí mismos hackers y se vanaglorian de ello.
Newbie	Hacker novato.
Ciberterrorista	Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y saboteadores informáticos.
Programadores de virus	Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.
Carders	Personas que se dedican al ataque de los sistemas de tarjetas, como los cajeros automáticos.

Elaboración: Propia

Cabe mencionar que frente a las vulnerabilidades y amenazas que se presentan en el ciberespacio, la ciberseguridad brinda directrices de seguridad para la

protección de la información tanto a las organizaciones públicas como a las privadas, en donde se analiza, administra y se hacen los seguimientos de eventos e información a todos los niveles de cualquier fuente digital disponible para responder rápidamente y prevenir posibles ataques (Lloyd's, 2018). En América Latina y del resto del mundo, para solventar esta adversidad es necesario la implementación de políticas de ciberseguridad en los puntos informáticos vitales, donde se realiza el procesamiento, almacenamiento, envío y recepción de los datos de las instituciones que lo requieran, para así salvaguardar la integridad y confidencialidad de la información (Philco, 2017).

Según Burgos (2012) y Gómez (2017) manifiestan que la Ciberseguridad cubre otros ámbitos de seguridad, como redes, internet, información y aplicación. Esta investigación se enfocará en la seguridad de la Información y la seguridad de las aplicaciones que maneja el departamento tecnológico con respecto a los sistemas distribuidos que tienen las instituciones de Educación Superior públicas de Manabí, mediante la aplicación de la Norma ISO/IEC 27032:2012 con el objetivo de garantizar la seguridad en los intercambios de información en la red mediante directrices de seguridad que permita a los interesados minimizar los riesgos online (ISO, 2017). Además, facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo, de esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques (García, 2012).

Con relación al ciberespacio se puede definir como el lugar donde se puede encontrar componentes diversos como los geográficos, las redes físicas, las redes o conexiones lógicas junto a los dispositivos conectados, las personas o individuos que interactúan con el ciberespacio y la identidad digital (Bankinter, 2012). Conocido como un ambiente complejo resultado de la interacción entre personas, software y servicios en internet, soportado por dispositivos físicos de tecnologías de la información y comunicaciones (TIC) y conectados por redes, distribuidos mundialmente (GTDI, 2018). En donde los medios disponibles son los resultados alcanzados por los responsables de investigar y prevenir ataques en el ciberespacio (García, 2017).

Los ciberataques son las armas más destructivas que existen actualmente, afectando por igual a individuos particulares, empresas e incluso estados y sociedades, ya sean a sus fines ideológicos o de carácter lucrativo, los ciberataques son numerosos, y cada día más sofisticados, en vulnerabilidades de los equipos y redes, y la posibilidad del anonimato del atacante lo convierten en una práctica en aumento (Ruben, 2018) (Freire, 2017). Tomando en cuenta que es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, que usa y maneja información valiosa en su computadora desconoce que debe de tener ciertas herramientas para evitar ser víctimas de los ciberataques (Maldonado, 2017). En lo que va del año 2018, se han detectado más de 8,000 vulnerabilidades en los sistemas informáticos que usan las entidades financieras, gobiernos y empresas de todo el mundo, lo cual representa casi la mitad de lo reportado en todo el 2017, informó la security research de ESET Latinoamérica (Pastorino, 2018).

2.2. CIBERSEGURIDAD EN EL ECUADOR

La Armada del Ecuador actualmente posee un Sistema de Gestión de Seguridad de la Información, el cual está encargado de precautelar y velar por la seguridad de los datos, descubrir la penetración de ataques informáticos; así como también ejecutar mecanismos de recuperación en caso de producirse este tipo de eventualidad. Se desarrolló un estudio que se centró en la ciberseguridad y su influencia en las políticas de seguridad de la información de la Armada del Ecuador, CSRIT (Equipo de Respuesta ante Incidentes de Seguridad Informática), ECUCERT (Centro de respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador), entre otras entidades dedicadas a este Ciberseguridad (Almeida, 2017).

Según los expertos, 2017 fue el año de los ciberataques en las instituciones de Educación Superior en el Ecuador, y es que la gran cantidad de brechas a la seguridad informática fueron el tormento de las organizaciones, la digitalización de los procesos de negocio y el uso de las nuevas herramientas tecnológicas para que las organizaciones sean más competitivas implica riesgos que afectan

directamente a los datos críticos y sensibles, lamentablemente la pesadilla no parece terminar ya que se espera que para para este año los ciberataques continúen en crecimiento, Cisco ha publicado su Reporte Anual de Ciberseguridad de 2018, en donde se muestran estadísticas de seguridad, hallazgos claves, información acerca de la evolución del malware, el tráfico cifrado malicioso y el aumento del uso de la inteligencia con el objetivo de reducir el tiempo de los atacantes (Fallas, 2018).

El uso de la tecnología en los campus universitarios aumenta a medida que los estudiantes dependen cada vez más de dispositivos y aplicaciones conectados para su vida académica y personal. Al mismo tiempo, las universidades enfrentan ciberataques más frecuentes y sofisticados de delincuentes que buscan datos personales valiosos. Las universidades deben integrar su acceso a la red con un protocolo de Ciberseguridad para proporcionar escalabilidad y visibilidad, y así mantenerse al día con las necesidades de los estudiantes mientras están preparados para hacer frente a las ciberamenazas actuales y futuras (Biddle, 2017).

En la actualidad existen normas enfocadas o direccionadas a Ciberseguridad, que, definidas en el mundo laboral y académico, para ayudar a entender la importancia de la Seguridad y el debido resguardo de la información e infraestructuras en el ciberespacio dentro de la Seguridad de la Información, entre estas Normas tenemos: ISO/IEC 27032 (Ciberseguridad); ISO/IEC 27000 (Seguridad de la Información); UIT-T X.1205 (Ciberseguridad); NIST SP 800-39 (Ciberseguridad) e ISACA Cybersecurity fundamentals (Ciberseguridad) (Gómez, 2017).

Por otra parte, las autoras resaltan que la norma ISO 27032:2012, permite preparar de manera correctiva y preventiva la lucha contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado; además aborda los riesgos no cubiertos por la internet actual, las redes y la seguridad de las tecnologías de la información y de la comunicación.

Para complementar a la Norma ISO/IEC 27032:2012 en la mitigación de riesgos también se toma en consideración la metodología Análisis Modal de Fallos y Efectos (AMFE) que se aplica a la hora de diseñar nuevos productos, servicios o procesos. Su finalidad es estudiar los posibles fallos futuros (“modos de fallo”) del producto para posteriormente clasificarlos según su importancia (Jimeno, 2013). En la que se puede determinar cómo beneficios de la Metodología AMFE en un SGRC los siguientes aspectos: 1) Permite reducir los tiempos de planificación de un plan de contingencia ante un hallazgo, 2) Promueve el trabajo en equipo y a un liderazgo con sentido organizacional, 3) Mecanismo para la conceptualización de lecciones aprendidas, 4) Conduce a identificar las acciones que pueden eliminar o reducir la oportunidad de que ocurra una falla potencial, 5) Fortalecer las practicas Institucionales hacia la calidad permitiendo satisfacer de manera más integral las necesidades y expectativas de los usuarios (Consuegra, 2015).

Esta metodología permite analizar los riesgos que se cubren en las siguientes fases: Identificación, Análisis del impacto y de la probabilidad de ocurrir, plan de contingencia o acciones correctivas y Monitorización. De las cuales se identifica, evalúa y monitoriza o hace seguimiento para llevar a cabo la utilización de una plantilla de análisis de riesgos, de la cual se generan un numero de prioridad del riego (NPR), teniendo en cuantos parámetros como gravedad/seguridad; importantica, probabilidad e impacto, por motivo que las herramientas en formato Excel saca mejor provecho de la información y permite filtrar los riesgos por orden de importancia y de prioridad en todo momento (García, 2018).

CAPÍTULO III. DESARROLLO METODOLÓGICO

Este trabajo se desarrolló en las Instituciones de Educación Superior (IES) públicas de Manabí, con la finalidad de determinar la Ciberseguridad mediante la aplicación de la norma ISO 27032-2012 en los sistemas distribuidos que manejan estas entidades. La metodología que se utilizó para el desarrollo de la investigación fue mediante la consecución de objetivos específicos, donde el primer objetivo se desarrolló con instrumentos como *Checklists* para verificar el cumplimiento de la norma antes mencionada, y de esta manera determinar vulnerabilidades referentes a la documentación. Para la detección de vulnerabilidades de los sistemas distribuidos académicos, se aplicaron herramientas tecnológicas (Shodan, Nessus y Acunetix), mismas que fueron elegidas de acuerdo con el campo de estudio (redes, datos y aplicación). Cabe mencionar que cada herramienta tiene características diferentes y se ajustan a los requerimientos de la investigación.

Para el desarrollo del segundo objetivo, se utilizó la metodología AMFE (Análisis Modal Fallos y Efectos) para la identificación, evaluación y análisis de los riesgos hallados en el objetivo uno, y de esta manera sugerir acciones de mitigación según el nivel del riesgo identificado.

El tercer objetivo se determinó de acuerdo con los resultados obtenidos, permitiendo plantear un plan de acción para mitigar los riesgos encontrados, con medidas a implementar a corto y mediano plazo según la exigencia que amerite el caso. Esta metodología de investigación se utilizó con el fin de detallar paso a paso el desempeño de cada objetivo planteado y tener una mejor comprensión de este apartado.

3.1. OBJETIVO 1: DETERMINACIÓN DEL CONTROL, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DISTRIBUIDOS EN LAS INSTITUCIONES PÚBLICAS DE NIVEL SUPERIOR DE ACUERDO CON LA NORMA ISO 27032.

Para el desarrollo de este objetivo, se inició con la solicitud respectiva para el levantamiento de información (Anexo 1), a cada una de las IES Públicas de Manabí.

Posterior a la autorización del levantamiento de información, se procedió con la entrevista (Anexo 2) al coordinador de TI de cada una de las Instituciones de Educación Superior (IES) públicas que fueron objeto de estudio, tales como ESPAM MFL, UTM, ULEAM, UNESUM, con la finalidad de recoger la mayor información posible, con preguntas estructuradas y de esta manera conocer la situación actual del departamento en cuestión de documentación en la seguridad de la información, redes y aplicaciones.

Una vez aplicada la entrevista se continuó con la elaboración de las preguntas para la herramienta *Checklist* (Anexo 3) a los departamentos tecnológicos de estas instituciones. La estructura de las preguntas fue basada al estándar ISO/IEC 27032 de directrices de Ciberseguridad, el mismo que permitió evaluar el cumplimiento en la documentación de los sistemas académicos de acuerdo a los dominios de seguridad (redes, datos y aplicación) que maneja la norma. De acuerdo a cada uno de ellos, se elaboró un *checklist*, especificando las secciones que tiene cada dominio y a su vez efectuando preguntas relacionadas a esta sección. A su vez con este estándar aplicado, los coordinadores y directores de TI pudieron notar lo importante que es llevar buenas prácticas en seguridad de la información de los sistemas en el ciberespacio.

Posterior a esto, se verificó las vulnerabilidades encontradas en el *checklist* mediante pruebas de escaneo con herramientas tecnológicas como Shadon, Nessus y Acunetix a los sistemas distribuidos que manejan académicamente, para esto se solicitó oficialmente a las IES Públicas de Manabí la lista con el

nombre y enlaces (dominios y subdominios) de los sistemas académicos con acceso a la Web implementados en las instituciones (Anexo 4).

Cabe mencionar, que esta solicitud fue realizada para determinar el número de sistemas académicos que maneja cada institución, y así efectuar el escaneo de vulnerabilidades formalmente, además, en la página principal no están todos los enlaces de estos sistemas, por lo que se requiere de fuente oficial su dirección y de esta manera ejecutar las pruebas sin problemas de autorización.

Los requerimientos para efectuar las pruebas de vulnerabilidad en los sistemas académicos fueron:

IES PÚBLICAS DE MANABÍ

- ESPAM MFL
- ULEAM
- UTM
- UNESUM

HERRAMIENTAS

- Shodan
- Nessus
- Acunetix

TIPO DE VULNERABILIDAD

- Errores en la gestión de recursos de la información
- Errores en configuraciones
- Errores humanos
- Validaciones de entrada
- Errores en directorios
- Errores en los permisos, privilegios y /o control de accesos.

NIVEL DE VULNERABILIDAD

- Critico
- Alto
- Mediano
- Bajo
- Informativo

CONSIDERACIONES DEL ANÁLISIS

- Detección de las vulnerabilidades a través del uso las herramientas.
- Análisis del muestreo
- Reporte cuantitativo y cualitativo de los datos obtenidos.
- Sugerencias.
- Estrategia de Ciberseguridad.

Estas herramientas permitieron escanear cada enlace e identificar y clasificar el tipo de vulnerabilidad que tenían los sistemas web. Este proceso se llevó a cabo colocando la dirección IP o el enlace de los sistemas web implementados en las universidades; posteriormente se procedió a escanear cada una, obteniendo como resultado las vulnerabilidades en los mismos.

Es bueno recalcar que no se está efectuando un ataque, y accediendo a la información, simplemente se está verificando el tipo de vulnerabilidad con respecto al cumplimiento de la documentación con la norma ISO a los enlaces de dichos sistemas. Sería diferente si fuese un ataque, ya que no se necesitaría permisión para conseguir los enlaces sino acceder directamente a la información, violando la seguridad que tienen los mismos.

Estas tres herramientas son de fácil instalación, y se puede realizar en sistemas operativos Windows como en Linux, ya que mantienen aspectos similares en momento de proporcionar reportes de vulnerabilidades diferentes.

En el caso de la herramienta SHODAN, los resultados son más orientados a dirección IP, puesto que es un motor de búsqueda de dispositivos conectados al Ciberespacio (tecnologías, puertos, servicios, entre otros aspectos), en donde se puede ven las vulnerabilidades obtenidas luego del escaneo y los reportes generados de manera individual, como se pudieron observar en el Anexo 5A respectivamente.

Luego de estos análisis se pudo apreciar que se mostró información de los aspectos de red en cuestión descriptiva pero solo detallaba las vulnerabilidades, pero no especificaba el nivel como tal. La siguiente herramienta aplicada fue NESSUS, de la que se podría decir que no se especializa tanto en la parte web, sino más bien en el escaneo de pruebas las efectúa en redes o dispositivos de redes o host de redes, debido a que es poco más tedioso realizar el escaneo haciéndolos por dominios o subdominios, pero si bien es más factible es efectuarlos por dirección IP, en la cual la mayor parte de las vulnerabilidades que arrojaba eran de niveles bajo y unas cuantas en mediana eventuales, en ese caso no es que determinó una información de tan altos niveles, pero a diferencia de la herramienta anterior si permitió lleva a cabo análisis generales y luego específicos por cada sistema, después de aquello permitió generar reportes de cada uno de los sistemas analizados, en los cuales mostros los contenidos niveles y el conteo de vulnerabilidades consecutivamente, como podemos apreciar en el Anexo 5B

Por último se aplicó la herramienta Acunetix, que si bien a nivel de servicios o página web la herramienta esta brinda información mucho más completa o especializada en ese tema es petríficamente, porque cuando uno quiere personalizar o escanear un sitio, una IP o servicio mediante un escaneo, tiene muchas opciones, no solo las típicas configuraciones, sino que análisis más profundos que engloba gestores de contenidos, directorios, versiones anteriores de los sistemas, entre otros descuidos que están instinticos en el desarrollo del servicio o aplicación, como se aprecia en el Anexo 5C.

3.2. OBJETIVO 2: IDENTIFICACIÓN LOS RIESGOS DE CIBERSEGURIDAD MEDIANTE LA METODOLOGÍA AMFE (ANÁLISIS MODAL DE FALLOS Y EFECTOS).

En este objetivo se identificó los riesgos que pueden tener cada una de las vulnerabilidades halladas mediante los datos del *Checklist* y las pruebas de vulnerabilidad de las cuales se identificaron y se puedo clasificar por dominio, además se pondero por Probabilidad, Impacto y Nivel, para brindar acciones de mitigación y criterios de aceptación respectivamente para las IES de manera independiente.

3.3. OBJETIVO 3: ELABORAR UN PLAN DE MEJORA PARA MITIGAR LOS RIESGOS A LA CIBERSEGURIDAD EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS.

Para efectuar este último objetivo, se tomó en cuenta los resultados del objeto 1 y 2, con los cuales se elaboró el Plan de acción, y se dividió para cada universidad, de manera que se tomó en consideración que la información proporcionada de manera individual a las IES públicas de Manabí, deben promover la ética y la moral en la información compensada, una vez efectuado este proceso, se dio paso a la entrega del Plan y una copia de la Norma ISO 27032 a cada una de las instituciones objeto de estudio de manera formal para su respectiva aplicación y mejoras en los procesos de los sistemas distribuidos y como mitigar algún tipo de riesgo.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

En este capítulo se mostrarán los resultados de acuerdo con el desarrollo de la metodología por fase de objetivos específicos que se ampliaron en el capítulo anterior.

4.1.1. OBJETIVO 1: DETERMINACIÓN DEL CONTROL, AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS DISTRIBUIDOS EN LAS INSTITUCIONES PÚBLICAS DE NIVEL SUPERIOR DE ACUERDO CON LA NORMA ISO 27032

Se realizó el análisis de la entrevista aplicada a las IES Públicas de Manabí, que permitió determinar el control y las amenazas relacionadas a la documentación de procesos, reglamentos, normativas, estándares en la seguridad de los sistemas distribuidos.

Luego de ello se aplicó un *Checklist* a cada una de las IES Públicas de Manabí, en donde se puedo constatar el cumplimiento de los parámetros de Ciberseguridad por Dominios (Seguridad de Información, Seguridad de Aplicación y Seguridad de Red), según la Norma ISO 27032 (Anexo 6). Cabe destacar que las preguntas que se trabajaron en los diferentes cuestionarios estuvieron estructuradas de la siguiente forma: poseen una ponderación de 4 ítems de acuerdo con la escala de Likert, donde 4 es un proceso **no vulnerable**, 3 poco **vulnerable** y 2 vulnerable y 1 **muy vulnerable**. Con base a las respuestas y evidencias obtenidas por parte de cada uno de los entrevistados del Departamento Tecnológico, se hizo la clasificación de las vulnerabilidades mediante una matriz elaborada en Excel.

En la tabla 4.1, se puede determinar las vulnerabilidades del Dominio de seguridad de información en donde se puede apreciar que la UTM obtuvo 11 vulnerabilidades muy altas a comparación de las demás instituciones. Es decir,

muy vulnerable en la UTM en comparación con las demás Instituciones, por otra parte, podemos observar que el estado vulnerable radicó más en la ESPAM MFL y poco vulnerable en la ULEAM y la UNESUM respectivamente.

Tabla 4. 1. Clasificación de Vulnerabilidades del Dominio seguridad de Información.

SEGURIDAD DE LA INFORMACIÓN			
IES PÚBLICAS DE MANABÍ	**VULNERABILIDADES**		
	MUY VULNERABLE	**VULNERABLE**	**POCO VULNERABLE**
UTM	11	2	0
ULEAM	1	1	2
UNESUM	4	3	2
ESPAM MFL	6	5	0

Elaboración: Las autoras.

Por lo consiguiente, tenemos las vulnerabilidades de Seguridad de las Aplicaciones, en las cuales se puede observar que, en la tabla 4.2, la UNESUM obtuvo resultados muy vulnerables en comparación a las demás universidades, por otra parte, podemos observar que el estado vulnerable radicó en la ESPAM MFL y poco vulnerable en la ULEAM.

Tabla 4. 2. Clasificación de Vulnerabilidades del Dominio seguridad de Aplicaciones.

SEGURIDAD DE APLICACIONES			
IES PÚBLICAS DE MANABÍ	**MUY VULNERABLE**	**VULNERABLE**	**POCO VULNERABLE**
UTM	1	7	3
ULEAM	0	3	8
UNESUM	5	9	2
ESPAM MFL	1	11	2

Elaboración: Las autoras.

Finalmente están las vulnerabilidades de Seguridad de las Redes, en las cuales se puede observar en la tabla 4.3, de la cual la ESPAM MFL obtuvo resultados muy vulnerables en comparación a las demás Instituciones, por otra parte, podemos observar que el estado vulnerable radicó así mismo en la UNESUM y poco vulnerable en la ULEAM.

Tabla 4. 3. Clasificación de Vulnerabilidades del Dominio seguridad de Aplicaciones.

SEGURIDAD DE REDES			
IES PÚBLICAS DE MANABÍ	**MUY VULNERABLE**	**VULNERABLE**	**POCO VULNERABLE**
UTM	1	5	1
ULEAM	0	0	3
UNESUM	3	6	0
ESPAM MFL	2	6	0

Elaboración: Las autoras.

En la tabla 4.4, se muestra el total de vulnerabilidades que se obtuvieron al aplicar el Checklist basado en los dominios de la norma ISO/IEC 27032, el mismo que reflejó los siguientes datos:

Tabla 4. 4. Total de vulnerabilidades encontradas en los dominios de la norma ISO/IEC 27032

VULNERABILIDADES EN DOCUMENTACIÓN				
IES PÚBLICAS DE MANABÍ	**DOMINIOS ISO/IEC 27032**			**TOTAL DE VULNERABILIDADES**
	INFORMACIÓN	**REDES**	**APLICACIONES**	
UTM	13	7	11	**31**
ULEAM	4	3	11	**18**
ESPAM MFL	11	8	14	**33**
UNESUM	9	9	16	**34**
TOTAL	**37**	**27**	**52**	**116**

Elaboración: Las autoras.

Se puede observar en la tabla 4.5, que el porcentaje de vulnerabilidades que obtuvo cada IES en los sistemas académicos por cada dominio de seguridad fueron los siguientes: En el de Información, la UTM tuvo el 35% seguida de la ESPAM MFL con el 30%, siendo el de mayor porcentaje en comparación con las demás instituciones; así mismo, en el de Aplicaciones, la UNESUM con el 31% y la ESPAM MFL con el 27% y en Redes, la UNESUM con el 33% y 30% la ESPAM MFL, siendo las entidades con mayor número de vulnerabilidades y por ende tienden a ser propensas a sufrir riesgos en la ciberseguridad.

Tabla 4. 5. Total de vulnerabilidades por dominio en resumen de todas las IES de Manabí.

DOMINIOS	PORCENTAJE DE VULNERABILIDADES ENCONTRADAS EN LOS SISTEMAS ACDÉMICOS BASADAS EN LA ISO/IEC 27032 DE CIBERSEGURIDAD			
	UTM	ULEAM	ESPAM MFL	UNESUM
Seguridad de la Información	35%	11%	30%	24%
Seguridad de las Aplicaciones	21%	21%	27%	31%
Seguridad de las Redes	26%	11%	30%	33%

Elaboración: Las autoras.

A partir de ello, se realizaron las pruebas de verificación en los sistemas distribuidos de las IES para constatar la efectividad de la información recaudada, en el cual se tomaron en cuenta 3 herramientas de escaneo de vulnerabilidad, las mismas que fueron aplicadas para determinar la seguridad por dominios, como se puede considerar a continuación en la tabla 4.6:

Tabla 4. 6. Total de vulnerabilidades por dominio en resumen de todas las IES de Manabí.

HERRAMIENTA	DOMINIO			TOTAL	OBSERVACIÓN
	RED	DATOS	APLICACIÓN	VULNERABILIDADES	
SHODAN	0	0	0	0	La herramienta de SHODAN no muestra ningún dato porque sus vulnerabilidades son de tipo informativa.
NESSUS	162	86	123	371	
ACUNETIX	1109	691	1045	2845	
TOTAL				**3216**	

Elaboración: Las autoras.

En el gráfico 4.1, se detalla la cantidad de vulnerabilidades por dominio, evidenciando que las vulnerabilidades más altas del total de sistemas analizados son de aplicación, seguido de red y datos. Además, en la tabla 4.4, se muestra que la herramienta SHODAN no muestra ningún dato, debido a que esta herramienta clasifica las vulnerabilidades de tipo informativa; también se observa que la herramienta ACUNETIX una vez obtenidos los reportes correspondientes al análisis ejecutado en los sistemas de la IES de Manabí, arrojo más vulnerabilidades que la herramienta NESSUS.

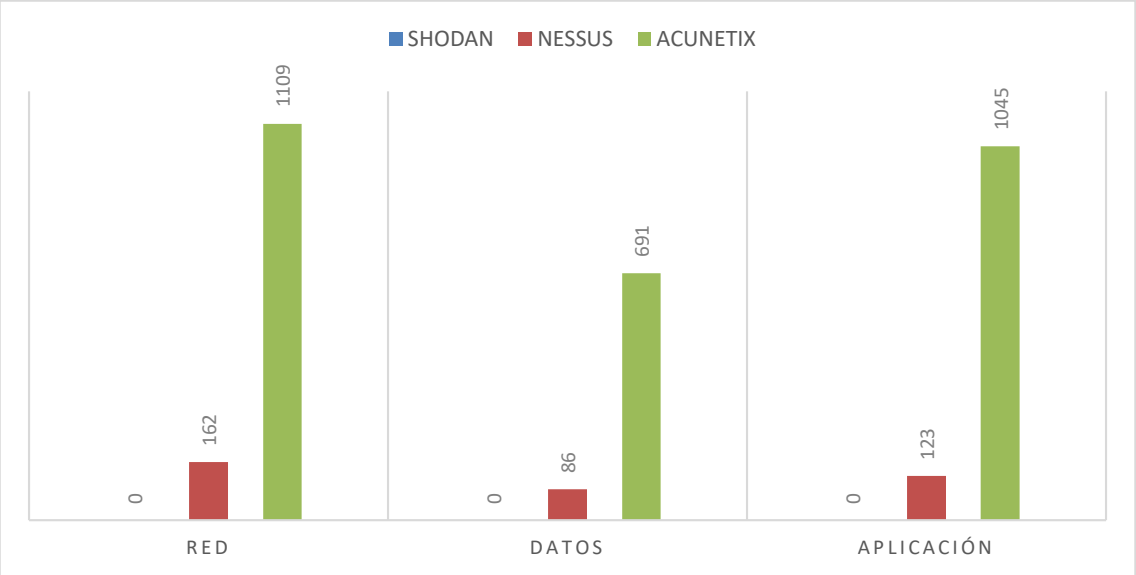


Gráfico 4. 1. Total de vulnerabilidades por dominio.
Elaboración: Las autoras.

El total de vulnerabilidades obtenidas de los sistemas distribuidos analizados de la ESPAM MFL, ULEAM, UNESUM y UTM, se puede apreciar en la tabla 4.7.

Tabla 4. 7. Total de vulnerabilidades por IES

INSTITUCIÓN	SHODAN	NESSUS	ACUNETIX
ESPAM MFL	273	543	683
ULEAM	39	642	890
UTM	351	1092	1329
UNESUM	237	461	466
TOTAL	**900**	**2738**	**3368**

Elaboración: Las autoras.

Los datos fueron extraídos de un total de 61 sistemas; 19 ESPAM MFL, 15 ULEAM, 10 UNESUM Y 17 UTM; y criterios presentes en los reportes generados por las herramientas empleadas.

Los datos obtenidos por cada una de las herramientas de análisis de vulnerabilidades se clasificaron de acuerdo a los niveles establecidos por las herramientas (alto, medio, bajo, informativo y crítico) y que fueron extraídos previo a los reportes generados por cada sistema informático examinado de cada

una de las instituciones, y que a continuación podemos observar su detalle en la

HERRAMIENTAS	NIVEL	ESPAM MFL	ULEAM	UNESUM	UTM	OBSERVACIONES
SHODAN	Crítico	0	0	0	0	En este caso la herramienta de SHODAN arrojó más vulnerabilidades de carácter informativo al realizar el escaneo de vulnerabilidades en los sistemas distribuidos de la ESPAM MFL MF.
	Alto	0	0	0	0	
	Medio	0	0	0	0	
	Bajo	0	0	0	0	
	Informativo	273	39	237	351	
NESSUS	Crítico	14	1	0	2	En el análisis de NESSUS, se observó todos los criterios o niveles de vulnerabilidad con cifras y en tiempos diferentes.
	Alto	22	3	8	5	
	Medio	38	43	49	102	
	Bajo	14	19	9	42	
	Informativo	455	576	395	941	
ACUNETIX	Crítico	0	0	0	0	En el análisis de vulnerabilidades con la herramienta ACUNETIX, se determinó que no hubo nivel Crítico en su categoría, pero si en los demás niveles, de los cuales se efectuó un escaneo más profundo que en comparación a las demás herramientas, esta proporciona mayor información en cuanto a vulnerabilidades.
	Alto	42	41	17	356	
	Medio	503	539	289	312	
	Bajo	86	108	122	430	
	Informativo	52	202	38	231	

tabla 4.8:

Tabla 4. 8 Total de vulnerabilidades por criterio.

Elaboración: Las autoras.

De las cuales se pueden apreciar según el gráfico 4.2, el resultado de vulnerabilidades por herramientas, y de las cuales la herramienta ACUNETIX arrojo más cantidad de estas. Es decir, se observa la cantidad de vulnerabilidades por cada herramienta y universidad, para la herramienta ACUNETIX se puede evidenciar que tiene el mayor número de vulnerabilidades a diferencia de SHODAN.

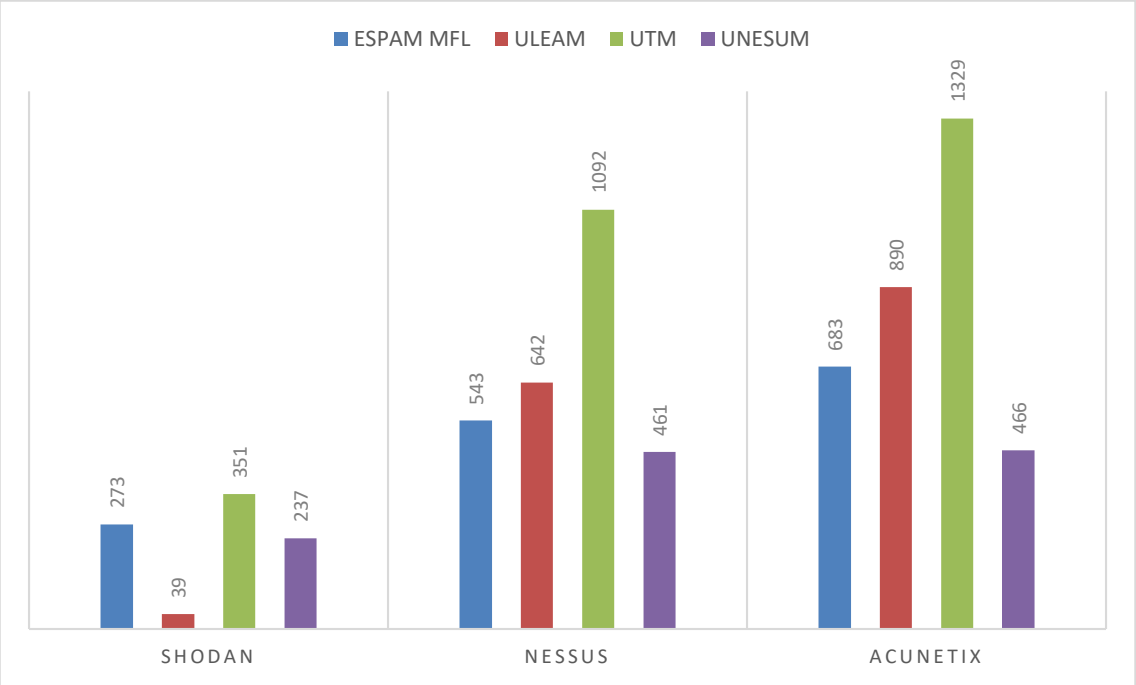


Gráfico 4. 2. Total de vulnerabilidades por herramienta.
Elaboración: Las autoras.

En el gráfico 4.3. Se muestra las vulnerabilidades para la herramienta SHODAN, se puede observar que esta herramienta clasifica las vulnerabilidades de forma informativa como único criterio.

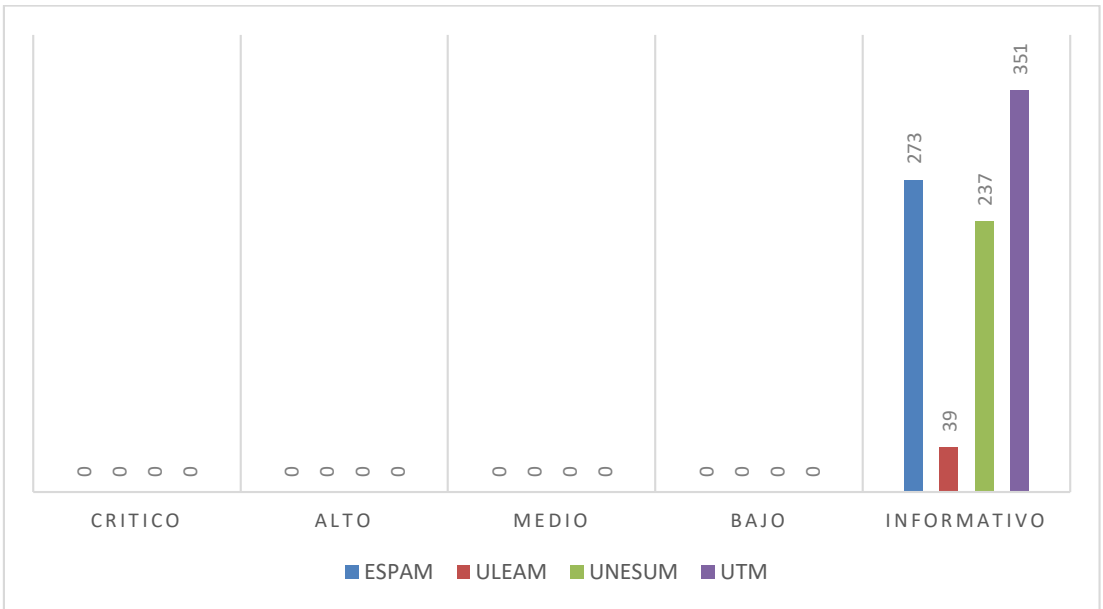


Gráfico 4. 3 Total de vulnerabilidades SHODAN.
Elaboración: Las autoras.

En el gráfico 4.4. Se evidencia que la herramienta NESSUS obtuvo el mayor número de vulnerabilidades en el criterio de informativo y el menor se encuentra el crítico.

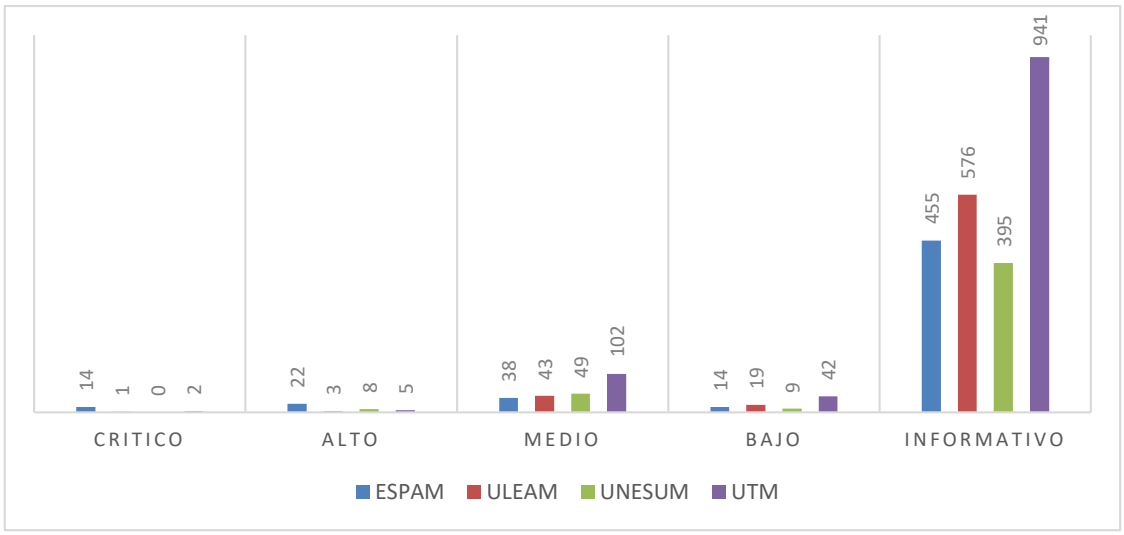


Gráfico 4. 4. Total de vulnerabilidades NESSUS.
Elaboración: Las autoras.

En el gráfico 4.5, se pudo determinar que con la herramienta ACUNETIX se obtuvo el mayor número de vulnerabilidades en el rango de medio, a diferencia de crítico que no se obtuvo ninguna vulnerabilidad, debido a que esta herramienta no valida ese criterio.

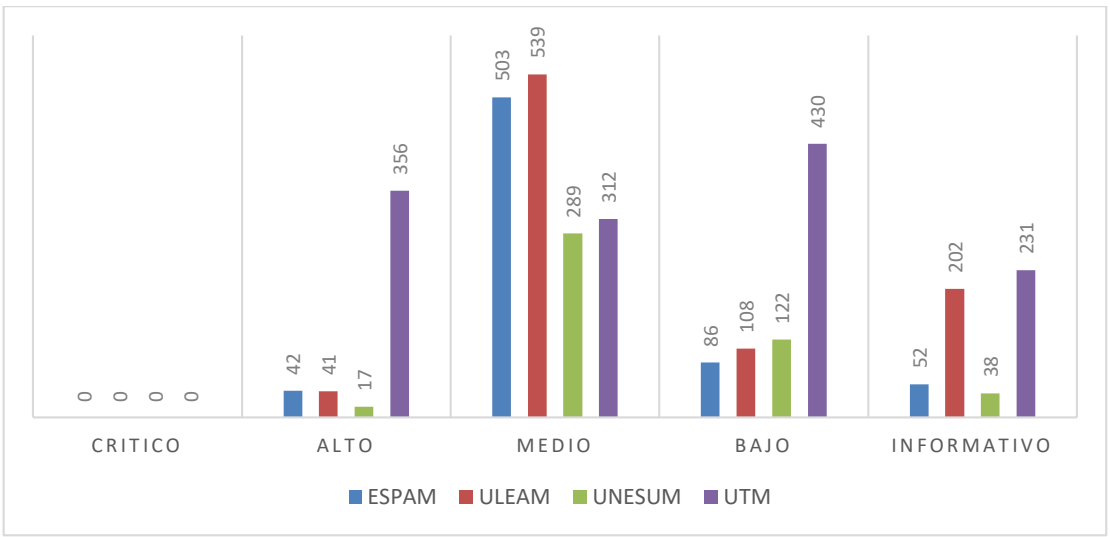


Gráfico 4. 5 Total de vulnerabilidades ACUNETIX.

Elaboración: Las autoras.

En la tabla 4.9 muestra el tiempo de respuesta de escaneo de cada herramienta por cada institución, en donde se observa que la herramienta ACUNETIX tomó más tiempo en realizar los análisis, seguido de NESSUS y SHODAN.

Tabla 4. 9 Tiempo de análisis por herramienta.

HERRAMIENTAS	RESULTADOS	ESPAM MFL	ULEAM	UTM	UNESUM
SHODAN	**TOTAL DE VULNERABILIDADES**	273	39	351	237
	TIEMPO DE RESPUESTA	10 minutos	5 minutos	12 minutos	9 minutos
NESSUS	**TOTAL DE VULNERABILIDADES**	543	642	1092	461
	TIEMPO DE RESPUESTA	7 Horas 26 segundo	11 Horas 13 segundo	18 Horas 43 segundo	17 Horas 34 segundo
ACUNETIX	**TOTAL DE VULNERABILIDADES**	683	890	1329	466
	TIEMPO DE RESPUESTA	4 Horas 1 minutos 26 segundo	45 Horas 30 minutos	8 Horas 13 minutos	28 Horas 1 minutos 25 segundo

Elaboración: Las autoras

Cabe mencionar que el número de vulnerabilidades encontradas en los sistemas escaneados no tienen relación con el tiempo de respuesta, debido a que las herramientas hacen un análisis profundo y exhaustivo cuando el grado de éstas son severas (crítico, alto y medio), mientras que si son de grado leves (bajas e informativas), la respuesta es un tiempo mínimo, por esta razón en el tiempo de ejecución hay casos de pocas vulnerabilidades y mayor tiempo de repuesta y viceversa. Referente a la semejanza que tienen las 3 herramientas aplicadas para encontrar vulnerabilidades, se pudo determinar que, son similares descriptivamente hablando, pero con diferentes aspectos en tiempos, funcionalidad, reportes, seguridad en el momento de la ejecución, puesto que se ha notado en los resultados, en términos generales, las similitudes en ellas.

Cabe recalcar que hubo sistemas que se encontraron en mantenimiento en el periodo de prueba con la herramienta, puesto no se puedo realizar dicha prueba,

dado que se necesitaba ver su desenvolviendo en el ciberespacio y no de manera local.

Luego de la obtención de resultados de cada uno estos reportes, se pudo ver que todos dieron a conocer los resultados a excepción del sistema de gestión académica de la ULEAM, que no arrojo resultados al parecer por que el sistema estaba en algún mantenimiento o probablemente la IP fue cambiada, de allí se notó que durante el escaneo que los niveles altos eran pocos, más bien el sistema de la UNESUM arrojo solo 1 nivel alto y 3 medianos y le seguía la UTM con 5 medianos, de allí los demás resultados eran bajos e informativos.

Al momento de la comparativa se pudo apreciar que Acunetix fue la más eficaz y óptima en resultados, puesto que mandaba de manera increíble las vulnerabilidades de niveles altos que quizás las demás herramientas no se lo generaban en gran proporción, otro aspecto importante de ella es que tiene entre sus opciones *fullscan, location*, entre otras que si bien dichas opciones permitieron ver una información más profunda pero estas se visualizaban dentro del escaneo de la aplicación en el Ciberespacio.

4.1.2. OBJETIVO 2: IDENTIFICACIÓN LOS RIESGOS DE CIBERSEGURIDAD MEDIANTE LA METODOLOGÍA AMFE (ANÁLISIS MODAL DE FALLOS Y EFECTOS).

Mediante la aplicación de la matriz de riesgos Análisis Modal de Fallos y Efectos (AMFE), se pudo determinar por cada vulnerabilidad obtenida en los *Checklists* basados en la Norma ISO/IEC 27032 y las herramientas de prueba de escaneo de vulnerabilidad Shodan, Nessus y Acunetix, los riesgos de cada IES pública de Manabí, de los cuales, fue clasificada por dominios de ciberseguridad (Seguridad de Información, Seguridad de Aplicación y Seguridad de Red) para su mejor compresión y adaptabilidad (tabla 4.10). Cabe mencionar que de los reportes que arrojaron las herramientas SHODAN, NESSUS, ACUNETIX, se tomaron acciones de mitigación y su respectivo criterio de aceptación (Anexo 7).

Tabla 4. 10. Riesgos General por dominios de Ciberseguridad ISO/IEC 27032

DOMINIOS	PORCENTAJE DE NIVEL DE RIESGO EN LAS IES PÚBLICAS DE MANABÍ APLICANDO ISO/IEC 27032 DE CIBERSEGURIDAD				
	NIVEL DE RIESGO	UTM	ULEAM	ESPAM MFL	UNESUM
Seguridad de la Información	Crítico	38%	27,27%	50%	38,46%
	Alto	30,77%	27,27%	16,67%	46,15%
	Medio	30,77%	36,36%	33,33%	15,39%
	Bajo	0%	9,10%	0%	0%
Seguridad de las Aplicaciones	Crítico	9,09%	0%	7,14%	20%
	Alto	45,45%	45,45%	42,86%	26,67%
	Medio	27,27%	36,36%	35,72%	40%
	Bajo	18,18%	18,19%	14,28%	13,13%
Seguridad de las Redes	Crítico	14,29%	0%	12,50%	28,57%
	Alto	28,57%	0%	37,50%	42,86%
	Medio	57,14%	100%	50%	28,57%
	Bajo	0%	0%	0%	0%

Elaboración: Las autoras

RIESGO – NIVEL CRÍTICO

En el dominio seguridad de la información la ESPAM MFL tiene el mayor riesgo en cuanto a las otras IES estudiadas con un nivel **Crítico** del 50%, en el dominio de seguridad de las aplicaciones y seguridad de las redes está la UNESUM con un nivel crítico del 20% y 42,86% respectivamente.

RIESGO – NIVEL ALTO

En el dominio de seguridad de la información y seguridad de las redes, la IES con un nivel **Alto** de riesgo es la UNESUM, con un 46,15% y 42,86% respectivamente; en cuanto corresponde al dominio seguridad de las aplicaciones están la UTM y la ULEAM con el 45,45% cada una.

RIESGO – NIVEL MEDIO

En el dominio de seguridad de la información la ULEAM tiene un nivel **Medio** del 36,36%; en el dominio de seguridad de las aplicaciones está la UNESUM con el 40%; en cuanto corresponde al dominio seguridad de las redes están la UTM y la ULEAM con el 100%.

RIESGO – NIVEL BAJO

La ULEAM tiene un nivel **Bajo** del 9,10% en el dominio de seguridad de la información; la UTM y la ULEAM tienen cada una el 18,18% en el dominio de seguridad de las aplicaciones y en el dominio de seguridad de las redes todas las IES públicas de Manabí no tienen nivel bajo.

4.1.3. OBJETIVO 3: ELABORAR UN PLAN DE MEJORA PARA MITIGAR LOS RIESGOS A LA CIBERSEGURIDAD EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICAS.

En este último objetivo, se procedió a la elaboración del Plan de Acción (Anexo 8), para mejorar en los aspectos de la Ciberseguridad, del cual se efectuó uno para cada IES Públicas de Manabí, y que para el efecto se consiguió separar los resultados arrojados de todo el procesos de manera que se promueva la ética profesional y cuidar la sensibilización de la información, además cabe indicar que los sistemas distribuidos analizados fueron de carácter académicos e implementados en estas intuiciones con acceso público al ciberespacio**.** Además, en el anexo antes mencionado solo se presentó el Plan de Acción de la ESPAM MFL, y a su vez se efectuó la entrega formal de los planes correspondientes a cada institución de educación superior pública de Manabí (UTM, ULEAM, UNESUM).

4.2. DISCUSIÓN

Quiñe (2011), menciona que el uso de herramientas de escaneo en el Ciberespacio, permiten tomar conciencia y ejecutar acciones en el corto plazo, que ayuden a la toma de decisiones en temas de seguridad Información. Y que si bien después de 5 años, esto ayudó para considerar: prevenir, prever, estar preparados, informarse, conocer, identificar, comprender, entender, capacidad de analizar, proteger, resolver, detectar, corregir, definir, determinar y establecer los niveles que emergen el desarrollo profesional dentro de la Ciberseguridad.

El análisis de las vulnerabilidades permite establecer un resumen óptimo en la identificación de las vulnerabilidades encontradas para su corrección, dado que asignan una priorización (por nivel de riesgo, nivel de impacto, nivel de ocurrencia, nivel de popularidad) y expuestos en Reporte de Vulnerabilidades Informe Ejecutivo, Informe Detallado, que incluye: Hallazgos Riesgos y, Recomendaciones de control Anexos: Reportes de hallazgos Estadísticas Información. (Quiñe, 2019).

Con base a este argumento las autoras manifiestan que implementar herramientas como pruebas de escaneo para las vulnerabilidades, permiten complementar la seguridad de los sistemas distribuidos a través de los reportes generados por estas herramientas, y de esta manera hacer las correcciones de las fallas o debilidades, amenazas o ataques a los que están expuestos los mismos efectuando acciones de mitigación.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- En el desarrollo de la investigación se pudo determinar que las vulnerabilidades encontradas en los sistemas distribuidos representan un promedio en la UTM del 27,33%, ULEAM 14,33%, ESPAM 29% y UNESUM 29,34%, de fallos en los procesos de documentación en el cumplimiento de los diferentes dominios de seguridad de la ISO/IEC 27032 (pág. 30). Con respecto a las herramientas de escaneo (página 31), se pudo comprobar que los sistemas académicos, están expuestos a ataques cibernéticos en un promedio del 20%, debido a la criticidad de las vulnerabilidades. El tiempo de ejecución (página 37) de cada herramienta, depende del grado de vulnerabilidad que tienen los sistemas académicos, y no del tiempo de respuesta de los servidores.

- En los riesgos identificados y evaluados con la matriz AMFE (Análisis Modal de Fallos y Efectos), se determinó que el promedio de riesgo crítico en los diferentes dominios de seguridad (información, aplicaciones y redes) de la UNESUM es del 29,02%, ESPAM MFL el 23,21%, UTM el 20,46% y la ULEAM el 9,09% (página 38).

- Las mejoras para mitigar los riesgos evaluados se establecieron mediante el desarrollo de un Plan de Acción (Anexo 8), donde se proponen acciones y criterios de aceptación a corto y mediano plazo de acuerdo a la urgencia del caso, con el fin de promover la ética en TI, la concientización y brindar mayor seguridad en el espacio de navegación de acuerdo con los resultados obtenidos de los sistemas académicos.

5.2. RECOMENDACIONES

- Se recomienda a las IES que fueron objeto de estudio, adoptar las directrices y controles que se proveen en la norma ISO/IEC 27032 para la seguridad de los sistemas distribuidos, de manera que se puedan disminuir las vulnerabilidades y amenazas que se generen en el ciberespacio, y así evitar ataques a futuro.

- Aplicar de una manera más segmentada la Matriz de Riegos AMFE, para la clasificación de las vulnerabilidades y riesgos a mitigar, según los niveles de probabilidad e impacto obtenidos luego de un levantamiento de información, que permita hacer un seguimiento y control de las vulnerabilidades, sobre todo a las de carácter severa.

- Socializar a los involucrados y responsables de tecnología, el Plan de Acción proporcionado por las autoras, para que puedan realizar los controles internos y de auditoría a los sistemas distribuidos de las IES Públicas de Manabí, con el fin de mejorar la seguridad, integridad, confiabilidad y disponibilidad de la información en la Web o el Ciberespacio.

BIBLIOGRAFÍA

Almeida, L. (2017). La ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la Armada del Ecuador. Revista electrónica ISSN, 1390, 9381.

Anchundia, E. (2017). Ciberseguridad en los sistemas de información de las universidades. Revista Cientifica Dominio de las Ciencias. 3, 200-217. DOI: https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.200-217

Ardita, J. (2018). Los riesgos de los sistemas informáticos. Disponible en: http://www.cybsec.com/upload/Julio_Ardita_Introduccion_seguridad_.pdf

Bankinter. (2012). El Ciberespacio y Gestion de Riesgos. Disponible en: https://blog.bankinter.com/economia/-/noticia/2012/11/7/el-ciberespacio-y-la-gesti-243-n-de-riesgos.aspx

Borghello, C., & Temperini, M. (2013). Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública. In Simposio de Informática y Derecho. Jornadas Argentinas De Informática (No. 42).

Biddle, S. (2017). La educación superior, blanco de ciberataques. Disponible en: http://www.prensariotila.com/21722-La-educacion-superior-blanco-de-ciberataques.note.aspx

Burgos, T. (2012). Qué es la norma iso 27032 “gestión de la ciberseguridad”. Disponible en: https://www.grupoacms.com/norma-iso-27032

Constitución del Ecuador. (2008). Asamblea Nacional. Disponible en: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Consuegra, O. (2015). Metodología AMFE como herramienta de gestión de riesgo en un hospital universitario. Cuadernos Latinoamericanos de Administración » Volumen XI » Número 20 » Págs. 37-50

Diaz, S. (2013). Vulnerabilidad de los Sistemas Informáticos. Disponible en: http://vulnerabilidadtisg.blogspot.com

Fallas, S. (2018). Lo más destacado del Reporte de Ciberseguridad Cisco 2018. Disponible en: https://gblogs.cisco.com/la/sg-stfallas-lo-mas-destacado-del-reporte-de-ciberseguridad-cisco-2018/

Flores, S. (2017). Desafíos de la ciberseguridad y respuestas estatales: el caso del estado ecuatoriano en el período 2008-2015 (Bachelor's thesis, PUCE).

Freire, B. (2017). Estudio y análisis de ciberataques en América Latina. Disponible en: http://repositorio.ucsg.edu.ec/bitstream/3317/9203/1/T-UCSG-PRE-TEC-ITEL-245.pdf

García, A. (2012). Norma ISO/IEC 27032, nuevo estándar de ciberseguridad. Disponible en: http://cso.computerworld.es/alertas/norma-isoiec-27032-nuevo-estandar-de-ciberseguridad

García, C. (2018). Gestión de la Calidad, Riesgos y Evaluación. Tema 3: Herramientas Gestión y Evaluación (II)

García, M. (2017). ¿Quién es el responsable de un ciberataque? Disponible en: http://www.expansion.com/economiadigital/protagonistas/2017/06/29/594d24b1ca474135688b4679.html

Gómez, G. (2017). Gestión de la Ciberseguridad según el ISO/IEC 27032:2012. Diponible en: https://es.linkedin.com/pulse/gestión-de-la-ciberseguridad-según-el-isoiec-gianncarlo-gómez-morales

GTDI. (2018). Lineamientos para Ciberseguridad. ISO/IEC 27032:2012. Disponible en: https://www.gtdi.pe/sites/all/themes/simplecorp/images/isoiec27032.pdf

Jimeno, J. (2013). AMFE: Análisis Modal de Fallos y Efectos – Guía y ejemplos de uso. Disponible en: https://www.pdcahome.com/3891/amfe-guia-de-uso-del-analisis-modal-de-fallos-y-efectos/

Information Security Breach Survey (2015). Mejore su estrategia de IT. Disponible en: http://www.lrqa.es/Images/124576-.pdf

ISO (Organization International for Standarization). (2018). ISO/IEC 27032:2012 Tecnología de la Información-Técnicas de seguridad-Directrices para la ciberseguridad. Disponible en: https://www.iso.org/standard/44375.html

Lloyd's (2018). Ciberseguridad. Disponible en: http://www.lrqa.es/seguridad-de-la-informacion/ciberseguridad/

Maldonado, S. (2017). Van 10 casos de ciberataques. Disponible en: https://www.elsiglodetorreon.com.mx/noticia/1382124.van-10-casos-de-ciberataques.html

Mayol, E. (2018). Sistemas de Información. Disponible en: https://www.fib.upc.edu/es/estudios/grados/grado-en-ingenieria informatica/plan-de-estudios/especialidades/sistemas-de-informacion

Medranda, S. (2017). Análisis e Implantación de un sistema de ciberdensas virtual para DataCenter Académico de la Universidad de las Américas. Disponible en: http://dspace.udla.edu.ec/handle/33000/7520

Pastorino, C. (2018). Ciberataques en el 2018 superarán cifras del 2017. Disponible en: https://www.eleconomista.com.mx/sectorfinanciero/Ciberataques-en-el-2018-superaran-cifras-del-2017-20180718-0103.html

Permalink. (2013). Amenazas y fraudes en los sistemas de la información. Disponible en: https://infosegur.wordpress.com/tag/vulnerabilidades/

Philco, L. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. Disponible en: http://repositorio.ucsg.edu.ec/handle/3317/9203

Quiñe, J. (2011). Técnicas y Herramientas para la Evaluación de Vulnerabilidades de Red. Disponible en: https://es.slideshare.net/hackspy/tcnicas-y-herramientas-para-la-evaluacin-de-vulnerabilidades-de-red

Quiñe, J. (2019). Arte de la ciber seguridad. Disponible en: https://es.slideshare.net/hackspy/arte-de-la-ciber-seguridad

Rodríguez, Q., & Acacio, D. (2014). Las políticas regionales sobre ataques informáticos y su incidencia en la vulnerabilidad de la defensa de la UNASUR en el período 2009-2013 (Master's thesis, Quito, Ecuador).

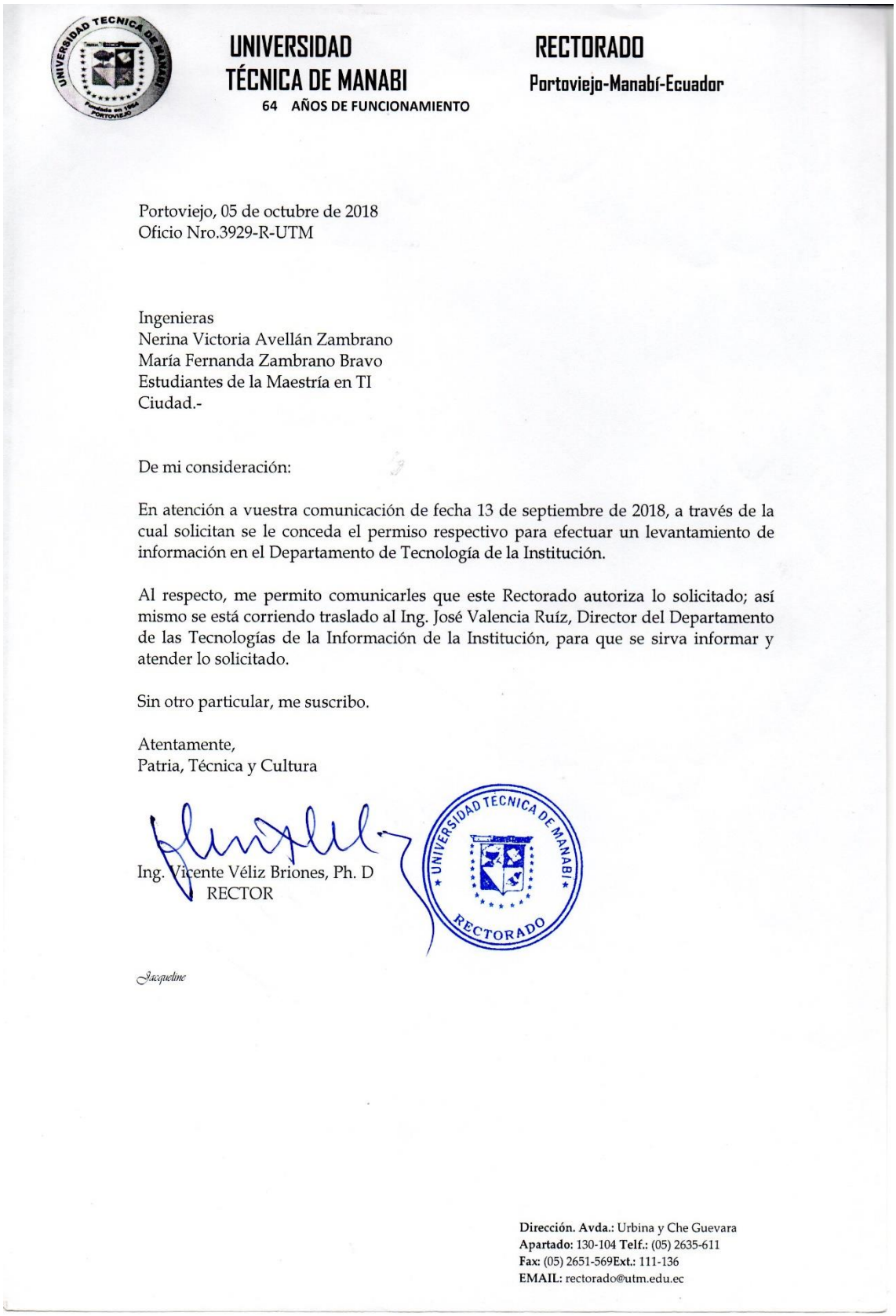
Ruben. (2018). Los ciberataques: tipos y previsiones para el 2018. Disponible en: http://rcg-comunicaciones.com/los-ciberataques-tipos-previsiones-2018/

Torres, E. (2015). Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002: 2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos)

ANEXOS

ANEXO 1.
OFICIOS DE PERMISOS PROPORCIONADOS POR LAS IES PÚBLICAS DE MANABÍ PARA REALIZAR LEVANTAMIENTO DE INFORMACIÓN

Anexo 1A. Solicitud de levantamiento de información en la Universidad Técnica de Manabí (UTM).



UNIVERSIDAD TÉCNICA DE MANABI
64 AÑOS DE FUNCIONAMIENTO

RECTORADO
Portoviejo-Manabí-Ecuador

Portoviejo, 05 de octubre de 2018
Oficio Nro.3929-R-UTM

Ingenieras
Nerina Victoria Avellán Zambrano
María Fernanda Zambrano Bravo
Estudiantes de la Maestría en TI
Ciudad.-

De mi consideración:

En atención a vuestra comunicación de fecha 13 de septiembre de 2018, a través de la cual solicitan se le conceda el permiso respectivo para efectuar un levantamiento de información en el Departamento de Tecnología de la Institución.

Al respecto, me permito comunicarles que este Rectorado autoriza lo solicitado; así mismo se está corriendo traslado al Ing. José Valencia Ruíz, Director del Departamento de las Tecnologías de la Información de la Institución, para que se sirva informar y atender lo solicitado.

Sin otro particular, me suscribo.

Atentamente,
Patria, Técnica y Cultura

Ing. Vicente Véliz Briones, Ph. D
RECTOR

UNIVERSIDAD TÉCNICA DE MANABI
RECTORADO

Jacqueline

Dirección. Avda.: Urbina y Che Guevara
Apartado: 130-104 Telf.: (05) 2635-611
Fax: (05) 2651-569Ext.: 111-136
EMAIL: rectorado@utm.edu.ec

Anexo 1B. Solicitud de levantamiento de información en la Universidad Laica Eloy Alfaro de Manabí (ULEAM).

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Rectorado

2016-2021

Memorando n.°: ULEAM-R-2018-6398-M

Manta, 29 de septiembre de 2018

PARA: Ing. Bécquer Briones Veliz
Director de la Unidad Central de Coordinación Informática

ASUNTO: Autorización de levantamiento de información.

En atención al oficio s/n de fecha 28 de septiembre de 2018, suscrito por la Ing. Nerina Victoria Avellán Zambrano y Ing. María Fernanda Zambrano Bravo, Estudiantes de la Maestría en TI, quienes solicitan permiso para efectuar un levantamiento de información en el Departamento de Tecnología con el propósito de desarrollar el trabajo de titulación; al respecto le pido a usted coordinar lo solicitado con las mencionadas estudiantes.

Atentamente,

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ
RECTOR
Manta - Ecuador

Arq. Miguel Camino Solórzano, PhD.
RECTOR UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

jv

RECIBIDO
0 1 OCT. 2018
12435

Teléfono: 05 2625095 / 2623740 Ext 102
Av. Circunvalación Vía San Mateo
www.uleam.edu.ec

Anexo 1C. Solicitud de levantamiento de información en la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM MFL).

República del Ecuador

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

RECTORADO

Ley 99 – 25 R.O. 181-30-04-1999
CALCETA – ECUADOR

Oficio Nº: ESPAM MFL-R -2018-329A-OF
Calceta, 05 de septiembre de 2018

Ing. Nerina Victoria Avellán Zambrano
Ing. María Fernanda Zambrano Bravo
ESTUDIANTES DE LA MAESTRÍA EN TECNOLOGÍA DE INFORMACIÓN, MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS DE LA ESPAM MFL
Ciudad.-

De mi consideración:

Reciba cordial saludo y los mejores deseos de éxitos en sus delicadas funciones.

Atendiendo vuestro requerimiento mediante oficio SN de fecha 5 de septiembre de 2018, se le concede el correspondiente permiso para que realicen el levamiento de información en el departamento de Tecnología de nuestra Universidad, a fin de desarrollar del trabajo de titulación: "**CIBERSEGURIDAD Y SU APLICACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICO DE MANABÍ"**; para lo cual puede coordinar acciones con el Lic. Geovanny García Montes, responsable de la Unidad de Tecnología.

Con sentimiento de consideración y estima.

Atentamente,

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
RECTORADO

Ec. Miryam Elizabeth Félix López. Ph.D.
RECTORA DE LA ESPAM MFL

Copia: Lic. Geovanny García Montes, responsable de la Unidad de Tecnología.

MFL/dzm

Recibido
05-09-2018
14H30

1/1

Dirección: *10 de Agosto Nº 82 y Granda Centeno.* ***Teléfonos:*** *053028808*
Correo: *rectorado@espam.edu.ec*

Anexo 1D. Solicitud de levantamiento de información en la Universidad Estatal del Sur de Manabí (UNESUM).

UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ
Creada el 7 de febrero del 2001, mediante Registro Oficial # 261
RECTORADO

Jipijapa, 31 de octubre de 2018
Of. N°.2459 ING. OEBL PhD. RECTOR.UNESUM

Ingenieras
Merina Victoria Avellán Zambrano
María Fernando Zambrano Bravo
ESTUDIATES DE LA MAESTRIA EN TI.
Calceta.-

De mi consideración:

En atención a su oficio s/n de fecha 20 de septiembre de 2018, a través del cual solicitan se le conceda el permiso respectivo para efectuar un levantamiento de información en el departamento de tecnología de la institución.

Al respecto me permito comunicarles que este Rectorado autoriza lo solicitado; dicha solicitud fue remitida al Ing. Holger Delgado Lucas, Decano de la Facultad de Ciencias Técnicas, con el fin de que atienda y brinde las facilidades de acuerdo a la petición realizada por ustedes.

Particular que comunico para los fines pertinentes

Fraternalmente,

"EXCELENCIA ACADÉMICA PARA EL DESARROLLO"

Ing. Omelio Enrique Borroto Leal, PhD.
RECTOR UNESUM.

RECTORADO

ANEXO 2.
ENTREVISTAS REALIZADAS A LOS DIRECTIVOS DE TECNOLOGÍAS DE LAS IES.

Anexo 2A. Entrevista aplicada al departamento TI de la UTM.

INSTITUCIÓN:	Universidad Técnica de Manabí (UTM)
ÁREA:	Dirección de Tecnología de Información
RESPONSABLE:	Ing. Jonathan Delgado C.
FUNCIÓN:	Seguridad y Centro Informático
TÉCNICA APLICADA:	Entrevista

ANÁLISIS

El departamento TI actualmente tiene dos áreas: Área de desarrollo y Área de Control y Pruebas. Con respecto a la seguridad de la información, esta unidad se maneja con la siguiente documentación: Políticas de seguridad alineada a la ISO/IEC 27001, 27002; COBIT 5 y Reglamentos y Acuerdos de Confidencialidad. El ataque informático que han tenido en los últimos 5 años es de Exploración (Scanning) de tipo Man in the Middle. Cabe mencionar que a todos estos ataques se les ha hecho un reporte y el seguimiento respectivo. Las aplicaciones web implementadas por el departamento, han estado sujetos a amenazas como DDOS (Pishing). Los parámetros de garantía de funcionamiento y disponibilidad de estas aplicaciones que maneja el área TI, son de tipo de Seguridad y Normativa. El total de aplicaciones web que tiene la universidad son 9, entre ellas están: Sistema de Gestión académica, Seguimiento a graduados, Becas, Inventario, Bienestar estudiantil, Sistema de planificación, Sistema de Planificación y Control académico, Parque automotor, Practicas Pre profesionales. Para el almacenamiento de la información utilizan el gestor de base de datos Posgrest SQL 9.6 y MySQL. La institución cuenta con 6 servidores físicos y 11 virtuales. Solo tienen políticas de respaldo de la información y un plan de contingencia, pero no tienen políticas de acceso a la data center. En los protocolos de comunicación tienen 64 IP públicas y 2032 IP privadas. El proveedor que suministra el servicio de internet a la universidad es CNT.

Anexo 2B. Entrevista aplicada al departamento TI de la UNESUM.

INSTITUCIÓN:	Universidad Estatal del Sur de Manabí (UNESUM)
ÁREA:	Sistemas Informáticos
RESPONSABLE:	Ing. Carlos Conforme.
FUNCIÓN:	Gestión de la Información
TÉCNICA APLICADA:	Entrevista

ANÁLISIS

El departamento TI actualmente no tiene una estructura definida en cuanto a seguridad o ciberseguridad. El tipo de documentación que manejan para la seguridad es el Sistema de Gestión de Seguridad de la Información (SGSI) aplicado al área académica. El ataque informático que han tenido en los últimos 5 años es de Manteniendo el acceso (Maintaining Access) de tipo Man in the Middle y DDOS. Cabe mencionar que a todos estos ataques no se les hace el respectivo reporte y seguimiento. Estos ataques son presentados al final de cada periodo académico. Las aplicaciones web implementadas por el departamento, han estado sujetos a amenazas como modificación de datos. Los parámetros de garantía de funcionamiento y disponibilidad de estas aplicaciones que maneja el área TI, son de tipo Firewall en servidores y Firewall en administración de ancho de banda. El total de aplicaciones web que tiene la universidad son 4, entre ellas están: Sistema Académico UNESUM, Repositorio digital UNESUM, Sistema de Evaluación Docente y Biblioteca virtual. Para el almacenamiento de la información utilizan el gestor de base de datos MySQL. La institución cuenta con 4 servidores físicos y 6 virtuales. La data center no cuenta con reglamentos, políticas o similares definidos para la seguridad de la información y tampoco tienen un plan de contingencia y de emergencia establecido. En los protocolos de comunicación tienen 124 IP públicas y el proveedor que suministra el servicio de internet a la universidad es TELCONET.

Anexo 2C. Entrevista aplicada al departamento TI de la ULEAM.

INSTITUCIÓN:	Universidad Laica Eloy Alfaro de Manabí (ULEAM)
ÁREA:	UCCI
RESPONSABLE:	Ing. Bécquer Briones V.
FUNCIÓN:	Director de Tecnología de la Información
TÉCNICA APLICADA:	Entrevista
ANÁLISIS	
El departamento TI actualmente se encuentra estructurado en cuanto a seguridad en Protección y respuestas que lo lleva la misma unidad junto con análisis y evaluación de riesgos TI el cual está en proceso de implementación. El tipo de documentación que manejan para la seguridad son Políticas de la seguridad de la información, Acuerdo de confidencialidad, Uso de infraestructura TI, Políticas de contingencia, correo electrónico, internet, Reglamento de seguridad de TI, el mismo que está en segundo debate por el Consejo universitario. El ataque informático que han tenido en los últimos 5 años es de Reconocimiento (Reconnaissance) de tipo Ransomware, XSS y DDOS. Cabe mencionar que a todos estos ataques se les hace el respectivo reporte y seguimiento. Estos ataques se presentan uno por cada periodo académico. Las aplicaciones web implementadas por el departamento, han estado sujetos a amenazas como XSS, ataques DDOS y SPAN y el proveedor que suministra el servicio de internet a la universidad es CEDIA.	

Anexo 2D. Entrevista aplicada al departamento TI de la ESPAM MFL.

INSTITUCIÓN:	Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM MFL).
ÁREA:	Departamento TI
RESPONSABLE:	Lcdo. Geovanny García Montes.
FUNCIÓN:	Coordinador de Tecnología de la Información
TÉCNICA APLICADA:	Entrevista
ANÁLISIS	
El departamento TI actualmente tiene estructurada las siguientes áreas: Área de desarrollo de aplicaciones, Área de redes, Área de Datos y Área de mantenimiento de equipos tecnológicos. Con respecto a la seguridad de la información, esta unidad se maneja con la siguiente documentación: Políticas de seguridad para el área de datos solamente, alineada a la ISO/IEC 27001, 27002 y Norma de Control Interno 410-09 TI. No cuenta actualmente con políticas de seguridad, procedimientos, manual de funciones y responsabilidades para todas las áreas que tiene el departamento, pero estas en proceso de aprobación. El ataque informático que han tenido en los últimos 5 años es de Exploración (Scanning) de tipo Man in the Middle. No se les ha hecho un reporte y el seguimiento respectivo a todos estos ataques. Las aplicaciones web implementadas por el departamento, han estado sujetos a amenazas como DoS (Pishing). Los parámetros de garantía de funcionamiento y disponibilidad de estas aplicaciones que maneja el área TI, son de tipo de Seguridad. El total de aplicaciones web que tiene la universidad son 14, entre ellas están: Sistema de Gestión académica, Seguimiento a graduados, Bienestar estudiantil, Sistema de planificación, Página institucional, Evaluación docente, entre otras. Para el almacenamiento de la información utilizan el gestor de base de datos SQL Server. El proveedor que suministra el servicio de internet a la universidad es CEDIA.	

ANEXO 3.
CHECKLIST APLICADO A LAS IES PÚBLICAS DE MANABÍ BASADO EN LA NORMA ISO/IEC 27032 POR DOMINIOS DE SEGURIDAD (INFORMACIÓN, APLICACIÓN Y RED)

Anexo 3A. *Checklist* General de Ciberseguridad en el Dominio Seguridad de la Información.

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD																			
DOMINIO: SEGURIDAD DE LA INFORMACIÓN (protección de la confidencialidad, integridad y disponibilidad de la información en general)																			
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.																			
			ESPAM MFL				UTM				ULEAM				UNESUM			
COMPONENTE	SECCIÓN	HITOS	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN
PARTES INTERESADAS	Universidad como consumidora de proveedores externos	¿La universidad consume servicios en la Web?	x				x				x							
		¿Los servicios que consumen son de aplicación?	x				x				x							
		Los tipos de servicios que consumen en la Web son:																
		a) Quipux	x				x					x						
		b) Sercop	x				x				x							
		c) Urkund	x					x			x							
		d) Otros servicios	x					x			x			Ministerio de finanzas, relaciones laboral senecyt				
		Dichos servicios forman parte los siguientes Web Services:																
		a) SOAP						x				x						
		b) REST						x			x							
		c) XML Web Services					x					x						
		d) otros						x			x			Jason				
		¿La universidad tiene algún proveedor de servicios de Internet?	x				x				x							

		¿Cuál de ellos son proveedores de servicios de Internet de la universidad:																	
		a) CNT					x					x							
		b) CEDIA	x					x			x								
		c) Telconet						x				x							
		d) Electrocom						x				x							
		e) Grupo TVCable Internet						x				x							
		f) Netlife						x				x							
		g) Perobeli						x				x							
		h) Puntonet						x				x							
		i) iPlanet						x				x							
		j) Clicknet						x				x							
		k) Otros proveedores						x				x							
		¿Los tipos de servicios que les proveen son:																	
		a) Internet	x				x				x								
		b) Aplicaciones	x					x			x								
		c) Sitios web	x					x			x								
		d) Otros servicios						x			x								
	Universidad como proveedora	¿La universidad se considera un proveedor de servicios en el ciberespacio?	x				x				x								
		Los servicios de aplicaciones virtuales de uso exclusivo para la institución son:																	
		a) Gestión Académica	x				x				x								
		b) Gestión de Talento Humano	x				x					x							
		c) Gestión Financiera						x				x							

		d) Gestión de Biblioteca	x				x				x							
		e) Gestión Investigación	x					x			x							
		f) Otros servicios				Seguimientos POA, Seguimiento a egresados		x			x			Vinculación, Practicas Pre Profesionales, Evaluación docente				
		Los servicios de aplicaciones y sitios web que brindan a los interesados son:																
		a) Edición de documentos, almacenamiento, distribución.							x			x						
		b) Entornos virtuales en línea para interacción con otros usuarios.	x				x				x							
		c) Repositorios en línea de medios digitales con la agregación, búsqueda, catálogo, servicios de pago.						x			x							
		d) Gestión de recursos empresariales como humanos, finanzas y nóminas, cadena de suministro, facturación.						x				x						
		Llevan registro de control de los servicios que brindan en la Web:																
		a) Usuarios	x				x				x							
		b) Contraseñas de usuarios	x				x				x							
		c) Quejas o comentarios de la disponibilidad de estos servicios.	x				x				x							
ACTIVOS EN EL CIBERESPACIO	**ACTIVOS EN LA ORGANIZACIÓN**	¿Tienen aplicaciones desarrollados e implementados en la universidad?	x				x				x							
		Los tipos de aplicaciones o software que se desarrollan son:																
		a) Gerenciales						x				x						
		b) Académicos	x				x				x							
		c) Expertos						x			x							

		d) Otros sistemas					x			RRTT - Bienestar estudiantil		x							
		¿Realizan la documentación de los sistemas de información desarrollados e implementados?	x					x			x			Parcialmente				
		¿Elaboran manuales de usuario para el manejo de estos sistemas de información?	x					x			x			Parcialmente				
		¿Protegen la identidad en línea (username, nickname) de los usuarios que se registran para acceder a los sistemas de información?	x				x				x							
		¿Implementan un control de seguridad en los sistemas web?					x				x							
		¿Los sistemas de información se desarrollan e implementan en diferentes infraestructuras de servicios?						x			x							
		¿Se monitorea el acceso a los sistemas de información web?					x				x							
		¿Los sistemas de información web implementados tienen reservados los derechos de autor o propiedad intelectual (procesos patentados, patentes, resultados de investigación)?	x				x				x							
		¿Disponen de estrategias para la continuidad del negocio (lanzamiento de productos, datos de informes, marketing?		x				x			x			Parcialmente, protocolos de respuestas				
		¿Existen controles de acceso al data center?	x					x			x							
AMENAZAS CONTRA LA CIBERSEGURIDAD	**Amenazas y vulnerabilidades**	¿Han sufrido ataques de robo de identidad o robo de información de los usuarios en:						x										
		a) Aplicaciones y sitios web	x								x							

		b) Bases de datos																	
		c) Otros ataques										x							
		Entre los tipos de ataques que se han presentado en la unidad son:							x										
		a) DDoS (Ataque de negación distribuida de servicios)	x									x							
		b) Ingeniería social										x							
		c) DMA (acceso directo a memoria)											x						
		d) Eavesdropping (intercepción del tráfico en la red)	x									x							
		e) Spoofing																	
		f) Phishing	x									x							
		g) Manipulación de URL											x						
		h) Escalonamiento de privilegios											x						
		i) Trashing											x						
		j) Shoulder Surfing											x						
		k) Decoy											x						
		l) DoS (Negación de Servicio)	x									x							
		m) Ataques contraseña	x										x						
		n) Otros ataques										x			Inyección código HTML				
		¿Se documentan estos tipos de ataques?							x			x			Parcialmente				
		¿Tienen medidas de seguridad para disminuir estos ataques?					x					x							
		¿Alerta a los usuarios cuando existe algún tipo de ataque o implantación de controles de seguridad?						x				x			Informe a autoridades y dueños de procesos				

		¿Los atacantes han utilizado código malicioso en archivos intercambiados como un caballo de Troya para sus ataques?						x				x							
		¿Es de conocimiento por parte de los interesados que la seguridad y privacidad según los riesgos involucrados para tomar controles, son relacionados a la información?						x			x			Tienen políticas y normas de seguridad de la información				
		¿Cómo director/coordinador de la unidad, constata y asegura que la información ha sido clasificada de manera que se evite cometer accidentes en cualquier sitio web en el ciberespacio?						x			x			Parcialmente - elemento crítico - página web institucional				
		¿Efectúa controles de gestión de riesgos de seguridad cibernética en medida y de acuerdo al nivel de madurez de cada proceso?						x				x							
		¿Mantiene preparación continua en Ciberseguridad en la institución?						x			x								
		¿Se usan técnicas de visualización de datos para presentar información de eventos?						x			x								
		¿Se estandarizan los datos en base a normas de calidad?					x					x							
		Qué Normas de calidad emplea en la estandarización de sus procesos:																	
		a) ISO					x				x			9000					
		b) INEN									x			Solo nuevos procesos					
		c) Control Interno										x							
		d) Otras normas										x							
		Se realiza el intercambio de archivos de:						x											
		a) Mensajería instantánea										x							
		b) Portal web									x								

		c) Foro de discusión considerando la seguridad										x						
		¿Se aplican regulaciones de normas en escenarios de seguridad?					x					x						
		Qué normas emplean en escenarios de seguridad de la información:																
		a) ISO 33000											x					
		b) ISO 8000											x					
		c) ISO 25012											x					
		d) ISO 27001					x					x						
		e) ISO 2000																
		h) ISO 29100																
		i) ISO 270018																
		j) ISO 20000-9																
		k) ISO 22301																
		l) Otras normas					x			COBIT 5								
		¿Qué normas emplean en escenarios de ciberseguridad:						x					x					
		a) ISO 27032																
		b) ISO/IEC 27032																
		c) Otras normas																

Anexo 3B. *Checklist* General de Ciberseguridad en el Dominio Seguridad de las Aplicaciones.

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD																			
DOMINIO: SEGURIDAD DE LAS APLICACIONES (proceso realizado para aplicar los controles y mediciones para aplicaciones de una organización con el fin de gestionar el riesgo de su uso)																			
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.																			
ÁREA: Tecnología			ESPAM MFL				UTM				ULEAM				UNESUM				
COMPONENTE	SECCIÓN	HITOS	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN
ACTIVOS EN EL CIBERESPACIO	ACTIVOS EN LA ORGANIZACIÓN	¿El departamento de tecnología cuenta con una metodología y procesos de desarrollo de aplicaciones maduros?					x				x							
		¿La universidad cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos que implican las ciberamenazas?					x				x			Insuficiente				
		¿Tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción?						x			x			Provee el marco de trabajo				

		¿El departamento de tecnología ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar continuamente la práctica?						x			x							
		¿Se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable?						x			x			Test no formales, herramientas Nessus de Cedia				
		¿La unidad tiene un analista entrenado para correlacionar y evaluar los hallazgos de vulnerabilidades existentes en las aplicaciones?					x				x							
		¿Qué tipo de aplicaciones se desarrollan en la unidad:																	
		a) Móviles					x				x								
		b) Web					x				x								
		c) Otros									x			Win 32					
		¿Qué tipo de herramientas tecnológicas utiliza la unidad para										x		No para la fuerza de código- Nessus					

		realizar pruebas de vulnerabilidades:																
		a) SAST (Static application security testing). - Analiza pasivamente el código fuente o binario de una aplicación en busca de vulnerabilidades conocidas.					x											
		b) DAST (Dynamic application security testing). - Prueba y analiza una aplicación en ejecución en busca de comportamientos que indiquen posibles vulnerabilidades.						x										
		c) RASP (Runtime application self-protection). - Herramienta de autoprotección integrada en la aplicación durante su ejecución, permite monitorearse a sí misma para evitar ataques en tiempo real.						x										
		d) SCA (Software composition analysis). - Identifica, evalúa y monitoriza todos los componentes de terceros (cadena de suministros del software) que						x										

		puedan contener vulnerabilidades.																	
		¿La unidad tiene firewalls de aplicaciones?					x					x			Provee Cedia - no esta implementado				
		¿Qué tipo de firewall tienen:																	
		a) Firewall de aplicaciones de red					x												
		b) Host apllication firewall						x											
		c) Firewall de aplicaciones web					x					x							
		¿Se han eliminado servicios y protocolos innecesarios e inseguros para disminuir el ataque cibernético?					x					x							
		¿Ha considerado la protección avanzada de antivirus o agentes que usen detección y protección basada en comportamiento e inteligencia artificial (AI)?					x					x							
		¿Se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto					x					x			Proyecto de tesis estudiantil				

		interna como externa?																	
AMENAZAS CONTRA LA SEGURIDAD DEL CIBERESPACIO	**Amenazas y Vulnerabilidades**	¿Se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software?						x			x			Parcialmente				
		¿Se aprueban de manera formal los cambios de equipos tecnológicos y software?					x					x							
		¿Se prohíbe el uso de software no autorizado por la institución?						x				x							
		¿Se instalan y actualizan periódicamente software de antivirus, firewall contra código malicioso?					x				x								
		¿Se mantienen los sistemas operativos actualizados con las últimas versiones?						x			x			Pero no todos, no hay actualizaciones porque no se han hecho pruebas				
		¿Posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos?						x			x							
		¿Tienen sitios web legítimos que han sido hackeados?						x			x							
		¿Se realiza informes de eventos sospechosos o encuentros maliciosos en las aplicaciones?						x			x			Parcialmente				

		¿ El equipo de desarrollo aplica seguimientos o revisión en los mensajes recibidos en el sitio, para asegurarse que no contengan algun tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas?						x				x		Operaciones lo realiza				
		Se toman en cuenta los controles de nivel de aplicación:																
		a) Exposición de avisos cortos						x			x							
		b) Manipulación segura de sesiones					x				x							
		c) Validación de entrada segura y prevención de ataques (SQL Inyeccion)					x				x							
		d) Scripting o encriptación en sitios o aplicaciones web					x				x							
		e) Servicio de la organización o autenticación del servicio					x				x							
		¿Se logra los objetivos desarrollados en base a la sensibilización y formación:																
		a) Proporciona informes periódicos sobre el estado de la Ciberseguridad						x			x							

		b) Sesiones de formación enfocados en escenarios simulados de ataque cibernéticos o talleres sobre áreas requeridas de acciones especificas						x				x							
		c) Pruebas regulares con recorridos en escenarios permanentes						x			x			Parcialmente					

Anexo 3C. *Checklist* General de Ciberseguridad en el Dominio Seguridad de las Redes.

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD																			
DOMINIO: SEGURIDAD DE LAS REDES (diseño, implementación y operación de redes para lograr los propósitos de seguridad de la información en las redes dentro de las organizaciones, entre las organizaciones, y entre las organizaciones y los usuarios)																			
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.																			
ÁREA: Tecnología			ESPAM MFL				UTM				ULEAM				UNESUM				
COMPONENTE	SECCIÓN	HITOS	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	S	N	N/A	OBSERVACIÓN	
ACTIVOS EN EL CIBERESPACIO	ACTIVOS EN LA ORGANIZACIÓN	¿Aplican seguridad en la red?						x		Solicitud de firewall en proceso	x								
		Entre las políticas, procedimientos y controles que tiene la unidad para seguridad de la red están:																	
		a) Políticas de control de acceso a la red						x			x								
		b) Controles de acceso a los servidores					x				x								
		c) Procedimientos de respaldo de información cuando existe pérdida debido a fallos físicos					x				x								
		d) Control de los filtros de tráfico entre la red interna y la externa								En proceso	x								
		¿Existen controles que restrinjan la dirección MAC de cada equipo?					x				x								
		¿Tienen acceso restringido a las redes inalámbricas?					x				x								
		¿Tienen protocolos de autenticación de computadoras dentro de la red?						x			x								

		¿Se realiza el proceso de autentificación de los usuarios antes de dejarlos entrar a la aplicación?					x					x						
		¿Utilizan mecanismos de encriptación para mantener la confidencialidad e integridad de los datos que se están transmitiendo en la web?					x					x						
		¿Qué método de encriptación utiliza:																
		a) Encriptación simétrica (Data Encryption Estándar - DES)						x					x					
		b) Encriptación asimétrica (llave pública, llave privada)					x					x						
AMENAZAS CONTRA LA SEGURIDAD DEL CIBERESPACIO	**Amenazas y Vulnerabilidades**	¿Utilizan protocolos de comunicación como :																
		a) HTTP					x					x						
		b) HTTPS					x					x						
		c) MAILTO					x					x						
		d) FTP					x					x						
		¿Cómo director /coordinador de la unidad se asegura que la URL de su contenido web este citado como un enlace seguro en su navegador?					x					x						
		¿El SSL que utiliza el sitio web, identifica el contenido original del nuevo contenido dañado, plantado por un atacante?					x					x						
		Entre los tipos de ataques en la seguridad de la red que han sufrido están:																
		a) Interrupción: destrucción física de equipos, borrado de aplicaciones, falla de sistema operativo, etc.					x						x					
		b) Intercepción: reproducción ilícita de archivos, intercepción de los cables para monitoreo de datos en una red, etc.					x						x					

		c) Modificación: modificaciones de bases de datos, cambios en la configuraciones de software del sistema, etc.						x					x					
		d) Fabricación: insertar registros en bases de datos, añadir transacciones a un sistema de comunicaciones, etc.						x			x							
		¿La unidad tiene medidas de prevención y respuestas a los ataques cibernéticos?					x				x				En algunos unos casos hay protocolos en otros no			
		Ha tenido atacantes que se hacen pasar por una entidad autorizada para robar información como:											x					
		a) Hombre en el medio (Man in the maddle)						x										
		b) Otro tipo de robo de información						x										
		¿Se toman medidas de autenticación de comunicación para evitar el ataque de Man in the Midle?						x			x							
		¿Han sufrido ataques de IP Spoofing para manipular las direcciones IP asociadas a los mensajes en un intento de disfrazar el ataque como fuente conocida para ganar el acceso no autorizado a los sistemas?						x					x					
		Las redes WIFI en la institución están protegidas en:																
		a) WIFI Gestionado (portal cautivo)						x			x							
		b) Claves de acceso a WIFI					x						x					
		c) Otros tipos de protección						x					x					
		d) Protocolos para Redes abiertas					x						x					
		¿Se han vistos comprometidos los servidores en Internet con el método de desbordamiento de búfer provocando que el servidor funcione fuera de su entorno normal (control), facilitando la insercón / ejecución de código malicioso?					x						x					

		¿Se realiza informes de eventos sospechosos o encuentros maliciosos en las redes?						x				x			Parcialmente					
		¿De qué manera protegen los servidores contra el acceso no autorizado y el alojamiento de contenido malicioso:																		
		a) Configuración de servidores					x					x								
		b) Implementa un sistema o nuevas actualizaciones de seguridad					x					x								
		c) Supervisar el rendimiento del servidor de seguridad mediante exámenes periódicos o auditorías							x			x								
		d) Revisa la configuración de seguridad					x					x								
		e) Ejecuta controles de software anti-maliciosos							x			x								
		f) Analizar el contenido alojado y subido regularmente hasta la fecha de controles de software anti-maliciosos							x				x							
		g) Realiza evaluaciones periódicas de vulnerabilidad y las pruebas de seguridad en los sitios en línea y aplicaciones					x					x								
		h) Regularmente escanea en busca de compromisos					x					x								

ANEXO 4.
LISTA DE ENLACES DE LOS SISTEMAS DISTRIBUIDOS EN LAS IES PÚBLICAS DE MANABÍ.

Anexo 4A. Enlaces de los sistemas distribuidos de la UTM.

SISTEMAS WEB	ENLACE
Página web institucional	https://www.utm.edu.ec/
Sga	https://sga.utm.edu.ec/sga/
Sga smna	https://sga.utm.edu.ec/smna/
Biblioteca virtual	https://biblioteca.utm.edu.ec/opac_css/
Utm online	https://online.utm.edu.ec/login/index.php
Sistema de prácticas pre profesionales y pasantías	https://pasantias.utm.edu.ec/
Sistema de inscripciones	https://inscripciones.utm.edu.ec/
Sistema de planificación y control académico	http://spca.utm.edu.ec/
Bienestar estudiantil	https://sga.utm.edu.ec/biestu/
Sistema de becas	https://sga.utm.edu.ec/becas/
Sistema de seguimiento de graduados e inserción laboral Ssgil - utm	https://sga.utm.edu.ec/ssg/
Utm – sipi – sistema de planificacion institucional	https://dpi.utm.edu.ec/planeacion/
Sistema de control y gestion de inventario	https://sga.utm.edu.ec/bodega/home
Sistema de gestion de transporte	https://sga.utm.edu.ec/parqueautomotor/
Siga	https://inscripciones.utm.edu.ec:3000/
Revistas utm	https://revistas.utm.edu.ec/
Zimbra utm	https://mail.utm.edu.ec/
Facultad de ciencias informaticas	https://fci.utm.edu.ec/

Anexo 4B. Enlaces de los sistemas distribuidos de la ULEAM.

SISTEMAS WEB	ENLACE
Página web institucional	http://www.uleam.edu.ec/
Refcale	http://refcale.uleam.edu.ec/
Micrositios instuticonales	http://discapacidades.uleam.edu.ec/?page_id=20
Segup - uleam	https://munayi.uleam.edu.ec/
Departamento de nivelación	http://departamentos.uleam.edu.ec/danu/
Aula virtual	https://aulavirtual.uleam.edu.ec
Observatorio de educación	https://www.uleam.toinn.org/
Sistema de gestión académica	https://sga.uleam.edu.ec/
Observatorio de graduados	http://observatoriograduados.uleam.edu.ec/
Repositorio digital	http://repositorio.uleam.edu.ec/
Talento humano	http://apptalentohumano.uleam.edu.ec:88/vacaciones/app_login/

Anexo 4C. Enlaces de los sistemas distribuidos de la ESPAM MFL.

SISTEMA PRINCIPAL	SUBSISTEMAS	ENLACE
Página web institucional	-	http://ESPAM MFL.edu.ec/
Gestión Académica	Notas y Matricula	http://gestionacademica.ESPAM MFL.edu.ec/
	Asistencia	
	CAAI	
	CI	
	Encuestas	
	Perfil TTHH	
Posgrado	Web	http://posgrado.ESPAM MFL.edu.ec/
	Gestión Maestrías	http://posgrado.ESPAM MFL.edu.ec/login.aspx
	Gestión Admisión	http://posgrado.ESPAM MFL.edu.ec/gestionAdmision/
	Sistema de Evaluación	http://app.ESPAM MFL.edu.ec/EVAposgrado/

	Reactivos Maestrías	
Investigación	PRODIGI	http://192.168.100.23/Panels/FormLogin.aspx
Bienestar	Gestión Medica	http://bienestar.ESPAM MFL.edu.ec/gestionmedica/
Idiomas	B-Learning	http://app.ESPAM MFL.edu.ec/gestionBlended/
Test	Sistema de Evaluación Reactivos	http://app.ESPAM MFL.edu.ec/EVACOMPLEXIVO/
Talento humano	Gestión TTHH	http://talentohumano.ESPAM MFL.edu.ec/
Micro sitio	Idiomas	http://idiomas.ESPAM MFL.edu.ec/
	CAAI	http://caai.ESPAM MFL.edu.ec/
	UPS	http://ups.ESPAM MFL.edu.ec/
Micro sitio	Otros institucionales	http://posgrado.ESPAM MFL.edu.ec http://ESPAM MFL.edu.ec/index.php/administracion-de-empresa/index.php http://web1.ESPAM MFL.edu.ec/index.php/about/pregrado/ingenieria-agricola http://web1.ESPAM MFL.edu.ec/index.php/about/pregrado/administracion-publica http://web1.ESPAM MFL.edu.ec/index.php/about/pregrado/agroindustria http://web1.ESPAM MFL.edu.ec/index.php/about/pregrado/medicina-veterinaria http://web1.ESPAM MFL.edu.ec/index.php/about/pregrado/ingenieria-ambiental http://web1.ESPAM MFL.edu.ec/index.php/about/pregrado/turismo http://web1.ESPAM MFL.edu.ec/ http://computacion.ESPAM MFL.edu.ec
Sistema de Evaluación Reactivos Maestrías	-	http://app.ESPAM MFL.edu.ec/EVAposgrado/
Gestión médica	-	http://bienestar.ESPAM MFL.edu.ec/gestionmedica/
Plan Operativo Anual	-	http://planificación.ESPAM MFL.edu.ec/gestionpoa#!/

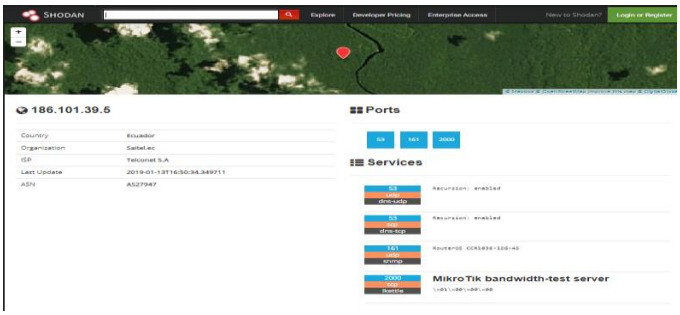
Anexo 4C. Enlaces de los sistemas distribuidos de la UNESUM.

SISTEMAS WEB	ENLACE
Página web UNESUM	http://unesum.edu.ec/
Sistema académico UNESUM	http://sistsau.unesum.edu.ec/
UNESUM online (biblioteca virtual)	http://unesum.edu.ec/bibliotecavirtual/
SIEGEDD evaluación del desempeño del personal académico	http://evaluacion.unesumedu.ec/SIEGEDD/index.php
SSGU Sistemas seguimiento graduados UNESUM	http://graduados.unesum.edu.ec/seguimiento/index.php
Aula virtual	http://aulavirtual.unesum.edu.ec/
Repositorio de la UNESUM	http://repositorio.unesum.edu.ec
Sistema de inventario	http://siu.unesum.edu.ec
Observatorio turístico	http://reports.unesum.edu.ec
Micro sitios institucionales	http://unesum.edu.ec/ingenieriacivil/ http://unesum.edu.ec/ingenieriasistemas/ http://unesum.edu.ec/computacionyredes/ http://unesum.edu.ec/gestionempresarial/ http://unesum.edu.ec/auditoria/ http://unesum.edu.ec/comercio/ http://unesum.edu.ec/ecoturismo/ http://unesum.edu.ec/administracionagropecuaria/ http://unesum.edu.ec/laboratorio/ http://unesum.edu.ec/enfermeria/ http://unesum.edu.ec/agropecuaria/ http://unesum.edu.ec/medioambiente/ http://unesum.edu.ec/forestal/

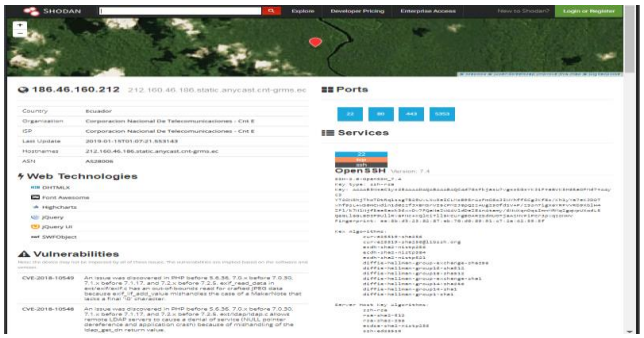
ANEXO 5.
HERRAMIENTAS UTILIZADAS PARA EL ESCANEO DE VULNERABILIDADES EN LOS SISTEMAS DISTRIBUIDOS DE LAS IES PÚBLICAS DE MANABÍ.

Anexo 5A.- Herramienta SHODAN para el Análisis de Vulnerabilidades

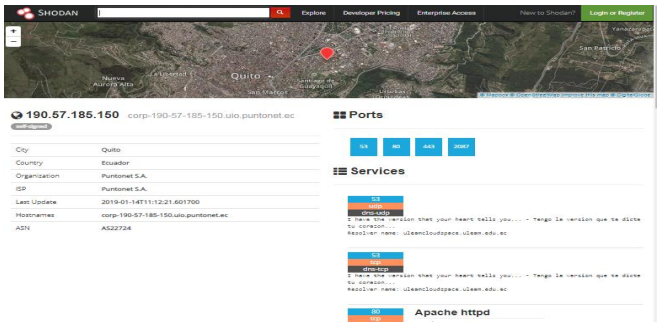
UTM



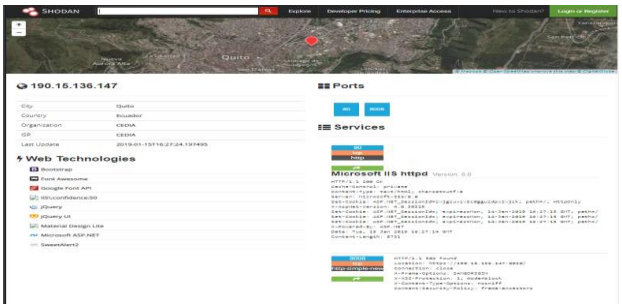
ULEAM



ESPAM MFL



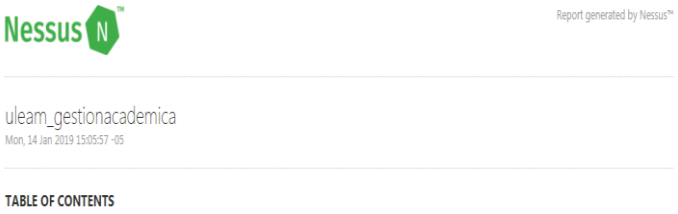
UNESUM



Anexo 5B.- Herramienta NESSUS para el Análisis de Vulnerabilidades

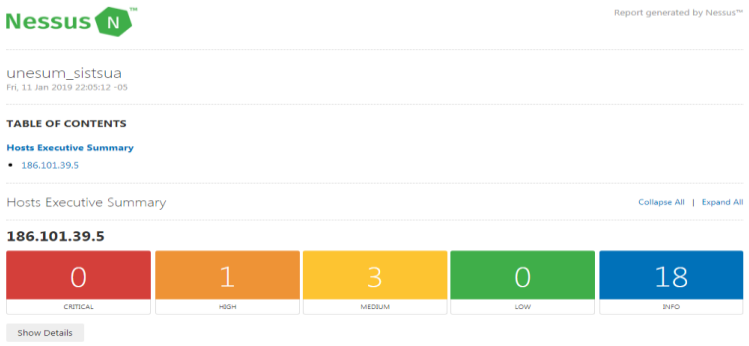
UTM

ULEAM (En mantenimiento).



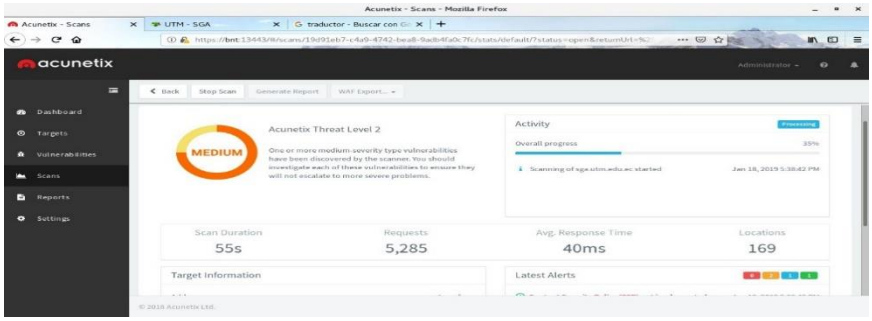
ESPAM MFL

UNESUM

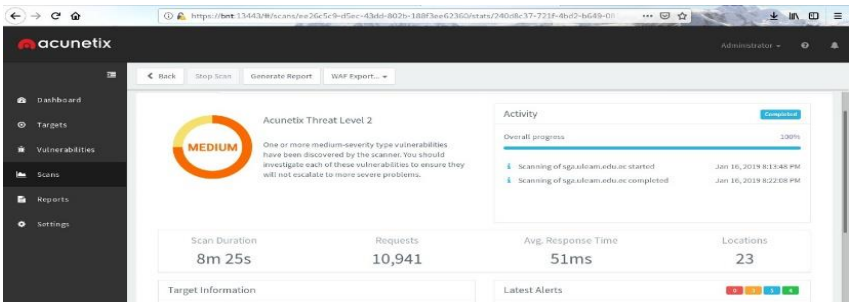


Anexo 5C.- Herramienta ACUNETIX para el Análisis de Vulnerabilidades

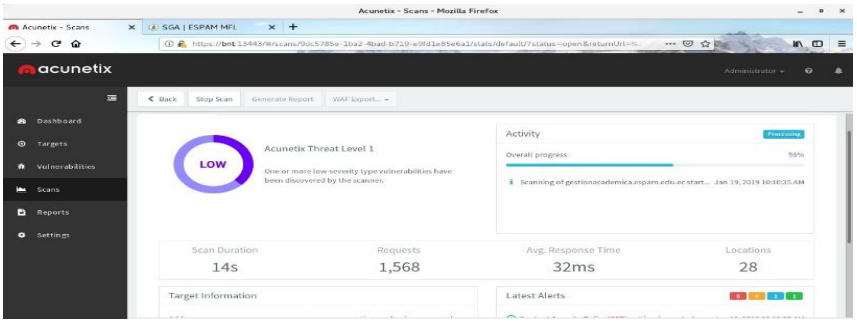
UTM



ULEAM



ESPAM MFL



UNESUM

Scan of unesum.edu.ec

Scan details

Scan information	
Start time	20/01/2019, 00:13:39
Start url	http://unesum.edu.ec/
Host	unesum.edu.ec
Scan time	347 minutes, 10 seconds
Profile	website
Server information	Apache/2.2.15 (CentOS)
Responsive	True
Server OS	Unix
Scan status	aborted

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	127
High	13
Medium	77
Low	31
Informational	6

ANEXO 6.
PONDERACIÓN DE LOS *CHECKLIST* BASADOS EN LA NORMA ISO/IEC 27032 APLICADO A LAS IES PÚBLICAS DE MANABÍ, CLASIFICADAS POR DOMINIOS.

Anexo 6A. Ponderación General de los *Checklist* - dominio Seguridad de la Información.

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD																								
DOMINIO: SEGURIDAD DE LA INFORMACIÓN (protección de la confidencialidad, integridad y disponibilidad de la información en general)																								
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.																								
ÁREA: Tecnología			ESPAM MFL					UTM					ULEAM					UNESUM						
COMPONENTE	SECCIÓN	HITOS	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN		
PARTES INTERESADAS	Universidad como consumidora de proveedores externos	¿La universidad consume servicios en la Web?	x			4	No vulnerable	x			4	No vulnerable	x			4	No vulnerable	x			4	No vulnerable		
		¿Los servicios que consumen son de aplicación?	x			4	No vulnerable	x			4	No vulnerable	x			4	No vulnerable	x			4	No vulnerable		
		Los tipos de servicios que consumen en la Web son:				4	No vulnerable				4	No vulnerable				4	No vulnerable				4	No vulnerable		
		a) Quipux	x					x						x					x					
		b) Sercop	x					x					x					x						
		c) Urkund	x						x				x					x						
		d) Otros servicios	x						x				x		Ministerio de Finanzas, Relaciones laborales, Senecyt									
		Dichos servicios forman parte los siguientes Web Services:									4	No vulnerable				4	No vulnerable				4	No vulnerable		

		a) SOAP							x					x					x			
		b) REST							x				x						x			
		c) XML Web Services	x					x						x				x				
		d) otros							x				x		JASON				x			
		¿La universidad tiene algún proveedor de servicios de Internet?						x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿Cuál de ellos son proveedores de servicios de Internet de la universidad:				**4**					**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) CNT						x														
		b) CEDIA	x										x									
		c) Telconet																x				
		d) Electrocom																				
		e) Grupo TVCable Internet																				
		f) Netlife																				

		g) Perobeli																				
		h) Puntonet																				
		i) iPlanet																				
		j) Clicknet																				
		k) Otros proveedores																				
		¿Los tipos de servicios que les proveen son:									**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Internet	x					x					x					x					
		b) Aplicaciones	x						x				x									
		c) Sitios web	x						x				x									
		d) Otros servicios							x				x									
	Universidad como proveedora	¿La universidad se considera un proveedor de servicios en el ciberespacio?	x					x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		Los servicios de aplicaciones virtuales de uso exclusivo para la institución son:				**4**					**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Gestión Académica	x					x					x					x					

		b) Gestión de Talento Humano	x					x														
		c) Gestión Financiera	x						x													
		d) Gestión de Biblioteca	x					x					x				x					
		e) Gestión Investigación	x						x				x									
		f) Otros servicios							x				x		Vinculación, practicas pre profesionales, evaluación docente							
		Los servicios de aplicaciones y sitios web que brindan a los interesados son:				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Edición de documentos, almacenamiento, distribución.	x																			
		b) Entornos virtuales en línea para interacción con otros usuarios.	x					x					x									
		c) Repositorios en línea de medios digitales con la agregación, búsqueda, catálogo, servicios de pago.	x						x				x					x				
		d) Gestión de recursos empresariales como humanos, finanzas y nóminas, cadena de suministro, facturación.	x						x													
		Llevan registro de control de los servicios que brindan en la Web:	x			**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**

		a) Usuarios						x					x					x				
		b) Contraseñas de usuarios						x					x					x				
		c) Quejas o comentarios de la disponibilidad de estos servicios.						x					x									
ACTIVOS EN EL CIBERESPACIO	**ACTIVOS EN LA ORGANIZACIÓN**	¿Tienen aplicaciones desarrollados e implementados en la universidad?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		Los tipos de aplicaciones o software que se desarrollan son:				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Gerenciales							x													
		b) Académicos	x					x					x					x				
		c) Expertos							x				x									
		d) Otros sistemas	x		financiero			x		RRTT-Bienestar estudiantil												
		¿Realizan la documentación de los sistemas de información desarrollados e implementados?	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**	x		parcialmente	**3**	**Poco vulnerable**	x			**4**	**No vulnerable**
		¿Elaboran manuales de usuario para el manejo de estos sistemas de información?	x		en proceso	**2**	**Vulnerable**		x		**1**	**Muy vulnerable**	x		parcialmente	**3**	**Poco vulnerable**	x			**4**	**No vulnerable**
		¿Protegen la identidad en línea (username, nickname) de los usuarios que se registran para acceder a los sistemas de información?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿Implementan un control de seguridad en los sistemas web?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**
		¿Los sistemas de información se desarrollan e implementan en diferentes infraestructuras de servicios?	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**

		¿Se monitorea el acceso a los sistemas de información web?		x		1	Muy vulnerable	x			1	Muy vulnerable	x			4	No vulnerable		x		1	Muy vulnerable
		¿Los sistemas de información web implementados tienen reservados los derechos de autor o propiedad intelectual (procesos patentados, patentes, resultados de investigación)?	x			4	No vulnerable	x			4	No vulnerable	x			4	No vulnerable		x		1	Muy vulnerable
		¿Disponen de estrategias para la continuidad del negocio (lanzamiento de productos, datos de informes, marketing?		x		2	Vulnerable		x		1	Muy vulnerable	x			4	No vulnerable	x			4	No vulnerable
		¿Existen controles de acceso al data center?	x			4	No vulnerable		x		1	Muy vulnerable	x			4	No vulnerable	x			4	No vulnerable
AMENAZAS CONTRA LA CIBERSEGURIDAD	Amenazas y vulnerabilidades	¿Han sufrido ataques de robo de identidad o robo de información de los usuarios en:				2	Vulnerable		x		4	No vulnerable				3	Poco vulnerable					
		a) Aplicaciones y sitios web											x					x				
		b) Bases de datos																				
		c) Otros ataques	x										x									
		Entre los tipos de ataques que se han presentado en la unidad son:				2	Vulnerable				4	No vulnerable				2	Vulnerable				3	Poco vulnerable
		a) DDoS (Ataque de negación distribuida de servicios)	x										x									
		b) Ingeniería social											x									
		c) DMA (acceso directo a memoria)																				
		d) Eavesdropping (intercepción del tráfico en la red)											x									
		e) Spoofing																				
		f) Phishing											x									
		g) Manipulación de URL																x				
		h) Escalonamiento de privilegios																				
		i) Trashing																				

		j) Shoulder Surfing																				
		k) Decoy																				
		l) DoS (Negación de Servicio)	x										x									
		m) Ataques contraseña																x				
		n) Otros ataques			Ipcheck								x		Inyección de código Html							
		¿Se documentan estos tipos de ataques?	x			**4**	**No vulnerable**				**4**	**No vulnerable**	x		Parcialmente	**3**	**Poco vulnerable**	x			**4**	**No vulnerable**
		¿Tienen medidas de seguridad para disminuir estos ataques?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerables**
		¿Alerta a los usuarios cuando existe algún tipo de ataque o implementación de controles de seguridad?	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**	x		Solo informes a autoridades y dueños de procesos	**3**	**Poco vulnerable**		x		**1**	**Muy vulnerables**
		¿Los atacantes han utilizado código malicioso en archivos intercambiados como un caballo de Troya para sus ataques?		x		**4**	**No vulnerable**		x		**4**	**No vulnerable**		x		**4**	**No vulnerable**		x		**1**	**Muy vulnerables**
		¿Es de conocimiento por parte de los interesados que la seguridad y privacidad según los riesgos involucrados para tomar controles, son relacionadas a la información?	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**	x		Tienen políticas y normas de seguridad de la información	**4**	**No vulnerable**		x		**1**	**Muy vulnerables**
		¿Cómo director/coordinador de la unidad, constata y asegura que la información ha sido clasificada de manera que se evite cometer accidentes en cualquier sitio web en el ciberespacio?	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**	x		Parcialmente, elementos críticos de página web	**3**	**Poco vulnerable**	x			**4**	**No vulnerable**

															institucional							
		¿Efectúa controles de gestión de riesgos de seguridad cibernética en medida y de acuerdo al nivel de madurez de cada proceso?	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**		x		**1**	**Muy vulnerable**		x	actualmente se desarrollan	**2**	**Vulnerable**
		¿Mantiene preparación continua en Ciberseguridad en la institución?		x		**1**	**Muy vulnerable**		x		**1**	**Muy vulnerable**	x		Capacitación individual no fomentada por la universidad	**3**	**Poco vulnerable**		x	actualmente se prepara plan de capacitación	**2**	**Vulnerable**
		¿Se usan técnicas de visualización de datos para presentar información de eventos?		x		**2**	**Vulnerable**		x		**1**	**Muy vulnerable**	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerables**
		¿Se estandarizan los datos en base a normas de calidad?		x		**1**	**Muy vulnerable**	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**		x		**1**	**Muy vulnerables**
		Qué Normas de calidad emplea en la estandarización de sus procesos:		x		**1**	**Muy vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) ISO						x					x		9000							
		b) INEN											x		solo nuevos procesos							
		c) Control Interno												x								
		d) Otras normas												x								
		Se realiza el intercambio de archivos de:		x		**4**	**No vulnerable**		x		**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Mensajería instantánea												x								
		b) Portal web											x					x				

		c) Foro de discusión considerando la seguridad											x									
		¿Se aplican regulaciones de normas en escenarios de seguridad?		x		**1**	**Muy vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x	actualmente en desarrollo	**2**	**Vulnerable**
		Qué normas emplean en escenarios de seguridad de la información:				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) ISO 33000												x								
		b) ISO 8000												x								
		c) ISO 25012												x								
		d) ISO 27001	x					x					x		versión ecuatoriana			x				
		e) ISO 2000																				
		h) ISO 29100																				
		i) ISO 270018																				
		j) ISO 20000-9																				
		k) ISO 22301																				
		l) Otras normas						x		COBIT 5 para sistemas de información												
		¿Qué normas emplean en escenarios de ciberseguridad:		x		**1**	**Muy vulnerable**		x		**1**	**Muy vulnerable**		x		**1**	**Muy vulnerable**				**3**	**Poco vulnerable**
		a) ISO 27032																				
		b) ISO/IEC 27032																				
		c) Otras normas																x				

Anexo 6B. Ponderación General de los *Checklist* - dominio Seguridad de las Aplicaciones.

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD																					
DOMINIO: SEGURIDAD DE LAS APLICACIONES																					
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032																					
ÁREA: Tecnología			ESPAM MFL					UTM					ULEAM					UNESUM				
COMPONENTE	SECCIÓN	HITOS	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN
ACTIVOS EN EL CIBERESPACIO	ACTIVOS EN LA ORGANIZACIÓN	¿El departamento de tecnología cuenta con una metodología y procesos de desarrollo de aplicaciones maduros?		x		2	Vulnerable	x			4	No vulnerable	x			4	No vulnerable		x		1	Muy vulnerable
		¿La universidad cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos		x		2	Vulnerable	x			4	No vulnerable	x		Insuficiente	2	Vulnerable		x		2	Vulnerable

		que implican las ciberamenazas?																		
		¿Tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción?		x		**1**	**Muy vulnerable**		x		**1**	**Muy vulnerable**	x		Lo provee el marco de trabajo	**4**	**No vulnerable**		x		**1**	**Muy vulnerable**
		¿El departamento de tecnología ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar		x		**2**	**Vulnerable**		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**		x		**1**	**Muy vulnerable**

		continuamente la práctica?																			
		¿Se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable?		x		**2**	**Vulnerable**		x		**2**	**Vulnerable**	x		Test no formales -CEDIA (Nessus)	**4**	**No vulnerable**		x		**1**	**Muy vulnerable**
		¿La unidad tiene un analista entrenado para correlacionar y evaluar los hallazgos de vulnerabilidades existentes en las aplicaciones?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x		No específico sino en su ámbito de aplicación	**3**	**Poco vulnerable**		x		**2**	**Vulnerable**
		¿Qué tipo de aplicaciones se desarrollan en la unidad:									**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Móviles						x					x									

		b) Web		x				x					x						x		
		c) Otros											x		Win 32						
		¿Qué tipo de herramientas tecnológicas utiliza la unidad para realizar pruebas de vulnerabilidades:		x		**2**	**Vulnerable**				**4**	**No vulnerable**		x	Para fuerza de código no solo Nessus	**3**	**Poco vulnerable**				**1**	**Muy vulnerable**
		a) SAST (Static application security testing).- Analiza pasivamente el código fuente o binario de una aplicación en busca de vulnerabilidades conocidas.						x											x		
		b) DAST (Dynamic application security testing).- Prueba y analiza una aplicación en ejecución en busca de comportamientos que indiquen																	x		

		posibles vulnerabilidades.																			
		c) RASP (Runtime application self-protection).- Herramienta de autoprotección integrada en la aplicación durante su ejecución, permite monitorearse a sí misma para evitar ataques en tiempo real.																	x		
		d) SCA (Software composition analysis).- Identifica, evalúa y monitoriza todos los componentes de terceros (cadena de suministros del software) que puedan contener																	x		

		vulnerabilidades.																				
		¿La unidad tiene firewalls de aplicaciones?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x		Provee CEDIA no implementado	**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿Qué tipo de firewall tienen:				**4**	**No vulnerable**				**3**	**Poco vulnerable**				**3**	**Poco vulnerable**				**3**	**Poco vulnerable**
		a) Firewall de aplicaciones de red	x					x														
		b) Host apllication firewall	x						x									x				
		c) Firewall de aplicaciones web	x					x					x									
		¿Se han eliminado servicios y protocolos innecesarios e inseguros para disminuir el ataque cibernético?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**

		¿Ha considerado la protección avanzada de antivirus o agentes que usen detección y protección basada en comportamiento e inteligencia artificial (AI)?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿Se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen las aplicaciones tanto internas como externas?		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**	x		Proyecto de Tesis estudiantil	**4**	**No vulnerable**		x		**2**	**Vulnerable**
AMENAZAS CONTRA LA SEGURIDAD DEL CIBERESPACIO	**Amenazas y Vulnerabilidades**	¿Se establecen responsables y procedimientos formales de aplicación		x		**2**	**Vulnerable**		x		**2**	**Vulnerable**	x		Parcialmente	**3**	**Poco vulnerable**		x		**2**	**Vulnerable**

		de seguridad en los equipos tecnológicos y software?																			
		¿Se aprueban de manera formal los cambios de equipos tecnológicos y software?		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**
		¿Se prohíbe el uso de software no autorizado por la institución?		x		**3**	**Poco vulnerable**		x		**3**	**Poco vulnerable**		x		**3**	**Poco vulnerable**	x			**4**	**No vulnerable**
		¿Se instalan y actualizan periódicamente software de antivirus, firewall contra código malicioso?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**
		¿Se mantienen los sistemas operativos actualizados con las últimas versiones?		x		**3**	**Poco vulnerable**		x		**3**	**Poco vulnerable**	x		No todos, porque no se han hecho pruebas de actualización	**3**	**Poco vulnerable**		x		**3**	**Poco vulnerable**

		¿Posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos?		x		**2**	**Vulnerable**		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**
		¿Tienen sitios web legítimos que han sido hackeados?		x		**4**	**No vulnerable**		x		**4**	**No vulnerable**	x			**2**	**Vulnerable**	x			**2**	**Vulnerable**
		¿Se realiza informes de eventos sospechosos o encuentros maliciosos en las aplicaciones?	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**	x		Parcialmente	**3**	**Poco vulnerable**	x			**4**	**No vulnerable**
		¿El equipo de desarrollo aplica seguimientos o revisión en los mensajes recibidos en el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas?		x		**2**	**Vulnerable**		x		**2**	**Vulnerable**		x	Operaciones lo realiza	**4**	**No vulnerable**		x		**2**	**Vulnerable**

		Se toman en cuenta los controles de nivel de aplicación:				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Exposición de avisos cortos							x				x									
		b) Manipulación segura de sesiones	x					x					x						x				
		c) Validación de entrada segura y prevención de ataques (SQL Inyeccion)	x					x					x						x				
		d) Scripting o encriptación en sitios o aplicaciones web						x					x							x			
		e) Servicio de la organización o autenticación del servicio						x					x							x			
		¿Se logra los objetivos desarrollados en base a la sensibilización y formación:		x		**2**	**Vulnerable**				**2**	**Vulnerable**				**3**	**Poco vulnerable**				**2**	**Vulnerable**

		a) Proporciona informes periódicos sobre el estado de la Ciberseguridad							x				x							x		
		b) Sesiones de formación enfocados en escenarios simulados de ataque cibernéticos o talleres sobre áreas requeridas de acciones especificas							x					x						x		
		c) Pruebas regulares con recorridos en escenarios permanentes							x				x		Parcialmente					x		

Anexo 6C. Ponderación General de los *Checklist* - dominio Seguridad de las Redes.

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD																						
DOMINIO: SEGURIDAD DE LAS REDES (diseño, implementación y operación de redes para lograr los propósitos de seguridad de la información en las redes dentro de las organizaciones, entre las organizaciones, y entre las organizaciones y los usuarios)																						
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.																						
			ESPAM MFL					UTM				ULEAM					UNESUM					
COMPONENTE	SECCIÓN	HITOS	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN	S	N	OBSERVACIÓN	PONDERACIÓN	IDENTIFICACIÓN
ACTIVOS EN EL CIBERESPACIO	ACTIVOS EN LA ORGANIZACIÓN	¿Aplican seguridad en la red?	x			4	No vulnerable		x	Solicitud en proceso	2	Vulnerable	x			4	No vulnerable		x		1	Muy Vulnerable
		Entre las políticas, procedimientos y controles que tiene la unidad para seguridad de la red están:		x	en proceso de aprobación	2	Vulnerable				3	Poco vulnerable				4	No vulnerable		x		1	Muy Vulnerable
		a) Políticas de control de acceso a la red							x				x						x			
		b) Controles de acceso a los servidores						x					x						x			
		c) Procedimientos de respaldo de información cuando existe pérdida debido a fallos físicos						x					x						x			

		d) Control de los filtros de tráfico entre la red interna y la externa							x	en proceso			x						x		
		¿Existen controles que restrinjan la dirección MAC de cada equipo?		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿Tienen acceso restringido a las redes inalámbricas?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**
		¿Tienen protocolos de autenticación de computadoras dentro de la red?		x		**2**	**Vulnerable**		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**
		¿Se realiza el proceso de autentificación de los usuarios antes de dejarlos entrar a la aplicación?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x		**2**	**Vulnerable**
		¿Utilizan mecanismos de encriptación para mantener la confidencialidad e integridad de los datos que se están transmitiendo en la web?	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿Qué método de encriptación utiliza:				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) Encriptación simétrica (Data Encryption Estándar - DES)	x						x					x					x			
		b) Encriptación asimétrica (llave pública, llave privada)						x					x					x				
AMENAZAS CONTRA LA SEGURIDAD DEL CIBERESPACIO	**Amenazas y Vulnerabilidades**	¿Utilizan protocolos de comunicación como :				**2**	**Vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**				**4**	**No vulnerable**
		a) HTTP	x					x					x									
		b) HTTPS						x					x					x				

		c) MAILTO						x					x								
		d) FTP						x					x								
		¿Como director /coordinador de la unidad se asegura que la URL de su contenido web este citado como un enlace seguro en su navegador?		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**
		¿El SSL que utiliza el sitio web, identifica el contenido original del nuevo contenido dañado, plantado por un atacante?		x		**2**	**Vulnerable**	x			**4**	**No vulnerable**	x			**4**	**No vulnerable**		x		**4**	**No vulnerable**
		Entre los tipos de ataques en la seguridad de la red que han sufrido están:		x		**4**	**No vulnerable**				**2**	**Vulnerable**				**3**	**Poco vulnerable**				**2**	**Vulnerable**
		a) Interrupción: destrucción física de equipos, borrado de aplicaciones, falla de sistema operativo, etc.						x						x					x		
		b) Intercepción: reproducción ilícita de archivos, intercepción de los cables para monitoreo de datos en una red, etc.						x						x					x		
		c) Modificación: modificaciones de bases de datos, cambios en la configuraciones de software del sistema, etc.							x					x				x			

		d) Fabricación: insertar registros en bases de datos, añadir transacciones a un sistema de comunicaciones, etc.							x				x							x			
		¿ La unidad tiene medidas de prevención y respuestas a los ataques cibernéticos?		x		1	Muy vulnerable	x			4	No vulnerable	x		En algunos casos hay protocolos y en otros casos no	3	Poco vulnerable		x		1	Muy vulnerable
		Ha tenido atacantes que se hacen pasar por una entidad autorizada para robar información como:		x		4	No vulnerable		x		4	No vulnerable		x		4	No vulnerable		x		4	No vulnerable
		a) Hombre en el medio (Man in the maddle)																			
		b) Otro tipo de robo de información																			
		¿Se toman medidas de autenticación de comunicación para evitar el ataque de Man in the Midle?	x			4	No vulnerable		x		2	Vulnerable	x			4	No vulnerable	x			4	No vulnerable
		¿Han sufrido ataques de IP Spoofing para manipular las direcciones IP asociadas a los mensajes en un intento de disfrazar el ataque como fuente conocida para ganar el acceso no autorizado a los sistemas?		x		4	No vulnerable		x		4	No vulnerable		x		4	No vulnerable		x		4	No vulnerable

		Las redes WIFI en la institución están protegidas en:				4	No vulnerable				4	No vulnerable				4	No vulnerable				4	No vulnerable
		a) WIFI Gestionado (portal cautivo)		x					x				x						x			
		b) Claves de acceso a WIFI	x					x						x					x			
		c) Otros tipos de protección	x						x					x					x			
		d) Protocolos para Redes abiertas	x					x						x				x				
		¿Se han vistos comprometidos los servidores en Internet con el método de desbordamiento de búfer provocando que el servidor funcione fuera de su entorno normal (control), facilitando la inserción / ejecución de código malicioso?		x		4	No vulnerable	x			2	Vulnerable		x		4	No vulnerable		x		4	No vulnerable
		¿Se realiza informes de eventos sospechosos o encuentros maliciosos en las redes?		x		1	Muy vulnerable		x		1	Muy vulnerable	x		Parcialmente	3	Poco vulnerable		x		2	Vulnerable
		¿De qué manera protegen los servidores contra el acceso no autorizado y el alojamiento de contenido malicioso:				4	No vulnerable				4	No vulnerable				4	No vulnerable				2	Vulnerable
		a) Configuración de servidores	x					x					x					x				

		b) Implementa un sistema o nuevas actualizaciones de seguridad		x				x					x						x			
		c) Supervisar el rendimiento del servidor de seguridad mediante exámenes periódicos o auditorías	x										x						x			
		d) Revisa la configuración de seguridad	x					x					x						x			
		e) Ejecuta controles de software anti-maliciosos		x									x						x			
		f) Analizar el contenido alojado y subido regularmente hasta la fecha de controles de software anti-maliciosos		x										x					x			
		g) Realiza evaluaciones periódicas de vulnerabilidad y las pruebas de seguridad en los sitios en línea y aplicaciones		x				x					x						x			
		h) Regularmente escanea en busca de compromisos		x				x					x						x			

ANEXO 7.
MATRIZ ANÁLISIS MODAL DE FALLOS Y EVENTOS (AMFE) POR DOMINIOS DE CIBERSEGURIDAD.

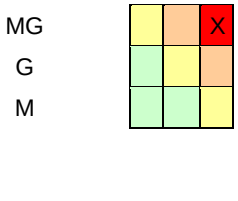
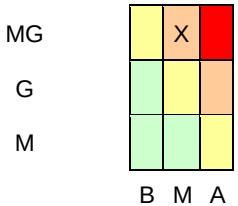
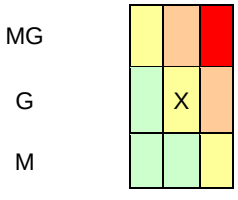
Anexo 7A.- Matriz de riesgos AMFE – Dominio Seguridad de la Información

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.1.1.	No se monitorea el acceso a los sistemas de información web.	Alto 3	Grave 2	Alto	MG G M B M A (X en G-A)	Coordinador TI	A.1.1.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Reportes de acceso a los sistemas mediante autenticación de usuario.
R.1.2.	No se mantiene preparación continua en Ciberseguridad en la institución.	Alto 3	Muy Grave 3	Critico	MG G M B M A (X en MG-A)	Coordinador TI	A.1.2.1	Capacitar al personal de TI en ciberseguridad de manera continua.	Capacitación a Congresos, seminarios, Talleres de seguridad informática.
R.1.3.	No se estandarizan los datos en base a normas de calidad.	Alto 3	Muy Grave 3	Critico	MG G M B M A (X en MG-A)	Coordinador TI	A.1.3.1	Estandarizar la gestión de calidad de los procesos de la información mediante normas de calidad.	Mejorar la calidad de los procesos de seguridad de la información en el ciberespacio
R.1.4.	No emplean normas de calidad como ISO, INEN, Control interno,	Alto 3	Muy Grave 3	Critico	MG G M (X en MG-A)	Coordinador TI	A.1.4.1	Implementar Normas de calidad como ISO 9000 y normas de control interno 410-09 para mejorar la calidad de los servicios y	Mejorar la gestión de calidad de los procesos y

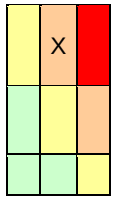
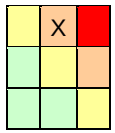
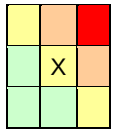
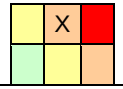
	entre otras para la estandarización de sus procesos.				B M A			brindar seguridad en sus procesos.	seguridad de la información
R.1.5.	No aplican regulaciones de normas en escenarios de seguridad.	Alto 3	Muy Grave 3	Critico	MG G M (X) B M A	Coordinador TI	A.1.5.1	Aplicar Normas de Control Interno 410-09 de TI de la Contraloría General del Estado ecuatoriano para escenarios de seguridad.	Complementar con norma ISO/IEC 27001 Sistema de Gestión de Seguridad de la información
R.1.6.	No se alerta a los usuarios cuando exite algún tipo de ataque o implementación de controles de seguridad.	Alto 3	Grave 2	Alto	MG G (X) M B M A	Coordinador TI	A.1.6.1	Informar a los usuarios de los controles de seguridad en los sistemas y de los ataques que se han presentado en los mismos a nivel institucional.	Reporte e informe de ataques y controles de seguridad a los usuarios.
R. 1.7.	No emplean normas en escenarios de ciberseguridad.	Alto 3	Muy Grave 3	Critico	MG (X) G M B M A	Coordinador TI	A.1.7.1	Seguir el plan propuesto de Ciberseguridad	Mejorar el escenario de ciberseguridad
R.1.8.	Los manuales de usuario para el manejo de los sistemas de información están en proceso de elaboración.	Medio 2	Grave 2	Medio	MG G (X) M B M A	Coordinador TI	A.1.8.1	Implementar manuales de usuarios para el uso efectivo de los sistemas o aplicaciones web.	Aplicar controles internos periódicos de cumplimiento.
R.1.9	No se llevan a cabo los datos de	Medio	Grave	Medio	MG	Coordinador TI	A.1.9.1	Elaborar estrategias para mejorar los servicios TI.	PETI (Plan estratégico de

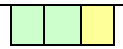
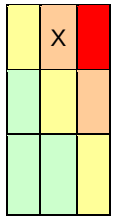
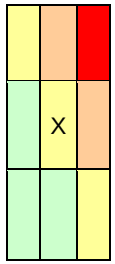
	informes como estrategia para la continuidad del negocio.				G / M × B M A				Tecnologías de Información)
		2	2						
R.1.10.	Han sufrido ataques de robo de identidad o robo de información de los usuarios en Aplicaciones web.	Medio	Grave	Medio	MG / G × / M × B M A	Coordinador TI	A.1.10.1	Elaborar medidas de prevención contra ataques de robo de información de los usuarios en aplicaciones web.	Mejorar la seguridad de las aplicaciones.
		2	2						
R.1.11.	Los tipos de ataques que se han presentado en la unidad son: DDoS, Dos.	Alto	Muy Grave	Critico	MG × / G / M B M A	Coordinador TI	A.1.11.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Mejorar el escenario de Ciberseguridad
		3	3						
R.1.12.	No se usan técnicas de visualización de datos para presentar información de eventos.	Medio	Grave	Medio	MG / G × / M B M A	Coordinador TI	A.1.12.1	Elaborar técnicas de visualización de datos para verificar la pérdida de información.	Escalabilidad y disponibilidad de las aplicaciones.
		2	2						

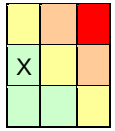
Anexo 7B.- Matriz de riesgos AMFE – Dominio Seguridad de las Aplicaciones

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.2.1	No tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción.	Alto 3	Muy Grave 3	Critico		Área de desarrollo de aplicaciones	A.2.1.1	Elaborar un plan de seguridad para todo el ciclo de desarrollo, prueba, y retroalimentación de las aplicaciones	Madurez en los procesos de desarrollo de aplicaciones.
R.2.2.	El departamento de tecnología no cuenta con una metodología y procesos de desarrollo de aplicaciones maduros.	Medio 2	Muy Grave 3	Alto		Área de desarrollo de aplicaciones	A.2.2.1	Elaborar flujogramas de procesos de desarrollo con metodologías ágiles como SCRUM.	Mejora de los procesos de desarrollo de aplicaciones.
R.2.3.	La universidad no cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los	Medio 2	Grave 2	Medio		Área de desarrollo de aplicaciones	A.2.3.1	Contratar talento humano especializado o capacitar al personal necesario en seguridad de las aplicaciones.	Contrarrestar los riesgos que implican las ciberamenazas .

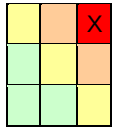
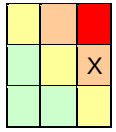
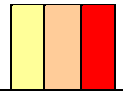
	riesgos que implican las ciberamenazas.								
R.2.4	El departamento de tecnología no ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar continuamente la práctica.	Medio 2	Grave 2	Medio	MG G M B M A	Área de desarrollo de aplicaciones	A.2.4.1	Elaborar un protocolo de autoevaluación de control para la efectividad de la seguridad de las aplicaciones.	Trabajar con la norma de seguridad de las aplicaciones ISO/IEC 27034
R.2.5.	No se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable.	Medio 2	Muy Grave 3	Alto	MG G M B M A	Área de desarrollo de aplicaciones	A.2.5.1	Utilizar las herramientas tecnológicas que brinda la norma ISO/IEC 27032 de ciberseguridad para efectuar pruebas de vulnerabilidades en las aplicaciones.	Nessus, Acunetix, Shodan
R.2.6.	No utilizan herramientas tecnológicas como SAST, DAST, RASP, SCA para realizar pruebas de vulnerabilidades.	Medio 2	Grave 2	Medio	MG G M B M A	Área de desarrollo de aplicaciones	A.2.6.1	Aplicar al menos una de estas herramientas o en su defecto utilizar las herramientas que sugiere la norma ISO/IEC 27032 de ciberseguridad.	Pruebas regulares con estas herramientas para detectar vulnerabilidades.

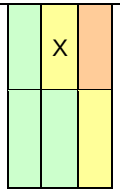
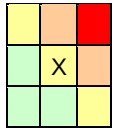
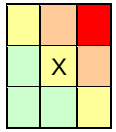
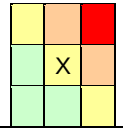
R.2.7.	No se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto internas como externas.	Medio 2	Muy Grave 3	Alto	MG G M  B M A	Área de desarrollo de aplicaciones	A.2.7.1	Implementar esta prueba de pentest para verificar las medidas de seguridad de las aplicaciones, red, plataforma de alojamiento, aplicación o sistemas web.	Proteger las aplicaciones de ataques cibernéticos.
R.2.8.	No se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software.	Medio 2	Muy Grave 3	Alto	MG G M  B M A	Área de desarrollo de aplicaciones y Coordinador TI	A.2.8.1	Establecer responsabilidades y procedimientos formales a custodios de los equipos tecnológicos y software para el buen uso y seguridad de las aplicaciones.	Políticas de seguridad de los equipos tecnológicos y software a cargo de los custodios.
R.2.9.	No se aprueban de manera formal los cambios de equipos tecnológicos y software.	Medio 2	Grave 2	Medio	MG S M  B M A	Coordinador TI	A.2.9.1	Elaborar actas de entrega-recepción de equipos tecnológicos cuando haya cambios de custodios.	Seguridad en los cambios de equipos tecnológicos y software.
R.2.10.	La unidad no posee alertas o fallas de los sistemas de	Medio	Muy Grave	Alto	MG S 	Área de desarrollo de aplicaciones y	A.2.10.1	Realizar reportes o informes de eventos maliciosos o	Mantener la seguridad de los sistemas en el ciberespacio.

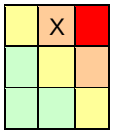
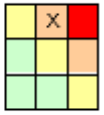
	información, sitios web, equipos tecnológicos.	2	3		M  B M A	Coordinador TI		fallas en los sistemas de información, sitios web, equipos tecnológicos.	
R.2.11.	El equipo de desarrollo no aplica seguimientos o revisión en los mensajes recibidos en el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas.	Medio	Muy Grave	Alto	MG S M  B M A	Área de desarrollo de aplicaciones y Área de Redes	A.2.11.1	Asegurar que los mensajes recibidos en los sitios web no contengan contenido malicioso, enlaces de sitios web de phishing o descargas maliciosas.	Seguimiento de la seguridad de las aplicaciones.
		2	3						
R.2.12.	No se logra los objetivos desarrollados en base a la sensibilización y formación en proporcionar informes periódicos sobre el estado de la Ciberseguridad, Sesiones de formación enfocada en escenarios simulados de ataque cibernética o talleres sobre	Medio	Grave	Medio	MG G M  B M A	Coordinador TI	A.2.12.1	Considerar como objetivos de sensibilización y formación a informes periódicos sobre el estado de ciberseguridad, enfoques de escenarios simulados de ataques cibernéticos o talleres de acciones específicas y pruebas regulares en	Mejorar la ciberseguridad.
		2	2						

	áreas requeridas de acciones específicas y tampoco en pruebas regulares con recorridos en escenarios permanentes.							escenarios permanentes.	
R.2.13.	No se prohíbe el uso de software no autorizado por la institución.	Bajo 1	Grave 2	Bajo	MG G M  B M A	Coordinador TI	A.2.13.1	Usar software legal o software libre según lo requiera la aplicación a desarrollar.	Visual, SQL, Windows, Linux
R.2.14.	No se mantienen los sistemas operativos actualizados con las últimas versiones.	Bajo	Menor	Bajo		Coordinador TI	A.2.14.1	Mantener actualizados los sistemas operativos de acuerdo a las características de los equipos.	Mejorar la productividad del desarrollo de aplicaciones.

Anexo 7C.- Matriz de riesgos AMFE – Dominio Seguridad de las Redes

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R. 3.1.	La unidad no tiene medidas de prevención y respuestas a los ataques cibernéticos.	Alto 3	Muy Grave 3	Critico	MG G M  B M A	Coordinador TI	A.3.1.1	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Controlar los ataques cibernéticos.
R.3.2.	No se realiza informes de eventos sospechosos o encuentros maliciosos en las redes.	Alto 3	Grave 2	Alto	MG G M  B M A	Coordinador TI y Área de Redes	A.3.2.1	Elaborar o adquirir una herramienta que permita detectar eventos maliciosos en las redes y emitan reportes de los mismos.	Informes mensuales de eventos sospechosos o maliciosos en las redes.
R.3.4.	Entre las políticas, procedimientos y controles que están en proceso de aprobación en	Medio	Grave	Medio	MG 	Coordinador TI, Área de Redes y Área de Datos (Data Center)	A.3.4.1	Agilizar el proceso de aprobación de las políticas, procedimientos y controles	Política de control de acceso, política de filtros de tráfico en la

	la unidad para seguridad de la red están: Políticas de control de acceso a la red, controles de acceso a los servidores, procedimientos de respaldo de la información cuando existen pérdidas de fallos físicos, control de filtros de tráfico en la red interna y externa.	2	2		G M  B M A			de la seguridad de la red.	red interna y externa.
R.3.5.	No tienen protocolos de autenticación de computadoras dentro de la red.	Medio 2	Grave 2	Medio	MG G M  B M A	Área de Redes.	A.3.5.1	Utilizar protocolos de autenticación de computadoras dentro de la red para evitar posibles ataques.	Evitar los ataques de Man in the middle.
R.3.6.	No existen controles que restrinjan la dirección MAC de cada equipo.	Medio 2	Grave 2	Medio	MG G M  B M A	Área de Redes.	A.3.6.1	Autenticar los equipos para que haya mayor control y seguridad en la comunicación entre equipos.	Mejorar la seguridad en las redes.
R.3.7.	El director /coordinador de la unidad no se asegura que la URL de su	Medio 2	Grave 2	Medio	MG G M 	Coordinador TI	A.3.7.1	Asegurar que toda la información que vaya a subirse en una	Proteger la información en el ciberespacio

	contenido web este citado como un enlace seguro en su navegador.				B M A			aplicación web, debe estar con un enlace seguro en la URL. Como HTTPS.	
R.3.8.	El SSL que utiliza el sitio web, no identifica el contenido original del nuevo contenido dañado, plantado por un atacante.	Medio 2	Muy Grave 3	Alto	MG S M  B M A	Área de Redes.	A.3.8.1	Verificar que el tráfico de la información esté cifrado para evitar ataques como DDoS.	SSL certificado.
R.3.9.	Utilizan protocolos de comunicación como HTTP.	Medio	Muy Grave	Alto	MG S M  B M A	Área de Redes y Área de desarrollo de aplicaciones.	A.3.9.1	Utilizar protocolos de comunicación seguro en el ciberespacio como HTTPS.	Mejorar la Seguridad en la transmisión de datos en las redes.

ANEXO 8.
PLAN DE ACCIÓN DE CIBERSEGURIDAD PARA LAS IES PÚBLICAS DE MANABÍ.

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

PLAN DE ACCIÓN DE CIBERSEGURIDAD APLICADO A LA ESPAM MFL SEGÚN LA NORMA ISO/IEC27032

MAYO 2019

CONTENIDO

1. INTRODUCCIÓN

El objetivo de presente documento es definir un plan de acción de Ciberseguridad, que permita mejorar aspectos de seguridad, disponibilidad y confidencialidad en los sistemas distribuidos de las Instituciones de Educación Superior Públicas de Manabí, mediante la descripción de controles y mecanismos de seguridad que deben ser aplicados según la Norma ISO/IEC27032.

El mismo describe las vulnerabilidades presentes en los sistemas distribuidos previamente analizados, mediante el uso de herramientas de escaneo y por una matriz de riesgos según la metodología Análisis Modal de Fallos y Efectos (AMFE), que detalla cada una de estas vulnerabilidades por institución, dominio y nivel de criterio.

Al realizar este Plan de Acción de Ciberseguridad, se pretende socializar con la ESPAM MFL, que previo a la autorización, formo parte de este trabajo, el hecho de tomar medidas mediante estrategias que permitan mejorar en conocimientos de Ciberseguridad y mitigar los posibles riesgos que presentan las vulnerabilidades y estas a su vez pueden ser propensas a eventos maliciosos o sospechosos en la seguridad de la información, seguridad de las aplicaciones y seguridad de las redes; con el desarrollo del plan se espera aplicar técnicas propuestas por la norma ISO/ICE 27032, que permitan mitigar riesgos de ciberseguridad en los sistemas distribuidos, para mejorar la seguridad de la información y amenazas de posibles ataques.

2. ALCANCE

Este plan de acción abarca lo siguiente:

- Identificación de las vulnerabilidades de los sistemas distribuidos en las Instituciones de Educación Superior Públicas en Manabí.
- Identificación de los riesgos mediante la metodología AMFE.
- Análisis y evaluación de los riesgos encontrados en el cumplimiento de la Norma ISO/IEC 27032 de Ciberseguridad y herramientas web Shodan, Nessus y Acunetix.
- Políticas de Ciberseguridad para mitigar los riesgos encontrados.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Desarrollar un Plan de acción que permita mejorar el estado de Ciberseguridad de los sistemas distribuidos de las instituciones públicas de educación superior de Manabí.

3.2. OBJETIVOS ESPECÍFICOS

- Definir vulnerabilidades de Ciberseguridad en los sistemas distribuidos de las instituciones públicas de educación superior de Manabí, basados en el estándar ISO/IEC 27032.
- Identificar los riesgos en aspectos de seguridad, disponibilidad y confidencialidad en los sistemas distribuidos que se encuentran alojado en la Web.
- Proponer estrategias preventivas y correctivas que permitan mejorar el estado Ciberseguridad en cuanto a los riesgos que podrían ocasionar por cada una de las IES Públicas de Manabí.

4. LA NATURALEZA DEL CIBERESPACIO

El ciberespacio puede ser descrito como un entorno virtual, que no existe en cualquier forma física, sino más bien, un entorno complejo o en el espacio resultante de la aparición de Internet, además de las personas, organizaciones y actividades de todo tipo de aparatos de tecnología y redes que están conectados a él. La seguridad en el ciberespacio, o la seguridad cibernética, es la seguridad de este mundo virtual (ISO, 2012), en donde continuamente se ve afectado por ataques de diferentes índoles, los mismos que se pueden observar mediante la herramienta Digital Attack Map, en la figura 1, el análisis de estos mediante un sistema de monitorización de amenaza global o Arbor Networks y cuya actualización es diaria.

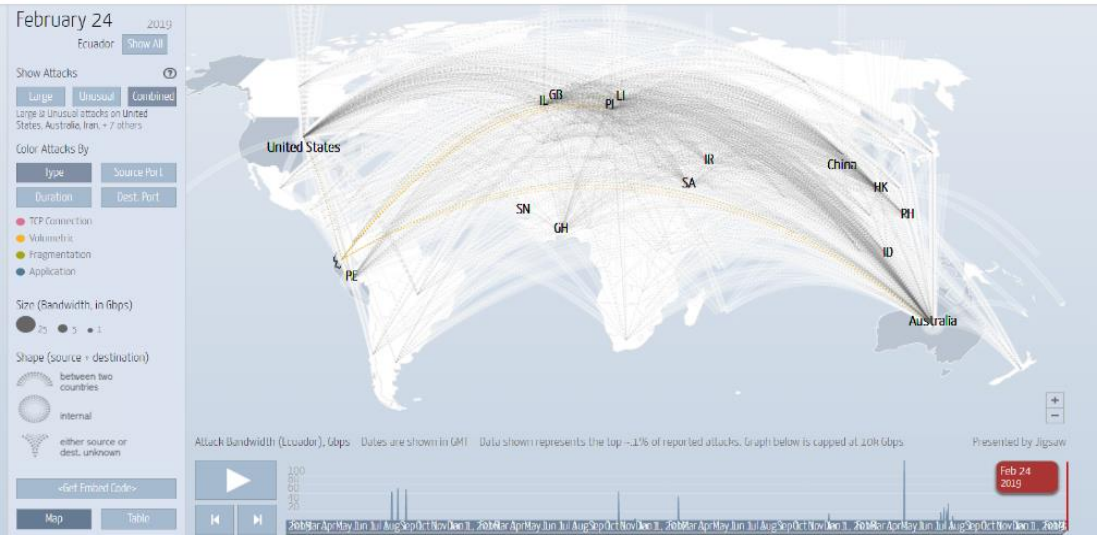


Figura 1. Análisis general de amenazas a nivel mundial
Fuente: Digital Attack Map

Dado a esto, la Ciberseguridad es la encargada de proteger la información, manteniendo la integridad y disponibilidad de esta, brindando confianza al momento de interactuar el usuario en la información con los sistemas distribuidos en el Ciberespacio.

Figura 2. Ciberseguridad: Riesgos y Amenazas
Fuente: (Rajoy, s.f.)

5. LA NATURALEZA DE LA CIBERSEGURIDAD

Según la ISO (2012), la Ciberseguridad se basa en la seguridad de la información, seguridad de aplicaciones, seguridad de red y de seguridad de Internet como bloques de construcción fundamentales. La seguridad cibernética es una de las actividades necesarias para la protección de infraestructuras críticas, y, al mismo tiempo, una protección adecuada de los servicios de infraestructura crítica contribuye a las necesidades básicas de seguridad (es decir, seguridad, fiabilidad y disponibilidad de la infraestructura crítica) para la consecución de los objetivos de la seguridad cibernética.

Sin embargo, la seguridad cibernética, no es sinónimo de seguridad de Internet, seguridad de red, seguridad de aplicaciones, seguridad de la información, o la protección de infraestructuras críticas. Tiene un alcance único que requiere partes interesadas a desempeñar un papel activo con el fin de mantener, si no mejora la utilidad y confiabilidad del ciberespacio. Esta Norma Internacional se

diferencia ciberseguridad y los otros dominios de la seguridad de la siguiente manera:

- Seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información en general, para servir a las necesidades del usuario la información aplicable.
- Seguridad de las aplicaciones es un proceso realizado para aplicar los controles y mediciones para aplicaciones de una organización con el fin de gestionar el riesgo de su uso. Controles y mediciones se pueden aplicar a la propia aplicación (sus procesos, componentes, software y resultados), a sus datos (datos de configuración, datos de usuario, datos de la organización), y para toda la tecnología, los procesos y los actores que participan en el ciclo de vida de la aplicación.
- Seguridad de la red se refiere al diseño, implementación y operación de redes para lograr los propósitos de seguridad de la información en las redes dentro de las organizaciones, entre las organizaciones, y entre las organizaciones y los usuarios.
- Seguridad en Internet tiene que ver con la protección de los servicios relacionados con Internet y los sistemas de TIC y redes conexas como una extensión de la seguridad de la red en las organizaciones y en el hogar, para lograr el propósito de la seguridad. La seguridad en Internet también garantiza la disponibilidad y fiabilidad de los servicios de Internet.
- La Protección de Infraestructuras Críticas de Información (PICI), se ocupa de la protección de los sistemas que se proporcionan y son operados por los proveedores de infraestructura crítica, como la energía, las telecomunicaciones, y los departamentos de agua. PICI asegura que esos sistemas y redes están protegidos y resistente contra los riesgos de seguridad de la información, los riesgos de seguridad de red, los riesgos de seguridad en Internet, así como los riesgos de seguridad cibernética.

La Figura 2 resume la relación entre Ciberseguridad y otros dominios de seguridad. La relación entre estos dominios de seguridad y la ciberseguridad es compleja.

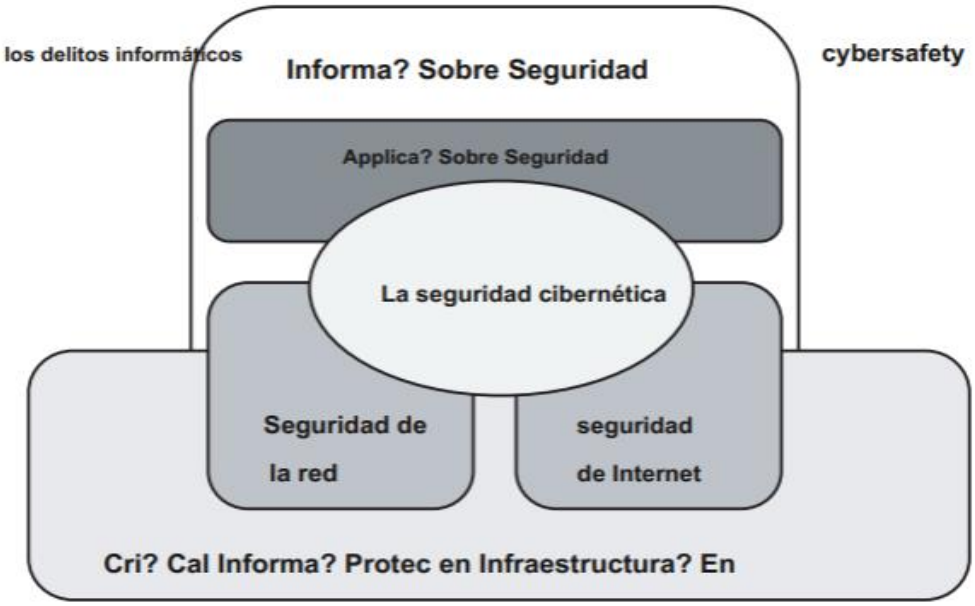


Figura 3. Relación entre Ciberseguridad y otros dominios de seguridad
Fuente: ISO (2012).

Por otro lado, la disponibilidad y la fiabilidad del ciberespacio en muchos aspectos dependen de la disponibilidad y fiabilidad de los servicios de infraestructura críticos relacionados, tales como la infraestructura de red de telecomunicaciones. La seguridad del ciberespacio también está estrechamente relacionada con la seguridad de la empresa de seguridad de Internet, redes / home y la información en general.

Cabe señalar que los dominios de seguridad identificadas en esta sección tienen sus propios objetivos y el alcance del foco. Para hacer frente a cuestiones de seguridad cibernética, por tanto, requiere considerables comunicaciones y la coordinación entre las diferentes entidades públicas y privadas de diferentes países y organizaciones. Servicios de infraestructura críticos son considerados por algunos gobiernos como los servicios relacionados con la seguridad nacional, y por lo tanto no pueden ser discutidos o revelados públicamente. Además, conocimiento de las debilidades de infraestructura crítica, si no se utiliza adecuadamente, puede tener una implicación directa en la seguridad nacional.

Por tanto, un marco básico para el intercambio de información y la coordinación emisión o incidente es necesario cerrar las brechas y proporcionar una seguridad adecuada a las partes interesadas en el ciberespacio (ISO, 2012).

Según la Unión Internacional de Telecomunicaciones (UIT), de los países del mundo en cuanto a preparación en ciberseguridad, encuentran que, 193 países, mantienen un rango específico de compromiso para enfrentar posibles ciberataques; y que se basa en cinco pilares básicos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación; el Ecuador se encuentra en el sexto puesto de América Latina de acuerdo con el Ministerio de Telecomunicaciones y Sociedad de la Información del año 2017; y ocupa el puesto 66 en el listado global de los países que formaron parte del estudio, no está en estado intermedio; no figura entre los líderes, pero tampoco está en la lista de países que se encuentran en etapas iniciales de su desarrollo (Dávila, 2017).

6. ENFOQUE

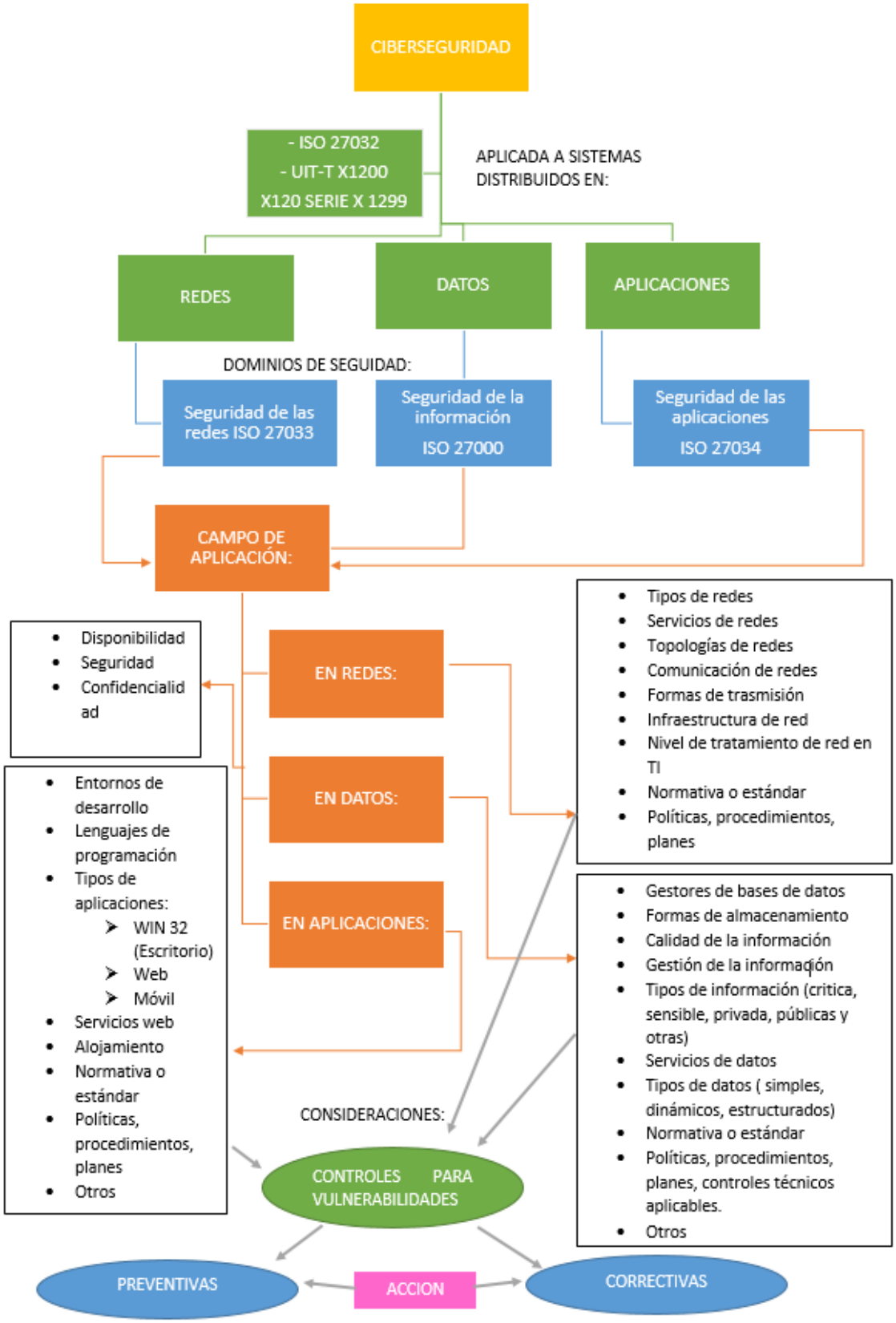


Figura 4. Esquema de Ciberseguridad

Elaboración: Las autoras.

7. MÉTODOS Y PROCESOS

Según la norma ISO/IEC27032 los métodos y procesos se clasificarán de la siguiente manera:

TIPO DE MÉTODO	APLICACIÓN DE PROCESO
Información general	Con el objetivo de llevar la ejecución de manera fiable en el intercambio de políticas de información y su coherencia de forma efectiva, deben asegurar que los métodos y procesos involucrados se basen en normas disponibles, por ello las instituciones de educación superior públicas, para lograr los objetivos y las políticas de intercambio de información y coordinación pertinentes en el contexto de la seguridad cibernética, se recomienda estar actualizados en la aplicación de normas en los sistemas que manejan para de esta manera asegurar la integridad y seguridad de los datos.
Clasificación y categorización de la información	Para asegurar la protección de la información, deben aplicarse para cada categoría y clasificación de la información involucrada, protocolos de seguridad que permitan controlar el acceso no autorizado de usuarios no identificados que puedan alterar la información, con la investigación realizada se obtuvo datos acerca de vulnerabilidades en los sistemas distribuidos analizados, registrando cada una de las vulnerabilidades en la matriz AMFE en donde se detalla el dominio y criterio al que pertenecen, con el propósito de brindar a las instituciones la información pertinente para que tomen medidas y apliquen las técnicas de seguridad necesarias.
No divulgación de acuerdo	Con este método se pretende asegurar el intercambio y coordinación de la información, haciendo uso de métodos apropiados para el intercambio de datos, evitando así ser recuperados por atacantes remotos.
Código de práctica	Este método asegura que la información no pueda ser recuperada por atacantes, por lo que recomienda hacer uso de técnicas de cifrados potentes y actualizados, para mantener la integridad de los datos y seguridad al momentos de ser manipulados.

Prueba y taladros	Este método propone realizar pruebas a los sistemas con el propósito de obtener una lista de vulnerabilidades que estos poseen y así poder perfeccionar la seguridad de los sistemas, en esta investigación en las instituciones involucradas se realizaron para cada uno de los sistemas analizados pruebas con tres herramientas (NESSUS, SHODAN, ACUNETIX), las cuales permitieron identificar vulnerabilidades según criterios (critico, alto, medio, bajo e informativo) y el dominio al que pertenecen.
El tiempo y la programación del intercambio de información	Este método establece la disponibilidad de la información, asegurando en horarios no autorizados (no laborables) a usuarios no autorizados pueda acceder a ella.

8. MEDIDAS Y CONTROLES

Para llevar a cabo las medidas y control de Ciberseguridad, pueden basarse a los contenidos de la Norma ISO/IEC27032, en donde se especifica las acciones a tomar para llevar a cabo una adecuada aplicación en cuento a la prevención y mitigación de los riesgos, amenazas o posibles ataques que pueden tener los sistemas distribuidos de su Institución.

9. GLOSARIO DE TÉRMINOS

TÉRMINOS	**DEFINICIÓN**
Acunetix	Acunetix Web Vulnerability Scanner es una herramienta que será capaz de escanear sitios web en busca de posibles fallos de seguridad que puedan poner en peligro la integridad de la página publicada en Internet (White, 2014).
Amenazas	Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información (INCIBE, 2017).
AMFE	Es un análisis de fallos y efectos dirigido a lograr el aseguramiento de la calidad (López, 2016).
Análisis	Es un proceso mediante el cual la se determina el nivel de exposición y la predisposición a la pérdida de un elemento o grupo de elementos ante una amenaza específica (Cardona, 2015).
Aplicación	Es el área de aplicación o donde establece el estudio (Castaño, 2014).
Atacantes	Son los expertos o individuos que estaban roles de amenazas o ataques al momento que se presente una vulnerabilidad (INCIBE, 2017).

Campo de aplicación	El escenario donde se establece el estudio o puesta en marcha de la investigación (Castaño, 2014).
Causas técnicas	Cuando las vulnerabilidades son producto de causas provocadas por la administración dentro del ciberespacio (Candau, 2010).
Checklist	Son listados de control, listados de chequeo, Checklist u hojas de verificación, siendo formatos generados para realizar actividades repetitivas, controlar el cumplimiento de un listado de requisitos o recolectar datos ordenadamente y de manera sistemática (ISOTOOL, 2018).
Ciberespacio	El uso generalizado de las Tecnologías de la Información y Comunicación (TIC), implica nuevos desafíos para la seguridad. En el ámbito militar estas nuevas tecnologías se han incorporado a todos los niveles y han planteado cambios en algunas de las concepciones clásicas de seguridad y defensa así como en sus planteamientos estratégicos (Gil, 2017).
Ciberseguridad	Es la encargada de la protección de infraestructura computacional y todo lo relacionado con esta, especialmente la información que se maneja (Rondero, 2018).
Confidencialidad	Es la propiedad con la que cuenta la información que no se encuentre a disposición de cualquier persona o sea divulgada (LPI, 2016; LPI, 2016).
Conflictos	Es todo aquello que genera problema una vez que se exista una causa o motivo (Chopra, 2012).
Controles	Son aquellos que se toman en cuenta para promover la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados (Carvajal, 2017).
Crimen organizado	Son los grupos que intentan dominar un mercado criminal, mientras que la mafia va más allá, ya que se trata de grupos del crimen organizado que intentan controlar todos los mercados criminales (Mendoza, 2018).
Defensa	Es aplicar mecanismos para controlar un potencial ciberataque se basa en mantener una posición de seguridad fundamental que incorpore monitorización continua, educación del usuario, gestión diligente de parches y controles básicos de configuración para abordar las vulnerabilidades (Castro, 2011).
Delincuencia	Son aquellos que buscan el fin de burlar los sistemas de ciberseguridad mediante ataques a través de canales de información (Mypime, 2016).
Detección	Es la manera de localizar diversas situaciones de riesgos o establecer gestión de incidentes de seguridad en sistemas de información (Microsoft, 2017).
Disponibilidad	Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran (Pérez, s.f.).

Dominio	Es como se encuentra dividida o clasificada las áreas de aplicación de la Ciberseguridad (Martínez, 2016).
Espionaje	Es en donde el atacante persigue información de muy diferente tipo, desde secretos comerciales a información de clientes, financiera o de marketing en el Ciberespacio (SIMARKS, 2018).
Estados extranjeros	Son las posiciones de un hecho en el extranjero en cuestión de Ciberseguridad (Lewis, 2016).
Estrategia	Es una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional.
Evaluación de riesgos	Es una gestión que se lleva a cabo en las organizaciones para determinar los riesgos efectuados en aspectos de seguridad, disponibilidad y confidencialidad de la información (Rozo, 2016).
Hacking	Son técnicas que usan los cibercriminales para acceder a la información pueden ser éticas o no éticas (Mendoza, Ética, el factor humano más importante en el ámbito de la ciberseguridad, 2016).
Hackinvistas	Son personas que combinan las habilidades del hacker con la militancia de un activista (Nuñez, 2017).
Herramientas para escaneo de vulnerabilidades	Son herramientas que se aplican para analizar el escaneo y explotación de vulnerabilidades en este caso en el Ciberespacio (Avila, 2018).
IES	Instituciones de Educación Superior
Individuos aislados	El individuo Coral pertenece a una sociedad integrada en su funcionamiento y desarrollo colectivos (Montalvo, 2012).
Información	Información denominamos al conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado (Guerra, 2017).
Informática	INFORMÁTICA es la ciencia que estudia el tratamiento automático y racional de la información (UCLA, s.f.).
Infraestructuras de tecnología	Es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que la Universidad necesita tener en funcionamiento para poder llevar a cabo toda su actividad, tanto docente como de investigación o de gestión interna (UOC, s.f.).
LEC	Legislación Ecuatoriana en Ciberseguridad
IoT	Internet de las Cosas que se refiere a la interconexión digital a través del internet (Perugini, 2018).
Líneas de acción	Las líneas de acción se conciben como estrategias de orientación y organización de diferentes actividades relacionadas con un campo de acción, de tal forma que se pueda garantizar la integración, articulación y continuidad de esfuerzos (Rodríguez, 2016).

Marco de referencia ciberseguridad	El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la Ciberseguridad (Rodríguez, 2016).
Marcos legales	El marco legal suele interpretarse como un conjunto de restricciones al quehacer de las empresas, en tanto su formulación, desde los planteamientos de los constituyentes, obedece más a la necesidad de encauzar el delineamiento de un proyecto (García, 2017)
Medidas de protección	Las medidas de protección son aquellas actitudes y decisiones, a fin de hacer efectivo el cuidado y protección de algo (García, 2017).
Mitigación de riesgos	La mitigación de riesgos sirve para aplicar acciones que permitan reducir la vulnerabilidad a ciertos peligros (García, 2017).
Plan de acción	Un plan de acción sirve para priorizar las iniciativas más importantes para cumplir con los objetivos y metas que has marcado (Grau, 2019).
Nessus	Nessus es el escaner de vulnerabilidades más usado en el mundo, obteniendo el primer lugar en el ranking mundial en 2000, 2003 y 2006 como la mejor herramienta de seguridad de red.
Niveles de vulnerabilidad	Se refiere a la poca o inexistente de riesgo.
Norma ISO/iec27032	La Norma ISO/IEC 27032 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad en una empresa (ACMS, 2012).
Política de ciberseguridad	La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos (Enagas, 2019).
Responsables	Ser capaz de tomar decisiones conscientemente, llevar a cabo conductas que persigan mejorarse a uno mismo y/o ayudar a los demás (Sanchéz, 2018).
Riesgos	El riesgo es la probabilidad de que una amenaza se convierta en un desastre.
Sabotajes	El sabotaje es un proceso por el cual se realiza una modificación, destrucción, obstrucción o cualquier intervención en una operación ajena, con el propósito de obtener algún beneficio para uno mismo (Lopez, 2012).
Seguridad	La seguridad es un estado en el cual los peligros y las condiciones que pueden provocar daños de tipo físico, psicológico o material son controlados para preservar la salud y el bienestar de los individuos y de la comunidad (INSPQ, s.f.).
Servicios	Un servicio es un conjunto de actividades que buscan satisfacer las necesidades de un cliente.
Shodan	Shodan es un motor de búsqueda que le permite al usuario encontrar iguales o diferentes tipos específicos de equipos conectados a Internet a través de una variedad de filtros.
Sistemas distribuidos	Un sistemas distribuido consiste en una colección de computadoras autónomas en lazadas por una red y equipadas por un sistema de red distribuido (Silva, 2004).

Sociedad	Sociedad es un concepto polisémico, que designa a un tipo particular de agrupación de individuos.
Terrorismo	El terrorismo es el uso de la fuerza o la violencia contra las personas o los bienes materiales en violación de las leyes penales (SASN, s.f.).
TICs	Tecnología de la información y comunicaciones.
UIT	Unión Internacional de Telecomunicaciones.
Vulnerabilidades	La vulnerabilidad es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre o riesgos (Carvajal, 2017).
Web	Es un conjunto de páginas web desarrolladas en código html, relacionadas a un dominio de Internet el cual se puede visualizar en la World Wide Web (www) mediante los navegadores web o también llamados browser como ser Chrome, Firefox, Edge, Opera entre otros (Pairuna, 2018).
Ciberconflicto	Es la expresión de intereses contrapuestos, entre dos o más partes, en relación a temas, intereses o valores que se manifiestan en el ciberespacio (MISP y MDN, 2015).
Ciberataque	Es una expresión del ciberconflicto consistente en acciones hostiles desarrolladas en el ciberespacio con el objetivo de irrumpir, explotar, denegar, degradar o destruir la infraestructura tecnológica, componente lógico o interacciones de éste y pueden tener distintos niveles según su duración, frecuencia y daño generado (MISP y MDN, 2015).
Ciberdefensa	El término posee dos acepciones. (A) En un sentido amplio, son acciones contempladas en el marco de una política nacional de ciberseguridad orientadas a proteger el ciberespacio ante cualquier acción que pueda dañarlo. (B) En un sentido restringido, es el conjunto de políticas y técnicas de la Defensa Nacional destinadas a enfrentar los riesgos y amenazas propias del ciberespacio, de acuerdo con sus atribuciones constitucionales y legales (MISP y MDN, 2015).
Cibercrimen	Son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos (MISP y MDN, 2015).
Sistema informático	Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa (MISP y MDN, 2015).
Dato informático	Toda representación de hechos, información o conceptos expresados de cualquier forma que se presente a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función (MISP y MDN, 2015).

Delito informático	Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos (MISP y MDN, 2015).
Incidente informático	Evento que afecta la confidencialidad, integridad o disponibilidad de la información, como también la continuidad del servicio proporcionado por los sistemas que la Contienen (MISP y MDN, 2015).

10. ANÁLISIS DE VULNERABILIDADES CON HERRAMIENTAS DE ESCANEO SHODAN, NESSUS Y ACUNETIX

Una vulnerabilidad es una debilidad de un activo o de un sistema de control que puede ser explotado por una amenaza. En el contexto de un sistema de información, ISO / IEC TR 19791: 2006 también define la vulnerabilidad como un defecto, la debilidad o la propiedad del diseño o la implementación de un sistema distribuidos (incluyendo sus controles de seguridad) o de su entorno que podría ser explotada con o sin intención para afectar adversamente activos u operaciones de una organización. Evaluación de la vulnerabilidad debe ser una tarea en curso. A medida que los sistemas reciben parches, actualizaciones o nuevos elementos se añaden, se pueden introducir nuevas vulnerabilidades (ISO, 2012).

Las soluciones a las vulnerabilidades deben buscarse, implementadas y, cuando una solución no es posible o factible, los controles deben ser puestos en su lugar. Este enfoque debe aplicarse con carácter prioritario por lo que las vulnerabilidades que presentan mayor riesgo se abordan en primer lugar (ISO, 2012).

Dado a que las vulnerabilidades pueden ser objetivo a futuro de riesgos en los sistemas distribuidos, o llevar a una amenaza que si bien al materializarse puede provocar un ataque, del cual puede producir un perjuicio a la Institución y con ello un peligro los recursos de información.

A continuación, se puede ver el total de vulnerabilidades obtenidas de los sistemas distribuidos analizados de la ESPAM MFL, con un total de 1499 vulnerabilidades, de las cuales se puede determinar que se obtuvieron niveles críticos y altos en los sistemas en las diferentes herramientas aplicadas SHODAN, NESSUS y ACUNETIX, como se muestra en la **tabla 1**:

HERRAMIENTAS	NIVEL	ESPAM MFL	OBSERVACIONES
SHODAN	Crítico	0	En este caso la herramienta de SHODAN arrojó más vulnerabilidades de carácter informativo al realizar el escaneo de vulnerabilidades en los sistemas distribuidos de la ESPAM MFL MF.
	Alto	0	
	Medio	0	
	Bajo	0	
	Informativo	273	
NESSUS	Crítico	14	En el análisis de NESSUS, se observó todos los criterios o niveles de vulnerabilidad con cifras y en tiempos diferentes.
	Alto	22	
	Medio	38	
	Bajo	14	
	Informativo	455	
ACUNETIX	Crítico	0	En el análisis de vulnerabilidades con la herramienta ACUNETIX, se determinó que no hubo nivel Crítico en su categoría, pero si en los demás niveles, de los cuales se efectuó un escaneo más profundo que en comparación a las demás herramientas, esta proporciona mayor información en cuanto a vulnerabilidades.
	Alto	42	
	Medio	503	
	Bajo	86	
	Informativo	52	

Tabla 1. Total de vulnerabilidades por nivel.

Elaboración: Las autoras.

Para el análisis de la siguiente tabla, cabe especificar que se tomó como referencia para el total de vulnerabilidades en los sistemas de la ESPAM MFL, la herramienta Acunetix, ya que esta muestra un escaneo de vulnerabilidades más profundo como se muestra en la tabla anterior.

En la **tabla 2**, se puede observar que el valor más elevado con un total de 498 vulnerabilidades es el de la página web institucional, donde se muestra que el nivel informativo con 242 vulnerabilidades es las más altas, seguidas del nivel medio con 241 vulnerabilidades. Así mismo está el sistema de Investigación con un total de 295 vulnerabilidades, correspondiente a 165 vulnerabilidades de nivel informativo y 103 vulnerabilidades en el nivel medio.

Otro sistema con un total de 154 vulnerabilidades es el Micro-Sitio Computación, que muestra un elevado número de 105 vulnerabilidades en el nivel informativo y 19 vulnerabilidades en el nivel medio.

Tabla 2. Vulnerabilidades ESPAM MFL.

NOMBRE DEL SISTEMA	NIVEL					TOTAL VULNERABILIDAD
	CRITICO	ALTO	MEDIO	BAJO	INFORMATIVO	
Página web institucional	3	3	241	9	242	498
Gestión académica	0	4	10	2	9	25
Sistema de control académico de CAAI	0	7	55	11	25	98
Sistema de control académico de idiomas	0	5	90	3	1	99
Bienestar	0	3	1	2	1	7
E-virtual	1	2	9	5	38	55
Gestión académica	0	3	3	7	12	25
Investigación	3	3	103	21	165	295
Postgrado	2	1	51	2	43	99
Sistema talento Humano	3	1	42	5	2	53
Unidad de producción de software (UPS)	2	1	40	9	4	56
Micro- Sitio Administración de Empresas	0	21	0	0	2	23
Micro- Sitio Computación	0	10	19	20	105	154
Micro Administración Pública	0	0	0	0	2	2
Micro- Sitio Agroindustria	0	0	0	0	2	2
Micro- Sitio Ingeniería Agrícola	0	0	0	0	2	2
Micro- Sitio Ingeniería Ambiental	0	0	0	0	2	2
Micro- Sitio Medicina Veterinaria	0	0	0	0	2	2
Micro- Sitio Turismo	0	0	0	0	2	2
	TOTAL					**1499**

Elaboración: Las autoras.

Los datos extraídos **(gráfico 1)**, pertenecen a las pruebas de vulnerabilidades efectuadas a un total de 19 sistemas informáticos de la ESPAM MFL, los que arrojaron un total de 1499 vulnerabilidades de todos los sistemas analizados, se obtuvo un total de 498 vulnerabilidades para sitio web institucional como uno de los más altos y como más bajo los micro sitios de la mayoría de las carreras.

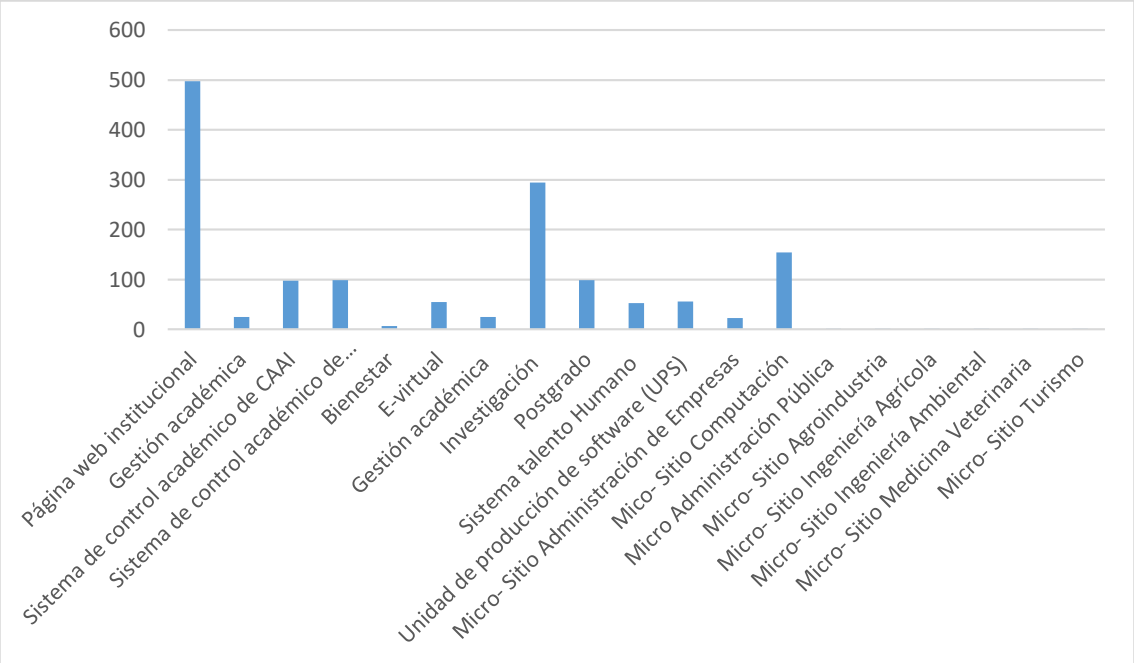


Gráfico 1. Vulnerabilidades ESPAM MFL.
Elaboración: Las autoras.

Por otro lado, se detalla cada una de las vulnerabilidades obtenidas por medio de las herramientas con resultados críticos, alto, medio y bajo de la Institución correspondiente a la ESPAM MFL, en la cual como se puede observar en las **tablas 3, 4** y **5** a continuación:

Tabla 3. Descripción vulnerabilidades – Dominio Red - ESPAM MFL.

VULNERABILIDADES	RIESGOS	TIPO (NIVEL)
Vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (verificación sin credenciales).	• Perdida de datos. • Falta en la disponibilidad del servidor.	Alta
Vulnerabilidad encontrada en MikroTik	• Atacante remoto • obtener la ejecución del código del sistema por atacantes.	Critica
Vulnerabilidad por falta de CPE: Enumeración de la plataforma común	• Riesgos en configuraciones. • Búsquedas no confiables.	Medio
Español:Riesgo en Device Type	• Atacantes remotos.	Alto
URLs externas	• Posible rastreo del servidor web remoto.	Bajo
MikroTik RouterOS <6.40.9 / 6.42.7 / 6.43 vulnerabilidades múltiples.	• Infectar al servidor.	Alta
MikroTik RouterOS <6.41.3 Desbordamiento de búfer SMB	• Ataques a través de la red, debido a que no necesita ninguna autenticación especifica.	Critica
(uncredentialed check): 82828 - MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (verificación sin credenciales)	• Ejecución remota de código arbitrario con privilegios del sistema.	Critica

Elaboración: Las autoras.

Tabla 4. Descripción de vulnerabilidades – Dominio Aplicación – ESPAM MFL.

Directorios web navegables	Depuración del servidor por atacantes.	Media
HP 5.6.x <5.6.27 Vulnerabilidades múltiples	Ataques en la denegación de servicios.	Critica
Servidor web transmite credenciales de cleartext	Permite a un atacante que espía el tráfico entre el navegador web y el servidor puede obtener inicios de sesión y contraseñas de usuarios válidos.	Alta
Aplicación web potencialmente vulnerable al clickjacking	Podría exponer al sitio a un ataque de clickjacking o reparación de UI, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que sea diferente de lo que el usuario percibe que es la página. Esto puede hacer que un usuario realice transacciones fraudulentas o malintencionadas.	Media
Se admiten suites de cifrado de resistencia media SSL	Ataques remotos.	Media

Elaboración: Las autoras

Tabla 5. Descripción vulnerabilidades – Dominio Datos - ESPAM MFL.

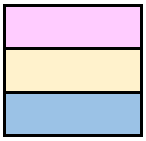
OpenSSL 1.0.2 <1.0.2i Vulnerabilidades múltiples (SWEET32)	• Divulgación de información. • Ataques remotos.	Critica
Cifras en modo CBC del servidor SSH habilitadas	• Permitir que un atacante recupere el mensaje de texto simple del texto cifrado.	Baja

Elaboración: Las autoras

11. RESULTADOS ANÁLISIS DE RIESGO

Para la comprensión de los riesgos que podría tener las vulnerabilidades en los sistemas distribuidos se usó la metodología Análisis Modal de Fallos y Efectos (AMFE), la cual detalla las vulnerabilidades presentes en los sistemas distribuidos de las instituciones, implicados los riesgos y dominios al cual pertenecen cada vulnerabilidad. La matriz de riesgos (AMFE) fue aplicado al cumplimiento de la Norma ISO 27032 cubriendo los dominios de Seguridad de la Información, Seguridad de las Aplicaciones y Seguridad de las Redes como se puede apreciar en las **tablas 6**, **7** y **8**, además se considera la siguiente información para separar la clasificación de las vulnerabilidades encontradas en el *Checklist* aplicado:

INFORMACIÓN:



Muy Vulnerable

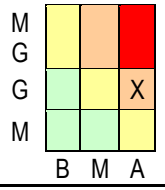
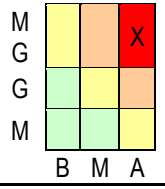
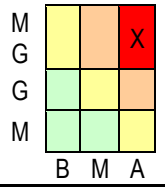
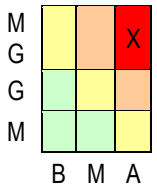
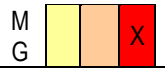
Vulnerable

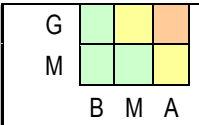
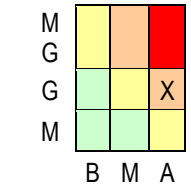
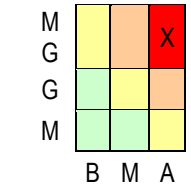
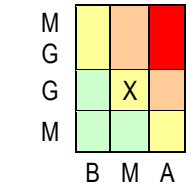
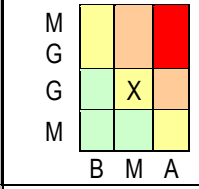
Poco vulnerable

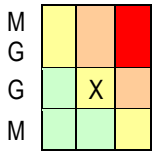
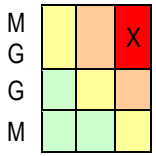
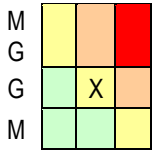
Los *Checklist* aplicados se elaboraron con el fin de realizar el levantamiento de información de la institución y verificar el cumplimento según lo indicado en la norma ISO 27032 para la gestión de ciberseguridad, con esta información se pudo identificar las vulnerabilidades, las cuales fueron ponderadas y clasificadas de acuerdo a la escala de Likert, tomando 4 ítems y considerando solo 3 ítems para esta investigación (Muy Vulnerable, Vulnerable y Poco vulnerable), para después con ello realizar la matriz AMFE.

En esta matriz se establecieron parámetros como, ID del riesgo, vulnerabilidad, probabilidad, la acción de mitigación y su criterio de aceptación, que servirán para mejorar el riesgo a ataques remotos o mal uso de la información que se maneja en los sistemas distribuidos de la ESPAM MFL. Cabe mencionar que se tomaron en cuenta parámetros, como probabilidad (Alto, Medio y Bajo) e impacto (Muy Grave, Grave y Menor), obteniendo así el nivel de riesgo (Crítico, Medio y Bajo) de las vulnerabilidades. Su aplicación permitió reconocer criterios de manera más explícita en la identificación de los riesgos presentes en los análisis efectuados, además de aplicar métodos basados en la norma ISO 27032 para la gestión de riesgos de ciberseguridad de los sistemas distribuidos.

Tabla 6. Matriz de riesgos según la metodología AMFE, dominio Seguridad de la Información

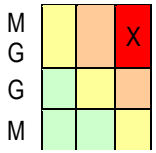
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.1.1.	No se monitorea el acceso a los sistemas de información web.	Alto 3	Grave 2	Alto		Coordinador TI	A.1.1.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Reportes de acceso a los sistemas mediante autenticación de usuario.
R.1.2.	No se mantiene preparación continua en Ciberseguridad en la institución.	Alto 3	Muy Grave 3	Critico		Coordinador TI	A.1.2.1	Capacitar al personal de TI en ciberseguridad de manera continua.	Capacitación a Congresos, seminarios, Talleres de seguridad informática.
R.1.3.	No se estandarizan los datos en base a normas de calidad.	Alto 3	Muy Grave 3	Critico		Coordinador TI	A.1.3.1	Estandarizar la gestión de calidad de los procesos de la información mediante normas de calidad.	Mejorar la calidad de los procesos de seguridad de la información en el ciberespacio
R.1.4.	No emplean normas de calidad como ISO, INEN, Control interno, entre otras para la estandarización de sus procesos.	Alto 3	Muy Grave 3	Critico		Coordinador TI	A.1.4.1	Implementar Normas de calidad como ISO 9000 y normas de control interno 410-09 para mejorar la calidad de los servicios y brindar seguridad en sus procesos.	Mejorar la gestión de calidad de los procesos y seguridad de la información
R.1.5.	No aplican regulaciones de normas en escenarios de seguridad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.5.1	Aplicar Normas de Control Interno 410-09 de TI de la Contraloría	Complementar con norma ISO/IEC 27001 Sistema de

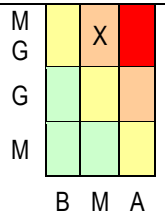
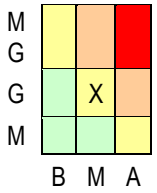
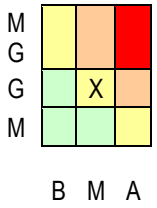
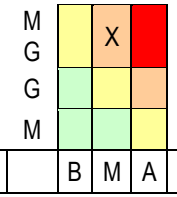
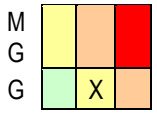
								General del Estado ecuatoriano para escenarios de seguridad.	Gestión de Seguridad de la información
		3	3						
R.1.6.	No se alerta a los usuarios cuando existe algún tipo de ataque o implementación de controles de seguridad.	Alto	Grave	Alto		Coordinador TI	A.1.6.1	Informar a los usuarios de los controles de seguridad en los sistemas y de los ataques que se han presentado en los mismos a nivel institucional.	Reporte e informe de ataques y controles de seguridad a los usuarios.
		3	2						
R. 1.7.	No emplean normas en escenarios de ciberseguridad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.7.1	Seguir el plan propuesto de Ciberseguridad	Mejorar el escenario de ciberseguridad
		3	3						
R.1.8.	Los manuales de usuario para el manejo de los sistemas de información están en proceso de elaboración.	Medio	Grave	Medio		Coordinador TI	A.1.8.1	Implementar manuales de usuarios para el uso efectivo de los sistemas o aplicaciones web.	Aplicar controles internos periódicos de cumplimiento.
		2	2						
R.1.9	No se llevan a cabo los datos de informes como estrategia para la continuidad del negocio.	Medio	Grave	Medio		Coordinador TI	A.1.9.1	Elaborar estrategias para mejorar los servicios TI.	PETI (Plan estratégico de Tecnologías de Información)
		2	2						
R.1.10.		Medio	Grave	Medio		Coordinador TI	A.1.10.1		

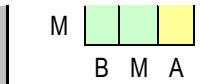
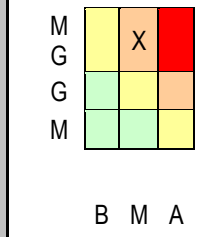
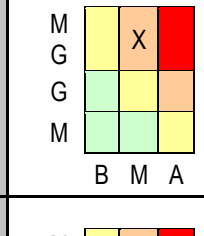
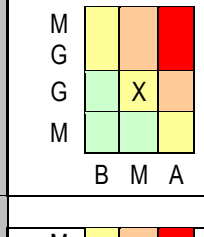
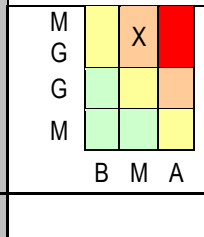
	Han sufrido ataques de robo de identidad o robo de información de los usuarios en Aplicaciones web.	2	2					Elaborar medidas de prevención contra ataques de robo de información de los usuarios en aplicaciones web.	Mejorar la seguridad de las aplicaciones.
R.1.11.	Los tipos de ataques que se han presentado en la unidad son: DDoS, Dos.	Alto	Muy Grave	Critico		Coordinador TI	A.1.11.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Mejorar controles contra ataques cibernéticos.
		3	3						
R.1.12.	No se usan técnicas de visualización de datos para presentar información de eventos.	Medio	Grave	Medio		Coordinador TI	A.1.12.1	Elaborar técnicas de visualización de datos para verificar la pérdida de información.	Escalabilidad y disponibilidad de las aplicaciones.
		2	2						

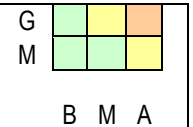
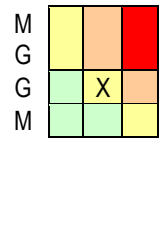
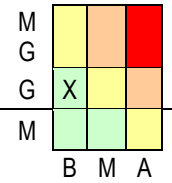
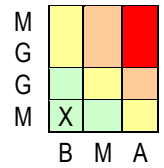
Elaboración: Las autoras.

Tabla 7. Matriz de riesgos según la metodología AMFE, dominio Seguridad de las Aplicaciones.

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.2.1	No tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción.	Alto	Muy Grave	Critico		Área de desarrollo de aplicaciones	A.2.1.1	Elaborar un plan de seguridad para todo el ciclo de desarrollo, prueba, y retroalimentación de las aplicaciones	Madurez en los procesos de desarrollo de aplicaciones.
		3	3						
R.2.2.		Medio		Alto			A.2.2.1		

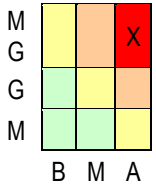
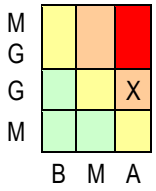
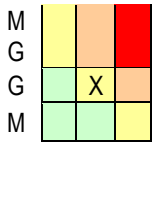
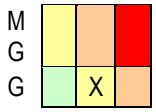
	El departamento de tecnología no cuenta con una metodología y procesos de desarrollo de aplicaciones maduros.	2	Muy Grave 3			Área de desarrollo de aplicaciones		Elaborar flujogramas de procesos de desarrollo con metodologías ágiles como SCRUM.	Mejora de los procesos de desarrollo de aplicaciones.
R.2.3.	La universidad no cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos que implican las ciberamenazas.	Medio 2	Grave 2	Medio		Área de desarrollo de aplicaciones	A.2.3.1	Contratar talento humano especializado o capacitar al personal necesario en seguridad de las aplicaciones.	Contrarrestar los riesgos que implican las ciberamenazas.
R.2.4	El departamento de tecnología no ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar continuamente la práctica.	Medio 2	Grave 2	Medio		Área de desarrollo de aplicaciones	A.2.4.1	Elaborar un protocolo de autoevaluación de control para la efectividad de la seguridad de las aplicaciones.	Trabajar con la norma de seguridad de las aplicaciones ISO/IEC 27034
R.2.5.	No se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable.	Medio 2	Muy Grave 3	Alto		Área de desarrollo de aplicaciones	A.2.5.1	Utilizar las herramientas tecnológicas que brinda la norma ISO/IEC 27032 de ciberseguridad para efectuar pruebas de vulnerabilidades en las aplicaciones.	Nessus, Acunetix, Shodan
R.2.6.	No utilizan herramientas tecnológicas como SAST, DAST, RASP, SCA para	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.6.1	Aplicar al menos una de estas herramientas o en su defecto utilizar las herramientas que	Pruebas regulares con estas herramientas para

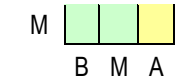
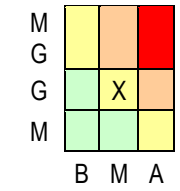
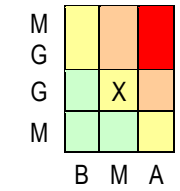
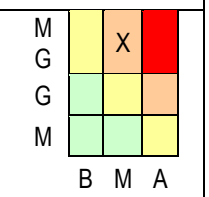
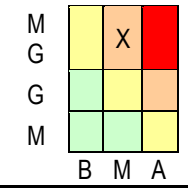
	realizar pruebas de vulnerabilidades.	2	2					sugiere la norma ISO/IEC 27032 de ciberseguridad.	detectar vulnerabilidades.
R.2.7.	No se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto internas como externas.	Medio 2	Muy Grave 3	Alto		Área de desarrollo de aplicaciones	A.2.7.1	Implementar esta prueba de pentest para verificar las medidas de seguridad de las aplicaciones, red, plataforma de alojamiento, aplicación o sistemas web.	Proteger las aplicaciones de ataques cibernéticos.
R.2.8.	No se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software.	Medio 2	Muy Grave 3	Alto		Área de desarrollo de aplicaciones y Coordinador TI	A.2.8.1	Establecer responsabilidades y procedimientos formales a custodios de los equipos tecnológicos y software para el buen uso y seguridad de las aplicaciones.	Políticas de seguridad de los equipos tecnológicos y software a cargo de los custodios.
R.2.9.	No se aprueban de manera formal los cambios de equipos tecnológicos y software.	Medio 2	Grave 2	Medio		Coordinador TI	A.2.9.1	Elaborar actas de entrega-recepción de equipos tecnológicos cuando haya cambios de custodios.	Seguridad en los cambios de equipos tecnológicos y software.
R.2.10.	La unidad no posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos.	Medio 2	Muy Grave 3	Alto		Área de desarrollo de aplicaciones y Coordinador TI	A.2.10.1	Realizar reportes o informes de eventos maliciosos o fallas en los sistemas de información, sitios web, equipos tecnológicos.	Mantener la seguridad de los sistemas en el ciberespacio.
R.2.11.	El equipo de desarrollo no aplica seguimientos o revisión en los mensajes recibidos en	Medio	Muy Grave	Alto		Área de desarrollo de	A.2.11.1	Asegurar que los mensajes recibidos en los sitios web no contengan contenido malicioso,	Seguimiento de la seguridad de las aplicaciones.

	el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas.	2	3			aplicaciones y Área de Redes		enlaces de sitios web de phishing o descargas maliciosas.	
R.2.12.	No se logra los objetivos desarrollados en base a la sensibilización y formación en proporcionar informes periódicos sobre el estado de la Ciberseguridad, Sesiones de formación enfocada en escenarios simulados de ataque cibernética o talleres sobre áreas requeridas de acciones específicas y tampoco en pruebas regulares con recorridos en escenarios permanentes.	Medio	Grave	Medio		Coordinador TI	A.2.12.1	Considerar como objetivos de sensibilización y formación a informes periódicos sobre el estado de ciberseguridad, enfoques de escenarios simulados de ataques cibernéticos o talleres de acciones específicas y pruebas regulares en escenarios permanentes.	Mejorar la ciberseguridad.
		2	2						
R.2.13.	No se prohíbe el uso de software no autorizado por la institución.	Bajo	Grave	Bajo		Coordinador TI	A.2.13.1	Usar software legal o software libre según lo requiera la aplicación a desarrollar.	Visual, SQL, Windows, Linux
		1	2						
R.2.14.	No se mantienen los sistemas operativos actualizados con las últimas versiones.	Bajo	Menor	Bajo		Coordinador TI	A.2.14.1	Mantener actualizados los sistemas operativos de acuerdo a las características de los equipos.	Mejorar la productividad del desarrollo de aplicaciones.
		1	1						

Elaboración: Las autoras.

Tabla 8. Matriz de riesgos según la metodología AMFE, dominio Seguridad de las Redes.

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R. 3.1.	La unidad no tiene medidas de prevención y respuestas a los ataques cibernéticos.	Alto 3	Muy Grave 3	Critico		Coordinador TI	A.3.1.1	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Controlar los ataques cibernéticos.
R.3.2.	No se realiza informes de eventos sospechosos o encuentros maliciosos en las redes.	Alto 3	Grave 2	Alto		Coordinador TI y Área de Redes	A.3.2.1	Elaborar o adquirir una herramienta que permita detectar eventos maliciosos en las redes y emitan reportes de los mismos.	Informes mensuales de eventos sospechosos o maliciosos en las redes.
R.3.3.	Entre las políticas, procedimientos y controles que están en proceso de aprobación en la unidad para seguridad de la red están: Políticas de control de acceso a la red, controles de acceso a los servidores, procedimientos de respaldo de la información cuando existen pérdidas de fallos físicos, control de filtros de tráfico en la red interna y externa.	Medio 2	Grave 2	Medio		Coordinador TI, Área de Redes y Área de Datos (Data Center)	A.3.4.1	Agilizar el proceso de aprobación de las políticas, procedimientos y controles de la seguridad de la red.	Política de control de acceso, política de filtros de tráfico en la red interna y externa.
R.3.4.	No tienen protocolos de autenticación de computadoras dentro de la red.	Medio	Grave	Medio		Área de Redes.	A.3.5.1	Utilizar protocolos de autenticación de computadoras dentro de la red para evitar posibles ataques.	Evitar los ataques de Man in the middle.

		2	2						
R.3.5.	No existen controles que restrinjan la dirección MAC de cada equipo.	Medio 2	Grave 2	Medio		Área de Redes.	A.3.6.1	Autenticar los equipos para que haya mayor control y seguridad en la comunicación entre equipos.	Mejorar la seguridad en las redes.
R.3.6.	El director /coordinador de la unidad no se asegura que la URL de su contenido web este citado como un enlace seguro en su navegador.	Medio 2	Grave 2	Medio		Coordinador TI	A.3.7.1	Asegurar que toda la información que vaya a subirse en una aplicación web, debe estar con un enlace seguro en la URL. Como HTTPS.	Proteger la información en el ciberespacio
R.3.7.	El SSL que utiliza el sitio web, no identifica el contenido original del nuevo contenido dañado, plantado por un atacante.	Medio 2	Muy Grave 3	Alto		Área de Redes.	A.3.8.1	Verificar que el tráfico de la información esté cifrado para evitar ataques como DDoS.	SSL certificado.
R.3.8.	Utilizan protocolos de comunicación como HTTP.	Medio 2	Muy Grave 3	Alto		Área de Redes y Área de desarrollo de aplicaciones.	A.3.9.1	Utilizar protocolos de comunicación seguro en el ciberespacio como HTTPS.	Mejorar la Seguridad en la transmisión de datos en las redes.

Elaboración: Las autoras.

De acuerdo con los datos obtenidos en la matriz AMFE se puede mostrar la siguiente tabla con el porcentaje de riesgo basado en el cumplimiento de la norma ISO/IEC 27032 según los dominios de Seguridad de la Información, Seguridad de las Aplicaciones y Seguridad de las Redes en cada IES pública de Manabí:

Tabla 9. Riesgo por Dominios de la norma ISO/IEC 27032

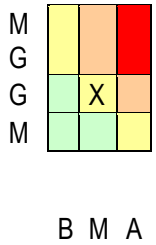
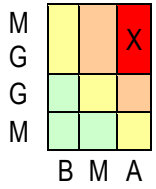
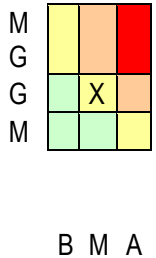
DOMINIOS	PORCENTAJE DEL RIESGO SEGÚN AMFE BASADOS EN LA NORMA ISO/IEC 27032			
	PROBABILIDAD	IMPACTO	NIVEL	%
Seguridad de la Información	Alto	Muy Grave	Crítico	50%
	Alto	Grave	Alto	16,67%
	Medio	Grave	Medio	33,33%
Seguridad de las Aplicaciones	Alto	Muy Grave	Crítico	7,14%
	Medio	Muy Grave	Alto	42,86%
	Medio	Grave	Medio	35,72%
	Bajo	Grave	Bajo	7,14%
	Bajo	Menor	Bajo	7,14%
Seguridad de las Redes	Alto	Muy Grave	Crítico	12,5%
	Alto	Grave	Alto	37,5%
	Medio	Grave	Medio	50%

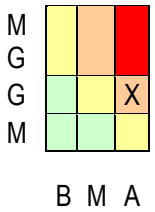
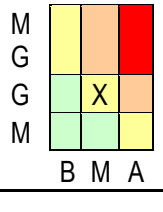
Elaboración: Las autoras.

Matriz de riesgos AMFE aplicado a las herramientas de escaneo de vulnerabilidades, como se puede apreciar en las tablas **10, 11 y 12**, donde detalla los riesgos de las vulnerabilidades, según el dominio de seguridad, además se establecen las acciones de mitigación y criterios de aceptación para reducir riesgos de ciberseguridad presentes en las vulnerabilidades de los sistemas distribuidos de la ESPAM MFL.

VULNERABILIDADES SEGÚN LAS HERRAMIENTAS SHODAN, NESUS, ACUNETIX	DOMINIO	COLOR
	Seguridad de Información	Celeste
	Seguridad de aplicaciones	Naranja
	Seguridad de Redes	Verde

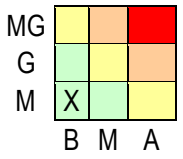
Tabla 10. Matriz de riesgos según la metodología AMFE, aplicada al análisis de vulnerabilidades de seguridad de aplicaciones en los sistemas distribuidos de la ESPAM MFL.

ID. Riesgo	Vulnerabilidades	Descripción	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.1.1.	Browsable Web Directories	• Depuración del servidor por atacantes.	Medio 2	Grave 2	Medio		Director/Coordinador de TI	A.1.1.7	Asegurar de que los directorios navegables no filtren información confidencial ni den acceso a recursos confidenciales. Además, use restricciones de acceso o deshabilite la indexación de directorios para cualquiera que lo haga.	Mejorar el acceso a directorios.
R.1.1.	HP 5.6.x < 5.6.27 Multiple Vulnerabilities	• Ataques en la denegación de servicios.	Alto 3	Muy Grave 3	Critico		Director/Coordinador de TI	A.1.1.11	Se recomienda Actualizar la versión de HP 5.6.x a una superior.	Actualizar HP 5.6.x.
R.1.1.	Web Application Potentially Vulnerable to Clickjacking	• Podría exponer al sitio a un ataque de clickjacking o reparación de UI, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que sea diferente de lo que el	Medio 2	Grave 2	Medio		Director/Coordinador de TI	A.1.1.13	Se aconseja del devolver el encabezado HTTP de X-Frame-Options o Content-Security-Policy (con la directiva 'frame-ancestors') con la respuesta de la página. Esto evita que el contenido de la página sea procesado por otro sitio cuando se usan las	Hacer uso de la directiva frame-ancestors.

		usuario percibe que es la página. Esto puede hacer que un usuario realice transacciones fraudulentas o malintencionadas.							etiquetas de marco o iframe HTML.	
R.1.2.	Web Server Transmits Cleartext Credentials	• Permite a un atacante que espía el tráfico entre el navegador web y el servidor puede obtener inicios de sesión y contraseñas de usuarios válidos.	Alto 3	Grave 2	Alto		Director/Coordinador de TI	A.1.1.14	Asegúrese de que cada formulario sensible transmita contenido a través de HTTPS.	Transmitir contenido a través de HTTPS.
R.1.1.	SSL Medium Strength Cipher Suites Supported	• Ataques remotos.	Medio 2	Grave 2	Medio		Director/Coordinador de TI	A.1.1.15	Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.	Reconfigura aplicación.

Elaboración: Las autoras.

Tabla 11. Matriz de riesgos según la metodología AMFE, aplicada al análisis de vulnerabilidades de seguridad de información en los sistemas distribuidos de la ESPAM MFL.

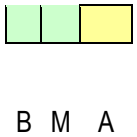
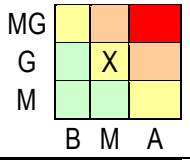
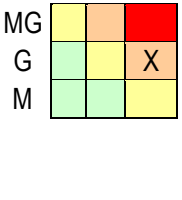
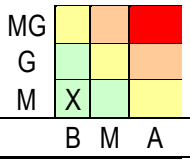
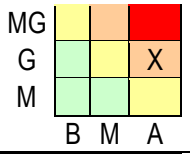
ID. Riesgo	Vulnerabilidades	Descripción	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.1.2.	SSH Server CBC Mode Ciphers Enabled	• Permitir que un atacante recupere el mensaje de	Bajo 1	Menor 1	Bajo		Director/Coordinador de TI	A.1.1.8	Se recomienda ponerse en contacto con el proveedor o consulte la documentación del producto para	Deshabilitar el cifrado de CBC y habilitar el CTR O GCM.

		texto simple del texto cifrado.							deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado de cifrado CTR o GCM.	
R.1.2.	OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)	• Divulgación de información. • Ataques remotos.	Alto 3	Muy Grave 3	Critico	MG / G / M — B M A (X)	Director de proyecto	A.1.1.10	Se recomienda actualizar a Opens SSL a una posterior.	Actualizar Open SSL.

Elaboración: Las autoras.

Tabla 12. Matriz de riesgos según la metodología AMFE, aplicada al análisis de vulnerabilidades de seguridad de redes en los sistemas distribuidos de la ESPAM MFL.

ID. Riesgo	Vulnerabilidades	Descripción	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	ID Mitigación	Acciones de mitigación	Criterio de aceptación
R.1.1.	Vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (verificación sin credenciales).	• Perdida de datos. • Falta en la disponibilidad del servidor.	Alto 3	Grave 2	Alto	MG / G / M — B M A (X)	Director/Coordinador de TI	A.1.1.1	Se recomienda mejorar la versión de Windows que se ejecuta en el host remoto ya que se ve afectada por una condición de desbordamiento de entero en la pila de protocolo HTTP (HTTP.sys).	Mejorar la versión del Windows server.
R.1.2.	Vulnerabilidad encontrada en MikroTik.	• Atacante remoto obtener la ejecución del código del sistema por atacantes.	Alto	Muy Grave	Critico	MG / G (X)	Director/Coordinador de TI	A.1.1.2	El dispositivo de red remota está ejecutando una versión de MikroTik RouterOS antes de las 6.41.3. Por lo tanto, se ve afectado por una vulnerabilidad de desbordamiento de búfer SMB remoto que puede ser aprovechada por un	Actualizar la versión de MikroTik.

			3	3					atacante remoto no autenticado para ejecutar código arbitrario.	
R.1.1.	Vulnerabilidad por falta de CPE: Enumeración de la plataforma común.	• Riesgos en configuraciones. • Búsquedas no confiables.	Medio 2	Grave 2	Medio		Director/Coordinador de TI	A.1.1.3	Se recomienda hacer uso adecuado de CPE.	Mejorar CPE.
R.1.2.	Riesgo en Device Type.	• Atacantes remotos.	Alto 3	Grave 2	Alto		Director/Coordinador de TI	A.1.1.4	Se recomienda mejorar el tipo de dispositivo que se usa, porque según el sistema operativo remoto, es posible determinar cuál es el tipo de sistema remoto (por ejemplo: una impresora, un enrutador, una computadora de uso general, etc.).	Mejora el tipo de dispositivo.
R.1.1.	External URLs	• Posible rastreo del servidor web remoto.	Bajo 1	Menor 1	Bajo		Director/Coordinador de TI	A.1.1.5	Se recomienda mejorar el uso HREF, debido se puede recopilar enlaces a sitios externos rastreando el servidor web remoto.	Mejorar el uso HREF.
R.1.2.	MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 múltiple vulnerabilities.	• Infectar al servidor.	Alto 3	Grave 2	Alto		Director/Coordinador de TI	A.1.1.6	Se recomienda actualizar la versión del MikroTik, debido a que el dispositivo de red remota está ejecutando una versión de MikroTik anterior a 6.40.9, 6.41,	Actualizar la versión de MikroTik.

									6.42.7, o 6.43. Es, por lo tanto, vulnerable a múltiples vulnerabilidades.	
R.1.1.	MikroTik RouterOS < 6.41.3 SMB Buffer Overflow	• Ataques a través de la red, debido a que no necesita ninguna autenticación especifica.	Alto 3	Muy Grave 3	Critico	MG G M B M A	Director/Coordinador de TI	A.1.1.9	Se recomienda actualizar a MikroTik RouterOS 6.41.3 o posterior.	Actualizar MikroTik.
R.1.2.	82828 - MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	• Ejecución remota de código arbitrario con privilegios del sistema.	Alto 3	Muy Grave 3	Critico	MG G M B M A	Director/Coordinador de TI	A.1.1.12	Se recomienda mejora el parche de Windows, debido a que la versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de entero en la pila de protocolo HTTP (HTTP.sys) debido a un análisis incorrecto de las solicitudes HTTP elaboradas.	Mejora parches.

Elaboración: Las autoras.

12. POLÍTICAS DE CIBERSEGURIDAD

En línea con las prácticas comunes para la gestión de riesgos de seguridad de la información, las políticas básicas que regulan la creación, recogida, almacenamiento, transmisión, distribución, procesamiento y uso general de información de la organización y el personal y la propiedad intelectual en Internet y en el ciberespacio deben determinarse y documentarse. En particular, esto se relaciona con aplicaciones como la mensajería instantánea, blogs, intercambio de archivos P2P, y las redes sociales, que son normalmente más allá del alcance de la red de la empresa y la seguridad de la información. Como parte de las políticas corporativas, las declaraciones y las sanciones relacionados con el mal uso de las aplicaciones del ciberespacio también deben incorporarse para disuadir contra las prácticas de uso indebido por parte de empleados y terceros de la red corporativa o el acceso a los sistemas ciberespacio (ISO, 2012).

Políticas administrativas que promueven la concienciación y la comprensión de los riesgos de seguridad cibernética, y alentador, si no se ordenan, el aprendizaje y desarrollo de habilidades contra los ataques de seguridad cibernética, en particular, los ataques de ingeniería social, deben ser desarrollados y promulgados. Esto debe incluir requisitos para la asistencia regular a este tipo de reuniones de información y formación. Mediante la promoción de políticas y sensibilización adecuadas sobre los riesgos de ingeniería social, los empleados ya no pueden alegar ignorancia de tales riesgos y requisitos, y al mismo tiempo desarrollar una comprensión de las mejores prácticas y las políticas que se esperan de las redes sociales externas y otras aplicaciones ciberespacio, por ejemplo, el acuerdo de la política de seguridad del proveedor de servicios (ISO, 2012)

12.1. POLÍTICAS DE LA CIBERSEGURIDAD APLICADAS A LAS INSTITUCIONES DE EDUCACIÓN PÚBLICA SUPERIOR:

- Establecer políticas de seguridad en el desarrollo y adquisición de los sistemas distribuidos, que permitan controlar el robo de datos como contraseñas, documentos relacionados con el trabajo, hojas de cálculo entre otros, que es algo esencial durante la comunicación en la actualidad.
- Configuración y acceso redes, haciendo uso de cortafuegos, que ayuden a controlar cuales servicios se encuentran expuestos a la red, es decir, que bloquean o restringen el acceso a todo puerto exceptuando únicamente aquellos que deben estar habilitados para el público, evitando así el acceso no autorizado.
- Adquirir protocolos de seguridad con certificaciones validas, que permitan establecer medidas de protección y acciones seguras, en el manejo de la información.
- Establecer sistemas del control de usuarios, que permitan verificar el tiempo de sesiones activas en diferentes horarios.
- Control en la divulgación de información de manera involuntaria como claves de inicio de sesión, por el uso de métodos inapropiados.
- Establecer estrategias de autentificación de usuarios, aplicando políticas de seguridad, como (verificación de inicios de sesión, uso de técnicas de encriptación de contraseñas entre otras).
- Control de proveedores de servicios (internet, software, equipos y dispositivos), para saber que tecnología se adquiere y el tipo de seguridad que estos proveen.
- Garantizar la calidad de los sistemas distribuidos en cuanto al nivel de ciberseguridad y su aplicación en base a la norma ISO/IEC27032.
- Dotar de procedimientos y herramientas que permitan llevar a cabo un debido proceso para agilizar las condiciones del entorno de la información en las IES Públicas de Manabí.
- Capacitar al personal de TI en escenarios de ciberseguridad y concientizar la aplicación de normas de seguridad en el ciberespacio.

12.2. MEDIDAS A TOMAR CON URGENCIA A CORTO Y MEDIANO PLAZO

De acuerdo con la Norma ISO/IEC 27032 de Ciberseguridad y el resultado obtenido en el análisis de riesgos con la metodología AMFE (Análisis Modal de Fallos y Efectos), se considera las siguientes medidas a implementar con un tiempo estimado de aplicación de 6 meses para corto plazo y 1 año para mediano plazo.

A CORTO PLAZO:

- Estandarizar la gestión de calidad de los procesos de seguridad de la información mediante normas de buenas prácticas como la ISO 9000.
- Aplicar herramientas tecnológicas de monitoreo de acceso a los sistemas de información como lo sugiere la Norma ISO/IEC en sus anexos.
- Emplear las Normas de Control Interno 410-09 TI para mejorar el escenario de la seguridad interna de los servicios y procesos.
- Para mejorar el entorno de ciberseguridad aplicar las directrices de la norma ISO/IEC 27032
- Elaborar un plan de seguridad para todo el ciclo de desarrollo, prueba y retroalimentación de las aplicaciones.
- Realizar pruebas de pentest para verificar las medidas de seguridad de las aplicaciones: red, plataforma de alojamiento, sistema web.
- Asegurar que los mensajes recibidos en los sitios web no contengan contenido malicioso, enlaces de phishing o descargas maliciosas.
- Emitir informes periódicos sobre el estado de Ciberseguridad, sesiones de formación en escenarios simulados de ataques cibernéticos, talleres de acciones específicas y pruebas regulares con recorridos en escenarios permanentes.
- Elaborar indicadores de prevención y respuestas frente a ataques cibernéticos.

- Presentar informes mensuales de eventos sospechosos o encuentros maliciosos en las redes.
- Aprobación de las políticas, procedimientos y controles de la seguridad de las redes.
- Asegurar que la información que se suba a la aplicación sea de forma segura verificando que debe estar en un enlace seguro en la URL como HTTPS.
- Verificar que el tráfico de la información esté cifrado o encriptado para evitar ataques como DDoS.
- Utilizar protocolos de comunicación seguros en el ciberespacio.

A MEDIANO PLAZO:

- Implementar manuales de usuarios para el uso efectivo de los sistemas o aplicaciones web.
- Elaborar estrategias para mejorar los servicios TI.
- Elaborar planes de acción para la prevención contra ataques de robo de información de los usuarios en aplicaciones web.
- Elaborar un protocolo de autoevaluación de control para la efectividad de la seguridad de las aplicaciones.
- Generar reportes o informes de eventos maliciosos o fallas de los sistemas de información que se manejan en la institución.

12.3. MEDIDAS A TOMAR CON MENOR URGENCIA A CORTO Y MEDIANO PLAZO

Las autoras consideran que el tiempo estimado de aplicación de estas medidas sea de acuerdo a las necesidades de implementación requeridas por el departamento TI de la institución.

A CORTO PLAZO:

- Capacitación al personal de TI en ciberseguridad de manera contínua.
- Elaborar flujogramas de procesos de desarrollo con metodología ágiles como SCRUM, MIDAS, XP, entre otras.
- Establecer responsabilidades y procedimientos formales a custodios de los equipos tecnológicos y software para el buen uso y seguridad de las aplicaciones.
- Implementar protocolos de autenticación de computadoras dentro de la red para evitar posibles ataques.
- Autenticar los equipos para un mayor control y seguridad en la comunicación entre equipos, como restringir la dirección MAC de cada equipo.

A MEDIANO PLAZO:

- Informar a los usuarios de los controles de seguridad en los sistemas y de los ataques que se han presentado en los mismos a nivel institucional.
- Contratar talento humano especializado o capacitar al personal necesario en seguridad de las aplicaciones.
- Elaborar actas de entrega y recepción de equipos tecnológicos cuando haya cambios de custodio.
- Usar software legal o software libre según lo requiera la aplicación a desarrollar.

- Mantener actualizados los sistemas operativos de acuerdo a las características de los equipos.

13. RESPONSABLES

Los puestos para responsables y/o interesados de llevar a cabo la aplicación del plan, serán contemplando en cuenta según lo establece la Norma 410 TI, Dirección de Autoría Internas DAI-AI-0207-2016 correspondiente a la Contraloría General del Estado, el mismo que refiere que TI debe tener un comité informático conformado por un Director, un coordinador y personal capacitado para las diferentes áreas tecnológicas. Por lo tanto, la máxima autoridad de la ESPAM MFL como órgano rector, debe asignar como responsable al coordinador de TI para el cumplimiento de este plan de acción, y este a su vez designará las responsabilidades a las áreas de desarrollo de aplicaciones, al área de redes y al área de datos (data center).

14. CONCLUSIONES Y RECOMENDACIONES

14.1. CONCLUSIONES

- Al definir las vulnerabilidades de los sistemas se logró concientizar con las instituciones para disminuir riesgos, mejorando la seguridad del manejo de la información de los sistemas distribuidos.
- Al controlar la seguridad de los datos de los sistemas distribuidos de las instituciones de educación superior públicas, en este caso la ESPAM MFL, brindara más seguridad a los usuarios al momento de proporcionar información en los sistemas.
- La evaluación de los riesgos en los procesos de documentación en los dominios de ciberseguridad según los *checklist* aplicados al departamento de TI, basados en la norma ISO/IEC 27032 en el dominio de seguridad de la información con un total de 12 vulnerabilidades, que corresponden al: 50% en el nivel Crítico, 16,67% nivel Alto y 33,33% nivel Medio; en seguridad de las aplicaciones con un total de 14 vulnerabilidades, se presentan en el nivel Crítico el 7,14%, en el nivel Alto 42,86%, en el nivel Medio el 35,72% y en el nivel Bajo el 8,28%; por último en seguridad de las redes con un total de 8 vulnerabilidades, se encuentran en el nivel Crítico el 12,5%, nivel Alto el 37,5% y nivel Medio el 50%, lo que permitió tomar acciones correctivas y establecerlas en el plan de acción para la mitigación de los mismos.
- Las propuestas definidas en este documento permitirán a las instituciones involucradas mejorar, la seguridad en el manejo de la información en los sistemas que estas manejan, aplicando técnicas y recomendaciones mostradas previo a los análisis efectuados con las herramientas de análisis de vulnerabilidad.

14.2. RECOMENDACIONES

- Es importante considerar el tipo o nivel de vulnerabilidad dentro de los dominios que consta un sistema distribuido, debido a que si no se contralan a tiempo, podrían llegar a materializarse y provocar ataques en la web o ciberespacio.
- Para mantener el control en aspectos de ciberseguridad, es necesario implementar como política un monitoreo constante, para que a futuro los sistemas no sean objetivos de ataques, y para sus efectos estos controles de riesgos deberán ser correctivos y preventivos.
- En criterios de normativas o buenas prácticas para los sistemas distribuidos en la web, es importante seguir las directrices de las Normas ISO/IEC 27032 (Ciberseguridad) – 27033 (Seguridad de las Redes) – 27034 (Seguridad de las Aplicaciones) – 27001 y 27002 (Seguridad de la Información) para mejorar la seguridad en el ciberespacio.
- Efectuar adecuadamente estrategias de Ciberseguridad en la institución, como aplicación de normativas, estándares, herramientas que permitan llevar un control y cuidado en la información que se maneja en la Web y de esta manera prevenir en lo más posible ser afectados por terceros en la comunicación de los sistemas distribuidos.

BIBLIOGRAFÍA

ACMS. (2012). NORMA ISO 27032 GESTIÓN DE LA CIBERSEGURIDAD. Disponible en: https://www.grupoacms.com/norma-iso-27032

Avila. (2018). Escaner de vulnerabilidades . Disponible en: https://securityhacklabs.net/articulo/escaner-de-vulnerabilidades-herramientas-2

Candau. (2010). Ciberespacio: delitos, amenazas a la seguridad y ¿guerras? Disponible en: https://www.anepe.cl/ciberespacio-delitos-amenazas-a-la-seguridad-y-guerras/

Cardona. (2015). EVALUACIÓN DE LA AMENAZA, LA VULNERABILIDAD Y EL RIESGO. Disponible en: http://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

Carvajal. (2017). Definición de ciberseguridad y riesgo. Disponible en: https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

Castaño. (2014). Estudio del Trabajo. Disponible en: http://www.cecma.com.ar/__mm/biblioteca/estudio-del-trabajo-rev1-solo-lectura-modo-de-compatibilidad.pdf

Castro. (2011). ¿Qué controles de seguridad posee en su empresa? Disponible en: https://www.welivesecurity.com/la-es/2011/05/11/controles-seguridad-empresa/

Contraloria General del Estado. (2016). Direcciones de Auditorias Internas. DAI-AI-0207-2016
. Disponible en: http://www.contraloria.gob.ec/WFDescarga.aspx?id=31176&tipo=inf

Chopra. (2012). Ley de causa y efecto. Disponible en: https://www.juevesfilosofico.com/la-ley-de-causa-y-efecto/

Enagas. (2019). Politicas de ciberseguridad. Disponible en: https://www.enagas.es/stfls/ENAGAS/Documentos/Politicas/Pol%C3%ADtica%20de%20ciberseguridad%20nf.pdf

García. (2017). Marco Legal - Formas o modalidades legales para operar. Disponible en: http://www.contactopyme.gob.mx/guiasempresariales/guias.asp?s=10&g=4&sg=27

García. (2017). Prevención y mitigación en Gestión de Riesgos de origen natural. Disponible en: https://www.ealde.es/gestion-de-riesgos-prevencion-mitigacion-natural/

Gil. (2017). LA INTEGRACIÓN DEL CIBERESPACIO EN EL ÁMBITO MILITAR. Disponible en: http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar

Grau. (2019). Los 5 paso para crear el plan de acción definitivo. Disponible en: https://agustingrau.com/plan-de-accion/

Guerra. (2017). Significado de Información. Disponible en: https://www.significados.com/informacion/

INCIBE. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INSPQ. (s.f.). Definición del concepto de seguridad. Disponible en: https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

ISOTOOL. (2018). ¿Qué es un checklist y cómo se debe utilizar? Disponible en: https://www.isotools.org/2018/03/08/que-es-un-checklist-y-como-se-debe-utilizar/

BIBLIOGRAPHY ISO. (2012). Tecnología de la información - Técnicas de seguridad -. ESTÁNDAR INTERNACIONAL ISO / IEC 27032, Primera edición 2012-07-15. Revisado y confirmado en 2018.

Lewis. (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad. Disponible en: https://publications.iadb.org/.../Experiencias-avanzadas-en-politicas-y-practicas-de-cibers

Lopez. (2012). Obtenido de ¿Cuál es el origen del término sabotaje?: Disponible en: https://blogs.20minutos.es/yaestaellistoquetodolosabe/cual-es-el-origen-del-termino-sabotaje/

López. (2016). ESTUDIO DEL ESTADO ACTUAL DEL EQUIPO CAMINERO DEL CANTÓN QUERO Y SU INCIDENCIA EN LA DISPONIBILIDAD. Ambato. Disponible en: http://repo.uta.edu.ec/bitstream/123456789/22451/1/Tesis%20I.M.%20326%20-%20Secaira%20L%C3%B3pez%20Alex%20Omar.pdf

LPI. (2016). DERECHOS DE PROPIEDAD INTELECTUAL. Disponible en: http://www.ftaa-alca.org/intprop/natleg/ecuador/L320g.asp

Martínez. (2016). Ciberseguridad una Guía de supervición. Disponible en: https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

Mendoza. (2016). Ética, el factor humano más importante en el ámbito de la ciberseguridad. Disponible en: https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

Mendoza. (2018). El cibercrimen y su relación con el crimen organizado. Disponible en: https://www.welivesecurity.com/la-es/2018/08/10/el-cibercrimen-y-su-relacion-con-el-crimen-organizado/

Microsoft. (2017). Respuesta a incidentes de seguridad de TI. Disponible en: https://docs.microsoft.com/es-es/security-updates/security/respuestaaincidentesdeseguridaddeti

MISP, & MDN. (2015). Disponible en: Base de una política nacional de ciberseguridad: https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

Montalvo. (2012). El individuo Aislado . Disponible en: http://loscuadernosdeixion.blogspot.com/2012/07/el-individuo-aislado-y-el-individuo.html

Mypime. (2016). Guía para la Implementación de Seguridad de la Información en una MIPYME. Disponible en:

https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Nuñez. (2017). Hacktivistas: la amenaza del ciberespacio. Disponible en: https://www.elmundo.es/papel/historias/2017/08/22/599ac51e468aeba4728b4570.html

Pairuna. (2018). ¿Qué es y para que sirve un sitio web? Disponible en: https://www.codedimension.com.ar/noticias-sobre-tecnologia/noticias/que-es-y-para-que-sirve-un-sitio-web/1

Pérez. (s.f.). Seguridad y Alta Disponibilidad. Disponible en: http://www3.gobiernodecanarias.org/medusa/ecoblog/flopmarl/seguridad-y-alta-disponibilidad/

Perugini. (2018). Internet de las cosas - IOT. Disponible en: https://tecnicanet.odoo.com/blog/noticias-1/post/internet-de-las-cosas-iot-8

Rajoy, M. (s.f.). ESTRATEGIA DE CIBERSEGURIDAD NACIONAL. Obtenido de ESTRATEGIA DE CIBERSEGURIDAD NACIONAL: https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Rodríguez. (2016). Definición de línea de acción. Disponible en: http://www.naocluster.com/2016/02/definicion-de-lineas-de-accion-y-grupos.html

Rondero. (2018). LA SEGURIDAD INFORMÁTICA. Obtenido de https://www.lainter.edu.mx/blog/2018/04/23/la-seguridad-informatica/

Rozo. (2016). GESTION DE SEGURIDAD DE LA INFORMACION EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/659/Rozo%20Suarez%20Proyecto%20trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Sanchéz. (2018). Responsabilidad: ¿Qué es? Concepto y claves para ser más responsable. Disponible en: https://blog.cognifit.com/es/responsabilidad/

SASN. (s.f.). Sistema de avisos de seguridad nacional. Disponible en: https://www.fema.gov/media-library-data/20130726-1717-25045-8322/terrorismo.pdf

Silva. (2004). Sistemas distribuidos. Disponible en: http://www1.frm.utn.edu.ar/soperativos/Archivos/Sistemas_Distribuidos.pdf

SIMARKS. (2018). Ciberseguridad en el espionaje industrial. Disponible en: http://www.redseguridad.com/sectores-tic/industria-y-utilities/ciberseguridad-en-el-espionaje-industrial?platform=hootsuite

UCLA. (s.f.). IMPORTANCIA DE LA INFORMATICA. Disponible en: http://www.ucla.edu.ve/dac/Departamentos/coordinaciones/informaticai/documentos/Resumen%20tema2.pdf

UOC. (s.f.). Infraestructura tecnológica. Disponible en: https://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

White. (2014). Escaner de vulnerabilidades Parte I - Acunetix. Disponible en: http://pentest-angelwhite.blogspot.com/2014/04/escaner-de-vulnerabilidades-parte-i.html

ANEXOS

Anexo 1. Oficio de solicitud de levantamiento de información.

República del Ecuador

ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

RECTORADO

Ley 99 – 25 R.O. 181-30-04-1999
CALCETA – ECUADOR

Oficio Nº: ESPAM MFL-R -2018-329A-OF
Calceta, 05 de septiembre de 2018

Ing. Nerina Victoria Avellán Zambrano
Ing. María Fernanda Zambrano Bravo
ESTUDIANTES DE LA MAESTRÍA EN TECNOLOGÍA DE INFORMACIÓN, MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS DE LA ESPAM MFL
Ciudad.-

De mi consideración:

Reciba cordial saludo y los mejores deseos de éxitos en sus delicadas funciones.

Atendiendo vuestro requerimiento mediante oficio SN de fecha 5 de septiembre de 2018, se le concede el correspondiente permiso para que realicen el levamiento de información en el departamento de Tecnología de nuestra Universidad, a fin de desarrollar del trabajo de titulación: "**CIBERSEGURIDAD Y SU APLICACIÓN EN INSTITUCIONES DE EDUCACIÓN SUPERIOR PÚBLICO DE MANABÍ"**; para lo cual puede coordinar acciones con el Lic. Geovanny García Montes, responsable de la Unidad de Tecnología.

Con sentimiento de consideración y estima.

Atentamente,

ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
RECTORADO

Ec. Miryam Elizabeth Félix López. Ph.D.
RECTORA DE LA ESPAM MFL

Copia: Lic. Geovanny García Montes, responsable de la Unidad de Tecnología.

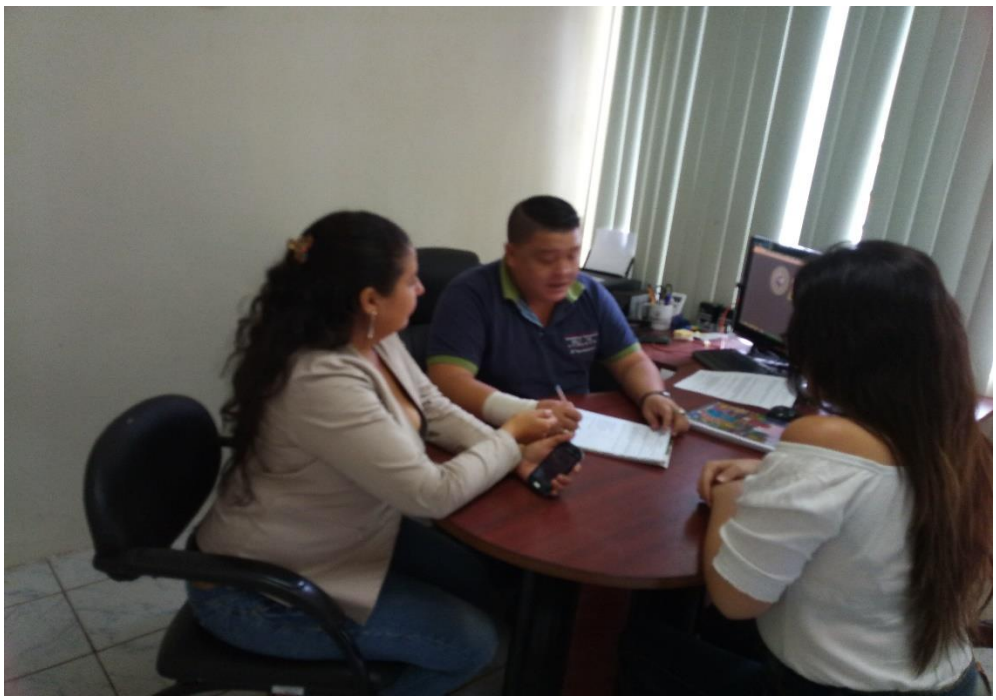
MFL/dzm

Recibido
05-09-2018
14H30

1/1

Dirección: *10 de Agosto Nº 82 y Granda Centeno.* ***Teléfonos:*** *053028808*
Correo: *rectorado@espam.edu.ec*

Anexo 2. Levantamiento de información realizado en la Coordinación de Tecnología de la ESPAM MFL.



Anexo 3. *Checklist*

Anexo 3A. Dominio de Seguridad de la Información

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD							
DOMINIO: SEGURIDAD DE LA INFORMACIÓN (protección de la confidencialidad, integridad y disponibilidad de la información en general)							
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032.							
ÁREA: Tecnología			**ESPAM MFL**				
COMPONENTE	**SECCIÓN**	**HITOS**	**S**	**N**	**OBSERVACIÓN**	**PONDERACIÓN**	**IDENTIFICACIÓN**
PARTES INTERESADAS	**Universidad como consumidora de proveedores externos**	¿La universidad consume servicios en la Web?	x			**4**	**No vulnerable**
		¿Los servicios que consumen son de aplicación?	x			**4**	**No vulnerable**
		Los tipos de servicios que consumen en la Web son:				**4**	**No vulnerable**
		a) Quipux	x				
		b) Sercop	x				
		c) Urkund	x				
		d) Otros servicios	x				
		Dichos servicios forman parte los siguientes Web Services:					
		a) SOAP					

		b) REST					
		c) XML Web Services	x				
		d) otros					
		¿La universidad tiene algún proveedor de servicios de Internet?					
		¿Cuál de ellos son proveedores de servicios de Internet de la universidad:				**4**	
		a) CNT					
		b) CEDIA	x				
		c) Telconet					
		d) Electrocom					
		e) Grupo TVCable Internet					
		f) Netlife					
		g) Perobeli					
		h) Puntonet					

		i) iPlanet					
		j) Clicknet					
		k) Otros proveedores					
		¿Los tipos de servicios que les proveen son:					
		a) Internet	x				
		b) Aplicaciones	x				
		c) Sitios web	x				
		d) Otros servicios					
	Universidad como proveedora	¿La universidad se considera un proveedor de servicios en el ciberespacio?	x				
		Los servicios de aplicaciones virtuales de uso exclusivo para la institución son:				**4**	
		a) Gestión Academíca	x				
		b) Gestión de Talento Humano	x				
		c) Gestión Financiera	x				

		d) Gestión de Biblioteca	x				
		e) Gestión Investigación	x				
		f) Otros servicios					
		Los servicios de aplicaciones y sitios web que brindan a los interesados son:				**4**	**No vulnerable**
		a) Edición de documentos, almacenamiento, distribución.	x				
		b) Entornos virtuales en línea para interacción con otros usuarios.	x				
		c) Repositorios en línea de medios digitales con la agregación, búsqueda, catálogo, servicios de pago.	x				
		d) Gestión de recursos empresariales como humanos, finanzas y nóminas, cadena de suministro, facturación.	x				

		Llevan registro de control de los servicios que brindan en la Web:	x			4	No vulnerable
		a) Usuarios					
		b) Contraseñas de usuarios					
		c) Quejas o comentarios de la disponibilidad de estos servicios.					
ACTIVOS EN EL CIBERESPACIO	ACTIVOS EN LA ORGANIZACIÓN	¿Tienen aplicaciones desarrollados e implementados en la universidad?	x			4	No vulnerable
		Los tipos de aplicaciones o software que se desarrollan son:				4	No vulnerable
		a) Gerenciales					
		b) Académicos	x				
		c) Expertos					
		d) Otros sistemas	x		financiero		
		¿Realizan la documentación de los sistemas de información desarrollados e implementados ?	x			4	No vulnerable
		¿Elaboran manuales de usuario para el manejo de estos sistemas de información?	x		en proceso	2	Vulnerable
		¿Protegen la identidad en línea (username, nickname) de los usuarios	x			4	No vulnerable

		que se registran para acceder a los sistemas de información?					
		¿Implementan un control de seguridad en los sistemas web?	x			4	**No vulnerable**
		¿Los sistemas de información se desarrollan e implementan en diferentes infraestructuras de servicios ?	x			4	**No vulnerable**
		¿Se monitorea el acceso a los sistemas de informacion web?		x		1	**Muy vulnerable**
		¿Los sistemas de información web implemetados tienen reservados los derechos de autor o propiedad intelectual (procesos patentados, patentes, resultados de investigación)?	x			4	**No vulnerable**
		¿Disponen de estrategias para la continuidad del negocio (lanzamiento de productos, datos de informes, marketing?		x		2	**Vulnerable**
		¿Existen controles de acceso al data center?	x			4	**No vulnerable**
AMENAZAS CONTRA LA	**Amenazas y vulnerabilidades**	¿Han sufrido ataques de robo de				2	**Vulnerable**

CIBERSEGURIDAD		identidad o robo de información de los usuarios en:					
		a) Aplicaciones y sitios web					
		b) Bases de datos					
		c) Otros ataques	x				
		Entre los tipos de ataques que se han presentado en la unidad son:				**2**	**Vulnerable**
		a) DDoS (Ataque de negación distribuida de servicios)	x				
		b) Ingeniería social					
		c) DMA (acceso directo a memoria)					
		d) Eavesdropping (intercepción del tráfico en la red)					
		e) Spoofing					
		f) Phishing					
		g) Manipulación de URL					
		h) Escalonamiento de privilegios					
		i) Trashing					
		j) Shoulder Surfing					
		k) Decoy					
		l) DoS (Negación de Servicio)	x				

		m) Ataques contraseña					
		n) Otros ataques			Ipcheck		
		¿Se documentan estos tipos de ataques?	x			4	**No vulnerable**
		¿Tienen medidas de seguridad para disminuir estos ataques?	x			4	**No vulnerable**
		¿ Alerta a los usuarios cuando exite algún tipo de ataque o implementación de controles de seguridad ?	x			4	**No vulnerable**
		¿Los atacantes han utilizado código malicioso en archivos intercambiados como un caballo de Troya para sus ataques?		x		4	**No vulnerable**
		¿Es de conocimiento por parte de los interesados que la seguridad y privacidad según los riesgos involucrados para tomar controles, son relacionados a la información?	x			4	**No vulnerable**
		¿ Como director/coordinador de la unidad, constata y asegura que la información ha sido clasificada	x			4	**No vulnerable**

		de manera que se evite cometer accidentes en cualquier sitio web en el ciberespacio?					
		¿ Efectúa controles de gestión de riesgos de seguridad cibernética en medida y de acuerdo al nivel de madurez de cada proceso?	x			4	**No vulnerable**
		¿ Mantiene prepración continua en Ciberseguridad en la institución?		x		1	**Muy vulnerable**
		¿ Se usan técnicas de visualización de datos para presentar información de eventos?		x		2	**Vulnerable**
		¿ Se estandarizan los datos en base a normas de calidad ?		x		1	**Muy vulnerable**
		Qué Normas de calidad emplea en la estandarización de sus procesos:		x		1	**Muy vulnerable**
		a) ISO					
		b) INEN					
		c) Control Interno					
		d) Otras normas					
		Se realiza el intercambio de archivos de:		x		4	**No vulnerable**

		a) Mensajería instantánea					
		b) Portal web					
		c) Foro de discusión considerando la seguridad					
		¿ Se aplican regulaciones de normas en escenarios de seguridad?		x		1	**Muy vulnerable**
		Qué normas emplean en escenarios de seguridad de la información:				4	**No vulnerable**
		a) ISO 33000					
		b) ISO 8000					
		c) ISO 25012					
		d) ISO 27001	x				
		e) ISO 2000					
		h) ISO 29100					
		i) ISO 270018					
		j) ISO 20000-9					
		k) ISO 22301					
		l) Otras normas					
		¿Qué normas emplean en en escenarios de ciberseguridad:		x		1	**Muy vulnerable**
		a) ISO 27032					
		b) ISO/IEC 27032					
		c) Otras normas					

Anexo 3B. Dominio de la Seguridad de las Aplicaciones

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD							
DOMINIO: SEGURIDAD DE LAS APLICACIONES							
OBJETIVO: Determinar el control, amenazas y vulnerabilidades de los sistemas distribuidos en las instituciones públicas de nivel superior de acuerdo con la norma ISO 27032							
ÁREA: Tecnología			ESPAM MFL				
COMPONENTE	**SECCIÓN**	**HITOS**	**S**	**N**	**OBSERVACIÓN**	**PONDERACIÓN**	**IDENTIFICACIÓN**
ACTIVOS EN EL CIBERESPACIO	**ACTIVOS EN LA ORGANIZACIÓN**	¿El departamento de tecnología cuenta con una metodología y procesos de desarrollo de aplicaciones maduros?		x		**2**	**Vulnerable**
		¿La universidad cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos que implican las ciberamenazas?		x		**2**	**Vulnerable**
		¿Tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas		x		**1**	**Muy vulnerable**

		y producción?					
		¿El departamento de tecnología ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar continuamente la práctica?		x		**2**	**Vulnerable**
		¿Se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable?		x		**2**	**Vulnerable**
		¿La unidad tiene un analista entrenado para correlacionar y evaluar los hallazgos de vulnerabilidades existentes en las aplicaciones?	x			**4**	**No vulnerable**

		¿Qué tipo de aplicaciones se desarrollan en la unidad:					
		a) Móviles					
		b) Web		x			
		c) Otros					
		¿Qué tipo de herramientas tecnológicas utiliza la unidad para realizar pruebas de vulnerabilidades		x		**2**	**Vulnerable**
		a) SAST (Static application security testing).- Analiza pasivamente el código fuente o binario de una aplicación en busca de vulnerabilidades conocidas.					
		b) DAST (Dynamic application security testing).- Prueba y analiza una aplicación en ejecución en busca de comportamientos que indiquen posibles vulnerabilidades					

		c) RASP (Runtime application self-protection).- Herramienta de autoprotección integrada en la aplicación durante su ejecución, permite monitorearse a sí misma para evitar ataques en tiempo real.					
		d) SCA (Software composition analysis).- Identifica, evalúa y monitoriza todos los componentes de terceros (cadena de suministros del software) que puedan contener vulnerabilidades.					
		¿La unidad tiene firewalls de aplicaciones ?	x			**4**	**No vulnerable**
		¿Qué tipo de firewall tienen:				**4**	**No vulnerable**
		a) Firewall de aplicaciones de red	x				
		b) Host apllication firewall	x				
		c) Firewall de aplicaciones web	x				

		¿Se han eliminado servicios y protocolos innecesarios e inseguros para disminuir el ataque cibernético?	x			**4**	**No vulnerable**
		¿Ha considerado la protección avanzada de antivirus o agentes que usen detección y protección basada en comportamiento e inteligencia artificial (AI)?	x			**4**	**No vulnerable**
		¿Se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto interna como externa?		x		**2**	**Vulnerable**
AMENAZAS CONTRA LA SEGURIDAD DEL CIBERESPACIO	**Amenazas y Vulnerabilidades**	¿Se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software?		x		**2**	**Vulnerable**

		¿Se aprueban de manera formal los cambios de equipos tecnológicos y software?		x		**2**	**Vulnerable**
		¿Se prohíbe el uso de software no autorizado por la institución?		x		**3**	**Poco vulnerable**
		¿Se instalan y actualizan periódicamente software de antivirus, firewall contra código malicioso?	x			**4**	**No vulnerable**
		¿Se mantienen los sistemas operativos actualizados con las últimas versiones?		x		**3**	**Poco vulnerable**
		¿Posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos ?		x		**2**	**Vulnerable**
		¿Tienen sitios web legítimos que han sido hackeados?		x		**4**	**No vulnerable**
		¿Se realiza informes de eventos sospechosos o encuentros maliciosos en las aplicaciones ?	x			**4**	**No vulnerable**

		¿El equipo de desarrollo aplica seguimientos o revisión en los mensajes recibidos en el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas?		x		**2**	**Vulnerable**
		Se toman en cuenta los controles de nivel de aplicación:				**4**	**No vulnerable**
		a) Exposición de avisos cortos					
		b) Manipulación segura de sesiones	x				
		c) Validación de entrada segura y prevención de ataques (SQL Inyección)	x				
		d) Scripting o encriptación en sitios o aplicaciones web					
		e) Servicio de la organización o autenticación del servicio					
		¿Se logra los objetivos desarrollados en base a la sensibilizació		x		**2**	**Vulnerable**

		n y formación:					
		a) Proporciona informes periódicos sobre el estado de la Ciberseguridad					
		b) Sesiones de formación enfocados en escenarios simulados de ataque cibernéticos o talleres sobre áreas requeridas de acciones especificas					
		c) Pruebas regulares con recorridos en escenarios permanentes					

Anexo 3C. Dominio de Seguridad de las Redes

CUESTIONARIO DE GESTIÓN DE CIBERSEGURIDAD DOMINIO: SEGURIDAD DE LAS REDES							
COMPONENTE	**SECCIÓN**	**HITOS**	**SI**	**NO**	**OBSERVACIÓN**	**PONDERACIÓN**	**IDENTIFICACIÓN**
ACTIVOS EN EL CIBERESPACIO	**ACTIVOS EN LA ORGANIZACIÓN**	¿Aplican seguridad en la red?	x			**4**	**No vulnerable**
		Entre las políticas, procedimientos y controles que tiene la unidad para seguridad de la red están:		x	en proceso de aprobación	**2**	**Vulnerable**
		a) Políticas de control de acceso a la red					
		b) Controles de acceso a los servidores					
		c) Procedimientos de respaldo de información cuando existe pérdida debido a fallos físicos					
		d) Control de los filtros de tráfico entre la red interna y la externa					
		¿Existen controles que restrinjan la dirección MAC de cada equipo?		x		**2**	**Vulnerable**
		¿Tienen acceso restringido a las redes inalámbricas?	x			**4**	**No vulnerable**
		¿Tienen protocolos de autenticación de computadora		x		**2**	**Vulnerable**

		s dentro de la red?					
		¿Se realiza el proceso de autentificación de los usuarios antes de dejarlos entrar a la aplicación?	x			**4**	**No vulnerable**
		¿Utilizan mecanismos de encriptación para mantener la confidencialidad e integridad de los datos que se están transmitiendo en la web?	x			**4**	**No vulnerable**
		¿Qué método de encriptación utiliza:				**4**	**No vulnerable**
		a) Encriptación simétrica (Data Encryption Estándar - DES)	x				
		b) Encriptación asimétrica (llave pública, llave privada)					
AMENAZAS CONTRA LA SEGURIDAD DEL CIBERESPACIO	**Amenazas y Vulnerabilidades**	¿Utilizan protocolos de comunicación como :				**2**	**Vulnerable**
		a) HTTP	x				
		b) HTTPS					
		c) MAILTO					
		d) FTP					
		¿ Como director /coordinador de la unidad se asegura		x		**2**	**Vulnerable**

		que la URL de su contenido web este citado como un enlace seguro en su navegador?					
		¿El SSL que utiliza el sitio web, identifica el contenido original del nuevo contenido dañado, plantado por un atacante?		x		**2**	**Vulnerable**
		Entre los tipos de ataques en la seguridad de la red que han sufrido están:		x		**4**	**No vulnerable**
		a) Interrupción: destrucción física de equipos, borrado de aplicaciones, falla de sistema operativo, etc.					
		b) Intercepción: reproducción ilícita de archivos, intercepción de los cables para monitoreo de datos en una red, etc.					
		c) Modificación: modificaciones de bases de datos, cambios en la configuraciones de software del sistema, etc.					
		d) Fabricación: insertar registros en bases de datos, añadir transacciones a un sistema					

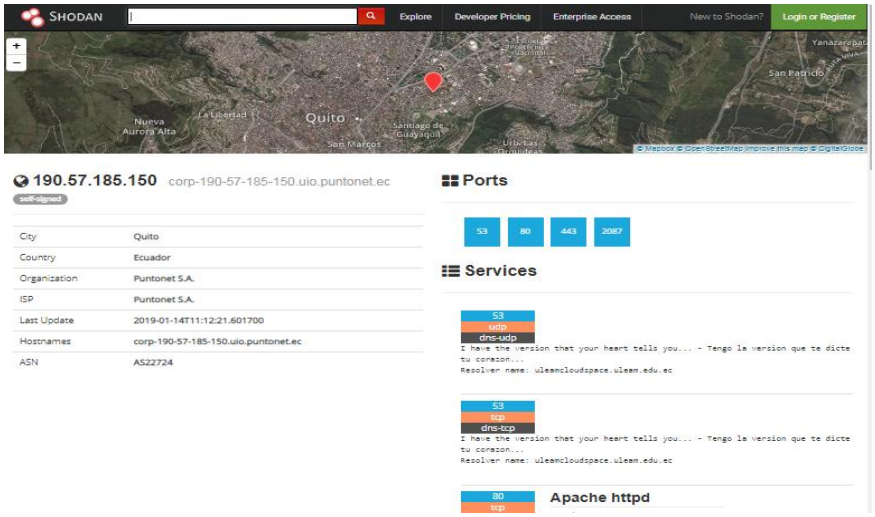
		de comunicaciones, etc.					
		¿ La unidad tiene medidas de prevención y respuestas a los ataques cibernéticos?		x		**1**	**Muy vulnerable**
		Ha tenido atacantes que se hacen pasar por una entidad autorizada para robar información como:		x		**4**	**No vulnerable**
		a) Hombre en el medio (Man in the maddle)					
		b) Otro tipo de robo de información					
		¿Se toman medidas de autenticación de comunicación para evitar el ataque de Man in the Midle?	x			**4**	**No vulnerable**
		¿Han sufrido ataques de IP Spoofing para manipular las direcciones IP asociadas a los mensajes en un intento de disfrazar el ataque como fuente conocida para ganar el acceso no autorizado a los sistemas?		x		**4**	**No vulnerable**
		Las redes WIFI en la institución están protegidas en:				**4**	**No vulnerable**
		a) WIFI Gestionado (portal cautivo)		x			

		b) Claves de acceso a WIFI	x				
		c) Otros tipos de protección	x				
		d) Protocolos para Redes abiertas	x				
		¿Se han vistos comprometidos los servidores en Internet con el método de desbordamiento de búfer provocando que el servidor funcione fuera de su entorno normal (control), facilitando la inserción / ejecución de código malicioso?		x		**4**	**No vulnerable**
		¿ Se realiza informes de eventos sospechosos o encuentros maliciosos en las redes?		x		**1**	**Muy vulnerable**
		¿De qué manera protejen los servidores contra el acceso no autorizado y el ajoamiento de contenido malicioso:				**4**	**No vulnerable**
		a) Configuración de servidores	x				
		b) Implementa un sistema o nuevas actualizaciones de seguridad		x			
		c) Supervisar el rendimiento del servidor de seguridad	x				

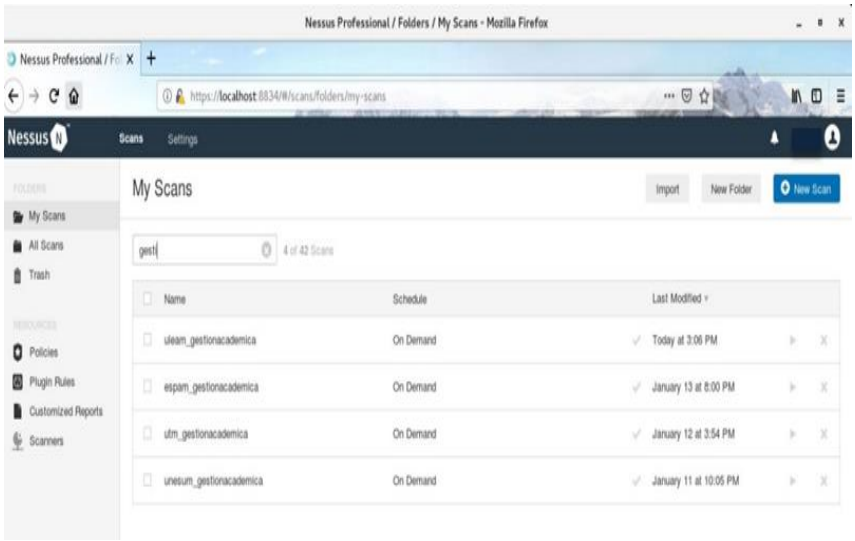
		mediante examenes periódicos o auditorías					
		d) Revisa la configuración de seguridad	x				
		e) Ejecuta controles de software anti-maliciosos		x			
		f) Analizar el contendio alojado y subido regularmente hasta la fecha de controles de software anti-maliosos		x			
		g) Realiza evaluaciones periódicas de vulnerabilidad y las pruebas de seguridad en los sitios en línea y aplicaciones		x			
		h) Regularmente escanea en busca de compromisos		x			

Anexo 4. Análisis de las herramientas de escaneo de vulnerabilidades.

SHODAN:



NESSUS:



ACUNETIX: