Universidad CENFOTEC

Maestría en Ciber Seguridad

Documento Final de Proyecto de Investigación Aplicada 2

Tema

Implementación de un Marco de Referencia para el Análisis de Vulnerabilidades de los Sitios Web en las Instituciones Públicas de Costa Rica

Autor

Aguilar Mora Kenneth Josué

Fecha

Julio-2022

Declaración de derechos de autor

Este documento es propiedad de Kenneth Josué Aguilar Mora, el cual se presenta como una investigación en el área de seguridad informática, como trabajo de graduación de la carrera de Maestría en Ciber Seguridad de la Universidad CENFOTEC, y su información es de carácter confidencial, debido a que se habla de posibles vulnerabilidades de las instituciones públicas de Costa Rica, y es de uso EXCLUSIVO de la Universidad CENFOTEC, para el fin que fue realizado.

Dedicatoria y agradecimientos

Agradecer a mi padre, Johnny Aguilar Fernández, y mi madre, Leticia Mora Ávila, que siempre me han alentado en mi vida a lograr las cosas y ser una mejor persona; a mi esposa, Susana Matarrita Arce, que me ha acompañado durante este trayecto final de la carrera impulsándome en cada momento para culminar el trabajo.

A todos los profesores, que, durante toda la carrera con su conocimiento, han hecho un gran aporte a mi desarrollo profesional y como persona.

Al profesor, Miguel Pérez Montero, que ha sido un gran profesor y gran tutor, que me ha guiado durante todo este proyecto, y a poder finalizarlo de manera exitosa.

Y por último, a la Universidad CENFOTEC y todo su equipo de trabajo, por brindarme todo lo necesario para poder culminar de manera exitosa la carrera, y en todo momento orientar en el proceso que esta implica.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Aguilar Mora Kenneth Josué.**

MIGUEL PEREZ MONTERO (FIRMA)
Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2022.07.08 14:01:37 -06'00'

M. Sc. Miguel Pérez Montero
Tutor

MARIO ANDRES ZAMORA MADRIZ (FIRMA)
Firmado digitalmente por MARIO ANDRES ZAMORA MADRIZ (FIRMA)
Fecha: 2022.07.09 08:52:56 +02'00'

MSEG. Mario A. Zamora Madriz
Lector 1

ALVARO CORDERO PEÑA (FIRMA)
Firmado digitalmente por ALVARO CORDERO PEÑA (FIRMA)
Fecha: 2022.07.12 22:16:55 -06'00'

MAP. Álvaro Cordero Peña
Lector 2

San José, Costa Rica, 07 de julio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Contenido

ABSTRACT **10**

CAPÍTULO 1. INTRODUCCIÓN **11**

1.1. GENERALIDADES 11

1.1.1. Antecedentes *11*

1.2. DEFINICIÓN Y DESCRIPCIÓN DEL PROBLEMA 11

1.3. JUSTIFICACIÓN 12

1.4. VIABILIDAD 12

1.4.1. Punto de vista técnico *12*

1.4.2. Punto de vista operativo *12*

1.4.3. Punto de vista económico *13*

1.5. OBJETIVOS 13

1.5.1. Objetivo general *13*

1.5.2. Objetivo específico *13*

1.6. ALCANCES Y LIMITACIONES 13

1.6.1. Alcance *13*

1.6.2. Limitaciones *13*

CAPÍTULO 2. MARCO TEÓRICO **14**

2.1. CIBER SEGURIDAD 14

2.1.1. ¿QUÉ ES CIBER SEGURIDAD? 14

2.1.2. COSTA RICA 15

2.1.3. INCONVENIENTES 23

2.2. MAYORES AMENAZAS EN CIBER SEGURIDAD 24

2.2.1. Nivel Mundial *25*

2.2.2. Costa Rica *26*

CAPÍTULO 3. MARCO METODOLÓGICO **29**

3.1. TIPO DE INVESTIGACIÓN 29

3.1.1. Población *29*

3.1.2. Técnicas *29*

3.1.3. Procedimientos *29*

3.1.4. Enfoque de la investigación *29*

CAPÍTULO 4. PROPUESTA DE SOLUCIÓN **29**

4.1. MARCO DE REFERENCIA PARA EL ANÁLISIS DE VULNERABILIDADES 30

4.1.1. Introducción *30*

4.1.2. Análisis de Vulnerabilidades *30*
4.1.3. Enumeración de Servicios *32*
4.1.4. MITIGAR LAS VULNERABILIDADES DE LOS SITIOS WEB 37
4.1.4.1. Control de acceso+ *37*
4.1.4.2. Fallas criptográficas *37*
4.1.4.3. Inyección de código *38*
4.1.4.4. Diseño no seguro *38*
4.1.4.5. Configuración incorrecta de seguridad *39*
4.1.4.6. Componentes vulnerables y desactualizados *39*
4.1.4.7. Fallas de identificación y autenticación *39*
4.1.4.8. Fallas de integridad del software y datos *39*
4.1.4.9. Errores de registro y supervisión de seguridad *39*
4.1.4.10. Falsificación de solicitudes del servidor (SSRF) *40*

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES 40

5.1. CONCLUSIONES 40
5.2. RECOMENDACIONES 41

REFERENCIAS 42

APÉNDICES 46

ANEXOS 47

Tabla de figuras

FIGURA 1 ..... **15**

FIGURA 2 ..... **18**

FIGURA 3 ..... **19**

FIGURA 4 ..... **20**

FIGURA 5 ..... **21**

FIGURA 6 ..... **21**

FIGURA 7 ..... **22**

FIGURA 8 ..... **23**

FIGURA 9 ..... **24**

FIGURA 10 ..... **25**

FIGURA 11 ..... **25**

FIGURA 12 ..... **28**

FIGURA 13 ..... **28**

FIGURA 14 ..... **32**

FIGURA 15 ..... **33**

FIGURA 16 ..... **33**

FIGURA 17 ..... **34**

FIGURA 18 ..... **35**

FIGURA 19 ..... **35**

FIGURA 20 ..... **36**

FIGURA 21 ..... **36**

FIGURA 22 ..... **37**

FIGURA 23 ..... **38**

Índice de tablas

TABLA 1.....**16**

TABLA 2.....**25**

Abstract

Esta investigación pretende mostrar herramientas y posibles soluciones a los problemas que tienen las instituciones públicas de Costa Rica, respecto a las vulnerabilidades de los sitios web, para ayudar a mitigar los posibles ataques, que en muchos casos se materializan por cosas tan sencillas como un software desactualizado, poniendo como plano un panorama general de las vulnerabilidades de los sistemas de información, a nivel internacional y cómo se encuentra Costa Rica en esta materia en las instituciones públicas, que bien se sabe que muchas de ellas no cuentan con el personal, ni el presupuesto para hacerle frente a posibles ataques que puedan ocurrir.

Capítulo 1. Introducción

1.1. Generalidades

Esta investigación tiene como propósito proveer un marco de referencia para el análisis de vulnerabilidades de los sitios web, que pueda ser de ayuda para las instituciones públicas, ya que son las que menos recursos poseen a nivel nacional, y donde surgen muchos ataques, y se exponen grandes cantidades de información, la cual puede ser información sensible, e incluso llegar a dejar sin el uso de los servicios que dichas páginas ofrecen.

1.1.1. Antecedentes

Actualmente no existe, como tal, un marco de referencia para el análisis de vulnerabilidades de sitios web en Costa Rica, el cual pueda ser utilizado de manera general por las instituciones públicas, solamente existe una Estrategia Nacional de Ciber Seguridad, que es promovida por el Ministerio de Ciencia y Tecnología y Telecomunicaciones en el año 2017.

1.2. Definición y descripción del problema

Costa Rica ha sido blanco de los ciber ataques, y ha ido en aumento en los últimos años. Un ejemplo de entidades públicas que han sufrido ciber ataques es el Banco de Costa Rica, con el hackeo del grupo MAZE, y su filtración de información confidencial, como así lo expuso el noticiero CR Hoy, donde dicho grupo de hackers, expusieron en un sitio web los datos que extrajeron de dicha entidad bancaria. (Solano, 2020). Algunas otras entidades como Archivo Nacional, Ministerio de Relaciones Exteriores y la Asamblea Legislativa han sufrido vulnerabilidades en sus sistemas informáticos, donde fueron atacados con *malware* de tipo *ransomware* (Jiménez, 2019)

Los sitios web de las municipalidades de Costa Rica, tampoco están exentos de dichos ataques, y es que en 2018, algunas municipalidades del país como Corredores, Puntarenas, Matina, San Isidro, sufrieron ciber ataques por parte de un grupo de hackers llamado "*Pak Monster Cyber Thunder*" según artículo de ESET. (Harán, We Live Security, 2018) Como se ha evidenciado, muchas entidades públicas de Costa Rica sufren de diversos ataques, esto sin contar los posibles ataques que sufren por usuarios internos, donde existen filtraciones de información, como por ejemplo datos bancarios de ciudadanos, que los obtienen los privados de libertad desde diferentes centros penales, para intentar realizar estafas.

Una situación que es un gran problema es que a nivel mundial ha existido un faltante de profesionales en el campo de ciber seguridad. "Según un informe reciente de *Cybersecurity Ventures*, el crecimiento de las vacantes en el sector de la ciberseguridad se espera que crezca en un 350% para el 2021. Sin embargo, la escasez de profesionales con

las habilidades suficientes para cubrir esa demanda se estima que generará, para ese mismo año, tres millones y medio de vacantes a lo largo del mundo que no serán cubiertas.” (Harán, We Live Security, 2019). En Costa Rica, evidentemente no es una excepción la falta de profesionales en este campo, prueba de ello es que en el Ministerio de Obras Públicas y Transportes (MOPT) en 2018, no existía una unidad que atendiera incidentes de seguridad, además, el viceministro de Ciencia y Tecnología y Coordinador Nacional en Ciberseguridad en esa época, calificó en 8,5 la situación general de las instituciones públicas, en una escalada de 1 a 10. El 25% de las entidades estatales estaría por debajo del 7, además dijo, “En promedio se necesitan tres especialistas por institución y en la gran mayoría hay uno, que además está a cargo de otras labores”, situación que no deja ser muy diferente en muchas otras entidades. (Pérez, 2018).

Independientemente de la entidad pública, se deberían establecer políticas de seguridad para así poder disminuir ciber ataques, que en algunas ocasiones, suelen ocurrir por situaciones como no tener los sistemas actualizados. Y es que dichas situaciones pueden provocar grandes pérdidas financieras y una mala reputación, como la filtración de datos del Banco de Costa Rica, por la cual posiblemente algunos clientes quisieron cambiar de banco.

1.3. Justificación

Uno de los principales motivos de esta investigación es poder ayudar a las instituciones públicas en materia de ciber seguridad, ya que como se menciona en la descripción del problema, muchas carecen de los recursos necesarios para poder combatir las ciber amenazas que se puedan presentar. Así mismo, aunque no esté orientado a las PYMES del país, estas también podrían aprovechar esta guía y adaptarla a sus realidades.

1.4. Viabilidad

1.4.1. Punto de vista técnico

Para la realización del marco de referencia de análisis de vulnerabilidades de los sitios web de las instituciones públicas, se requiere el conocimiento técnico adecuado sobre todo lo que conlleva las vulnerabilidades que se puedan encontrar, para de esta forma determinar cuáles son los pasos adecuados a seguir para su detección y corrección, además de poder diseñar una guía, de tal forma que cualquier persona la comprenda sin necesidad de tener el conocimiento en materia de ciber seguridad.

1.4.2. Punto de vista operativo

La parte operativa está en manos del encargado de realizar el marco de referencia sobre el análisis de vulnerabilidades de los sitios web de las instituciones públicas, ya que deberá distribuirlo a cada una de las instituciones que deseen implementar dicho marco,

posteriormente guiarles, y poner en marcha para que sean capaces de aplicarlo periódicamente.

1.4.3. Punto de vista económico

La investigación como tal realmente requiere un esfuerzo de tiempo, para poder obtener el conocimiento adecuado, para realizar el marco de referencia, y poder así llevar a cabo su implementación, lo que no tiene un costo como tal, y las herramientas (*software*) que se lleguen a utilizar, serán las de versión gratuita, para que las instituciones no tengan que recurrir a un gasto, ya que esto es uno de los principales problemas para poder tener un mejor nivel de ciber seguridad, el costo que representa todo esto, y poder alivianar un poco, para de esta forma mermar posibles ataques.

1.5. Objetivos

Para la realización de los objetivos, se está utilizando la Taxonomía de Bloom de 1956, para mostrar la jerarquización de los conocimientos y tener un mayor orden a la hora de mostrar cada uno de ellos.

1.5.1. Objetivo general

Elaborar un marco de referencia para el análisis de vulnerabilidades de los sitios web de las instituciones públicas de Costa Rica para construir un ciclo de revisión y mejora de la seguridad.

1.5.2. Objetivo específico

- Identificar los mayores problemas para solventar las fallas en ciber seguridad en las instituciones públicas.
- Determinar los mayores inconvenientes en ciber seguridad.
- Aplicar un plan piloto para determinar las vulnerabilidades de los sitios web en las instituciones públicas.

1.6. Alcances y limitaciones

1.6.1. Alcance

Se realizará una implementación de un marco de referencia para el análisis de las vulnerabilidades de los sitios web de las instituciones públicas, con el fin de que les pueda brindar una herramienta más para poder mitigar los posibles ataques que puedan sufrir de ciber seguridad.

1.6.2. Limitaciones

Al ser un marco de referencia general puede ser aplicado a la mayoría de instituciones públicas, pero existirán limitaciones de materia legal, dependiendo de la institución donde se vaya a aplicar, ya que no todas trabajan de la misma manera, a pesar de ser públicas.

Capítulo 2. Marco teórico

2.1. Ciber Seguridad

Se va a definir qué es la ciber seguridad, para tratar de dar un preámbulo, y así poder abarcar poco a poco cada uno de los objetivos planteados en este proyecto, y llegar a cumplir el objetivo general de la elaboración de un marco de referencia.

2.1.1. ¿Qué es ciber seguridad?

La ciber seguridad según la Unión Internacional de Telecomunicaciones es "(…) el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno" (PROSIC, 2012, p. 310).

Se puede ver que la ciber seguridad es un conjunto de muchas cosas, a las que en muchas ocasiones no se les presta atención, y por esto muchas amenazas se materializan. Todo comienza con lo más sencillo, y en algunas ocasiones lo que es un poco tedioso de establecer: las políticas de seguridad, definir bien todos los conceptos alrededor de este tema, para así poder establecer esas normas adecuadamente, y principalmente que sigan los objetivos de cualquier organización.

La seguridad de la información busca resguardar tres características muy importantes, que pueden llamarse los pilares de la seguridad informática, que son: confidencialidad, integridad y disponibilidad (ver figura 1). Los atacantes tratan de vulnerar cualquiera de ellas y poner en jaque a la organización. La ciber seguridad es la seguridad de la información en el ciber espacio, es decir, aplicaciones expuestas a Internet.

Figura 1
Triángulo de la Seguridad de la Información

Fuente (PROSIC, 2012)

2.1.2. Costa Rica

Costa Rica en los últimos años ha reportado mayores incidencias de ciber seguridad, haciendo ver a los directores de seguridad que no están exentos de este tipo de amenazas, y que se debe prestar mayor atención a este tipo de situaciones. Y no es para menos, Costa Rica en 2021 inició el año con más de 87 millones de intentos en ciber ataques, esto solo en el primer trimestre (CAMTIC, 2021), y tomando en cuenta que los datos son a nivel de cualquier organización o institución en el país, que posiblemente las instituciones públicas sean las de mayor incidencia, a estos datos no se le suman los del año anterior que fueron casi 200 millones de ataques (Castro, 2021).

Si bien es cierto, Costa Rica aumentó 39 puestos en el Índice Global de Ciberseguridad, y actualmente se ubica en la posición 76, lo cual hace que el país sea uno de los 10 más ciberseguros de América Latina (ver tabla 1) (MICIT, MICIT, 2021), pero hay algunos aspectos que no han mejorado del todo.

Tabla 1

Resultados de la Región Americana

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10
Paraguay	57.09	11
Peru	55.67	12
Argentina	50.12	13
Panama	34.11	14
Jamaica**	32.53	15
Suriname	31.2	16
Guyana	28.11	17
Venezuela	27.06	18
Ecuador	26.3	19

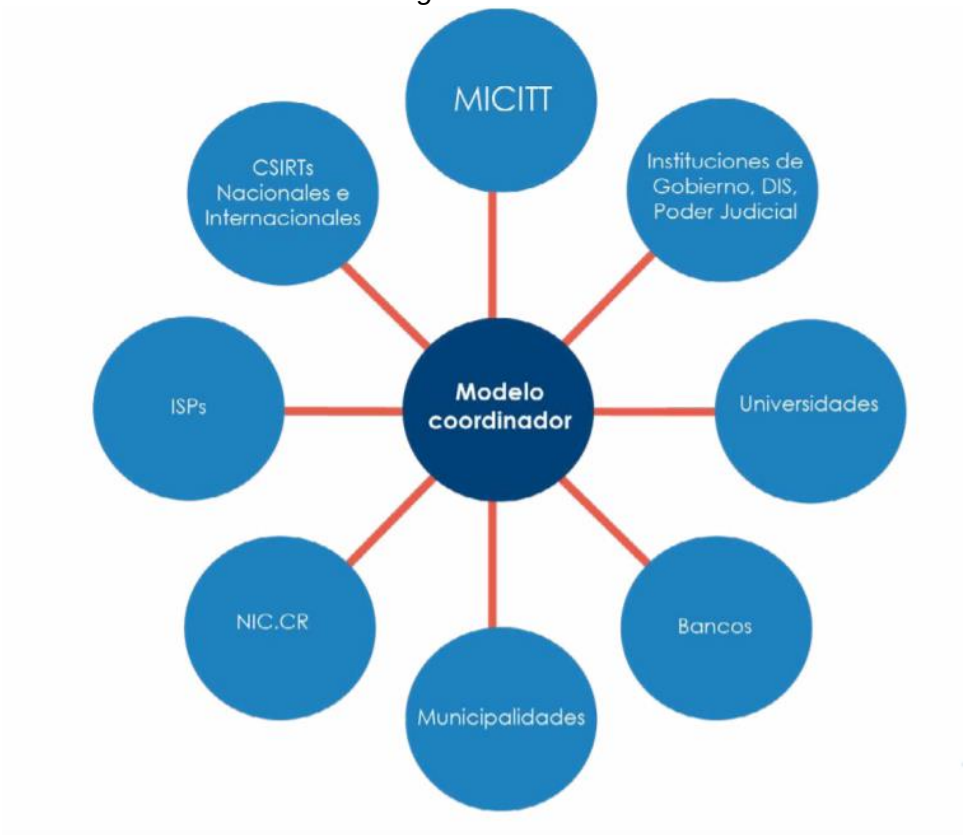
Tabla 1. Se muestra el puntaje y puesto de cada país en materia de ciber seguridad. (Global Security Index, 2020).

En Costa Rica, se cuenta con algunas herramientas para incorporar la ciber seguridad, incluso está explícito en MIDEPLAN (Ministerio de Planificación Nacional y Política Económica), en el aparte denominado Ciberseguridad en el Sistema de Planificación Nacional, donde se muestran esas herramientas. Se cuenta con el CSIRT-CR que es el Centro de Respuesta de Incidentes de Seguridad Informática, el cual fue creado mediante el Decreto Ejecutivo 37052-MICIT y se encuentra en las instalaciones del MICITT (Ministerio de Ciencia, Tecnología y Telecomunicaciones), este Centro se encarga de prevenir y responder ante cualquier incidente de ciber seguridad que ocurra en las instituciones gubernamentales. (MIDEPLAN, 2020). También está la Estrategia Nacional de Ciberseguridad de Costa Rica, la cual dice que “plantea un esfuerzo conjunto y articulado entre todos los sectores del país, para así garantizar que los objetivos que se establezcan sean equilibrados, eficaces y acordes a la realidad nacional, definiendo los principios generales que marcarán la pauta en esta materia.” (MICIT, MICIT, 2017). Además de esto existe todo un marco legal que acuerpa los esfuerzos que se indican en MIDEPLAN y el MICITT, a saber:

- Ley 4573: Código Penal.
- Ley 8968: Protección de la Persona frente al tratamiento de sus datos personales.
- Ley 8454: Ley de Certificados, Firmas Digitales y Documentos Electrónicos.
- Ley 7975: Ley de Información No Divulgada.
- Ley 8934: Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos.
- Ley 7472: Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor y su reglamento.
- Ley 9452: Adhesión al Convenio de Europa sobre Ciberseguridad (Budapest, 2001).
- Decreto Ejecutivo 37052-MICIT: Crea Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR.
- Decreto Ejecutivo 019-MP-MICITT: Desarrollo del Gobierno Digital del Bicentenario.
- Decreto Ejecutivo 41248-MP-MICITT-PLAN-MEIC-MC: Creación de la Comisión de alto nivel de Gobierno Digital del Bicentenario.
- Decreto Ejecutivo 031-MICITT-H: Mejoras en la eficiencia del gasto público mediante el uso adecuado de tecnologías digitales en el sector público.
- Decreto Ejecutivo 053-H-MICITT: Regulación y normalización de adquisiciones de tecnología o desarrollo de sistemas informáticos de apoyo a la gestión.
- Directriz Ejecutiva 051-MTSS-MICITT: Implementación de sitios Web accesibles en el sector público costarricense.

  Se puede ver todo en conjunto como un modelo que se encarga de coordinar todas las acciones pertinentes de ciber seguridad en Costa Rica.

Figura 2
Modelo Coordinador de Ciberseguridad Costa Rica



Fuente (MIDEPLAN, 2020)

A pesar de los grandes esfuerzos por tratar de mejorar en materia de ciber seguridad, incorporándolo en MIDEPLAN, teniendo una Estrategia Nacional propuesta por el MICITT, y haber alcanzado el puesto 8 según *Global Security Index* a nivel americano, hay cosas en las cuales aún se está debiendo y mucho, ya que un informe de ciberseguridad del 2020, por parte del BID (Banco Interamericano de Desarrollo), muestra un modelo de madurez de la capacidad de ciberseguridad, basado en 5 dimensiones, que son:

1. Política y estrategia de ciber seguridad.
2. Cultura cibernética y sociedad.
3. Educación, Capacitación y habilidades en ciberseguridad.
4. Marco legales y regulatorios.
5. Estándares y organizaciones tecnológicas.

Las siguientes dimensiones se mostrarán una a una en una figura, la cual contempla una comparativa a cómo estaba el país en el año 2016 y cómo se estuvo en el año 2020.

En la figura 3 que respecta a la dimensión uno, de Políticas y Estrategia de Seguridad Cibernética, se puede ver que en el apartado 1.1, 1.2, se ha avanzado enormemente. Es interesante que en el 1.3, 1.4 y 1.5, aún sigue igual a como se estaba hace 4 años, estos son

apartados muy importantes, y se siguen teniendo grandes carencias, y si se suman los ataques mencionados anteriormente, algo no está del todo bien.

Figura 3

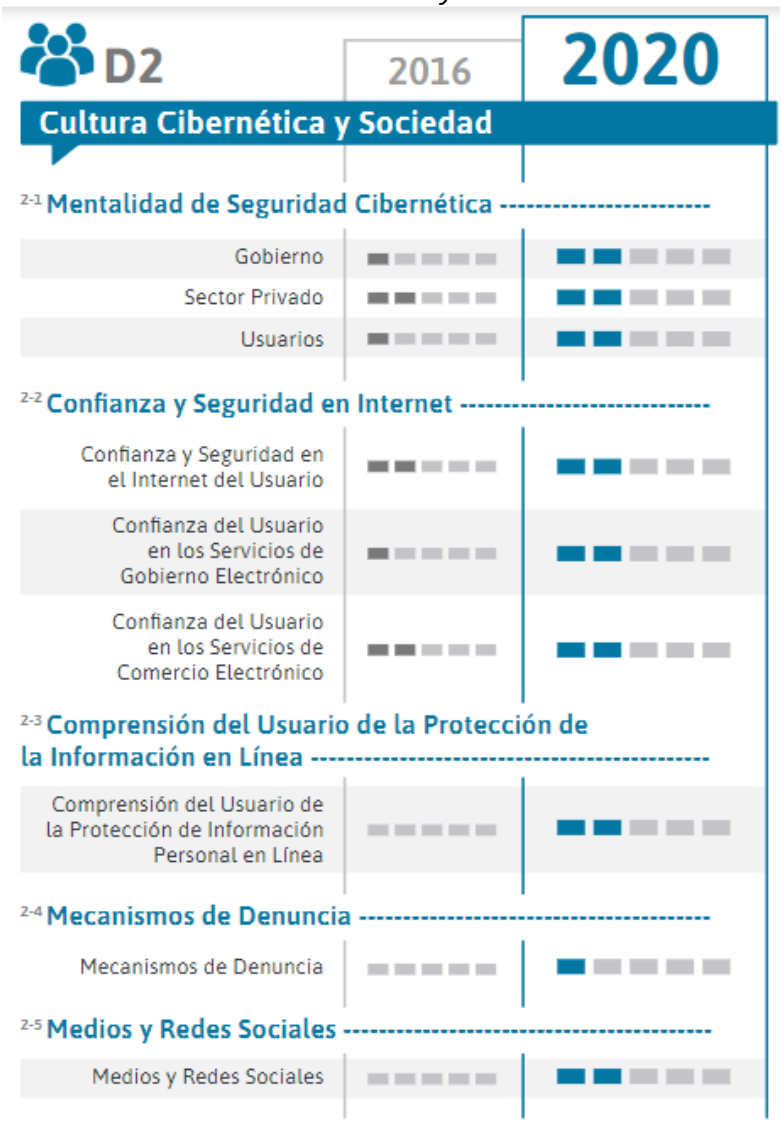
Dimensión 1: Política y Estrategia de Seguridad Cibernética

Fuente (BID, OEA, 2020).

La dimensión dos, que habla sobre cómo se encuentra el país en Cultura Cibernética y Sociedad (ver figura 4), se ha logrado avanzar un poco, quizá no de la manera que se quisiera, pero en cada uno de los apartados, se logró avanzar a como se estaba hace 4 años.

Figura 4

Dimensión 2: Cultura Cibernética y Sociedad



Fuente (BID, OEA, 2020).

La dimensión tres se enfoca en Formación, Capacitación y Habilidades de Seguridad Cibernética (ver figura 5), en la cual el país está prácticamente igual que hace 4 años, y es lamentable que en este campo no se haya avanzado mucho, y actualmente una de las universidades que brinda una carrera como tal en esta área es la Universidad CENFOTEC.

Figura 5

Dimensión 3: Formación, Capacitación y Habilidades de Seguridad Cibernética

Fuente (BID, OEA, 2020).

La dimensión cuatro hace referencia al marco legal y regulaciones que existen en Costa Rica, y como se puede ver en la figura 6, en el año 2020 se tuvo un gran avance, y esta es de las 5 dimensiones en la que se ha logrado mayor mejoría, en relación al 2016.

Figura 6

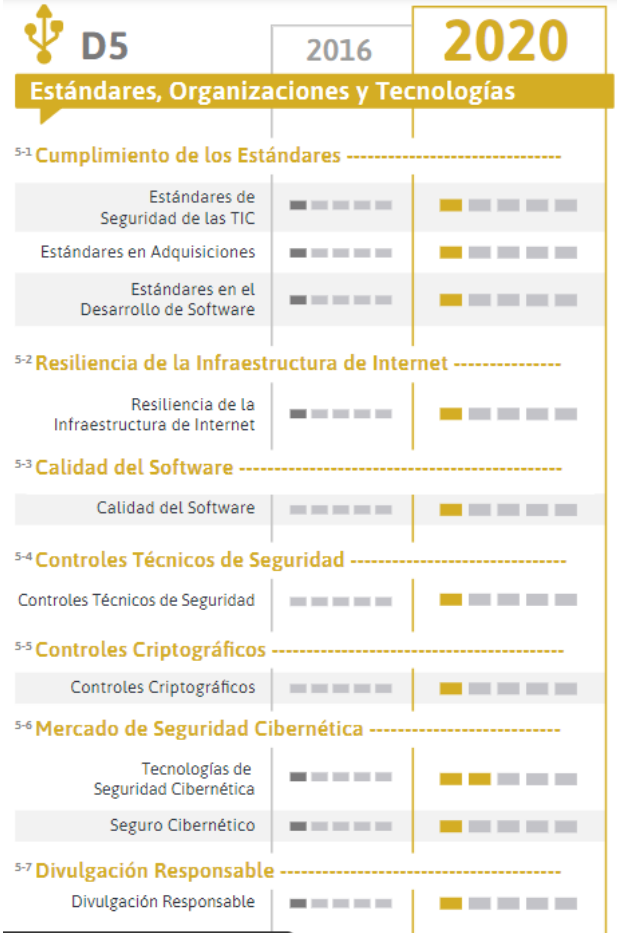
Dimensión 3: Marcos Legales y Regulatorios

Fuente (BID, OEA, 2020)

La dimensión 5 se centra en estándares, organización y tecnología, esta es otra de las partes que, en lo que respecta al 2016 en comparación con 2020, no cambió mucho, solamente unos cuantos puntos fueron los que tuvieron una leve mejoría.

Figura 7

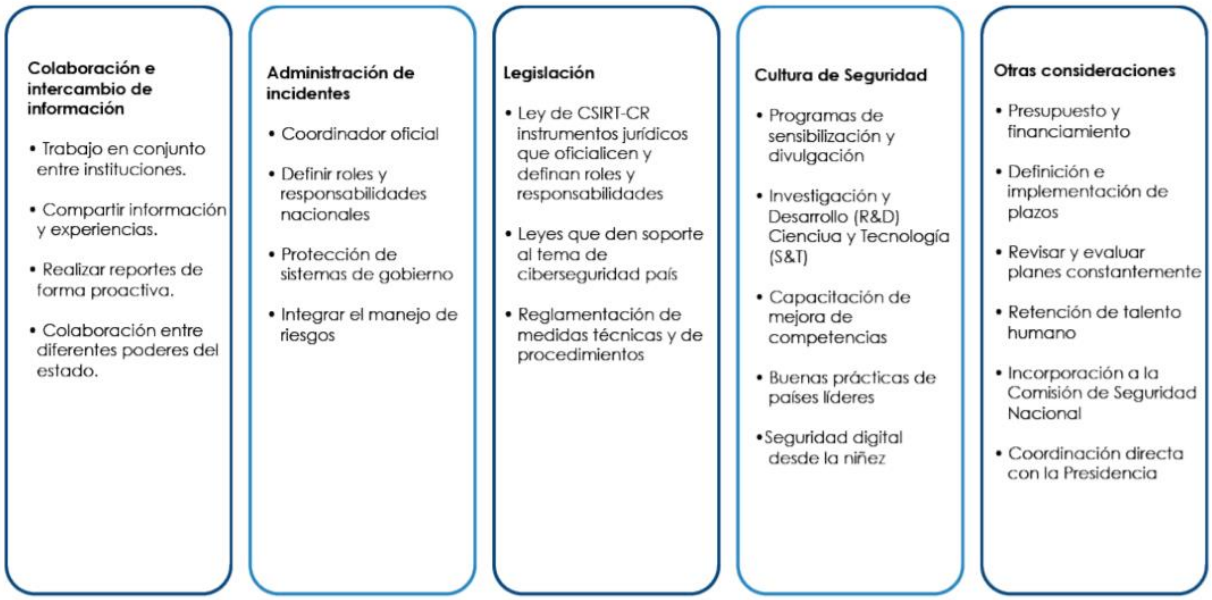
Dimensión 5: Estándares, Organizaciones y Tecnologías



Fuente (BID, OEA, 2020).

Costa Rica cuenta con algunos retos y acciones que se plantean en MIDEPLAN, en materia de ciberseguridad (ver figura 8), donde se menciona una de las más importantes variables que es “Presupuesto y financiamiento”, ya que muchas organizaciones no quieren invertir en materia de ciberseguridad dado que no se considera oportuno, a pesar de tener las estadísticas y demás datos al alcance.

Figura 8
Retos y Acciones



Fuente (MIDEPLAN, 2020)

2.1.3. Inconvenientes

Teniendo en cuenta todo lo anterior, se nota que hay grandes inconvenientes para poder tener un Estado seguro en relación con ciberseguridad, y uno de los factores débiles principales es la importancia que se le da a la ciberseguridad, y que los altos mandos lo tomen en cuenta para invertir en dicho campo. También como se vio en las dimensiones anteriores, otro punto a favor, a pesar que se ha avanzado mucho, es la legislación desactualizada, y una ciudadanía que no está informada y que le toma poca importancia a este tipo de situaciones. Kevin Moraga, docente e investigador en el Centro Académico de Alajuela, indica que “vivimos en un país muy contento, con muchas cosas positivas, pero hay que darles su importancia a temas de seguridad cibernética. Podemos incluso decir que estamos perdiendo competitividad, porque no existe la seguridad para tener bases de datos que alberguen datos de otros países”, (Venegas, 2018).

Laura Chaves Lavagni, Abogada, Letrada de la Sala de Casación Penal, Jueza Penal e Integrante Suplente del Consejo Superior del Poder Judicial, da a conocer datos sumamente importantes del OIJ, de acuerdo con esto, el número de denuncias aumentó significativamente en el año 2020, y solo en lo que tiene que ver con fraudes, estas se debieron a timos (9.279), estafas (4.031), estafa informática (777) y suplantación de identidad (643), demostrando cómo es el modus operandi de los delincuentes, y una de las técnicas más usadas por ellos es el *phishing*[1], para de esta forma poder obtener los credenciales de

[1] Delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. (MalwareBytes, 2021)

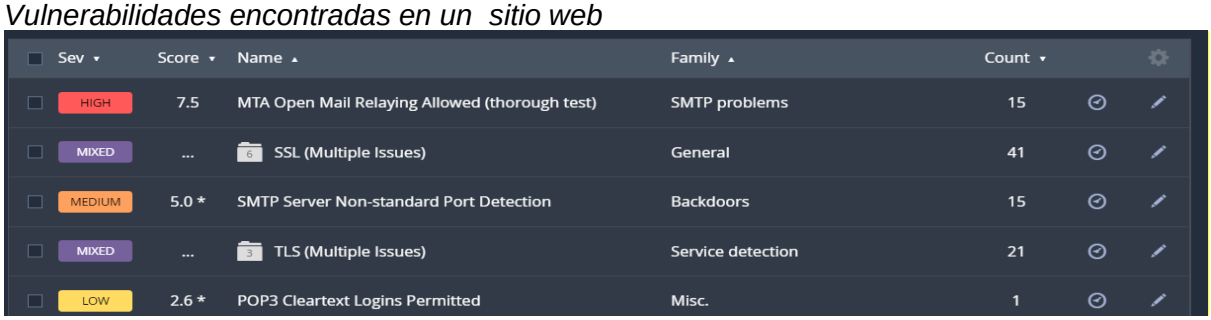
las personas y acceder a sus cuentas, esto se observa constantemente cuando se realizan llamadas por parte de personas inescrupulosas haciendo creer que son del banco para robar los datos de los usuarios. (Lavagni, 2021).

Por otra parte, Lavagni considera que hay 2 tipos de brechas en seguridad que se deberían enfocar, las cuales son la parte técnica y una inadecuada política de contraseñas. Si se toma la primera que ella menciona, esto implica sistemas desactualizados, malas configuraciones, o errores de desarrollo. (Lavagni, 2021).

No es para menos que se tengan grandes problemas en el área técnica, y es que uno de los hackeos ocurrido a una municipalidad de la provincia de Limón, en el 2018, por un grupo de hackers denominado "*Pak Monster Cyber Thunders*", aprovechó alguna vulnerabilidad que tenía el sitio web e hizo que dejara de funcionar por varios minutos. (Eillyn Jiménez B. y Monserrath Vargas L., 2018). Pero al parecer, a pesar de que ya ocurrió un incidente en 2018, en la figura 9 se puede ver un ejemplo de análisis de vulnerabilidades, utilizando la herramienta *Nessus Essential* para realizar este tipo de escaneos, en busca de alguna vulnerabilidad en sitios web, donde se presentan algunos fallos como lo es en cifrado y los protocolos de correo electrónico SMTP y POP3, fallos que pueden solucionarse fácilmente con reconfigurar adecuadamente los protocolos o el cifrado, según la solución planteada por la herramienta *Nessus Essential* , que haciendo uso de una herramienta como esta se pueden prevenir algún ataque como el ocurrido en la Municipalidad de Matina.

Figura 9

Vulnerabilidades encontradas en un sitio web



Fuente elaboración propia 2021

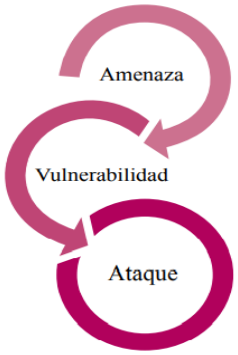
2.2. Mayores Amenazas en Ciber Seguridad

En el mundo de la informática, existen muchísimas amenazas, y no existe ningún sistema que sea 100% seguro, lo que sí se puede hacer es minimizar aquellas amenazas que puedan afectar a los sistemas críticos.

Una amenaza se puede definir como "cualquier ocurrencia potencial, maliciosa o no, que pueda tener un efecto indeseable en los recursos de una organización. Una vulnerabilidad está siempre asociada a una amenaza y es básicamente cualquier característica de un sistema que permita (potencialmente) que una amenaza ocurra."

(Sliesarieva, 2010, p. 39), amenaza y vulnerabilidad siempre van a ir de la mano, ya que la amenaza se aprovecha de la vulnerabilidad para así poder materializar el ataque. (Ver figura 10).

Figura 10
Relación entre Amenaza, Vulnerabilidad y Ataque



Fuente (PROSIC, 2012)

2.2.1. Nivel Mundial

Alrededor del mundo, existen diferentes tipos de amenazas, e incluso se ha creado un *TOP10* de amenazas de las aplicaciones web. Grandes compañías, como Soluciones Seguras y ESET, dieron a conocer una lista de las 10 principales amenazas cibernéticas del 2020 y qué dejó el 2019, evidentemente en los siguientes años los cibercrímenes aumentarán, esto abonado a la pandemia. Los cibercrímenes llegarán a costar al mundo alrededor de 6 mil millones de dólares. (Murillo, CRHoy, 2020).

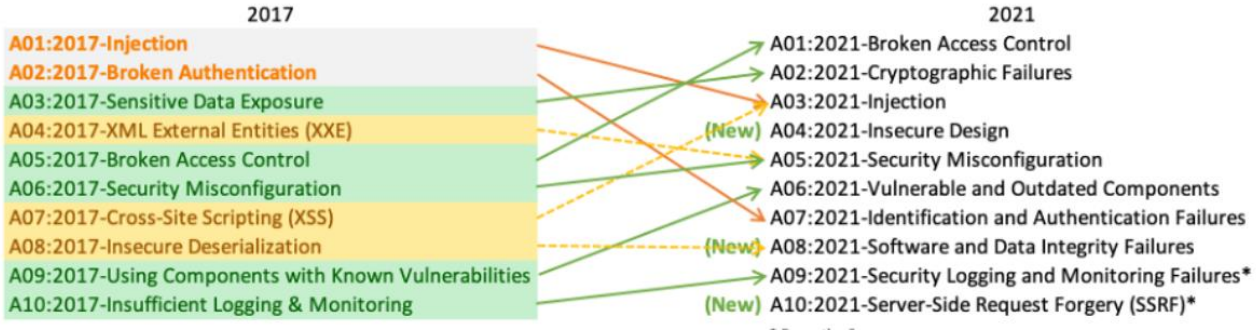
Tabla 2
Ciber amenazas 2019/2010

Año 2019	**Año 2020**
Suspensión de soporte Windows 7	Nueva guerra fría cibernética
Vulnerabilidad WinRaR	Fake news 2.0, elecciones EEUU
Vulnerabilidad Bluekeep	Ataques infraestructura crítica
Filtración de datos privados	*Ransomware* dirigido
Gandrab dejo de operar	*Phishing* más allá del email
Ransomware dirigido	Ataques de *malware* a móviles
Problemas con Facebook	5G: más dispositivos, más velocidad, más riesgo
Grupo de ATP The Dukes continúa activo	Inteligencia Artificial
Ciber espionaje América Latina	Empresas buscan la nube
Varenyky: sextorsión y posibilidad de grabar pantallas a sus víctimas	Empresas de alto perfil en la mira

Fuente (Murillo, CRHoy, 2020).

Como se mencionó anteriormente, existe un TOP10 de ataques y vulnerabilidades sobre las aplicaciones web, y esta ha sido creada por Proyecto Abierto de Seguridad de Aplicaciones Web, OWASP por su acrónimo en inglés, esto con el fin de que se desarrollen web seguras.

Figura 11
Top10 de OWASP 2017-2021



Fuente (OWASP, OWASP, 2021).

Como se puede observar en la figura 11, uno de los que ha subido de puesto para este 2021 ha sido el control de acceso, que de estar en la quinta posición, llegó hasta el primer lugar, y es que, debido a la pandemia, muchas personas trabajan desde sus hogares, dejando de lado la seguridad de sus equipos y no teniendo cuidado de quiénes puedan manipular sus equipos, esto se ha vuelto un poco más complicado para las organizaciones, tomando en cuenta que muchas no tenían políticas de teletrabajo.

En el puesto dos, se encuentran los fallos criptográficos, y como se pudo ver en la figura 9, uno de los sitios web escaneados con *Nessus Essential*, que presentaba un problema en TLS y SSL, ya que según esta herramienta *Nessus Essential* , para TLS se le dio un puntaje de 6.5, con una severidad “Medium”, esto basado en CVSS[2] v3.0, y para SSL se le dio un puntaje de 7.5, con una severidad “High”.

2.2.2. Costa Rica

A pesar de que Costa Rica es un país pequeño, no queda exento de los ciber ataques, y es que a lo largo de los años, cada vez son más frecuentes los ataques. Sitios web de páginas del gobierno fueron hackeadas, Ministerio de Trabajo en 2014 (Guerrero, CRHoy, 2014), en 2015 hackearon el sitio web de Consejo Nacional de Persona Adulta (CONAPAM) (CRHoy, 2015), ese mismo año el Instituto Costarricense de Ferrocarriles (INCOFER) fue la víctima de los hackers (CRHoy, 2015), el 05 de enero del 2016 fue el turno del Ministerio de Ambiente, Energía y Mares, (Guerrero, CRHoy, 2016), en mayo del 2018 algunas páginas con extensión .go.cr fueron hackeadas, entre ellas, las Municipalidades de Puntarenas, Corredores y Matina dejaron de funcionar (Eillyn Jiménez B. y Monserrath Vargas L., 2018), en 2019 Archivo Nacional, Ministerio de Relaciones Exteriores y la Asamblea Legislativa (Jiménez, 2019), 2020 uno de los bancos públicos más grandes del país fue parte de un robo

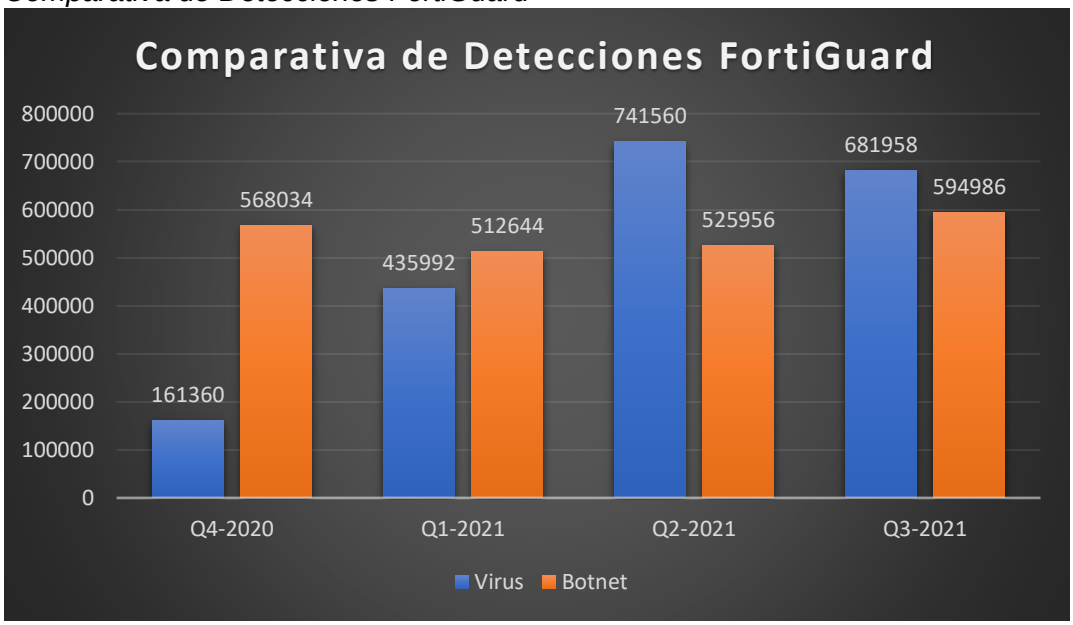
[2] Common Vulnerability Scoring System, es un sistema (métrica) de score con el que poder medir el impacto que una vulnerabilidad puede tener si es explotada.

de información, según lo dijo el grupo de hackers Maze, que realizó un robo al Banco de Costa Rica (Solano, 2020), como se puede ver, desde el 2015 hasta el 2020, muchas instituciones del gobierno sufrieron inconvenientes en sus sitios web. En el 2018, un artículo de El Financiero, expone como título, “Falta de especialistas expone a instituciones públicas en seguridad informática”, y no es para menos, en la nota se indica que el Ministerio de Obras Públicas y Transporte (MOPT), no tiene un área dedicada a la ciber seguridad, “Las limitaciones presupuestarias que afectan al Gobierno han limitado las contrataciones”, respondió Allan Borges Quesada, director de informática del MOPT. “Es importante reiterar que la institución no tiene de lado el tema”. En Costa Rica, aún no le están dando la importancia que se debería, en el MICITT se hacen esfuerzos junto con MIDEPLAN, pero aún no es suficiente, falta ese empuje económico que les ayude. Sanders Pacheco, viceministro de Ciencia y Tecnología y Coordinador Nacional en Ciberseguridad en el 2018, dijo “En promedio se necesitan tres especialistas por institución y en la gran mayoría hay uno, que además está a cargo de otras labores”. (Pérez, 2018).

Otra institución que resaltamos es el Ministerio de Educación Pública (MEP), en 2021, se ha visto implicado por muchas situaciones, tanto con las pruebas FARO, con su cuestionario de factores asociados, y la revista con frases sexuales explícitas. Este ministerio en su POLÍTICA EN TECNOLOGÍAS DE LA INFORMACIÓN DEL MINISTERIO DE EDUCACIÓN PÚBLICA, de marzo de 2020, está implementando correcciones solicitadas por la auditoría en informes 17-16 (MEP, MEP, 2020, p. 3). Estos informes, mediante el resultado de las auditorias, indican que “la BD Bachilleres se encontraron debilidades, como: la carencia de una política de seguridad de la información, la inexistencia de un procedimiento formal de administración de roles, perfiles y cuentas de usuario, y la ausencia de manuales técnicos y de usuario para el Sistema de “Consulta de Bachilleres”; así también se observaron, deficiencias en la seguridad lógica de datos y problemas de integridad referencial.” (MEP, MEP), algo que en estos tiempos no debería ser así.

FortiGuard, una organización de investigación e inteligencia de amenazas, realiza escaneos a nivel mundial, para encontrar amenazas en cada región. A nivel de Costa Rica, en la figura 12, se muestra una comparación de los últimos 4 cuatrimestres desde 2020 a la fecha, de cómo han ido variando las detecciones, respecto a virus y botnet, siendo los virus los que han tenido un gran incremento con el pasar del tiempo.

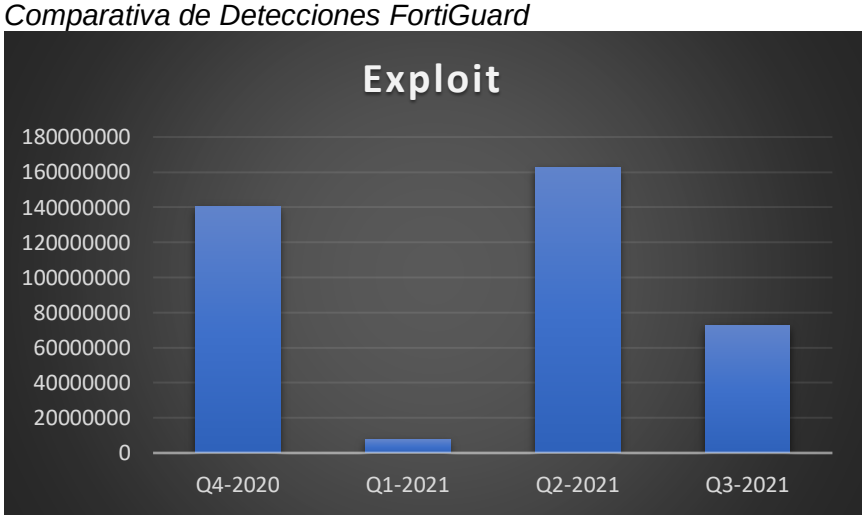
Figura 12
Comparativa de Detecciones FortiGuard



Fuente (FortiGuard, 2021).

En la figura 13, se observan las detecciones respecto a los *exploit* encontrados en Costa Rica, y se ve que es muy cambiante, en el primer trimestre del 2021 realmente hubo muy pocas detecciones de *exploit* , los demás cuatrimestres tienen muchas detecciones.

Figura 13
Comparativa de Detecciones FortiGuard



Fuente (FortiGuard, 2021).

Capítulo 3. Marco metodológico

3.1. Tipo de investigación

3.1.1. Población

La población son las instituciones públicas, y la muestra serán las Municipalidades de la provincia de Limón.

3.1.2. Técnicas

Se realizará un análisis de vulnerabilidades con la herramienta *Nessus*, para ver el estado de los sitios web de algunas municipalidades del país (se reservan los nombres por aspectos de seguridad calificada), para tomarlo como base de la necesidad de dicha investigación, que además será tomado para el marco de referencia, del qué hacer y cómo.

3.1.3. Procedimientos

El principal procedimiento es el trabajar en un marco de referencia, que pueda ayudar a realizar el análisis de vulnerabilidades de los sitios web, para que de esta forma, una vez detectado, aquellas vulnerabilidades, trabajar sobre ellas, y ver las correcciones que se deben realizar en cada una de las encontradas, esto para que cualquier funcionario de T.I. pueda llevar a cabo sin necesidad de conocimientos extras en ciber seguridad.

3.1.4. Enfoque de la investigación

El tipo de investigación a realizar es del tipo aplicada, ya que “guarda íntima relación con la básica y pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos, pero se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación aplicada busca el conocer para hacer, para actuar, para construir, para modificar.” (Zorrilla, 1993)

Se busca crear un marco de referencia para el análisis de vulnerabilidades de los sitios web, para que este pueda ser aplicado en las instituciones públicas, que pueda ser de gran ayuda para poder minimizar los posibles ataques que puedan recibir en ciber seguridad, creando un ciclo, que se pueda ver las vulnerabilidades, actuar, construir mejores procedimientos de seguridad, modificar los posibles errores que se encuentren o mejorar los procedimientos, y estar en una constante revisión, algo similar a lo que menciona Zorrilla “para hacer, para actuar, para construir, para modificar.”

Capítulo 4. Propuesta de solución

Se propone un marco de referencia explicando cada proceso para realizar un análisis de vulnerabilidades utilizando la herramienta *Nessus Essential,* qué vulnerabilidades corregir de acuerdo con su severidad y calificación obtenida según la herramienta, y los planes de acción a realizar.

Para efectos de los sitios Web analizados, y dada la confidencialidad de las posibles vulnerabilidades encontradas en los mismos, las gráficas en este capítulo tienen protegidas las direcciones IP y los nombres de los sitios escaneados, con el propósito de anonimizar las instituciones utilizadas en la prueba de concepto.

4.1. Marco de referencia para el análisis de vulnerabilidades

4.1.1. Introducción

El fin de este marco de referencia es poder describir el procedimiento que conlleva el realizar un análisis de vulnerabilidades en un sitio web, para de esta forma poder mitigar los riesgos que puedan existir a partir de una mala configuración o software desactualizado.

Toda vulnerabilidad cuenta con un "score" y una severidad, que previamente ha sido establecida, y además cuenta con un CVE-ID[3]. Los "score" y severidad de cada vulnerabilidad encontrada serán basados en la métrica que la herramienta *Nessus Essential* da, posterior al análisis a cada vulnerabilidad encontrada en los diferentes sitios web, y para la consulta de CVE-ID se puede utilizar la información dada por el *National Institute of Standards and Technology* | *NIST* de su base de datos nacional de vulnerabilidades, o la base de datos de CVE - CVE (mitre.org), cualquiera de ellas posee la misma información.

4.1.2. Análisis de Vulnerabilidades

Es una técnica que se utilizará para evaluar los sitios web de las municipalidades de la provincia de Limón, de manera externa, identificando cualquier tipo de servicio disponible, puertos abiertos, versiones de servicios, para a partir de ahí, detectar posibles vulnerabilidades, presentes en el objetivo, para de esta forma poder elaborar un plan de acción adecuado para así mermar las vulnerabilidades y afectaciones que puedan sufrir los sistemas a partir de dichas vulnerabilidades. En este caso, el análisis solo será de manera externa, ya que muchos de los ataques perpetrados anteriormente por grupos de hackers, fueron realizados desde afuera, valiéndose de posibles vulnerabilidades. Además, para no realizar ningún tipo de prueba que pueda resultar invasiva y ser detectada como un potencial ataque, lo cual puede tener repercusiones hasta legales.

El objetivo como tal de un análisis de vulnerabilidades es encontrar aquellas debilidades antes de que un atacante logre materializarlas, y que a partir de cualquier cambio realizado en el sistema se logre ver cuáles afectan al sistema, y además poder ponerse del lado del atacante y tener un panorama desde ese punto de vista.

[3] Common Vulnerabilities and Exposures, "es una lista de fallas de seguridad informática divulgadas públicamente. Cuando alguien se refiere a un CVE, se refiere a una falla de seguridad al que se le ha asignado un número de identificación CVE." (RedHat, 2020)

No existe ningún documento que recomiende la periodicidad con que deben realizarse los análisis de vulnerabilidades. En ESET, se considera que debe realizarse continuamente el análisis de las vulnerabilidades, esto debido a que constantemente están saliendo nuevas amenazas, lo cual lo vuelve un “contra reloj”, ya que los desarrolladores buscan cómo parchar la aplicación que es vulnerable, y los atacantes en desarrollar *exploit* y códigos maliciosos para aprovechar esa debilidad encontrada en el sistema. (Mendoza, 2015).

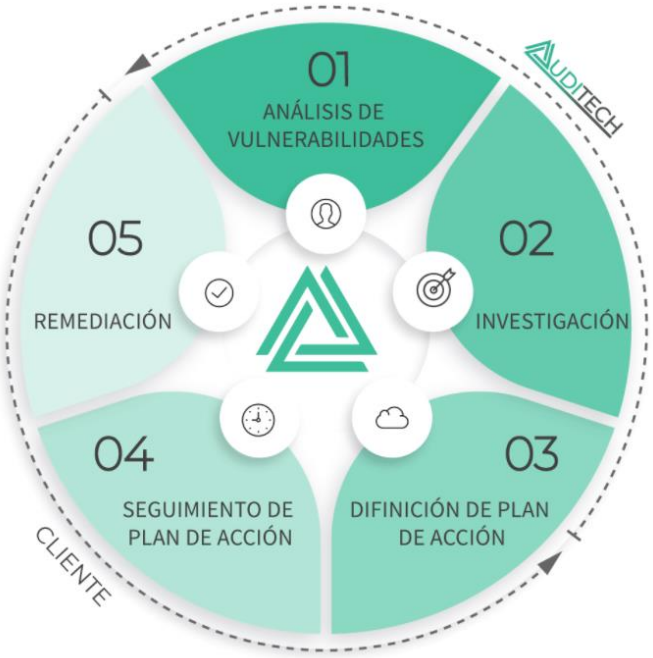
Para realizar un análisis de vulnerabilidad, se deben considerar ciertas variables, tales como:

- Cada vez que se realice un cambio en el sistema de información, desde un dispositivo o la implementación de un nuevo módulo en alguna aplicación, o todo un sistema nuevo.
- Cuando se anuncien nuevas vulnerabilidades que puedan afectar al sistema de información directa o indirectamente, por ejemplo: *Log4Shell*.
- Si previamente se ha establecido en alguna política,
- Y cada tres meses en el sistema, indiferentemente si ocurre de alguna de las situaciones anteriores, esto debido al cambio constante que sufren los sistemas de información, con la incorporación de nuevos dispositivos.

4.1.3. Ciclo de vida del análisis

El análisis de vulnerabilidades es un proceso de mejora continua, como bien se menciona anteriormente, ya que los atacantes constantemente están buscando cómo perpetrar ataques a los sistemas constantemente. En la figura 14, se puede observar, por llamarlo de alguna forma ,el ciclo de vida del análisis de vulnerabilidades, el cual ya previamente debe tener su objetivo para realizarlo, para seguidamente realizar una investigación de los servicios y puertos abiertos que puedan contener alguna vulnerabilidad. Luego de encontrar esas vulnerabilidades, saber qué se va a hacer con ellas, ya que no basta encontrarlas, sino realizar las correcciones necesarias y realizar los informes necesarios con las evidencias encontradas. En el seguimiento del plan de acción, se deben hacer dichas correcciones, con el personal correspondiente o encargado, para ya por último realizar las recomendaciones necesarias para evitar tener vulnerabilidades, o al menos mermarlas, ya que bien se sabe que no existe un sistema 100% seguro.

Figura 14
Ciclo de vida del análisis de vulnerabilidades



Fuente (López, 2022).

4.1.3. Enumeración de Servicios

La enumeración de servicios se utiliza en análisis de vulnerabilidades para poder extraer información de usuarios, nombres de máquinas, recursos de red compartidos y servicios, puertos que se encuentran abiertos y servicios que están corriendo en dichos puertos (EC-Council, 2022), con el fin de poder ver si se encuentra algún servicio vulnerable a partir de la versión de dicho servicio. Posteriormente, también es utilizado para realizar pruebas de penetración, pero lo que interesa es solo conocer dichas vulnerabilidades para corregirlas y evitar que puedan ser penetrados los sistemas de información.

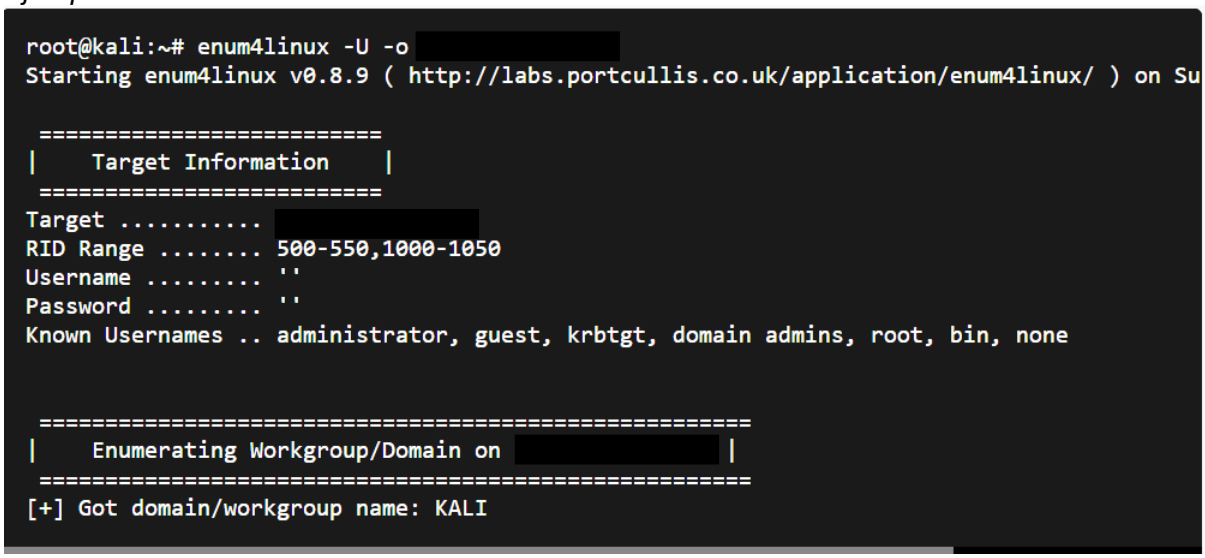
4.1.3.1. Tipos de enumeración de servicios

Dentro de la enumeración existen muchos tipos de técnicas para obtener la información que se desea, en este caso se describirán algunos, pudiendo existir muchos otros que no se detallan acá.

1. Enum4Linux: Es una herramienta que permite poder obtener la información de sistemas como Windows y Samba (Kali Linux, 2021), la cual será muy útil la información recolectada, si se quisiera hacer pruebas de penetración.

Figura 15

Ejemplo de Enum4Linux

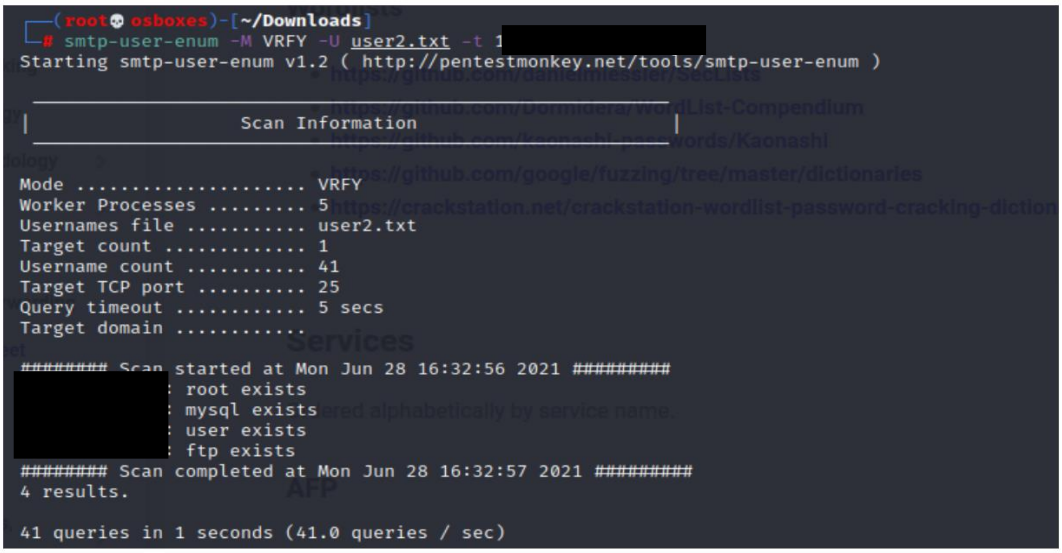


Fuente (Kali Linux, 2021).

2. SMTP-User-Enum: Es un protocolo de transferencia de correo simple, el cual permite enumerar los usuarios que hay en el sistema, utilizando una lista de usuarios que se haya creado con anterioridad o descargado de internet.

Figura 16

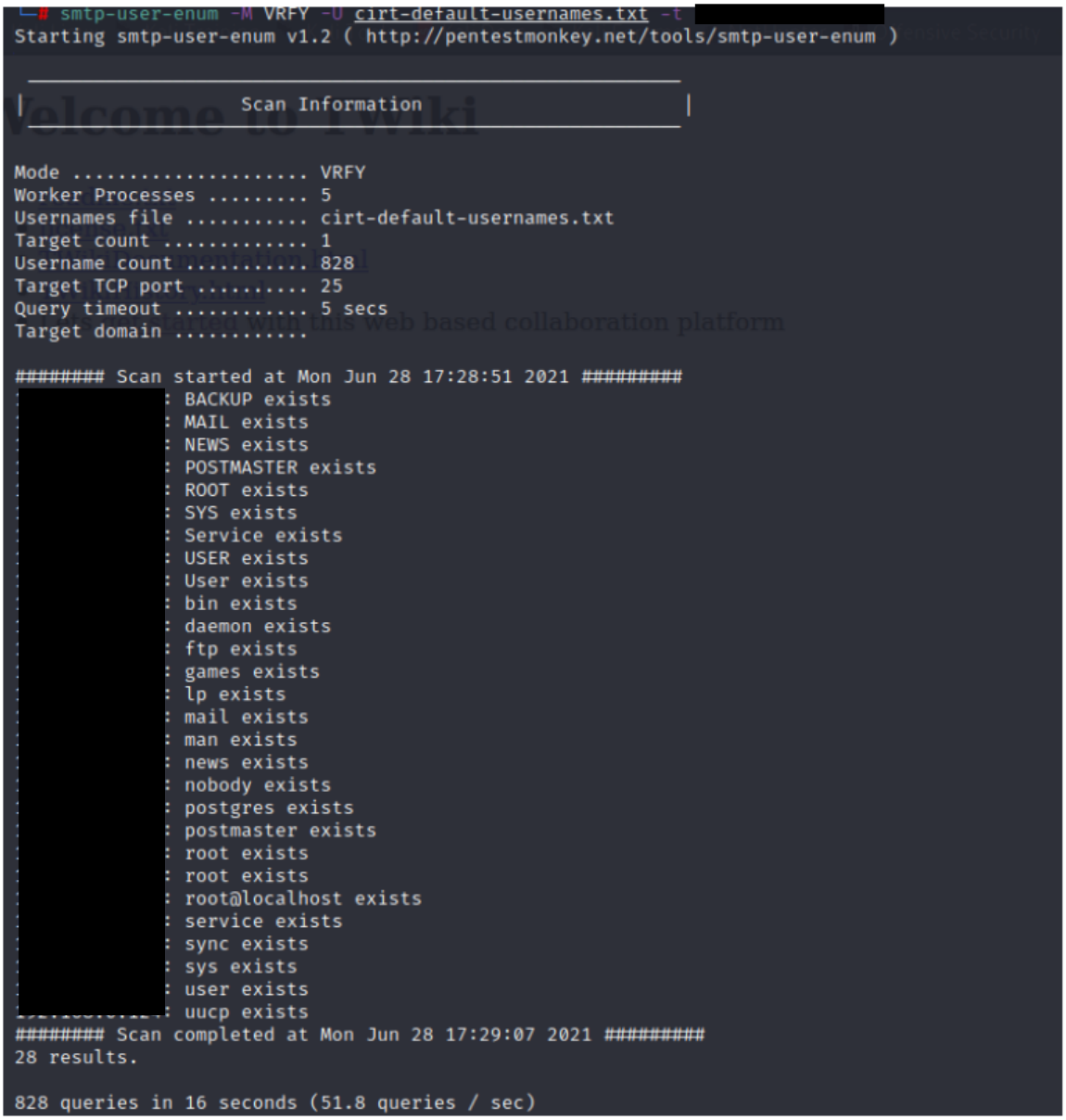
Ejemplo de uso de SMTP-User-Enum



Fuente Elaboración propia 2021.

Figura 17

Ejemplo de uso de Smtp-User-Enum

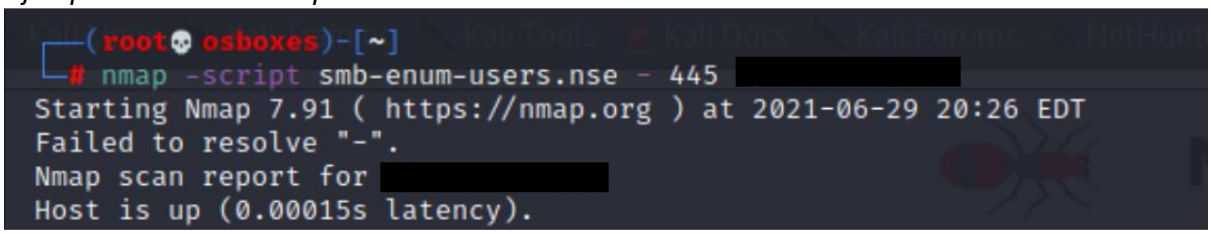


Fuente Elaboración propia 2021.

3. SMB-Enum-User: Este tipo de enumeración, se utiliza en conjunto con una herramienta llamada nmap descrita en el punto 6, el cual permitirá hacer uso del *script* smb-enum-users.nse para poder ver los usuarios con los que cuenta el sistema.

Figura 18

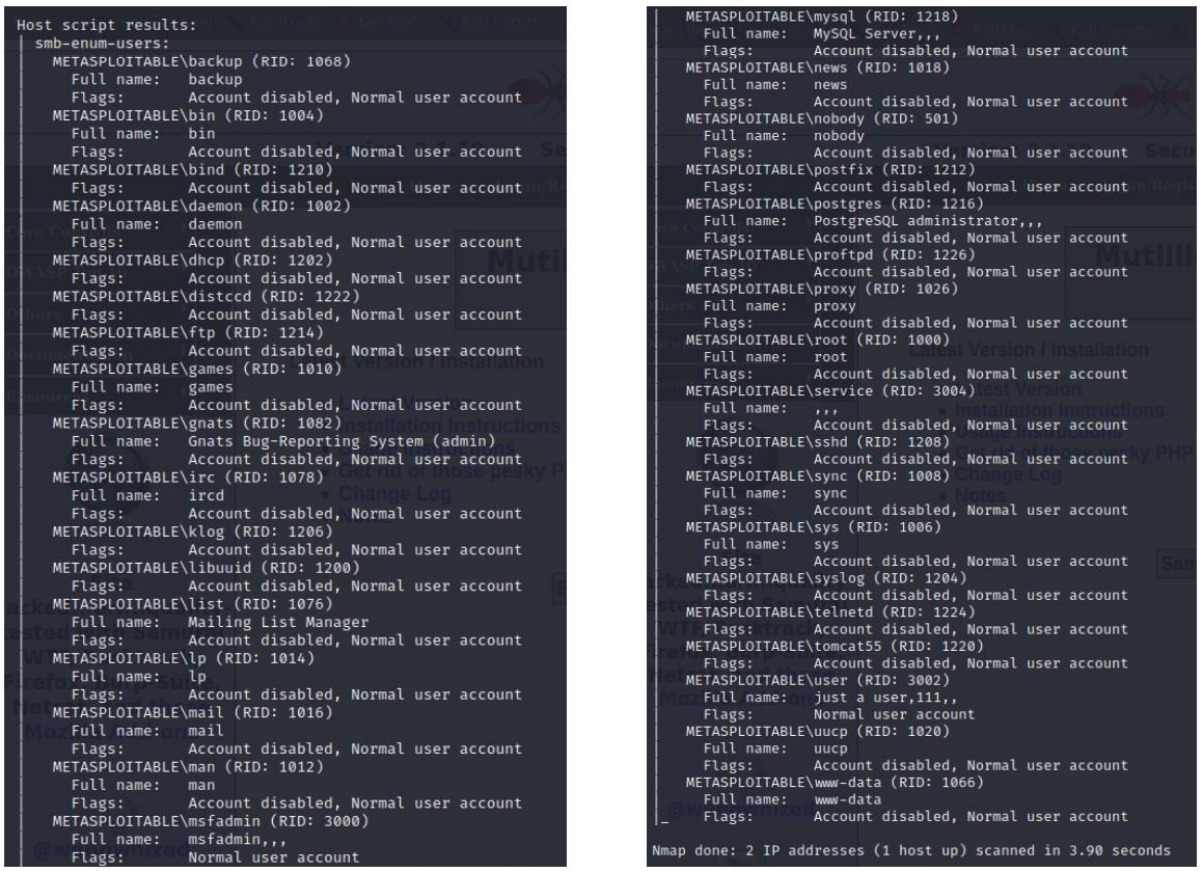
Ejemplo del uso del script smb-enum-users.nse



Fuente Elaboración propia 2021.

Figura 19

Información obtenida a partir del script smb-enum-users.nse

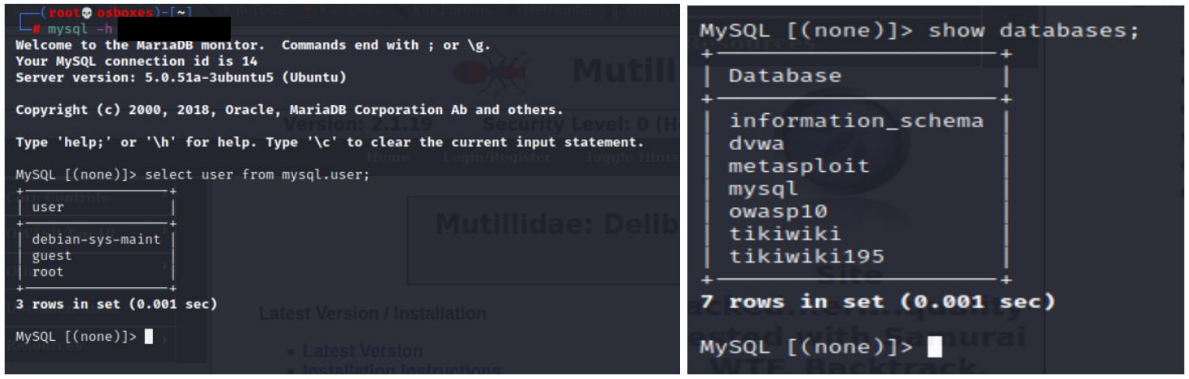


Fuente Elaboración propia 2021.

4. MySQL: Es un gestor de base de datos muy utilizado por muchas empresas, como YouTube, Netflix, Walmart, entre otras compañías, para almacenar la información de sus clientes (MySQL, 2022). Al ser una herramienta muy utilizada, será objeto de muchas amenazas, y otra prueba que se realiza para enumerar es realizar una conexión vía MySQL, para ver si dejaron conexiones default, y además buscar bases de datos existentes.

Figura 20

Ejemplo de una conexión MySQL sin credenciales



Fuente Elaboración propia 2021.

5. Nmap: Es una herramienta de código abierto que permitirá realizar una búsqueda de los puertos de una dirección IP en específico, de esta forma se pueden ver todos los puertos TCP/UDP y los servicios que corre cada uno de ellos, lo cual va a servir para poder auditar la red, y que además se pueden conocer todos los host de la red, y demás detalles de la misma. (Nmap, 2022).

Figura 21

Ejemplo del uso de nmap

```
# nmap -A -T4 scanme.nmap.org saladejuegos

Starting nmap ( https://nmap.org/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on saladejuegos.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Fuente (Nmap, 2022).

4.1.4. Mitigar las vulnerabilidades de los sitios web

Tal como se puede observar en la figura 11, OWASP establece alguna de las vulnerabilidades más relevantes que se pueden encontrar en los sitios web, para lo cual se mencionarán algunas medidas que pueden tomar para poder mitigar las vulnerabilidades allí mencionadas.

4.1.4.1. Control de acceso+

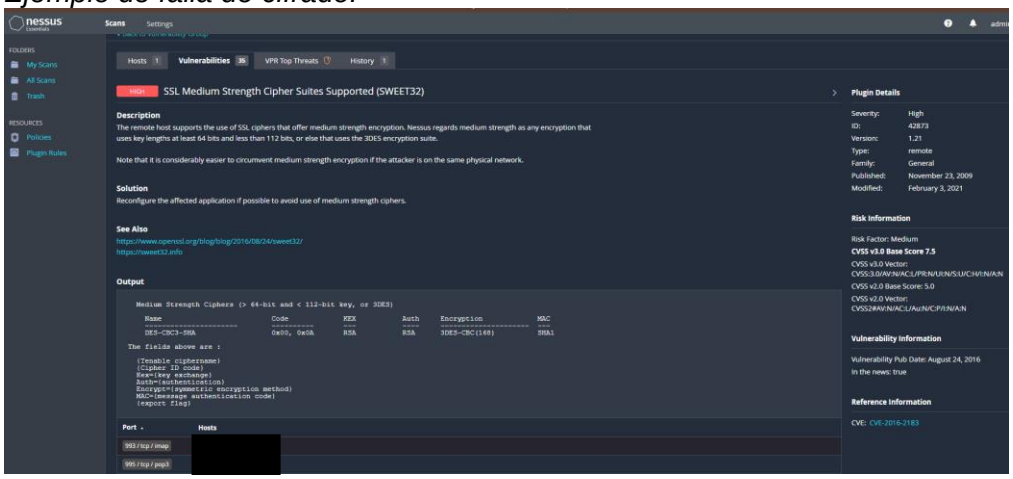
Algunos sitios web tienen problemas para con el control de acceso, ya que muchas veces no se le presta la atención debida, y a la hora de implementarlo queda con algunos errores que pueden provocar que, personas ajenas sin credenciales tengan acceso. Muchas veces una manera de mitigar este problema es, revisar los log del sistema, y analizar en qué parte se dio el inconveniente y corregir el código, ya sea reprogramando lo que ya está hecho para corregir, o implementar algún *API* que nos permita tener un mejor control de los accesos. (Google, 2021).

4.1.4.2. Fallas criptográficas

Estas fallas suelen suceder debido a la falta de encriptación, o una encriptación débil de los datos en tránsito en el sitio web. Para mitigar este fallo, se puede hacer mediante una implementación de un sistema de cifrado más fuerte, o configurando adecuadamente el que actualmente se posea. En la figura 22, se puede observar un ejemplo realizado en *Nessus Essential* a un sitio web, donde tiene una vulnerabilidad “SSL Medium Strength Cipher Suites Supported (SWEET32)”, que es marcada con una severidad ALTA, con un puntaje de 7.5, nos describe cuál es el inconveniente y en qué puertos se están presentando el problema, como además nos proporciona una solución.

Figura 22

Ejemplo de falla de cifrado.



Fuente Elaboración propia 2021.

4.1.4.3. Inyección de código

La inyección de código, en el pasado fue una de las primeras en el TOP de OWASP, y es que muchas veces, los sitios web por no estar bien programados, son vulnerables a inyección de código de SQL, haciendo que ejecuten código externo, pudiendo extraer datos sensibles de la base de datos del sitio web. Una manera de poder mitigar este tipo de problema, es realizar parámetros de seguridad, de esta forma lo que ingrese será considerado como un valor y no como código (ver figura 23), así como muchas otras formas existentes, todo dependerá de la programación que quiera darle cada programador. (Microsoft, 2022).

Figura 23
Ejemplo de implementación de parámetros de seguridad

C# Copiar

```
SqlDataAdapter myCommand = new SqlDataAdapter("AuthorLogin", conn);
myCommand.SelectCommand.CommandType = CommandType.StoredProcedure;
SqlParameter parm = myCommand.SelectCommand.Parameters.Add("@au_id",
    SqlDbType.VarChar, 11);
parm.Value = Login.Text;
```

Fuente (Microsoft, 2022).

4.1.4.4. Diseño no seguro

El diseño de cualquier software es sumamente importante, y debe realizarse correctamente durante el ciclo de vida del desarrollo, de manera tal, que se vaya probando lo que se va realizando, y hacer las cosas correctamente desde el inicio, y no dejar para después de haberse desarrollado por completo el software. En el 2015 Iván Arce, director del Programa de Seguridad en TIC para la Fundación Sadosky, presentó cómo evitar los 10 problemas de seguridad más frecuentes en el diseño de software. Se estima que un aproximado del 50% de las vulnerabilidades su origen se debe a un mal diseño del software. (ESET, 2015).

Los 10 consejos para minimizar las vulnerabilidades del diseño del software por parte de Iván, son:

1. Ningún componente es confiable hasta demostrar lo contrario.
2. Delinear mecanismos de autenticación difíciles de eludir.
3. Autorizar, además de autenticar.
4. Separar datos de instrucciones de control.
5. Validar todos los datos explícitamente.
6. Utilizar criptografía correctamente.
7. Identificar datos sensibles y cómo se los debería gestionar.
8. Considerar siempre a los usuarios del sistema.
9. La integración de componentes cambia la superficie de ataque.

10. Considerar cambios futuros en objetos y actores.

4.1.4.5. Configuración incorrecta de seguridad

Las configuraciones incorrecta de seguridad, si bien están en el 5º puesto, son unas de las más comunes por la mayoría de personas encargadas de configurar hardware, o software, ya que muchos de ellos, suelen dejar configuraciones de fábrica, o no aplicar los parches de seguridad actualizados, provocando los sistemas sean vulnerables y de fácil acceso. Lo más adecuado es siempre instalar los parches más recientes, cambiar contraseñas y puertos predeterminados que tenga cualquier sistema de software o hardware. (OWASP, A05:2021 – Security Misconfiguration, 2022)

4.1.4.6. Componentes vulnerables y desactualizados

Muchas veces, se utilizan software desactualizados, o componentes no adecuados para los sistemas que se están utilizando, pudiendo esto significar un gran problema, ya que el sistema no solo, no funcionará adecuadamente, sino también puede ser objeto de ataques. Se debe tener un control por medio de un inventario de las versiones que se manejan, estar revisando si no tienen algún problema de seguridad en National Vulnerability Database (NVD)[4], instalar componentes oficiales, tener un plan de mantenimiento de todos aquellos componentes que se utilizan y los que no. (OWASP, A06:2021 – Vulnerable and Outdated Components, 2022).

4.1.4.7. Fallas de identificación y autenticación

Para evitar los problemas de identificación y autenticación, se deben implementar ciertos métodos que pueden ayudar a mitigarlo, como lo es el uso de OAuth 2.0, que solo permite tener acceso limitado a los servicios HTTP, el uso de JSON Web Tokens, uso de autenticación de varios factores. (Google, 2021).

4.1.4.8. Fallas de integridad del software y datos

Muchas veces este fallo ocurre debido a que algunos sistemas tienen programadas actualizaciones automáticas, y no se verifica si el archivo que se va a descargar es legítimo, o ha sido alterado, para mermar este problema se debe verificar el software, mediante algoritmos de HASH, firmas digitales, tener respaldos del sistema en caso de que suceda algún problema. (OWASP, A08:2021 – Software and Data Integrity Failures, 2022).

4.1.4.9. Errores de registro y supervisión de seguridad

Todo sistema debe tener una bitácora donde se registre cualquier hecho que ocurra en el sistema, esto con el fin de poder controlar de manera más adecuada todo, para evitar

[4] Es el repositorio del gobierno de EE. UU. de datos de gestión de vulnerabilidades basados en estándares representados mediante el Protocolo de automatización de contenido de seguridad (SCAP).

que el sistema sea víctima de un *"Hackeo"*, se deben implementar sistemas de monitoreo y de registro, para de esta forma ver cuál es el comportamiento del sistema, y poder ver cualquier anomalía que se presente en él, control de versiones, y generar reportes al encargado de administrar el sistema para que de esta forma pueda tomar acción. (Google, 2021).

4.1.4.10. Falsificación de solicitudes del servidor (SSRF)

Para mitigar las falsificaciones del servidor, se debe implementar ciertos controles de seguridad de defensa profunda, como lo es tener fuertes políticas de acceso o bloqueo a la red en el *Firewall* desde la capa de red, desde la capa de aplicación, desactivando las direcciones *HTTP,* para evitar cualquier redireccionamiento, además se puede realizar una segmentación de la red. (OWASP, A10:2021 – Server-Side Request Forgery (SSRF), 2022).

Capítulo 5. Conclusiones y recomendaciones

5.1. Conclusiones

- El marco de referencia permitió mostrar diferentes herramientas las cuales pueden ser utilizadas por las instituciones públicas para poder ayudarles a mitigar las vulnerabilidades que puedan tener los sitios web, las herramientas para encontrarlas y la manera de cómo solventarla en caso de que se encuentre alguna.
- Se muestra cuáles son las 10 amenazas más comunes para los sitios web según OWASP para el año 2021, así podrán tener más claro qué deben reforzar y prestar atención para evitar posibles ataques, no sin dejar de lado posibles vulnerabilidades que no se presenten en dicho top 10.
- El personal de las instituciones públicas, no es tan calificado como se quisiera y que también, hay carencia de personal, para lo cual se debería tener al menos 2 funcionarios profesionales en el área de seguridad, y en muchos casos no hay ninguno, y cuando lo hay, no son preparados en esta área.
- A pesar de que muchas ocasiones los sitios web de las instituciones públicas han sido atacadas, siguen sin darle la atención debida a este problema, tomando en cuenta que durante el 2020 y 2021 se incrementaron los ataques informáticos, esto quizás debido al teletrabajo de muchas personas debido a la pandemia.
- Costa Rica ha dado grandes pasos en relación a la legislación de la seguridad de la informática, y ha tratado de mejorar muchas cosas, pero aún le falta mucho por avanzar, comparado con los países más desarrollados en temas de seguridad informática.

5.2. Recomendaciones

- Se debe establecer roles y políticas para la revisión de los sitios web de las instituciones públicas, con el fin de ver las versiones de todos los componentes del sistema, para evitar que estén desactualizados, tengan los parches de seguridad más recientes.
- Tener políticas bien definidas para la seguridad de la información en general, que vaya de la mano con la visión y misión de la institución pública, y alineado con sus objetivos, para poder así resguardar la información que sea procesada por ellos.
- Se debe tener al menos una persona que cumpla los roles del personal del departamento de informática, con el fin que pueda atender cualquier incidente que pueda ocurrir, y además capacitarle en materia de seguridad.
- Además, se debe entender que todo es un ciclo de vida, en el cual, después de tener roles, políticas, con el plan de gestión de la seguridad de la información, y las capacitaciones, cada cierto periodo establecido por los altos mandos, hacer revisión de políticas, constantes capacitaciones, para poder minimizar al máximo cualquier vulnerabilidad que pueda ocurrir.

Referencias

Benjamin S. Bloom, Max D. Engelhart, Edward J. Furst, Walker H. Hill, David R. Krathwohl. (1956). TAXONOMY OF EDUCATIONAL OBJECTIVES: The Classification of Educational Goals. United States of America: EDWARDS BROS • ., ANN AR.BOR„ MICHIGAN.

BID, OEA. (2020). *https://publications.iadb.org/.* Retrieved from https://publications.iadb.org/: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

CAMTIC. (2021, 06 28). *CAMTIC*. Retrieved from https://www.camtic.org/actualidad-tic/costa-rica-empieza-el-ano-con-mas-de-87-millones-de-intentos-de-ciberataques/

Castro, J. (2021, 03 17). *LaRepública.Net.* Retrieved from https://www.larepublica.net/noticia/mas-de-200-millones-de-intentos-de-ciberataques-afectaron-a-costa-rica-en-2020

Catoria, F. (2013, 11 20). *We Live Security By Eset*. Retrieved from https://www.welivesecurity.com/la-es/2013/11/20/eset-security-services-vulnerability-assessment/

CRHoy. (2015, 12 20). *CRHoy*. Retrieved from https://archivo.crhoy.com/hackean-sitio-web-del-conapam/tecnologia/

CRHoy. (2015, 10 07). *CRHoy*. Retrieved from https://archivo.crhoy.com/hackean-sitio-web-del-incofer/nacionales/

CyberSoc. (2022, 01 10). *ESET*. Retrieved from https://www.eset.com/fileadmin/ESET/LATAM/Overviews/cybersoc/CyberSOC-Vulnerability-Assessment.pdf

EC-Council. (2022, 01 13). *EC-Council.* Retrieved from http://it-docs.net/ddata/878.pdf

Eillyn Jiménez B. y Monserrath Vargas L. (2018, 05 14). *La Nación*. Retrieved from https://www.nacion.com/tecnologia/internet/gobierno-confirma-hackeo-de-paginas-web-oficiales/C2KZXTRTEBFQJMXKZECVJGFGCI/story/

ESET, W. L. (2015, 03 12). *We Live Security By ESET*. Retrieved from https://www.welivesecurity.com/la-es/2015/03/12/10-consejos-desarrollo-seguro-de-aplicaciones/

FortiGuard. (2021, 12 26). *Fortinet*. Retrieved from https://www.fortiguardthreatinsider.com/es/bulletin/

Global Security Index. (2020). *ITU Publications.* Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Google. (2021, 11 27). *Google Cloud*. Retrieved from https://cloud.google.com/architecture/owasp-top-ten-mitigation?hl=es-419

Guerrero, A. (2014, 12 12). *CRHoy*. Retrieved from https://archivo.crhoy.com/hackean-pagina-del-ministerio-de-trabajo/

Guerrero, A. (2016, 01 05). *CRHoy*. Retrieved from https://archivo.crhoy.com/hackean-pagina-del-minae/tecnologia/

Harán, J. M. (2018, 05 15). *We Live Security.* Retrieved from https://www.welivesecurity.com/la-es/2018/05/15/sitios-de-organismos-publicos-de-costa-rica-fueron-victimas-de-un-ciberataque/

Harán, J. M. (2019, 11 11). *We Live Security.* Retrieved from https://www.welivesecurity.com/la-es/2019/11/11/profesionales-en-seguridad-informatica-entre-la-formacion-academica-y-la-autodidacta/

Jiménez, K. C. (2019, 04 19). *El Financiero.* Retrieved from https://www.elfinancierocr.com/tecnologia/ciberataques-en-tres-instituciones-publicas/TU242IYLINH5RM4V22QPY3WGGI/story/

Kali Linux. (2021, 11 26). *Kali Linux*. Retrieved from https://www.kali.org/tools/enum4linux/

Lavagni, L. C. (2021, 11 05). *DelfinoCR*. Retrieved from https://delfino.cr/2021/11/ciberseguridad-y-la-nueva-normalidad

López, J. (2022, 01 10). *AudioTech*. Retrieved from https://auditech.es/principales-diferencias-entre-analisis-de-vulnerabilidades-pentesting-y-ethical-hacking/

MalwareBytes. (2021, 12 23). *MalwareBytes*. Retrieved from https://es.malwarebytes.com/phishing/

Mendoza, M. Á. (2015, 09 14). *We Live Security By Eset*. Retrieved from https://www.welivesecurity.com/la-es/2015/09/14/evaluacion-continua-de-vulnerabilidades/

MEP. (2020, 03). *MEP.* Retrieved from https://mep.go.cr/sites/default/files/documentos/politica-tic-mep.pdf

MEP. (n.d.). *MEP.* Retrieved from https://www.mep.go.cr/sites/default/files/descargas_etica/17-16.pdf

MICIT. (2017). *MICIT.* Retrieved from https://www.micitt.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

MICIT. (2021, 06 30). *MICIT*. Retrieved from https://www.micitt.go.cr/noticias/costa-rica-mejora-indice-global-ciberseguridad#:~:text=Costa%20Rica%20mostr%C3%B3%20un%20gran,pa%C3%ADs%20en%20materia%20de%20ciberseguridad.

Microsoft. (2022, 02 18). *Microsoft*. Retrieved from https://docs.microsoft.com/es-mx/sql/relational-databases/security/sql-injection?view=sql-server-ver15

MIDEPLAN. (2020). *Hacienda.* Retrieved from https://www.hacienda.go.cr/Sidovih/uploads//Archivos/Articulo/Ciberseguridad%20en%20el%20Sistema%20Nacional%20de%20Planificaci%C3%B3n-MIDEPLAN.pdf

Murillo, E. (2019, 06 07). *CR HOY*. Retrieved from https://www.crhoy.com/tecnologia/costa-rica-recibio-19-millones-de-ciberataques-este-semestre-sector-publico-no-esta-preparado/

Murillo, E. (2020, 01 20). *CRHoy*. Retrieved from https://www.crhoy.com/tecnologia/estas-son-las-principales-amenazas-de-ciberseguridad-del-2020/

MySQL. (2022, 01 14). *MySQL*. Retrieved from https://www.mysql.com/

Nmap. (2022, 01 13). *Nmap*. Retrieved from https://nmap.org/man/es/index.html

OWASP. (2021, 12 26). *OWASP*. Retrieved from https://owasp.org/Top10/

OWASP. (2022, 02 20). *A05:2021 – Security Misconfiguration*. Retrieved from https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

OWASP. (2022, 02 20). *A06:2021 – Vulnerable and Outdated Components*. Retrieved from https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

OWASP. (2022, 02 20). *A08:2021 – Software and Data Integrity Failures*. Retrieved from https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

OWASP. (2022, 02 22). *A10:2021 – Server-Side Request Forgery (SSRF)*. Retrieved from https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/

Pérez, C. C. (2018, 03 09). *El Financiero.* Retrieved from https://www.elfinancierocr.com/tecnologia/falta-de-especialistas-expone-a-instituciones/KUQYEYBF2RAUZMJHEI3CIIDODA/story/

PROSIC. (2012). *INFORMES HACIA LA SOCIEDAD DE LA INFORMACIÓN Y EL CONOCIMIENTO.* San José: Imprenta Lil. Retrieved from http://prosic.ucr.ac.cr/informe-2012

RedHat. (2020, 11 25). *RedHat*. Retrieved from https://www.redhat.com/en/topics/security/what-is-cve

Sliesarieva, E. G. (2010). Ciberseguridad en Costa Rica. San José: Impresión Gráfica del Este S.A.

Solano, J. (2020, 05 05). *CR HOY.* Retrieved from https://www.crhoy.com/tecnologia/hackers-lanzan-nueva-amenaza-al-bcr-y-publican-supuesta-informacion-confidencial/

Union Internacional de Telecomunicaciones. (2018). *CR HOY.* Retrieved from https://cdn.crhoy.net/imagenes/2019/06/Global-Cybersecurity-Index2018.pdf

Venegas, J. U. (2018, 05 04). *Tecnológico de Costa RIca*. Retrieved from https://www.tec.ac.cr/hoyeneltec/2018/05/04/ciberseguridad-costa-rica-no-puerto-seguro

Zorrilla, S. (1993). Introducción a la Metodología de la Investigación. España: Aguilar León y Cal Editores.

Apéndices

Anexos