# ANALISIS DE VULNERABILIDADES EN SITIO WEB DE LA ORGANIZACION INFRAESTRUCTURA TECNOLÓGICA DE COLOMBIA (ETHICAL HACKING)

Nombres y apellidos Autor 1, José Vicente Bello Olarte Autor 2, Nelson Eduardo Gacha Bernal Autor 3 David Piñeros Sánchez Autor 4 William Andres Vargas Vargas

Especialización Seguridad Informática, Fundación Universitaria Compensar

Proyecto fin de grado

Tutor

Carlos Alberto Cañón

18 de noviembre de 2022

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

# ANALISIS DE VULNERABILIDADES EN SITIO WEB DE LA ORGANIZACION INFRAESTRUCTURA TECNOLÓGICA DE COLOMBIA (ETHICAL HACKING)

JOSÉ VICENTE BELLO OLARTE

NELSON EDUARDO GACHA BERNAL

DAVID PIÑEROS SÁNCHEZ

WILLIAM ANDRÉS VARGAS VARGAS

FUNDACIÓN UNIVERSITARIA COMPENSAR

FACULTAD DE INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ING CARLOS ALBERTO CAÑON

16 DE NOVIEMBRE DE 2022

**INDICE**

**1. RESUMEN** 9

**2. ABSTRACT** 9

**3. INTRODUCCIÓN** 10

**4. DEFINICIÓN DEL PROBLEMA** 10

4.1 ANTECEDENTES DEL PROBLEMA 10

4.2 FORMULACIÓN DEL PROBLEMA 11

**5. OBJETIVOS** 12

5.1 OBJETIVO GENERAL 12

5.2 OBJETIVOS ESPECÍFICOS 12

**6. JUSTIFICACIÓN** 13

**7. ALCANCE Y LIMITACIONES** 14

7.1 ALCANCE 14

7.2 LIMITACIONES 14

**8. MARCO REFERENCIAL** 15

8.1 MARCO TEÓRICO 15

*8.1.1 Seguridad Informática* *15*

*8.1.2 Elementos esenciales de la seguridad* *15*

8.1.2.1 Confidencialidad. 15

8.1.2.2 Autenticidad. 15

8.1.2.3 Integridad. 15

8.1.2.4 Disponibilidad. 15

*8.1.3 Vulnerabilidades* *15*

*8.1.4 Amenazas* *15*

*8.1.5 Riesgo* *16*

*8.1.6 Ataques* *16*

*8.1.7 Intrusión* *16*

*8.1.8 Phishing* *16*

*8.1.9 Vishing* *16*

*8.1.10 Principales vulnerabilidades en sitios WEB* *17*

8.1.10.1 Ejecución remota de código. 17

8.1.10.2 Abrir una URL que redirecciona a un lugar malicioso. 17

8.1.10.3 Ataque de inyección SQL. 17

8.1.10.4 Secuestro de clics. 18

8.1.10.5 Mineros ocultos de criptomonedas. 18

*8.1.11 Hacking Ético* *18*

8.1.11.1 Fases del hacking ético. compuesto por las siguientes etapas: 18

8.1.11.1.1 Reconocimiento. 18

8.1.11.1.2 Escaneo. 18

8.1.11.1.3 Husmeo. 19

8.1.11.1.4 Enumeración. 19

8.1.11.1.5 Evaluación de Vulnerabilidades. 19

8.1.11.1.6 Intrusión a Sistemas. 19

8.1.11.2 Elaboración de Informe. 19

*8.1.12 Delitos informáticos más relevantes que afectan a Colombia* *19*

**9. MARCO LEGAL** **21**

*9.1.1 LEY 1273 DE 2009* *21*

9.1.1.1 Artículo 269A. 21

9.1.1.2 Artículo 269B. 21

9.1.1.3 Artículo 269C. 21

9.1.1.4 Artículo 269D. 22

9.1.1.5 Artículo 269E. 22

9.1.1.6 Artículo 269F. 22

9.1.1.7 Artículo 269G. 22

*9.1.2 ISO 31000 (numeral 4.3.3)* *23*

*9.1.3 Implementación de controles* *23*

**10. DISEÑO METODOLÓGICO 24**

10.1 FASE RECOPILACIÓN DE INFORMACIÓN 24

10.2 FASE ANÁLISIS DE VULNERABILIDADES 24

10.3 FASE DE EXPLOTACIÓN 24

10.4 FASE DE REPORTE 24

10.5 ESTRUCTURA LÓGICA DE ENTREGABLE (EDT) 25

*10.5.1 Parte 1 – Estructura Lógica De Entregables (EDT)* *25*

*10.5.2 Parte 2 – Requisitos Para Los Entregables* *26*

10.6 CRONOGRAMA 27

10.7 COSTOS 27

10.8 TABLERO DE GESTIÓN DE RIESGOS 28

**11. PROPUESTA VALOR 29**

11.1 ANÁLISIS DE VULNERABILIDADES 29

11.2 PRUEBAS WEB PENETRATION TESTING –WPT 29

**12. RESULTADOS 31**

12.1 INFORME TÉCNICO 31

12.2 INFORME EJECUTIVO 31

**13. CONCLUSIONES Y RECOMENDACIONES 32**

13.1 CONCLUSIONES 32

13.2 RECOMENDACIONES 33

**14. GLOSARIO 35**

14.1 ACTIVO DE INFORMACIÓN 35

14.2 AUTENTICACIÓN 35

14.3 CLASIFICACIÓN DE INFORMACIÓN 35

14.4 CÓDIGO MALICIOSO 35

14.5 INCIDENTE DE SEGURIDAD 35

14.6 POLÍTICA DE SEGURIDAD 35

14.7 RECURSOS TECNOLÓGICOS 35

14.8 USUARIOS 36

14.9 CIBERATAQUE 36

14.10 ATAQUE DE DENEGACIÓN DE SERVICIO DISTRIBUIDO 36

14.11 JAVASCRIPT 36

14.12 COOKIES 36

**15. BIBLIOGRAFÍA 37**

**16. ANEXOS 39**

16.1 CARTA DE APROBACIÓN 39

16.2 DIAGNOSTICO ESTADO PÁGINA WEB 39

## INDICE DE FIGURAS

Figura 1 Principales modalidades de ciberdelitos Primer trimestre 2020 ..... 20

Figura 2 Ciudades de mayor afectación de ciberdelitos Primer trimestre 2022 ..... 20

Figura 3 Mapeo de puertos ..... 39

Figura 4 Mapeo de puertos y servicios ..... 40

## INDICE DE TABLAS

Tabla 1 Parte 1 – Estructura Lógica de Entregables (EDT) ..... 25

Tabla 2 Parte 2 – Requisitos para Los Entregables ..... 26

Tabla 3 Cronograma ..... 27

Tabla 4 Costos ..... 27

Tabla 5 Tablero de Gestión de Riesgos ..... 28

## 1. Resumen

En el presente trabajo se realizará una propuesta de consultoría en seguridad informática que permita establecer estrategias de mitigación y gestión de los riesgos sobre las vulnerabilidades que se logren identificar y analizar sobre la plataforma web de la organización **Tecnológica de Colombia S.A.S**., con el fin de reducir posibles fraudes de robo de información y/o indisponibilidad de la plataforma web garantizando la confidencialidad, integridad y disponibilidad de la información. Durante el desarrollo de la propuesta se hará uso de diferentes herramientas de hacking ético basándose en pruebas de pentesting para la detección de vulnerabilidades comunes como Inyecciones SQL, Denegación de Servicio y Man in the Middle.

***Palabras clave:*** Consultoría Informática, Pentesting, Inyecciones SQL, Denegación de Servicio y Man in the Middle.

## 2. Abstract

In the present work, a proposal of consultancy in computer security will be made to establish mitigation strategies and risk management on vulnerabilities that are identified and analyzed on the web platform of the organization Tecnologica de Colombia S.A.S., in order to reduce possible fraud of information theft and / or unavailability of the web platform ensuring confidentiality, integrity and availability of information. During the development of the proposal, different ethical hacking tools will be used based on pentesting tests for the detection of common vulnerabilities such as SQL Injections, Denial of Service and Man in the Middle.

***Key words:*** IT Consulting, Pentesting, SQL Injections, Denial of Service and Man in the Middle.

# 3. Introducción

La organización brinda servicios y soluciones en infraestructura tecnológica aplicadas a las telecomunicaciones, acondicionamiento de aire para centros de datos y oficinas, instalaciones eléctricas, sistemas de detección y extinción de incendios, alimentación crítica y sistemas ininterrumpidos de energía.

Debido al aumento de usuarios internos y externos de la organización, y la diversificación de servicios atendidos por la misma, es necesario realizar un proceso de diagnóstico que permita establecer los criterios para proponer una consultoría sobre el estado de la seguridad informática en los procesos que son inherentes y transversales al modelo de negocio, para posteriormente establecer cuáles son las oportunidades de mejora que le permitan a Infraestructura Tecnológica de Colombia SAS cumplir con los requisitos y desafíos en materia de ciberseguridad y Ethical Hacking.

Para llevar a cabo este proceso es necesario tener en cuenta que la información es un activo muy importante para todas las organizaciones, en ese sentido implementar y/o fortalecer las estrategias, los controles y procedimientos que garanticen altos niveles de seguridad a la información, alineado a la norma internacional NTC / ISO 27001:2013, toma una relevancia estratégica en la coyuntura empresarial actual.

# 4. Definición Del Problema

## 4.1 Antecedentes Del Problema

En los últimos años se ha evidenciado un aumento en el volumen de los delitos informáticos en Colombia. Adicionalmente la pandemia del Covid-19 obligo a los sectores que estaban rezagados o no habían hecho uso de las TIC, a empezar a hacer uso de estos medios de manera inmediata sin poder implementar políticas de seguridad informática. Esto ocasionó que se aumentarán los riesgos de ciberseguridad y por consiguiente los delitos informáticos de los cuales son víctimas las personas y las organizaciones. El gobierno nacional estableció en el

CONPES 3995 la hoja de ruta en los próximos años para que el país en materia de política pública, las organizaciones, los profesionales relacionados con las TIC y los ciudadanos para conformar un ecosistema que permita hacer frente a estos desafíos en la actualidad. En ese sentido las organizaciones que tengan injerencia en ámbito tecnológico deben fortalecer sus procesos en ciberseguridad y seguridad de la información. Dado el papel relevante que tienen para contribuir al desarrollo del país, el cual es apalancado en el uso de las tecnologías mencionadas y la confianza digital de los entes estatales y organizaciones estratégicas en el marco de los procesos productivos como también de los ciudadanos.

### 4.2 Formulación Del Problema

Infraestructura Tecnológica de Colombia S.A.S tiene en su sitio web diferentes servicios que se encargan de recibir, gestionar y almacenar información vital tanto para su modelo de negocio, como para sus clientes, en ese sentido la organización debe garantizar la confidencialidad, integridad y disponibilidad de estos datos en el marco de altos estándares de calidad en seguridad de la información e informática, como también la normatividad colombiana.

Que recomendaciones técnicas se pueden dar a las brechas identificadas en el sitio web de la organización en el marco de referencia ISO-27001, y que permita que estos riesgos se mitiguen y puedan ser gestionados.

# 5. Objetivos

## 5.1 Objetivo General

Realizar un análisis del estado de seguridad del sitio web de la organización Infraestructura Tecnológica de Colombia S.A.S, ubicada en la ciudad de Bogotá, identificando las posibles vulnerabilidades que puedan afectar de manera directa o indirecta la información para generar un respectivo informe en el cual se identifiquen oportunidades de mejora en materia de calidad y confianza digital de los servicios prestados al cliente, con fin de brindar propuesta de consultoría.

## 5.2 Objetivos Específicos

- Diagnosticar el estado del sitio web dentro de la organización en materia de seguridad de la información y seguridad informática.
- Realizar proceso de Ethical hacking que identifique brechas de seguridad en el sitio web principal de la organización.
- Entregar informe con las recomendaciones en oportunidades de mejora para la organización en sus procesos de seguridad informática para la consideración de la alta gerencia.

## 6. Justificación

El gobierno nacional a través del CONPES 3995 expedido en el año 2020, establece que es necesario en los próximos años crear un ecosistema en el cual tanto entidades oficiales como sectores productivos estratégicos y ciudadanos deben contribuir a la mejora de los índices de confianza digital en el país. (CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, 2020)

En los últimos años el crecimiento de la economía en los diferentes países emergentes apalancado en las tecnologías de la información ha sido exponencial, sumado a esto la pandemia del COVID-19 acelero aún más este crecimiento y obligó a las personas tanto como a organizaciones que no hacían uso de la tecnología a usarla e implementarla en sus diferentes tareas o procesos.

Estos procesos coyunturales han permitido que en los últimos años hayan aumentado la cantidad de delitos informáticos en el país, dado que la tecnología se implementa con premura para satisfacer o implementar las soluciones, muchas veces en los procesos de implementación y puesta a producción los equipos de trabajo no alcanzan a establecer todas las necesidades y previsiones en materia de seguridad informática o seguridad de la información. Esto es un desafió para las organizaciones de hoy en día, sobre todo para las que tienen características menos robustas como los emprendimientos o startup.

# 7. Alcance y limitaciones

## 7.1 Alcance

Realizar prueba de Pentesting sobre la página web de la empresa Infraestructura Tecnológica de Colombia SAS, con el fin de descubrir posibles brechas de seguridad, que puedan afectar y exponer su confidencialidad, integridad y disponibilidad de la información, que pueda estar siendo manejada en proceso internos, con esto nos permitirá la entrega de dos informes detallados con los resultados encontrados y su mismo podamos sugerir que medidas preventivas y/o que pueda tomar a corto y mediano plazo sobre su servicio web.

## 7.2 Limitaciones

Teniendo en cuenta que la información alojada en el sitio web de la organización, con este tipo de análisis puede llegar a ocasionar inconvenientes de disponibilidad y/o intermitencia en el servicio web, sin embargo, este tipo de pruebas no serán totalmente intrusivas y en todo momento se estará monitoreando y controlando las actividades con el fin de evitar de que alguna forma se altere la confidencialidad, integridad y disponibilidad de la información

# 8. Marco Referencial

## 8.1 Marco Teórico

### *8.1.1 Seguridad Informática*

Proceso usado para la protección técnica y metodológica de los sistemas informáticos frente amenazas externas e internas, la cual está enfocada en apoyar los tres grandes pilares de la seguridad informática Disponibilidad, Confidencialidad e integridad. (Baca Urbina, 2016, pág. 10)

### *8.1.2 Elementos esenciales de la seguridad*

***8.1.2.1 Confidencialidad.*** Se refiere a ocultar y no divulgar la información o recurso.

***8.1.2.2 Autenticidad.*** Identificar y garantizar el origen de la información, por ejemplo: al recibir un mensaje se debe garantizar que el mensaje fue enviado por quien dice ser.

***8.1.2.3 Integridad.*** Garantiza que la información no ha sido alterada o manipulada en su contenido.

***8.1.2.4 Disponibilidad.*** Garantiza que los usuarios tengan acceso a la información cuando lo requieran. (León & León, 2021)

### *8.1.3 Vulnerabilidades*

En términos de seguridad informática es toda aquella debilidad a nivel de hardware y software, aprovechada por los ciber delincuentes comprometiendo los pilares de la seguridad informática.

### *8.1.4 Amenazas*

A diferencia de las vulnerabilidades informáticas, esta no es un problema de seguridad que existe en una implementación u organización, en cambio, es todo aquel elemento o acción la cual es capaz de atentar contra la seguridad de la información.

### *8.1.5 Riesgo*

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Seguridad de la información: Conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información.

Según Voutssas M , J (2010), define el riesgo como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto. (Quiroz-Zambrano & Macías-Valencia, 2017)

### *8.1.6 Ataques*

Toda aquella acción delictiva malintencionada, organizada y enfocada en causar daños a los sistemas informáticos en una organización.

### *8.1.7 Intrusión*

Aquellos delitos que comprenden acceso a la información sin autorización de un usuario dentro de una organización.

### *8.1.8 Phishing*

Es una técnica de ingeniería social que consiste en el envío de un email en el que los ciberdelincuentes suplantan la identidad de una compañía conocida o de una entidad pública para solicitar información personal y bancaria al usuario. A través de un enlace incluido en el correo electrónico intentan redirigirle a una página web fraudulenta para que introduzca su número de tarjeta de crédito, DNI, la contraseña de acceso a la banca virtual.

### *8.1.9 Vishing*

Modalidad de estafa que suplanta la identidad afectando a través de VOIP “Voz sobre protocolo de internet IP”, se recrea una voz automatiza, semejante a entidades bancarias, se

realiza llamada un usuario por medio de este tipo de ataque, donde se logra llamar la atención del usuario y lograr el objetivo que es extraer información confidencial. (Ventura Quijano, 2021)

### *8.1.10 Principales vulnerabilidades en sitios WEB*

Cabe resaltar que una vulnerabilidad de una página Web es lo que permite a un atacante aprovechar y afectar a los usuarios que la visiten. Existen muchas herramientas para proteger los sitios y, en definitiva, evitar que los usuarios se infecten. Sin embargo, pese a los controles que se puedan efectuar, siempre existirán vulnerabilidades ya sea de más alto o bajo de nivel de riesgo.

***8.1.10.1 Ejecución remota de código.*** Es una de las amenazas más presentes en las páginas. A través de este método un ciberdelincuente podría explotar un error en el sistema e inyectar el malware. Posteriormente aprovecharía la vulnerabilidad y ayudaría al atacante a ejecutar el código de forma remota. El ciberdelincuente podría tener acceso a todo el sistema con privilegios de administrador.

***8.1.10.2 Abrir una URL que redirecciona a un lugar malicioso.*** Esta vulnerabilidad provoca que el usuario, al visitar un sitio, realmente lo redirecciona a otro distinto llegando a ser muy peligroso, ya que es así como funciona el phishing. Puede ser a través de una aplicación. En general el usuario cree que accede a un sitio legítimo, pero realmente ingresa a una página controlada por el ciberdelincuente a la espera de robar los datos.

***8.1.10.3 Ataque de inyección SQL.*** La inyección de SQL es una técnica de inyección de código que se utiliza para atacar aplicaciones controladas por datos, en la que se insertan infinidad de código SQL en un campo de entrada para su ejecución. Sirve para atacar cualquier tipo de base de datos, aunque afecta a páginas webs. Un atacante podría falsificar la identidad del usuario. (Díaz, 2020)

***8.1.10.4 Secuestro de clics.*** Es lo que utilizan los ciberdelincuentes para que los usuarios de esa página hagan clic en un sitio determinado. Buscando que crean que siguen en la misma página visualizando contenido legítimo. Sin embargo, es probable que les redirijan a contenido de pago o webs fraudulentas que puedan comprometer seriamente los dispositivos. Lo que hace el atacante es secuestrar los clics. Lleva a los usuarios a su propia página.

***8.1.10.5 Mineros ocultos de criptomonedas.*** Los ciberdelincuentes infectan ese sitio en concreto y provoca que el equipo de la víctima sea utilizado para minar este tipo de monedas digitales. Puede afectar en gran medida al rendimiento a corto plazo del equipo, pero también dañar el hardware a largo plazo.

### *8.1.11 Hacking Ético*

Se trata de aquellas practicas seguras usadas en un sistema informático enfocadas en la detección, evaluación y prevención, con el fin de brindar seguridad no solo a la organización si no a sus potenciales clientes.

#### *8.1.11.1 Fases del hacking ético. compuesto por las siguientes etapas:*

***8.1.11.1.1 Reconocimiento.*** En esta etapa se obtiene información sobre equipos servicios y topologías de red.

***8.1.11.1.2 Escaneo.*** En esta etapa se realiza un barrido a lo largo de las direcciones IP consideradas como el objetivo de la prueba con el fin de determinar los puertos activos y los sistemas operativos de los equipos objeto del análisis. Una vez se determinan los puertos activos en cada equipo, se realizan validaciones sobre cada puerto con el fin de determinar las posibles vulnerabilidades existentes en cada puerto activo.

***8.1.11.1.3 Husmeo.*** En esta etapa se usan herramientas que permitan realizar una captura del tráfico generado por los equipos objetivos durante su funcionamiento normal, con el fin de realizar un análisis pasivo de identificación de vulnerabilidades.

8.1.11.1.4 ***Enumeración.*** En esta etapa se reúne toda la información recolectada en los procesos anteriores para determinar la información y datos útiles en la etapa de intrusión al sistema.

***8.1.11.1.5 Evaluación de Vulnerabilidades.*** Esta etapa consiste en realizar un análisis de la información recolectada en las etapas anteriores, de tal forma que se presenten más argumentos para la confirmación de las potenciales vulnerabilidades.

***8.1.11.1.6 Intrusión a Sistemas.*** En los escenarios de pruebas de intrusión se confirma la existencia de las potenciales vulnerabilidades identificadas ejecutando una explotación de estas. Dependiendo del grado de afectación se evaluará en conjunto con el cliente la viabilidad de la actividad.

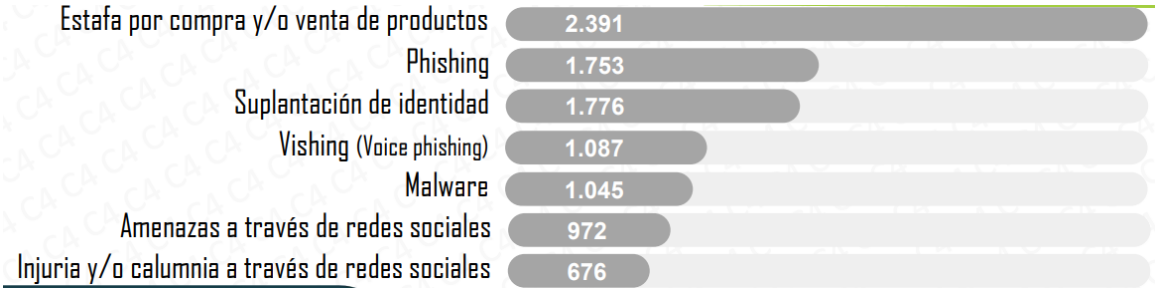
***8.1.11.2 Elaboración de Informe.*** Los resultados y la ejecución del proceso se sintetizan un documento físico de máxima confidencialidad. (LSCV SYSTEMS EIRL, s.f.)

### *8.1.12 Delitos informáticos más relevantes que afectan a Colombia*

El CAI virtual del Centro Cibernético de la Policía Nacional expone las principales formas de delito cibernético, así como el porcentaje de las ciudades afectadas, en su informe Balance Cibercrimen 2020 (Centro cibernetico Policia Nacional, 2020), los cuales se representan en las siguientes figuras, en la Figura 1 se evidencia las principales modalidades de ciberdelitos más sobresalientes en el primer trimestre del año 2020 de acuerdo con los incidentes que han sido reportado en el CAI virtual, donde sobresale Estafa por compra y/o venta de productos y phishing, en la Figura 2 se representa las ciudades más afectadas, donde se evidencia Bogotá con un porcentaje de 37%, Medellín 10% y Cali 7%.

**Figura 1.**

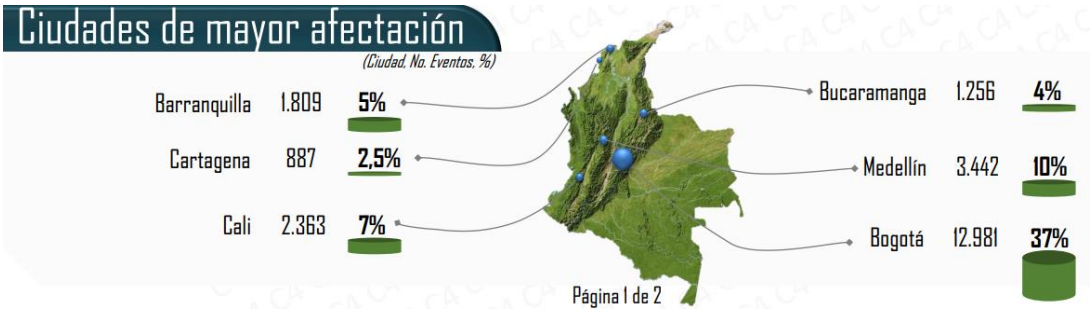
**Principales modalidades de ciberdelitos Primer trimestre 2020**




*Nota.* Datos expresados en cantidad de incidentes de reportes realizados al CAI virtual. Adaptada de Balance Cibercrimen 2020 Semana 45, de CAI Virtual Policía Nacional de Colombia, 2020 (https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf)

**Figura 2.**

**Ciudades de mayor afectación de ciberdelitos Primer trimestre 2022**




*Nota.* Datos expresados en porcentaje de incidentes de reportes realizados al CAI virtual por ciudad. Adaptada de Balance Cibercrimen 2020 Semana 45, de CAI Virtual Policía Nacional de Colombia, 2020 (https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf)

# 9. Marco Legal

### *9.1.1 LEY 1273 DE 2009*

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones**.** (Policia Nacional de Colombia, 2022)

***9.1.1.1 Artículo 269A.*** Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrir en una pena de prisión de (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (SMLMV).

***9.1.1.2 Artículo 269B.*** Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (SMLMV).

***9.1.1.3 Artículo 269C.*** Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, incurrirá en una pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

***9.1.1.4 Artículo 269D.*** Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (SMLMV).

***9.1.1.5 Artículo 269E.*** Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en penade prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (SMLMV).

***9.1.1.6 Artículo 269F.*** Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (SMLMV).

***9.1.1.7 Artículo 269G.*** Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (SMLMV), siempre que la conducta no constituya delito sancionado con pena más grave. (MINTIC, 2009).

### *9.1.2 ISO 31000 (numeral 4.3.3)*

La organización debería garantizar que existe responsabilidad, autoridad y competencia adecuada para gestionar el riesgo, incluyendo la implementación y mantenimiento del proceso para la gestión de riesgo y garantizando la idoneidad, eficacia y eficiencia de todos los controles.

### *9.1.3 Implementación de controles*

Para proponer unas estrategias efectivas que permitan establecer el plan de acción que se propondrá ejecutar en la consultoría, se tendrá como marco de referencia lo planteado en los controles establecidos en el anexo A de la norma ISO/IEC 27002:2013, aprobado por la NTC 294-13. Lo anterior de acuerdo con el contexto de la organización y las oportunidades de mejora que se logren identificar en los procesos de diagnóstico y hacking ético. En ese sentido se busca que la organización pueda hacer frente a los posibles ataques cibernéticos que pudieran afectar los principios de la seguridad de la información como lo son la disponibilidad, accesibilidad e integridad. Se propone implementar controles dentro de las organizaciones para cada una de las entidades u oficinas que las componen.

# 10. Diseño Metodológico

En búsqueda de diversas metodologías para el análisis de vulnerabilidades, para esta consultoría se plantea el uso de las siguientes fases

## 10.1 Fase Recopilación De Información

En esta fase desea recopilar todo tipo de información posible de la empresa a través de diferentes medios tales como:

- Dominio
- Direcciones ip o publica
- Publicaciones realizadas en redes sociales entre otras
- Obtención de metadato

## 10.2 Fase Análisis De Vulnerabilidades

En esta fase se pretende realizar un análisis sobre toda aquella información encontrada en la fase 1, las cuales nos permitirán realizar todas acciones que n os permitan comprometer a nuestro objetivo.

## 10.3 Fase De Explotación

**U**na vez se han identificado vulnerabilidades, en esta fase se obtendrá provecho de estas, para así poder obtener acceso sobre el recurso web.

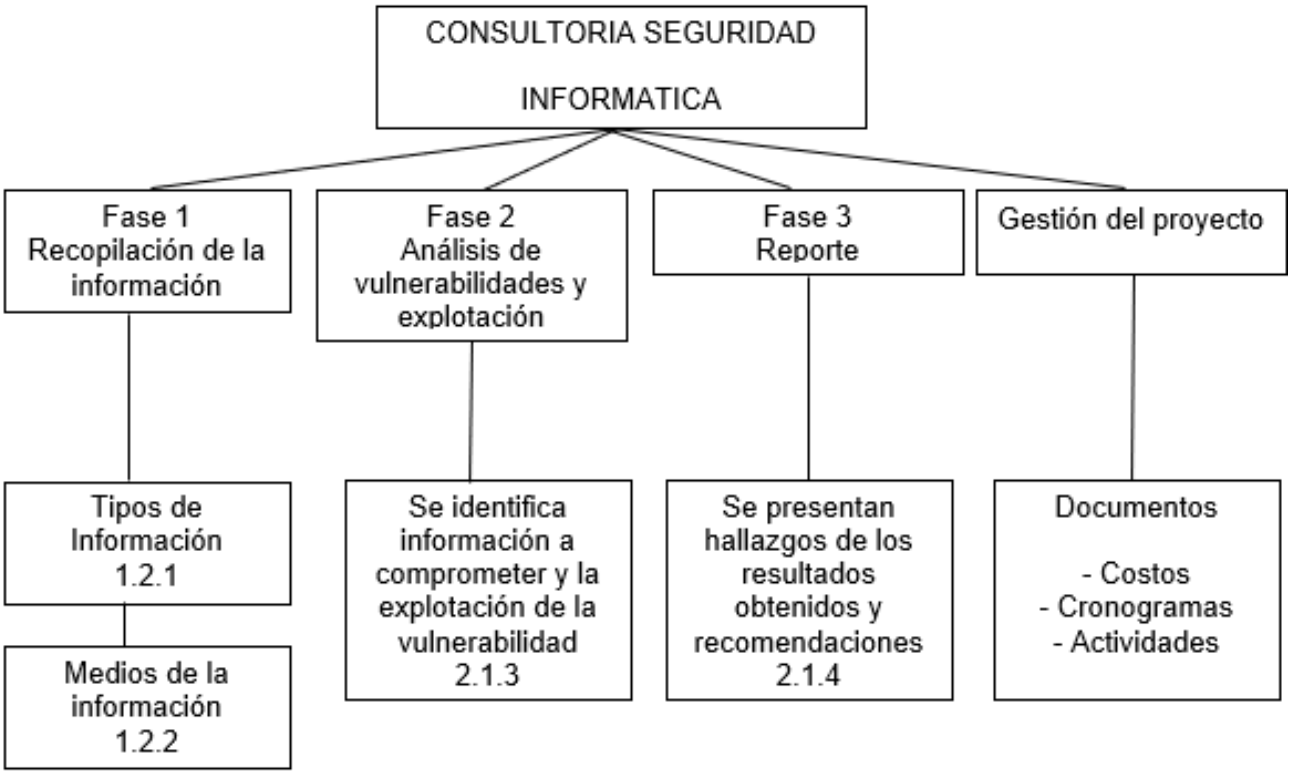
## 10.4 Fase de Reporte

Se presentará a la compañía los hallazgos por medio de un informa con resultados obtenidos y recomendaciones que se consideren adecuadas para reducir las brechas de seguridad que se tengas hasta el momento de la entrega de dicho informe.

## 10.5 Estructura Lógica de Entregable (EDT)

### *10.5.1 Parte 1 – Estructura Lógica De Entregables (EDT)*

**Tabla 1**




*Nota.* Esta tabla representa la estructura lógica de entregables

### *10.5.2 Parte 2 – Requisitos Para Los Entregables*

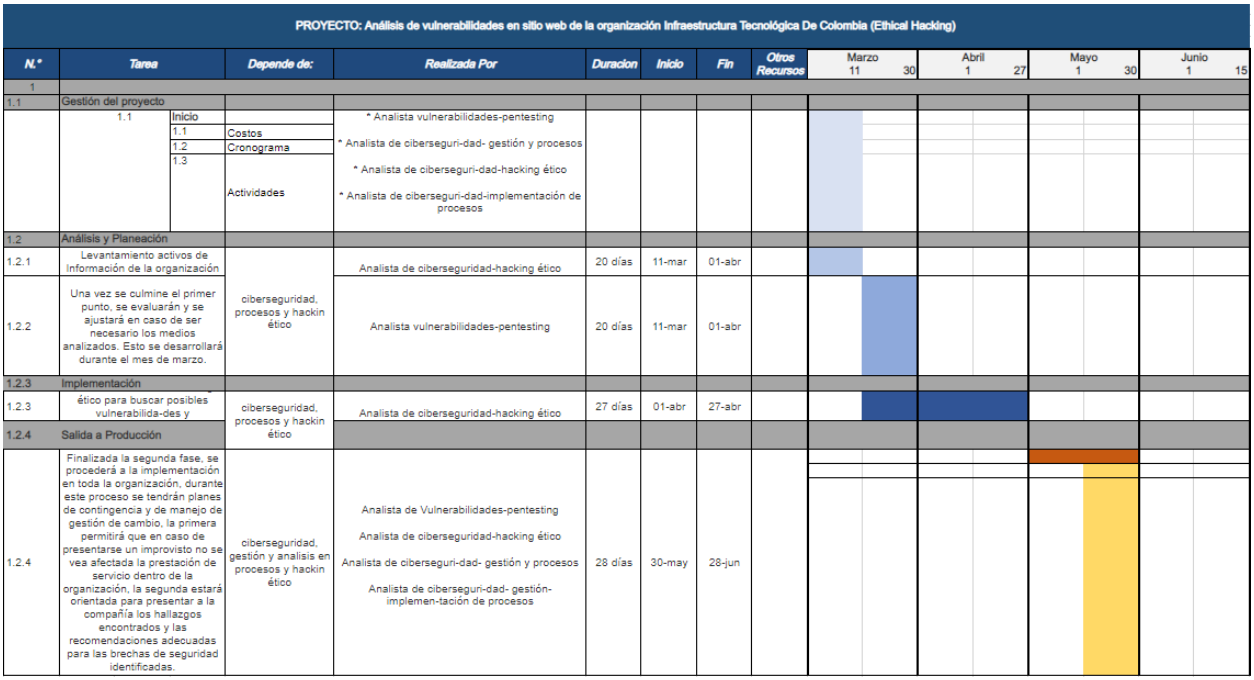
**Tabla 2**

| Componente / Fase | | Entregables | | Responsable | Requeri-mientos del entregable | Criterios de aceptación | Actividades (alto nivel) | Duración (semana, mes) | Recursos (humanos, pre-supuesto, equipamiento) | Riesgos / supuestos |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Recopilación de la información / Fase 1** | 1.2 | Tipos de información 1.2.1 | Analista de Vulnerabilidades-pentesting<br>Analista de ciberseguridad-hacking ético | Información de la organi-zación | 95% de la in-formación | Recopilación activos de la información | Duración de un mes. | * Analista vulnerabilidades-pentesting<br>* Analista de ciberseguridad-gestión y procesos<br>* Analista de ciberseguridad-hacking ético<br>* Analista de ciberseguridad-implementación de procesos<br>* Costo total recurso humano $52´500.000.00 | * No pago de honorarios<br>* Retrasos por autorizaciones y/o cambio equipo de trabajo. |
| | | 1.2.2 | Medios de información | Analista de Vulnerabilidades-pentesting<br>Analista de ciberseguridad-hacking ético<br>Analista de ciberseguri-dad- gestión y procesos | Medios de información<br>Dominio<br>Direcciones IP publicas<br>Obtención de metadato<br>Publicaciones redes socia-les | Comproba-ción 100% de los medios<br>Aprobación los medios | • Aprobación de los medios analizados | • 3 semanas. | * Infraestructura física y de datos de la organización. | * Inconsistencias infraestruc-tura tecnológica.<br>* Eventualidades ambientales.<br>* Inconsistencias infraestruc-tura tecnológica.<br>* Retrasos por autorizaciones y/o cambio equipo de trabajo. |
| 2 | **análisis de vulnerabilidades y explotación/ Fase 2** | 2.1.3 | Se analiza la información recopilada en la fase 1, se inician acciones de hacking ético para buscar posibles vulnerabilidades y compromisos en la información | Analista de Vulnerabilidades-pentesting<br>Analista de ciberseguridad-hacking ético<br>Analista de ciberseguridad- gestión y procesos<br>Analista de ciberseguridad- gestión-implementación de procesos | Acceso a recursos web y de red | Configuración del 90% de las herramientas de hacking necesarias.<br>. | * Aprobación de la configuración.<br>* Aprobación del hacking ético. | * Un mes. | * Analista vulnerabilidades-pentesting<br>* Analista de ciberseguridad-gestión y procesos<br>* Analista de ciberseguridad-hacking ético<br>* Analista de ciberseguridad-implementación de procesos<br>* Oficinas de la organización<br>* funcionarios.<br>* Infraestructura física y de datos de la organización. | * Analista operativo.<br>* Inconsistencias infraestructura tecnológica.<br>* Retrasos por autorizaciones y/o cambio equipo de trabajo. |
| 3 | **Reporte /Fase 3** | 1.2.4 | Se presenta a la compañía los hallazgos encontrados y las recomendaciones adecuadas para las brechas de seguridad identificadas. | Analista de Vulnerabilidades-pentesting<br>Analista de ciberseguridad-hacking ético<br>Analista de ciberseguridad- gestión y procesos<br>Analista de ciberseguridad- gestión-implementación de procesos | Configuración de la infraestructura tecnológica de la organización de acuerdo con los requerimientos de ciberseguridad.<br>Entrega de la documentación. | Configuración del 100% de la infraestructura<br>Servicios ofrecidos funcionando en un 100%.<br>Entrega del 100% de la documentación al área de TIC de la organización. | * Recibo a satisfacción por parte de la alta dirección en la organización.<br>* Recibo a satisfacción por parte del área TIC en la organización.<br>* Encuesta de medición en el grado de satisfacción del producto final. | * Un mes. | * Gerente del proyecto y equipo de trabajo.<br>* Alta gerencia de la organización.<br>* Usuarios finales de la organización.<br>* Infraestructura de la organización.<br>* Encuestas e indicadores finales. | * No recibo a satisfacción por parte de la organización.<br>* No recibo a satisfacción de la oficina TIC de la organización.<br>* Insatisfacción por parte de los usuarios finales de la herramienta. |

*Nota.* Esta tabla representa los requisitos para los entregables

## 10.6 Cronograma

### Tabla 3



| PROYECTO: Análisis de vulnerabilidades en sitio web de la organización Infraestructura Tecnológica De Colombia (Ethical Hacking) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N.° | Tarea | | Depende de: | Realizada Por | Duracion | Inicio | Fin | Otros Recursos | Marzo 11 30 | Abril 1 27 | Mayo 1 30 | Junio 1 15 |
| 1 | | | | | | | | | | | | |
| 1.1 | Gestión del proyecto | | | | | | | | | | | |
| | 1.1 | Inicio | | * Analista vulnerabilidades-pentesting | | | | | | | | |
| | | 1.1 | Costos | * Analista de ciberseguri-dad- gestión y procesos | | | | | | | | |
| | | 1.2 | Cronograma | * Analista de ciberseguri-dad-hacking ético | | | | | | | | |
| | | 1.3 | Actividades | * Analista de ciberseguri-dad-implementación de procesos | | | | | | | | |
| 1.2 | Análisis y Planeación | | | | | | | | | | | |
| 1.2.1 | Levantamiento activos de Información de la organización | | ciberseguridad, procesos y hackin ético | Analista de ciberseguridad-hacking ético | 20 días | 11-mar | 01-abr | | | | | |
| 1.2.2 | Una vez se culmine el primer punto, se evaluarán y se ajustará en caso de ser necesario los medios analizados. Esto se desarrollará durante el mes de marzo. | | | Analista vulnerabilidades-pentesting | 20 días | 11-mar | 01-abr | | | | | |
| 1.2.3 | Implementación | | | | | | | | | | | |
| 1.2.3 | ético para buscar posibles vulnerabilida-des y | | ciberseguridad, procesos y hackin ético | Analista de ciberseguridad-hacking ético | 27 días | 01-abr | 27-abr | | | | | |
| 1.2.4 | Salida a Producción | | | | | | | | | | | |
| 1.2.4 | Finalizada la segunda fase, se procederá a la implementación en toda la organización, durante este proceso se tendrán planes de contingencia y de manejo de gestión de cambio, la primera permitirá que en caso de presentarse un improvisto no se vea afectada la prestación de servicio dentro de la organización, la segunda estará orientada para presentar a la compañía los hallazgos encontrados y las recomendaciones adecuadas para las brechas de seguridad identificadas. | | ciberseguridad, gestión y analisis en procesos y hackin ético | Analista de Vulnerabilidades-pentesting<br>Analista de ciberseguridad-hacking ético<br>Analista de ciberseguri-dad- gestión y procesos<br>Analista de ciberseguri-dad- gestión-implemen-tación de procesos | 28 días | 30-may | 28-jun | | | | | |

*Nota.* En esta tabla se representa el cronograma identificado tareas, responsables y duración.

## 10.7 Costos

### Tabla 4

| N° | Item | Horas | Valor en pesos |
|---|---|---|---|
| 1. | Analisis de vulneravilidades 5 aplicaiones web WPT | 100 | $ 7.500.000,00 |
| 2. | Analisis de vulneravilidades 5 a 10 servidores | 32 | $ 2.500.000,00 |
| 3. | Recomendaciones de remendacion | 20 | $ 3.000.000,00 |
| | **Subtotal Analisis** | | $ 13.000.000,00 |
| **N°** | **Especielistas** | **Horas** | **Valor peso Colombiano** |
| 1. | Analista de vulneravilidades Pentesting | 12 | $ 13.000.000,00 |
| 2. | Analista de Ciberseguridad y Hacking etico | 12 | $ 13.000.000,00 |
| 3. | Analista de Cirberseguridad y gestion de procesos | 12 | $ 13.500.000,00 |
| 4. | Analista de Ciberseguridad e implementacion de proces | 12 | $ 15.000.000,00 |
| | **Subtotal mano de obra** | | $ 54.500.000,00 |
| | **Iva** | | $ 12.825.000,00 |
| | **Subtotal** | | $ 67.500.000,00 |
| | **Total$** | | $ 80.325.000,00 |

*Nota.* En esta tabla se representan los costos sobre el análisis de vulnerabilidades y mano de obra.

## 10.8 Tablero de Gestión De Riesgos

### Tabla 5

**Proyecto -** Análisis de vulnerabilidades en sitio web de la organización Infraestructura Tecnológica De Colombia

**Informe a fecha: 18-11-20221**

| Riesgo | | | Nivel de riesgo | | | Gestión del riesgo | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| N° | Riesgo | Status | Impacto | Probabilidad | Nivel | Disparador | Respon-sable | Plan de mitigación | Plan de contingencia | Recursos |
| 1 | No pago de honorarios | vigente | 3 | 1 | 3 | | Alta Dirección de la organización | Polizas de cumplimiento | Aseguradora | Legales |
| 4 | Retrasos por autorizaciones y/o cambio del equipo de trabajo | vigente | 3 | 1 | 3 | | Consultores de ciberseguridad | Polizas de cumplimiento | Backup para el equipo de personal | Legales y humanos |
| 2 | Inconsistencia en la infraestructura tecnológica | vigente | 3 | 2 | 6 | | Oficina TIC de la organización | Polizas de cumplimiento | Equipos de backup | Legales y técnicos |
| 3 | Eventualidades ambientales | vigente | 2 | 1 | 2 | | Alta Dirección de la organización | Polizas seguros todo riesgo | Aseguradora | Legales |
| 5 | No recibo a satisfacción por parte de la alta dirección de laorganización | vigente | 3 | 1 | 3 | | Consultores de ciberseguridad | Polizas de cumplimiento | Aseguradora | Legales |
| 6 | No recibo a satisfacción de la oficina TIC de la organización | vigente | 3 | 1 | 3 | | Consultores de ciberseguridad | Polizas de cumplimiento | Revisión y ajustes de los entregables acordados | Legales y metodológicos |
| 7 | Insatisfacción por parte de los usuarios finales | vigente | 2 | 2 | 4 | | Consultores de ciberseguridad y alta dirección | Planes de gestión del cambio | Políticas de seguridad en la información de la organización | Legales, contractuales, metodológicos y pedagogicos |

*Nota.* En esta tabla se representa la matriz de riegos identificados en el desarrollo del proyecto.

## 11. Propuesta Valor

Durante nuestra consultoría nos encargamos de prestar servicios de análisis a fallas y vulnerabilidades de seguridad de los sistemas de información de la organización antes de que lo hagan atacantes reales evitando perdidas de información, disponibilidad e incluso pérdidas económicas. Para esto desarrollamos unas auditorias sobre el alcance y tipos de activo para cada empresa; con la cual entregaremos unas recomendaciones para poder corregir las vulnerabilidades presentes y si la empresa afectada no cuenta con el soporte o el personal técnico capaz de subsanar dichas recomendaciones les brindamos una capacitación a su personal técnico con el único fin de mitigar las fallas o incluso mejorar su nivel de seguridad si así lo requiere la misma.

Para esta consultoría nos basamos en dos procesos para llevar a cabo cada caso con éxito:

### 11.1 Análisis de vulnerabilidades

Este proceso se realiza mediante las diferentes herramientas tecnológicas con las cuales evaluamos las diferentes infraestructuras tecnológicas identificando debilidades con las cuales un atacante pueda acceder, modificar y robar información de alto valor para la empresa. Entregando un informe técnico con dichas vulnerabilidades y sus posibles acciones con el fin de mitigar dicho déficit. Para esto atacamos cada uno de los componentes de la red realizando un análisis uno a uno siguiendo buenas prácticas de seguridad.

### 11.2 Pruebas WEB Penetration Testing –WPT

Esta metodología sigue una serie de pasos a lo largo de varias fases que pueden ser aplicables a múltiples pruebas de seguridad similares. Estas fases se enmarcan en un ciclo de pruebas de intrusión en el cual se recolecta información, se identifican los potenciales vectores de ataque, se realiza una explotación de las vulnerabilidades identificadas y finalmente se

analiza el resultado obtenido para retroalimentar el ciclo mismo de la prueba con nueva información.

# 12. Resultados

## 12.1 Informe Técnico

Este informe contiene el resultado de los hallazgos de las pruebas realizadas.

- Exposición
- Impacto
- Mitigación
- Evidencia (cuando aplique)
- Conclusiones.

## 12.2 Informe Ejecutivo

Este informe consolida a alto nivel los hallazgos de las pruebas presentándolos de forma visual y categorizada por criticidad para un fácil entendimiento de la alta dirección.

Este informe contiene:

- Presentación ejecutiva de las vulnerabilidades en relación con el Top 10 de OWASP.
- Hallazgos de las pruebas realizadas.
- Gráfica del consolidado de las vulnerabilidades clasificadas (Alto, Medio, Bajo).
- Gráfica grado de exposición (Alto, Medio, Bajo).
- Consolidado del número de vulnerabilidades por cada IP evaluada, denotando el grado de exposición.
- Conclusiones.

# 13. Conclusiones y Recomendaciones

## 13.1 Conclusiones

Al realizar el paso a paso para hallar las vulnerabilidades y análisis de estas en una red de datos, se obtiene un aprendizaje importante no solo para aquellos quienes realizan las labores, sino también para el personal de la empresa.

Los incidentes de seguridad afectan cada vez más a las empresas, por tal motivo se requiere aún más educación de los empleados responsables del manejo de la información, capacitación y concientización para todo el personal de las empresas en cuanto a mejores prácticas y seguridad informática.

La seguridad es un proceso que se requiere de manera vital y necesaria en las empresas, no se debe considerar la seguridad como un proceso innecesario, ya que debido a que no se tiene en cuenta este proceso, surgen los riesgos, amenazas, en cuanto a robo o secuestro de información en una empresa.

Por medio de las pruebas de pentesting permite hallar y demostrar las vulnerabilidades del sitio web, así mismo permite evaluar y encontrar los riesgos y por último nos permite desde software desarrollados para hacking ético prevenir posibles ataques que se intenten realizar sobre el sitio web de la organización.

Las empresas deben de manera recurrente realizar pruebas y simulaciones de Hacking ético sobre sus plataformas o sitios web con el fin de identificar riesgos en la seguridad de la información y plantear estrategias para prevenir y mitigar posibles daños o perdidas de la información que es vital para la empresa.

### 13.2 Recomendaciones

Es recomendable realizar este tipo de consultorías con regularidad sobre los servicios o plataformas web que se tienen en la organización, una vez detectadas las vulnerabilidades se debe implementar políticas que permitan dar tratamiento correctivo, de solución y prevención a los errores encontrados, con este procedimiento se garantiza la seguridad y funcionamiento del sitio web.

Es recomendable implementar políticas de prevención y concientización a los empleados de la empresa sobre el uso responsable del correo electrónico e identificación de correos sospechosos para que sean notificados de manera inmediata a la oficina TIC y al oficial de seguridad de la información o quien haga sus veces.

Se recomienda tener actualizados tanto los sistemas operativos, como los softwares instalados de terceros, tanto navegadores web, como antivirus, entre otros que se utilicen por parte de la empresa, ya que los fabricantes continuamente liberan actualización de seguridad, que permiten mitigar amenazas y riesgos desarrollados por parte de hackers, como virus, troyanos, gusanos, keyloggers, entre otras amenazas, siempre están en proceso continuo de creación y mejora.

Se recomienda configurar servicios de la empresa como proxys y firewalls para el filtrado y acceso a sitios web seguros y de confianza, identificar si dichos sitios web tienen certificado de seguridad, si la URL inicia con “HTTPS”, realizar análisis de sitios web sospechosos y que puedan encontrarse en listas negras.

Existen diferentes sitios web para analizar URL, Archivos, tanto de costo, como gratuitos, entre los gratuitos es recomendable validar desde el sitio web: https://www.virustotal.com/gui/home/upload, es un sitio web que realiza un análisis a cada URL o archivo, desde diferentes proveedores de seguridad, donde dichos proveedores analizan y

comparten las firmas de amenazas identificadas a nivel mundial, de acuerdo con los resultados obtenidos nos brinda una identificación del porcentaje y tipo de amenaza.

Se recomienda la implementación de políticas para el uso de contraseñas seguras, apoyados en herramientas como directorio activo o LDAP, es decir aquellas que no contienen nada de información personal, contienen caracteres especiales, adicional modificar dichas contraseñas con frecuencia, y evitar acceder a los servicios web de la organización desde redes desconocidas o públicas.

Se recomienda desde el directorio activo, modificar permisos de manera correcta adicional evitar que no permita realizar ping desde equipos internos, como externos a IP de servidores, sitios web, entre otros (excepto área de infraestructura y seguridad de la información), para de esta manera evitar un ataque de denegación de servicio.

Se recomienda a la empresa implementar estrategias de mitigación y control efectivas para ataques cibernéticos que busquen explotar vulnerabilidades, usar como marco de referencia lo planteado los controles establecidos en el anexo A de la norma ISO/IEC 27002:2013, aprobado por la NTC 294-13.

# 14. Glosario

## 14.1 Activo de información

Cualquier componente humano, software, tecnológico, documental o infraestructura, que soportan uno o más procesos de la organización y en consecuencia debe ser protegido.

## 14.2 Autenticación

Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico cuando accede a un sistema de información.

## 14.3 Clasificación de información

Es la decisión para asignar un nivel de sensibilidad a los datos cuando se crea, corrige, almacena o transmite. Debe usarse para crear un conjunto apropiado de niveles de protección.

## 14.4 Código malicioso

El software malicioso incluye todos los programas que codifican deliberadamente para causar un acontecimiento inesperado en el PC de un usuario.

## 14.5 Incidente de seguridad

Es un evento adverso, confirmado o sospechoso, que haya vulnerado la seguridad de la información o que intente vulnerar, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen.

## 14.6 Política de seguridad

Conjunto de reglas, protocolos, normas e Instrucciones documentadas que velan por la seguridad de la información dentro de una organización.

## 14.7 Recursos tecnológicos

Componentes de hardware y software como, servidores, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red y base de datos entre otros.

### 14.8 Usuarios

Personal de planta, clientes, personal en misión, proveedores, practicantes.

### 14.9 Ciberataque

Es una actividad tecnológica con intención de dañar o a lograr un acceso a documentos importantes y sistemas de una red empresarial o personal incluyendo el control y edición de estos.

### 14.10 Ataque de denegación de servicio distribuido

Es un ataque DDoS o ataque distribuido de denegación de servicio, el cual intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.

### 14.11 JavaScript

Es un lenguaje de programación o de secuencias de comandos que te permite implementar funciones complejas en páginas web, cada vez que una página web hace algo más que sentarse allí y mostrar información estática para que la veas.

### 14.12 Cookies

Son archivos que contienen datos en pequeños fragmentos, como un nombre de usuario y contraseña, que se intercambian entre la computadora de un usuario y un servidor web para identificar a los usuarios y mejorar su experiencia de navegación permitiendo recuperar su información de inicio de sesión individual y sus preferencias. (INCIBE, 2020)

## 15. Bibliografía

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria.

Centro cibernetico Policia Nacional. (2020). *Centro cibernetico Policia Nacional.* Obtenido de https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. (1 de julio de 2020). *Documento Conpes 3995.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Díaz, J. P. (31 de Mayo de 2020). *Análisis de vulnerabilidades basado en Pentesting y propuesta de aseguramiento de un escenario simulado de la infraestructura física y lógica para la Institución del Caso de Estudio Institución Registradora Nacional.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/35377/jparrad.pdf

INCIBE. (2020). *Glosario de términos de ciberseguridad.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

León, M., & León, P. (2021). Hacking ético en el sector financiero. *SUR ACADEMI Revista Academica Investigativa*, 86-87.

LSCV SYSTEMS EIRL. (s.f.). *FASES DEL HACKING ÉTICO*. Obtenido de http://www.lscvsystems.com/index.php/servicios/seguridad-de-la-informacion/hacking-etico

MINTIC. (2016). *Ley 1273 de 2009.* Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Policia Nacional de Colombia. (16 de Noviembre de 2022). *Normatividad sobre delitos informáticos*. Obtenido de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *REVISTA CIENTIFICA DOMINIO DE LAS CIENCIAS*, 685.

Ventura Quijano, M. A. (2021). *LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020.* Obtenido de https://repositorio.upn.edu.pe/bitstream/handle/11537/28942/Ventura%20Quijano%2c%20Mishell%20Alisson.pdf?sequence=11&isAllowed=y

# 16. ANEXOS

## 16.1 Carta de Aprobación

Aceptación Consultoría

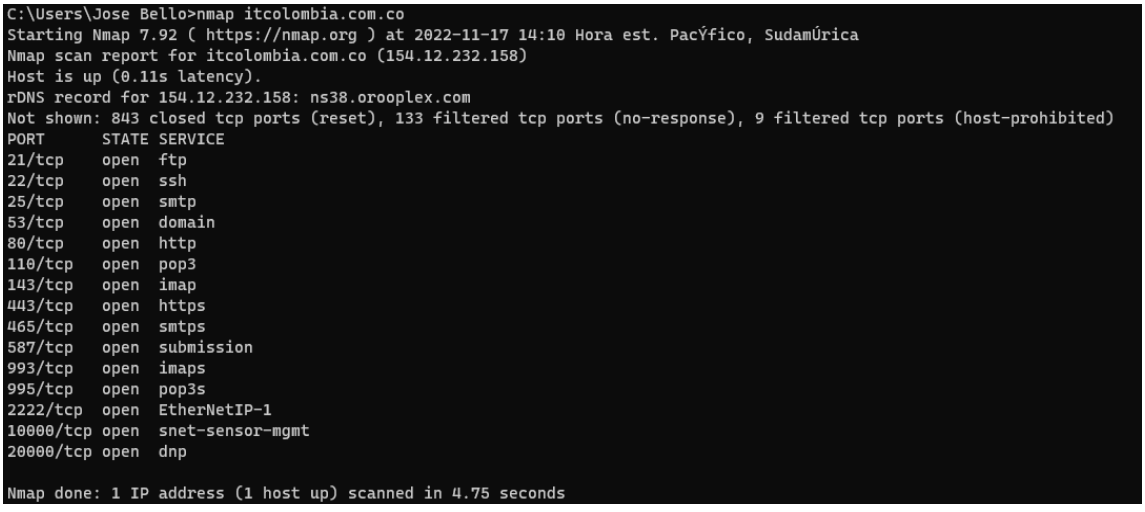
## 16.2 Diagnostico estado página web

Se realiza con el fin de brindar una previsualización del estado actual de la pagina www.itcolombia.com.co usada por la organización Tecnológica de Colombia S.A.S., para esto se realiza uso de la herramienta Nmap, Software de código abierto que se utiliza para el escaneo de red y sus puertos con el objetivo de obtener información la cual pueda ser útil al momento de gestionar la seguridad dentro de una organización, generalmente usada como herramienta de auditoría y monitoreo.

Como punto de partida, se toman los siguientes comandos los cuales que permiten realizar un mapeo de puertos asociados a la URL www.itcolombia.com.co

**Figura 3.**

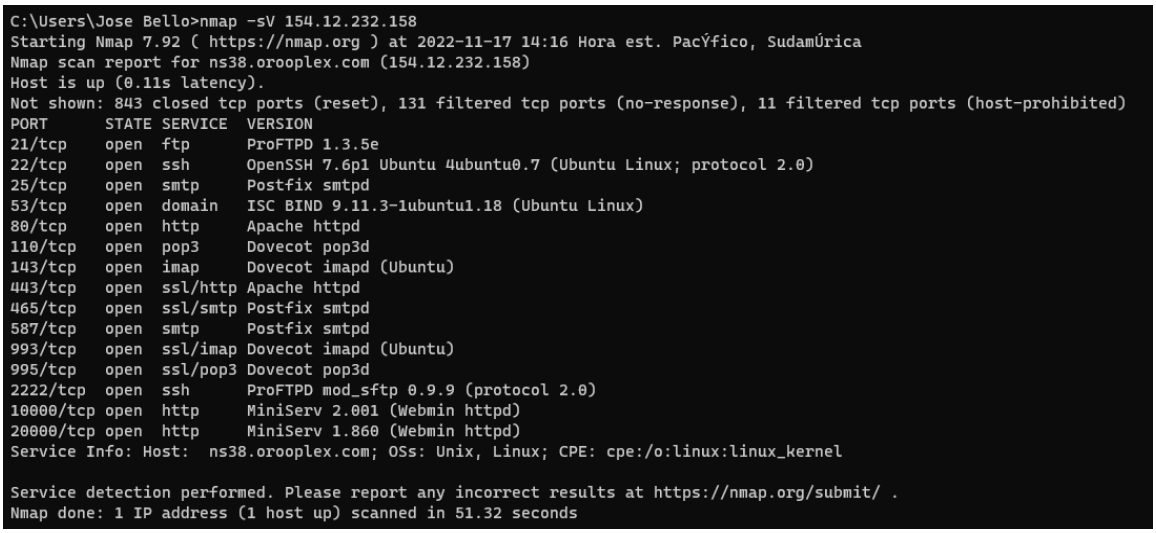
**Mapeo de puertos**




*Nota.* En la figura 3 se representa el mapeo de puertos realizado desde el comando nmap

**Figura 4.**

**Mapeo de puertos y servicios**



```
C:\Users\Jose Bello>nmap -sV 154.12.232.158
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 14:16 Hora est. PacÝfico, SudamÚrica
Nmap scan report for ns38.orooplex.com (154.12.232.158)
Host is up (0.11s latency).
Not shown: 843 closed tcp ports (reset), 131 filtered tcp ports (no-response), 11 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      ProFTPD 1.3.5e
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.11.3-1ubuntu1.18 (Ubuntu Linux)
80/tcp    open  http     Apache httpd
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd (Ubuntu)
443/tcp   open  ssl/http Apache httpd
465/tcp   open  ssl/smtp Postfix smtpd
587/tcp   open  smtp     Postfix smtpd
993/tcp   open  ssl/imap Dovecot imapd (Ubuntu)
995/tcp   open  ssl/pop3 Dovecot pop3d
2222/tcp  open  ssh      ProFTPD mod_sftp 0.9.9 (protocol 2.0)
10000/tcp open  http     MiniServ 2.001 (Webmin httpd)
20000/tcp open  http     MiniServ 1.860 (Webmin httpd)
Service Info: Host:  ns38.orooplex.com; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.32 seconds
```

*Nota.* En la figura 4 se representa el mapeo de puertos y el servicio desde el comando nmap -sv.

De acuerdo con estos comandos de búsqueda puertos y servicios podemos evidenciar riesgos potenciales con los cuales se pueden verse comprometidos la Confidencialidad, Integridad y disponibilidad del sitio web.