UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

ROL DEL PENTESTING EN EL CUMPLIMIENTO DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 2024

AUTOR:

JAIR ALEXANDER CACHIPUENDO AGUIAR

DIRECTOR:

ING. DARWIN PAÚL CARRIÓN BUENAÑO

GUARANDA – ECUADOR

2024

TEMA DEL PROYECTO DE INVESTIGACIÓN

ROL DEL PENTESTING EN EL CUMPLIMIENTO DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, 2024

LÍNEA DE INVESTIGACIÓN

Dominio	Línea	
Tecnologías de la Información y Comunicación	Gestión De Tecnologías de la Información y Comunicación	
	Ingeniería De Software, Redes y Telecomunicaciones	X
	Educación Virtual, Teleeducación	
	Big Data, Cloud Computing, Gestión de Datos e Inteligencia Artificial	
	Geomática	

Sublínea	Seguridad de las Aplicaciones

AGRADECIMIENTO

A mi tutor de tesis, Ing. Darwin Carrión, mis mas sinceros agradecimientos por su constancia y paciencia a lo largo del presente proyecto.

A mis pares académicos, Fis. Rafael Medina, por su gentil y valioso aporte en la elaboración de este proyecto. Al Ing. Christian Barragán, reconocer y agradecer su generosidad, tiempo y conocimiento transmitidos durante este proyecto, su aporte fue valioso y significativo.

Al Ing. Edgar Rivadeneira, por sus enseñanzas y consejos dirigidos a mi proyecto en el área de la investigación, su aporte fue invaluable para la culminación de este trabajo.

A mis familiares, mil gracias por su ayuda durante este recorrido. Quiero reconocer el papel fundamental de mi abuelita Esther y a mis tíos Ángel, Edison, Galo y Sandra, quienes con su ayuda también hicieron posible esta meta.

A la UEB, especialmente al personal docente, que gracias a su compromiso y profesionalismo han sido fundamentales para mi desarrollo profesional.

DEDICATORIA

A Dios, por brindarme el brío y la fuerza en los momentos más difíciles para poder salir adelante y poder culminar esta etapa profesional.

A mis padres, Carlos y Guicela, quienes han sido mi principal motivación durante el transcurso de esta carrera. Gracias a los valores y enseñanzas que me han transmitido a lo largo del tiempo y por enseñarme a jamás darme por vencido sin importar la adversidad. Siempre les estaré eternamente agradecido, han sido un pilar fundamental en mi vida. Este logro también es de ustedes, ya que, sin su apoyo y guía esta meta hubiese sido una utopía.

A mi hermano, Roger**,** mi compañero de vida con quien hemos compartido alegrías y tristezas.

CERTIFICADO DE VALIDACIÓN

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Darwin Carrión, Ing. Christian Barragán y Fis. Rafael Medina, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "ROL DEL PENTESTING EN EL CUMPLIMIENTO DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 2024" desarrollado por el señor Cachipuendo Aguiar Jair Alexander.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 07 de abril del 2025

Ing. Darwin Carrión

Director

Ing. Christian Barragán

Par Académico

Fis. Rafael Medina

Par Académico

DERECHOS DE AUTOR

UEB | UNIVERSIDAD ESTATAL DE BOLÍVAR

BIBLIOTECA GENERAL

DERECHOS DE AUTOR

Yo **Jair Alexander Cachipuendo Aguiar** portador de la Cédula de Identidad N **1750841817** en calidad de autor y titular de los derechos morales y patrimoniales
del Trabajo de Titulación: **Rol del pentesting en el cumplimiento de la Norma ISO 27001 para la gestión de la seguridad de la información 2024**, modalidad **Proyecto de Investigación**, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Jair Alexander Cachipuendo Aguiar
C.I: 1750841817

ÍNDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad, la seguridad de la información se ha convertido en un aspecto fundamental para las organizaciones que buscan proteger sus activos digitales y mantener la confidencialidad, integridad y disponibilidad de la información (Figueroa-Suárez et al., 2018). Ante la creciente amenaza de ciberataques y la necesidad de cumplir con estándares de seguridad reconocidos a nivel mundial, la Norma ISO 27001 para la Gestión de la Seguridad de la Información se ha establecido como un referente indispensable para garantizar la protección de los activos de información.

Muyón & Montaluisa (2020) mencionan que "La seguridad de la información permite gestionar los activos de información y controlar de mejor manera sus riesgos, en relación al impacto que representan para una organización.".

El pentesting, o pruebas de penetración, emerge como una herramienta esencial en este contexto. A través de simulaciones de ataques, el pentesting permite a las organizaciones evaluar la efectividad de sus controles de seguridad y descubrir debilidades antes de que puedan ser aprovechadas en un ataque real.

Dentro del marco de la norma ISO 27001, el pentesting o prueba de penetración adquiere un papel relevante como una herramienta estratégica para evaluar la fortaleza de los sistemas de seguridad implementados por una organización. En este contexto, resulta crucial analizar cómo el pentesting contribuye al cumplimiento de los requisitos establecidos por la norma ISO 27001 y cómo puede ayudar a identificar vulnerabilidades potenciales que podrían comprometer la seguridad de la información.

La presente investigación intenta demostrar la importancia del pentesting dentro de la Norma ISO 27001, demostrando su contribución dentro de algunos controles de esta norma, mejorando la postura de seguridad de las organizaciones.

RESUMEN

El presente proyecto de investigación analiza el rol del pentesting como una herramienta clave para el cumplimiento de la Norma ISO 27001 en la Gestión de la Seguridad de la Información. Se plantea como objetivo principal examinar cómo las pruebas de penetración contribuyen a fortalecer los controles de seguridad exigidos por la norma, especialmente en los dominios A.9 (Control de acceso), A.12 (Seguridad en las operaciones), A.13 (Seguridad en las comunicaciones) y A.14 (Seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información). La investigación es de tipo descriptiva, con un enfoque cualitativo y utiliza los métodos inductivo y deductivo, apoyándose en una revisión documental de tesis y artículos científicos.

El análisis evidencia que el pentesting permite identificar y mitigar vulnerabilidades que otros métodos tradicionales de auditoría no detectan, lo que refuerza el cumplimiento de los controles establecidos por la ISO 27001. En los resultados se muestra una evaluación detallada de los controles que se benefician de esta práctica, destacando la complementariedad del pentesting con las auditorías tradicionales, sus limitaciones y sus implicaciones para las organizaciones. Finalmente, se propone una guía metodológica que integra el pentesting en los dominios antes mencionados, describiendo la aplicación de sus seis fases en los controles donde es viable y aporta valor en la protección de los activos de información.

Palabras claves: Seguridad de la información, Norma ISO/IEC 27001, pentesting, auditoría de seguridad.

ABSTRACT

This research project analyzes the role of pentesting as a key tool for complying with the ISO 27001 Standard on Information Security Management Systems (ISMS). The main objective is to examine how penetration testing strengthens the security controls required by the standard, focusing specifically on Domain A.9 (Access Control), A.12 (Operations Security), A.13 (Communications Security), and A.14 (System Acquisition, Development, and Maintenance Security). This descriptive, qualitative study employs both inductive and deductive methods, supported by a documentary review of theses, scientific articles, and relevant regulations.

The findings show that pentesting identifies and mitigates vulnerabilities that traditional audit methods may overlook, thereby enhancing compliance with ISO 27001 controls. The results present a detailed assessment of controls benefiting from this practice, highlighting the complementarity between pentesting and traditional audits, as well as its limitations and organizational implications. Finally, a methodological guide is proposed, integrating pentesting into the aforementioned domains and outlining how its six phases are applied to the controls where it is effective and valuable in safeguarding information assets.

Keywords: Information security, ISO/IEC 27001 standard, pentesting, security audit.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1. Descripción del Problema

En la era tecnológica actual la seguridad de la información es un problema creciente, debido al aumento exponencial de los ataques informáticos, que van desde la extracción de información personal hasta el robo de registros comerciales y financieros. Bajo este contexto el pentesting se ha convertido en un instrumento esencial para la identificación de las vulnerabilidades de los sistemas informáticos mediante la simulación de amenazas que los ciberatacantes pueden utilizar a su favor.

La seguridad de la información va en auge y en todas las empresas u organizaciones que contengan algún sistema informático deben estar conscientes que las amenazas están por donde quiera y que la protección de su información debe ser prioridad para el cumplimiento de los objetivos de valor. La seguridad de la información cuenta con tres pilares fundamentales que son: la confidencialidad, la integridad y la disponibilidad (Vanegas & Alfonso, 2019) .

"Día a día las empresas están sometidas a amenazas que ponen en riesgo los tres pilares antes mencionados, estos riesgos pueden ser externos e inclusive aún más peligrosos, pueden ser internos"(Vanegas & Alfonso, 2019).

Hoy en día, los ataques cibernéticos son cada vez más frecuentes debido al rápido aumento de la cantidad de información. Los atacantes aprovechan cualquier brecha o posible vulnerabilidad para acceder a los datos confidenciales de las organizaciones. Por esta razón, la ciberseguridad se ha convertido en un factor clave y prioritario (Silva, 2023).

El número de incidentes relacionados con la ciberdelincuencia, al igual que el daño causado por ellos, aumenta cada año. También aumenta la complejidad de las investigaciones, los atacantes utilizan medios más sofisticados en la realización de ciberataques (Silva, 2023).

Los incidentes relacionados aumentan cada año, lo que hace que la gente tome conciencia de los daños causados por tales incidentes (Hung-Hsiou & Jyun-Rong, 2023).

A pesar de la implementación de medidas de seguridad avanzadas, el acceso no autorizado y las vulnerabilidades en los sistemas continúan aumentando. Estas vulnerabilidades exponen los sistemas de información a riesgos como el robo de datos y ataques de malware, que representan una amenaza considerable para la integridad de los datos de los usuarios y seguridad del sistema (Agalit Mohamed et al., 2023).

Bajo este contexto las organizaciones buscan adherirse a marcos y normas internacionales como la ISO 27001, que proporciona un enfoque sistemático para la gestión de la seguridad de la información a través de un Sistema de Gestión de Seguridad de la Información (SGSI).

A pesar de su importancia, el pentesting a menudo no se integra adecuadamente en los procesos de auditoría y gestión de riesgos que exige la ISO 27001, limitando su eficacia.

La falta de integración del pentesting en el SGSI presenta varios problemas:

Evaluación incompleta de riesgos: Sin un enfoque sistemático para realizar pentesting de manera periódica, muchas vulnerabilidades críticas pueden pasar desapercibidas, lo que aumenta el riesgo de sufrir brechas de seguridad.

Desconexión entre el cumplimiento normativo y la seguridad técnica real: Las organizaciones pueden cumplir con los requisitos de ISO 27001 sin haber evaluado de manera exhaustiva la seguridad técnica de sus sistemas, lo que genera una falsa sensación de seguridad.

Los procesos limitados de auditoría y mejora contínua: la ISO 27001 fomenta la mejora continua, pero si no se incluyen pruebas de penetración en el ciclo de auditoría interna, la capacidad de una organización para detectar y corregir vulnerabilidades de manera oportuna se ve comprometida.

Resistencia organizacional y falta de recursos: la implementación de pentesting puede enfrentarse a barreras dentro de las organizaciones, como la falta de personal capacitado, recursos financieros limitados, o una percepción de que es un proceso disruptivo o costoso.

1.2. Formulación del Problema

¿Cómo contribuye el pentesting al cumplimiento de la norma ISO 27001 en la gestión de la seguridad de la información y qué impacto tiene en la efectividad de los controles de seguridad?

1.3. Preguntas de Investigación

¿Cuáles son los controles de la norma ISO 27001 que se benefician directamente de la implementación del pentesting?

¿Cuáles son las barreras y desafíos que enfrenta la integración del pentesting en el cumplimiento de ISO 27001?

¿Cómo el pentesting complementa los métodos tradicionales de auditoría en la identificación de vulnerabilidades dentro del marco de la ISO 27001?

1.4. Justificación

Muyón & Montaluisa (2020) señalan que "la seguridad de la información permite gestionar los activos de información y controlar de mejor manera sus riesgos, en relación al impacto que representan para una organización".

Examinar cómo el pentesting (pruebas de penetración) no solo ayuda a cumplir con los requisitos de la norma ISO 27001, sino que también juega un papel importante en mejorar la ciberseguridad de las organizaciones, protegiendo la integridad y confidencialidad de la información en un mundo cada vez más interconectado (Parra, 2014).

El pentesting es un método eficaz para determinar el nivel de seguridad y permite identificar muchas deficiencias, a menudo evasivas en las auditorías organizativas de seguridad de la información, tales como:

- Errores de configuración de hardware, sistema y software de aplicación
- Ausencia de actualizaciones instaladas y parches de seguridad
- Uso de contraseñas débiles y fáciles de adivinar
- Segmentación incorrecta de la red
- Errores de software cometidos por los desarrolladores aplicaciones web y de negocios.

La ISO 27001 establece buenas prácticas y controles para proteger los activos de información, manejar incidentes de seguridad y evaluar y reducir los riesgos. Sin embargo, aunque robusta, la norma no especifica de manera precisa cómo se deben realizar ciertos controles técnicos, lo que permite que las organizaciones interpreten e implementen una variedad de enfoques para abordar la seguridad técnica.

Las organizaciones que cuentan con esta certificación pueden demostrar su capacidad para implementar de manera continua medidas de seguridad que protejan sus activos de información, brindando confianza sobre un nivel adecuado de seguridad de la información. Los requisitos establecidos en este estándar son de carácter general y están diseñados para ser aplicables a todo tipo de organizaciones, sin importar su tamaño, tipo o naturaleza (Svatá, 2023).

Una de las áreas críticas dentro de estos controles es la gestión de vulnerabilidades técnicas (control A12.6), que es fundamental para garantizar que las infraestructuras y aplicaciones no presenten fallas que puedan ser explotadas por atacantes.

Las pruebas de penetración (pentesting) tienen un rol fundamental, mediante técnicas que simula ataques cibernéticos para identificar vulnerabilidades en sistemas, aplicaciones, redes, servicios entre otros. Aunque muchas organizaciones utilizan herramientas automatizadas para detectar vulnerabilidades, el pentesting manual o automatizado permite una evaluación más profunda y exhaustiva, proporcionando un análisis práctico de cómo los controles de seguridad resisten ataques del mundo real (Jiménez et al., 2024).

La integración de manera efectiva del pentesting dentro de un SGSI certificado bajo ISO 27001, de tal forma que no solo se logre el cumplimiento normativo, sino también una gestión de la seguridad técnica más sólida, que permita a las organizaciones mitigar proactivamente riesgos y fortalecer su capacidad de respuesta ante incidentes.

La presente investigación permitirá demostrar cómo el pestenting juega un rol fundamental en el cumplimiento parcial de la Norma ISO 27001. Además de establecer buenas prácticas para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) respaldado en la Norma ISO 27001 para evitar vulnerabilidades en los diferentes sistemas de software.

Este estudio es importante debido a la creciente necesidad que tienen las organizaciones de seguir las especificaciones técnicas de la ISO 27001 sin la obligación de certificarse bajo esta misma norma como establece el Esquema Gubernamental de Seguridad de la Información. Dado que el pentesting es una técnica orientada a la detección de vulnerabilidades, el análisis de esta herramienta dentro del contexto de la Norma ISO 27001 permitirá establecer su verdadero impacto en el cumplimiento de los dominios (especificar) de esta norma y sus respectivos controles de seguridad.

1.5. Objetivos: General y Específicos

1.5.1. Objetivo General

Analizar el rol del pentesting para el cumplimiento de la Norma ISO 27001 en la Gestión de la Seguridad de la Información

1.5.2. Objetivos Específicos

- Identificar los controles de la norma ISO 27001 del Anexo A que se benefician directamente de la implementación del pentesting.

- Determinar las barreras y desafíos que enfrenta la integración del pentesting en el cumplimiento de ISO 27001.

- Estudiar a través de revisiones bibliográficas y análisis documental, cómo el pentesting complementa los métodos tradicionales de auditoría en la identificación de vulnerabilidades dentro del marco de la ISO 27001.

1.6. Idea a Defender

El pentesting es una herramienta esencial en el proceso de cumplimiento de la norma ISO 27001, permitiendo identificar y mitigar vulnerabilidades que otros métodos de auditoría de seguridad no lo hacen, mejorando los controles de seguridad.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

Argudo Vera (2024) en su tesis titulada "Optimización y colaboración en ciberseguridad: diseño y desarrollo de una plataforma de soporte para equipos de pentesting", este proyecto de enfocó en el desarrollo de PentesHub, una plataforma que facilita el diseño integral de las operaciones de pentesting. La solución integra herramientas de análisis de vulnerabilidades, escaneo de puertos y comunicación en tiempo real, promoviendo la eficiencia y colaboración entre los miembros del equipo. Este trabajo demuestra la importancia de contar con plataformas que apoyen la coordinación efectiva en el ámbito de la ciberseguridad.

Filippov (2018) en su trabajo de titulación "Sistema de pruebas para realizar auditorías de seguridad de la información en la empresa sobre la base de estándares internacionales." señala que la esfera de la seguridad de la información se formó, se desarrolló ampliamente y se popularizó universalmente en relación con el número cada vez mayor de ataques de información, junto con la necesidad de protegerse contra ellos y todo tipo de riesgos. En sí mismo, la definición de riesgo de seguridad de la información se puede considerar genéricamente como la posibilidad de que pueda ocurrir un evento adverso específico que tenga una cierta cantidad de daño causado y la probabilidad esperada de que ocurra con consecuencias negativas. Los principales riesgos de seguridad de la información son:

- El riesgo de fuga de información confidencial.
- El riesgo de pérdida y/o inaccesibilidad de datos importantes.
- El riesgo de violación de la integridad de la información y/o datos importantes.
- El riesgo de explotación no autorizada de los recursos de información.
- El riesgo de difusión de información difamatoria en el entorno externo, amenazando la reputación de la organización, etc.

Como antecedente en el área de la ciberseguridad se destaca la tesis de Pilleux (2021) "Sistema de pruebas de penetración automatizadas para aplicaciones web",

presentada en la Universidad de Chile. Este proyecto desarrolló una plataforma modular que centraliza y automatiza la ejecución de diversas herramientas de análisis de vulnerabilidades en aplicaciones web, permitiendo simplificar el proceso de pentesting incluso para usuarios con conocimientos limitados en seguridad informática. Este trabajo sirve como referente en el desarrollo de soluciones que promuevan la automatización de los procesos de pentesting y el fortalecimiento de la seguridad en aplicaciones web dentro de entornos de desarrollo ágil.

Curcio (2023) en su tesis titulada "Fortalecimiento de la Ciberseguridad en la Era Digital: La Sinergia de las Pruebas de Penetración y la ISO/IEC 27001", presentada de la Universidad de Bologna. Este trabajo propone la integración del pentesting dentro sel sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001.

La investigación de Curcio propone una metodología práctica para el desarrollo de sistema de seguridad automatizados en entornos digitales, reforzando la importancia de adoptar enfoques normativos con herramientas de evaluación de vulnerabilidades. Además, se desarrolla en un entorno de laboratorio para demostrar la efectividad de estas prácticas, utilizando herramientas de pentesting reconocidas como Nmap, Nikto y OWASP ZAP (Curcio, 2023).

2.2. Científico

2.2.1. Seguridad de la información

Es el conjunto de técnicas y procedimientos orientados proteger los sistemas de información dentro de una organización. Su objetivo es garantizar la integridad, confidencialidad y disponibilidad de la información (Escrivá Gascó et al., 2013).
La seguridad de la información tiene como objetivo proteger los datos y activos de la empresa, que pueden presentarse en varios formatos, como documentos físicos o correos electrónicos. El uso inadecuado de esta información puede tener consecuencias negativas y perjudicar a la empresa (De La Cruz Rodríguez et al., 2023).

2.2.2. Norma ISO/IEC 27001:2013

Esta norma creada en el año 2005 tiene como finalidad establecer un modelo para

la implementación y administración de un sistema de gestión para la seguridad de la
información, con énfasis en procesos, análisis de riesgos y formulación de controles que
contribuyan a la protección de los datos y mitiguen los riesgos existentes (Ramírez & Rinconc, 2022).

La norma ISO/IEC 27001:2013 se utiliza para certificar un Sistema de Gestión de Seguridad de la Información. A través de su aplicación, una organización puede demostrar a sus clientes y a las entidades con las que mantiene relaciones, su compromiso con la integridad en la gestión de la seguridad de la información. Esta cualidad se convierte en un valor añadido para la disponibilidad de la empresa(Contero, 2019).

Svatá (2023) señala que "la certificación es válida por tres años y después de este período se necesita una auditoría de recertificación."

2.2.2.1 Dominios de seguridad de la ISO/IEC 27001

A continuación, se detallan los 14 dominios de seguridad que establece la Norma ISO 27001 en su Anexo A:

Tabla 1

Dominios de Seguridad de la Norma ISO 27001

Anexo A	Dominios de Seguridad
A.5	Políticas de seguridad de la información
A.6	Organización de la seguridad de la información
A.7	Seguridad de los Recursos Humanos
A.8	Gestión de activos
A.9	Control de Accesos
A.10	Criptografía –Cifrado y gestión de claves
A.11	Seguridad física y del entorno
A.12	Seguridad operacional
A.13	Seguridad de las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de la información
A.15	Relación con proveedores

A.16	Gestión de incidentes de la Seguridad de la Información
A.17	Aspectos de Seguridad de la Información en la gestión de continuidad del negocio
A.18	Cumplimiento

Elaborado por: Jair Cachipuendo, 2024

2.2.2.2 Dominio A.9: Control de Accesos

Se refiere a los requisitos y políticas establecidos para gestionar y controlar el acceso a los activos de información. Esto incluye la implementación de mecanismos de autenticación, autorización y monitoreo que garanticen que solo las personas autorizadas puedan acceder a la información sensible o crítica (Monteza Mera, 2019).

Tabla 2

Objetivos de control y controles del dominio: Control de accesos

A.9 Control de accesos		
A.9.1 Requisitos de negocio para el control de accesos		
Objetivo: Restringir el acceso a la información y a las áreas donde se lleva a cabo el procesamiento de datos (Yance, 2024).		
N°	**Control**	**Descripción del control**
A.9.1.1	Política de control de accesos	Establecer una política formal que defina los requerimientos para el control de accesos, alineada con las necesidades del negocio y los niveles de seguridad necesarios.
A.9.1.2	Control de acceso a las redes y servicios asociados	Asegurar que el acceso a las redes y servicios esté restringido a usuarios autorizados.
A.9.2 Gestión de acceso de usuarios		
Objetivo: Garantizar que solo los usuarios autorizados puedan acceder a los sistemas y servicios, evitando cualquier intento de acceso no permitido (Yance, 2024).		
N°	**Control**	**Descripción del control**
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Definir procedimientos formales para registrar, modificar y eliminar accesos de usuarios.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Garantizar que los derechos de acceso estén limitados según las responsabilidades del usuario.

A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Controlar estrictamente los accesos con privilegios elevados para evitar abusos.
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	Proteger contraseñas y otros datos sensibles de autenticación contra accesos no autorizados.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Revisar periódicamente los derechos de acceso para asegurar su validez.
A.9.2.6	Retirada o adaptación de los derechos de acceso	Modificar o retirar los accesos cuando ya no sean necesarios (por ejemplo, al cambiar de puesto).
A.9.3 Responsabilidades de los usuarios		
Objetivo: Responsabilizar a los usuarios por la protección y el uso adecuado de sus credenciales de autenticación (Yance, 2024).		
N°	**Control**	**Descripción del control**
A.9.3.1	Uso de información confidencial para la autenticación	Educar a los usuarios sobre el manejo seguro de contraseñas y otros datos confidenciales.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el ingreso no autorizado a los sistemas y aplicaciones (Yance, 2024).		
N°	**Control**	**Descripción del control**
A.9.4.1	Restricción del acceso a la información	Configurar sistemas para garantizar que los usuarios accedan únicamente a la información que necesitan.
A.9.4.2	Procedimientos seguros de inicio de sesión	Implementar procesos de autenticación seguros.
A.9.4.3	Gestión de contraseñas de usuario	Aplicar políticas de contraseñas robustas (longitud, complejidad, etc.).
A.9.4.4	Uso de herramientas de administración de sistemas	Restringir el uso de herramientas administrativas a personal autorizado.
A.9.4.5	Control de acceso al código fuente de los programas	Limitar el acceso al código fuente solo a desarrolladores autorizados.

Elaborado por: Jair Cachipuendo, 2024

2.2.2.3 Dominio A12: Seguridad de las operaciones

Se enfoca en garantizar la correcta gestión y protección de los sistemas de información durante sus operaciones diarias. Incluye controles sobre la protección contra malware, la realización de copias de seguridad, la gestión de cambios y la supervisión de eventos de seguridad (Tigse, 2020).

Tabla 3

Objetivos de Control y Controles del Dominio: Seguridad de las Operaciones

A.12 Seguridad de las operaciones		
A.12.1 Responsabilidades y procedimientos de operación		
Objetivo: Garantizar el funcionamiento adecuado y seguro de las instalaciones donde se procesan datos e información (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.12.1.1	Documentación de procedimientos de operación	Formalizar y documentar los procedimientos operativos para garantizar consistencia.
A.12.1.2	Gestión de cambios	Implementar procesos para gestionar cambios en los sistemas de información.
A.12.1.3	Gestión de capacidades	Monitorizar recursos para garantizar que los sistemas puedan manejar las cargas de trabajo.
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	Mantener separados los entornos de desarrollo, prueba y producción.
A.12.2 Protección contra código malicioso		
Objetivo: Velar por la protección de la información y de los entornos de procesamiento de datos frente a amenazas de software malicioso (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.12.2.1	Controles contra el código malicioso	Implementar soluciones como antivirus y firewalls para prevenir ataques de software malicioso.
A.12.3 Copias de seguridad		
Objetivo: Prevenir la pérdida de información (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.12.3.1	Copias de seguridad de la información	Asegurar que la información crítica esté respaldada regularmente.
A.12.4 Registro de actividad y supervisión		
Objetivo: Documentar las actividades y producir evidencias (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.12.4.1	Registro y gestión de eventos de actividad	Monitorizar y registrar actividades para detectar anomalías.
A.12.4.2	Protección de los registros de información	Asegurar la integridad y confidencialidad de los registros.
A.12.4.3	Registros de actividad del	Mantener registros detallados de las actividades realizadas por administradores.

	administrador y operador del sistema	
A.12.4.4	Sincronización de relojes	Sincronizar relojes de sistemas para garantizar la precisión en registros.
A.12.5 Control del software en explotación		
Objetivo: Garantizar la preservación de la integridad en los sistemas en operación (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.12.5.1	Instalación del software en sistemas en producción	Implementar procesos seguros para instalar software.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Evitar que se exploten las debilidades técnicas (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.12.6.1	Gestión de las vulnerabilidades técnicas	Identificar y mitigar vulnerabilidades en los sistemas.
A.12.6.2	Restricciones en la instalación de software	Regular qué software puede instalarse en los sistemas.
A.12.7 Consideraciones de las auditorías de los sistemas de información		
Objetivo: Reducir al mínimo los efectos de las auditorías en los sistemas operativos (Ministerio de Salud y Protección Social, 2023)		
N°	**Control**	**Descripción del control**
A.12.7.1	Controles de auditoría de los sistemas de información	Proteger la seguridad de la información durante auditorías.

Elaborado por: Jair Cachipuendo, 2024

2.2.2.4 Dominio A13: Seguridad de las Comunicaciones

Trata sobre la protección de la información en tránsito, asegurando la confidencialidad e integridad de los datos que se transmiten por redes internas y externas. Incluye la gestión de redes y el uso seguro de servicios de comunicación (Chimborazo, 2021).

Tabla 4

Objetivos de Control y Controles del Dominio: Seguridad de las Comunicaciones

A.13 Seguridad en las Telecomunicaciones

A.13.1 Gestión de la seguridad en las redes		
Objetivo: Garantizar la seguridad de la información que circula por las redes y en las instalaciones que respaldan su procesamiento (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.13.1.1	Controles de red	Garantizar la protección de la información durante su transferencia a través de redes mediante la implementación de controles adecuados.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Asegurar que los servicios de red, como VPNs o firewalls, proporcionen niveles adecuados de seguridad en línea con los requisitos del negocio.
A.13.1.3	Segregación de redes	Separar las redes para proteger la información crítica o confidencial de accesos no autorizados.
A.13.2 Intercambio de información con partes externas		
Objetivo: Asegurar la protección de la información que se intercambia tanto dentro de la organización como con entidades externas (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.13.2.1	Políticas y procedimientos de intercambio de información	Definir políticas y procedimientos formales para garantizar que el intercambio de información se realice de manera segura.
A.13.2.2	Acuerdos de intercambio	Establecer acuerdos claros y documentados para las condiciones bajo las cuales se comparte información con terceros.
A.13.2.3	Mensajería electrónica	Asegurar el uso seguro del correo electrónico y otros servicios de mensajería para proteger la información transmitida.
A.13.2.4	Acuerdos de confidencialidad y secreto	Implementar acuerdos legales con las partes involucradas para proteger la confidencialidad de la información compartida.

Elaborado por: Jair Cachipuendo, 2024

2.2.2.5 Dominio A14: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Asegura que la seguridad sea parte integral del ciclo de vida de los sistemas de información, desde su adquisición y desarrollo hasta su mantenimiento. Se enfoca en proteger el software, las aplicaciones y los sistemas frente a vulnerabilidades (Monteza Mera, 2019).

Tabla 5

Objetivos de Control y Controles del Dominio: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de la información		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la protección de la información esté incorporada de manera fundamental en los sistemas de información a lo largo de todo su ciclo de vida. Esto abarca también los requisitos para los sistemas de información que ofrecen servicios a través de redes públicas (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.14.1.1	Análisis y especificación de los requisitos de seguridad	Asegurar que los requisitos de seguridad se identifiquen y documenten durante la fase de diseño de sistemas de información.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	Proteger la información que se transmite mediante servicios accesibles desde redes públicas, como el cifrado de datos.
A.14.1.3	Protección de las transacciones por redes telemáticas	Garantizar la seguridad en transacciones electrónicas mediante controles como autenticación y cifrado.
A.14.2 Seguridad en los procesos de desarrollo y soporte		
Objetivo: Garantizar que la protección de la información esté integrada y aplicada en el ciclo de vida del desarrollo de los sistemas de información (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.14.2.1	Política de desarrollo seguro de software	Establecer directrices para garantizar que el desarrollo de software siga prácticas seguras.
A.14.2.2	Procedimientos de control de cambios en los sistemas	Implementar procesos para controlar los cambios realizados en los sistemas y prevenir riesgos.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Asegurar que cualquier cambio en el sistema operativo no afecte la seguridad de las aplicaciones.
A.14.2.4	Restricciones a los cambios en los paquetes de software	Limitar modificaciones en paquetes de software estándar para prevenir problemas de seguridad.
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	Incorporar principios de seguridad desde las etapas iniciales de diseño del sistema.
A.14.2.6	Seguridad en entornos de desarrollo	Proteger los entornos de desarrollo para evitar la introducción de vulnerabilidades.

A.14.2.7	Externalización del desarrollo de software	Garantizar que los desarrollos tercerizados cumplan con los mismos estándares de seguridad internos.
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Realizar pruebas regulares para identificar y corregir errores de seguridad en las aplicaciones.
A.14.2.9	Pruebas de aceptación	Definir criterios de aceptación que incluyan evaluaciones de seguridad antes de poner un sistema en producción.
A.14.3 Datos de prueba		
Objetivo: Garantizar la seguridad de los datos utilizados para las pruebas (Ministerio de Salud y Protección Social, 2023).		
N°	**Control**	**Descripción del control**
A.14.3.1	Protección de los datos utilizados en pruebas	Garantizar que los datos utilizados en pruebas estén protegidos contra accesos no autorizados y sean irreversibles si son datos reales.

Elaborado por: Jair Cachipuendo, 2024

2.2.3. Pentesting o Pruebas de Penetración

El Pentesting o pruebas de penetración son ataques controlados a los sistemas para encontrar agujeros de seguridad. Es importante verificar las vulnerabilidades en las aplicaciones y redes informáticas. Consiste en un proceso sistemático que se utiliza para probar las debilidades que se encuentran en las aplicaciones y redes informáticas. Es decir, se trata de un ciberataque controlado realizado por una empresa especializada en redes corporativas (Mata García, 2023).

Este tipo de auditoría busca evaluar las medidas de seguridad técnicas de un sistema u organización, como pueden ser firewalls, IDS/IPS o SIEM. La forma de auditar este tipo de sistemas siempre va a ser emulando a un posible atacante real, para identificar cuáles son las vulnerabilidades explotables que deben ser corregidas, y que, de lo contrario, podrían materializarse en vías para que se produzcan incidentes de seguridad (Chicano Tejada, 2023).

En las pruebas de penetración, se encuentran vulnerabilidades y también se explotan para comprometer otros hosts y detectar vulnerabilidades en la infraestructura de una organización. Los testers de penetración actúan como verdaderos adversarios de la organización, por lo que deben actualizarse con las

últimas herramientas y metodologías para poder imitar los últimos ataques (Casado de Gracia & Sanchez, 2024).

El pentesting puede efectuarse de manera automatizada con aplicaciones informáticas o manualmente por pentesters. Se puede realizar desde fuera de la infraestructura (pentest externo) a través de cualquier conexión a Internet, o desde el interior de una red interna de la empresa (pentest interno) (cporet, 2022).

2.2.3.1 Clasificación del Pentesting

- ***Caja Negra***

  El las pruebas de Pentesting de tipo Caja Negra (Black Box), los pentesters se enfrentan al reto de evaluar sistemas y aplicaciones sin contar con información previa. Este enfoque se centra en simular un ciberataque desde una perspectiva externa, sin tener conocimiento interno de la infraestructura objetivo.

- ***Caja Blanca***

  Según Pérez (2024) "En el White Box Testing, prueba de caja blanca, el evaluador tiene acceso total a la información interna del sistema, incluyendo el código fuente, la arquitectura y la documentación.".

- ***Caja Gris***

  Pérez (2024) menciona que "En este enfoque de pentesting quien evalúa debe combinar elementos de los métodos de caja blanca y caja negra".

- ***Ingeniería Social***

  Consiste en dirigir ataques a los usuarios con el fin con el fin que revelen información, ejecuten software malicioso, accedan a sitios web controlados por el atacante o realicen acciones que le otorguen una ventaja o acceso indebido (Herrero Pérez, 2022).

2.2.3.2 Clasificación del pentesting (según el tipo de objetivo)

Esta clasificación es importante ya que evalúa la capacidad

- ***Pruebas de penetración de red***

  Las pruebas de penetración de la red evalúan la seguridad y las vulnerabilidades ante ataques reales y modela los ataques para medir su

efectividad. Esto es importante para las empresas que manejan grandes cantidades de datos o dependen de la nube (Felipe Redondo & Núñez Cárdenas, 2024).

- ***Pruebas de penetración en apps móviles***

  Las pruebas de penetración de aplicaciones móviles tienen como objetivo identificar vulnerabilidades, que van desde pruebas funcionales hasta pruebas de seguridad. A medida que crecía el número de dispositivos móviles y usuarios, estas pruebas continuaron mejorando, especialmente en plataformas como Android e iOS. El objetivo es detectar posibles accesos a datos confidenciales o interrupciones en la funcionalidad de las aplicaciones para que los desarrolladores puedan minimizar los riesgos y mejorar la seguridad de sus aplicaciones (Felipe Redondo & Núñez Cárdenas, 2024).

- ***Pruebas de penetración de apps web***

  Las pruebas de penetración en aplicaciones web identifican vulnerabilidades para prevenir filtraciones, fraudes y robo de identidad. Las pruebas como la inyección SQL, XSS y la falsificación de consultas ayudan a reducir los riesgos antes de que se utilicen (Felipe Redondo & Núñez Cárdenas, 2024).

- ***Pruebas de penetración de API***

  Las pruebas de penetración de la API identifican vulnerabilidades en el back-End de aplicaciones web y móviles, evitando la divulgación de datos y los ataques. Son especialmente importantes para las empresas que utilizan API de terceros o API nativas (Felipe Redondo & Núñez Cárdenas, 2024).

- **Pruebas de penetración en la nube**

  Una prueba de penetración en la nube analiza las vulnerabilidades en una infraestructura en la nube, ya sea manualmente o mediante un proceso de CI / CD para evaluar la efectividad de los controles de seguridad (Felipe Redondo & Núñez Cárdenas, 2024).

- **Pruebas de penetración de blockchain**

  Las pruebas de penetración de blockchain evalúan la seguridad de las redes, aplicaciones y contratos inteligentes y prueba su resistencia a posibles

ataques dirigidos a comprometer la seguridad de la red (Felipe Redondo & Núñez Cárdenas, 2024).

- **Pruebas de penetración de ingeniería social**

  Las pruebas de penetración de ingeniería social evalúan la seguridad de los empleados de una empresa, identificando vulnerabilidades que pueden ser explotadas por atacantes y aumentando la identificación y prevención de los ataques (Felipe Redondo & Núñez Cárdenas, 2024).

2.2.3.3 Desafíos en la integración del pentesting

Los sistemas de TI modernos, complejos e integrados requieren un enfoque más holístico para las pruebas y sofisticado. Esto requiere que los profesionales de la seguridad mantengan actualizados sus conocimientos y habilidades. Con la condición de falta de expertos que tengan habilidades profundas de prueba de penetración a menudo se convierten en un obstáculo. Además, las sofisticadas herramientas de prueba de penetración a menudo requieren inversión significativa, tanto en términos de costo como de tiempo de capacitación (Fadhli, 2024).

2.2.3.4 Principales herramientas de código abierto para pentesting

Las herramientas de pentesting de código abierto son fundamentales, ya que, permiten ayudar a identificar y explotar vulnerabilidades. Estas herramientas incluyen herramientas de escaneo de vulnerabilidades, herramientas de explotación y herramientas de prueba de aplicaciones web (Fadhli, 2024).

A continuación, se detallan las herramientas de pentesting open source más populares y utilizadas:

- ***Metasploit***

  Metasploit un proyecto de código abierto enfocado a la seguridad informática. Es una de las herramientas de prueba de penetración más populares que se utilizan para desarrollar e implementar exploits. Sin embargo, esta herramienta también puede ser mal utilizada por partes irresponsables. Para usuarios novatos se requiere un conocimiento profundo del sistema de destino para explotar al máximo su potencial (Fadhli, 2024).

- ***Network Mapper (Nmap)***

Nmap es una herramienta de código abierto, destaca por su capacidad para realizar análisis de red de forma rápida y eficiente, identificando hosts y servicios que se ejecutan en la red. Fácil de configurar y dirigido a auditorías de seguridad (Felipe Redondo & Núñez Cárdenas, 2024).

- ***Burp Suite***

  Burp Suite es una herramienta que se centra en la seguridad de las aplicaciones web y proporciona varias funciones para identificar y explotar las debilidades en las aplicaciones web. La mayoría de sus funciones son gratuitas, pero se requiere de una licencia para acceder a sus funciones premium (Garza, 2024).

- ***Wireshark***

  Wireshark es una herramienta utilizada para analizar el tráfico de red y es muy útil para identificar problemas de seguridad a nivel de protocolo. Su ventaja es su capacidad para capturar y analizar paquetes de datos en tiempo real. Sin embargo, usar Wireshark requiere un conocimiento profundo de los protocolos de red y una comprensión de las funciones disponibles (Fadhli, 2024).

- ***OWASP ZAP***

  OWASP ZAP web application security scanner es un escáner de aplicaciones web de código abierto diseñado para descubrir vulnerabilidades en aplicaciones web. Puede funcionar como un servidor proxy donde se puede usar para manipular el tráfico que pasa a través de él, incluido el tráfico que usa https (Ogechi, 2019).

- ***John the Ripper***

  John the Ripper es una herramienta gratuita de pentesting para descifrar contraseñas. Se utiliza para probar y descifrar contraseñas. Es una combinación de algunos descifradores de contraseñas, detecta automáticamente los tipos de hash de contraseñas (Ogechi, 2019).

- ***Nessus***

  Nessus es una herramienta de escaneo de vulnerabilidades compatible con mútiples sistemas operativos. Funciona mediante un demonio llamado “nessusd” que realiza los escaneos y un cliente que muestra los resultados.

Puede usarse por consola o mediante interfaz gráfica. Comienza con un escaneo de puertos, utilizando Nmap o su propio escáner, y es muy valorado en el hacking ético por automatizar la detección de vulnerabilidades, ahorrando tiempo al auditor (Laprovittera, 2024).

- ***Dradis***

  Byte-Mind (2019) menciona que "Dradis es un framework open source, en su versión Comunity, para reportes y visualización de información. Además puede integrar información de multitud de herramientas como pueden ser Nmap, Nessus, Nikto, Burp Suite, etc."

2.2.3.5 Distribuciones de Linux más comunes para realizar pentesting

- ***Kali Linux***

  Es una distribución Linux diseñada orientado a la seguridad informática. Kali Linux fue la sucesora de otra distribución, BackTrack OS, creada en 2006 con el propósito de crear un SO con herramientas de hacking preinstaladas y un repositorio para mantenerlas actualizadas. Kali Linux fue lanzado en 2012 como reemplazo de BackTrack debido a la decisión de cambiar de Knoppix a Debian como la distribución utilizada como base. Unos años más tarde, Kali Linux se convirtió en la herramienta más popular para los hackers éticos (Laseca, 2019).

  Kali Linux no es una distribución liviana, ya que viene con más de 600 herramientas que funcionan listas para usar. Un buen punto sobre Kali es la gran y sólida comunidad de usuarios que lo respalda, lo que lo convierte en una buena opción, ya que será fácil encontrar soporte en Internet (Moreno, 2022).

- ***Parrot OS***

  Es una distribución de Linux lanzada en el año 2013, está basado en Debian y su versión actual es la 4.10.

  Las aplicaciones y herramientas que incluye este sistema operativo tratan sobre ciberseguridad, análisis forense, ingeniería inversa y herramientas diseñadas para uso rutinario y desarrollo de software. Parrot OS tiene un entorno gráfico liviano que le permite trabajar de manera rápida y fluida

incluso en dispositivos más antiguos. La ventaja es que es posible elegir entre dos versiones, donde una está enfocada a la seguridad y las pruebas de penetración. La segunda versión no tiene estas herramientas y, por lo tanto, está diseñada para uso doméstico normal, pero es posible instalar las herramientas adicionalmente (Ředina, 2021).

2.2.3.6 Fases del pentesting

Una prueba de penetración es una de las maneras más efectivas para evaluar la seguridad de un sistema informático. Este proceso es realizado por uno o varios especialistas en hacking ético, quienes buscan identificar y aprovechar cualquier vulnerabilidad existente (Cilleruelo, 2024).

A continuación, se detallan las fases estándar del pentesting:

Reconocimiento

En esta etapa, se recopila la mayor cantidad de datos disponibles acerca del objetivo, aplicando métodos como OSINT (Inteligencia de Fuentes Abiertas), escaneo de puertos, revisión de metadatos y técnicas de footprinting. Se detectan nombres de dominio, direcciones IP, subdominios, servidores, tecnologías empleadas y otros aspectos importantes de la infraestructura. Mientras más información se logre reunir en este proceso, mayor será la precisión del ataque simulado (Palacio, 2025).

Escaneo

Una vez reunida la información, se realiza un análisis de vulnerabilidades usando herramientas como Nmap, siempre con autorización. Algunas empresas cuentan con programas Bug Bounty que indican qué activos pueden ser escaneados (Cilleruelo, 2024).

Explotación

En esta fase se explotan, de forma controlada, las vulnerabilidades detectadas. Según el tipo de pentesting, se aplican ataques como inyección SQL, explotación de servicios, fuerza bruta o escalación de privilegios. Es clave actuar con cautela para no comprometer el funcionamiento del sistema (Palacio, 2025).

Mantenimiento del acceso

Con la lista de vulnerabilidades, el hacker ético analiza qué exploits puede usar para acceder al sistema. Un exploit es un software que aprovecha una falla específica. Al ejecutarlo, se puede activar el payload, es decir, las acciones maliciosas que siguen en la post-explotación (Cilleruelo, 2024).

Borrado de huellas

Los pentesters borran sus huellas para simular cómo un atacante encubre sus acciones y evitar riesgos legales o de seguridad tras las pruebas (Laprovittera, 2024).

Elaboración del informe

Finalmente, se entrega un informe detallado con las vulnerabilidades explotadas, su impacto, evidencias, riesgos y recomendaciones. Un buen reporte no solo señala fallos, sino que ofrece soluciones prácticas y priorizadas (Palacio, 2025).

Ilustración 1: Fases del Pentesting
Fuente: (Laprovittera, 2024)

2.3. Conceptual

2.3.1 Activo

"Cualquier elemento propiedad de la empresa relacionado con la información" (Asensi, 2019).

2.3.2 Activo de Información

Un conjunto de datos que se organiza y gestiona como una entidad única para facilitar la comprensión, el intercambio, la protección y el uso. Es necesario identificar los activos de información y determinar su importancia para la organización, teniendo en cuenta las consecuencias de su posible compromiso en términos de reputación y finanzas (National Quality Assurance, 2022).

2.3.3 Amenaza

Asensi (2019) menciona que una amenaza es una "acción que utiliza una vulnerabilidad para atacar la seguridad de un activo de información".

2.3.4 Análisis de Vulnerabilidades

Argudo Vera (2024) define al análisis de vulnerabilidades como "Proceso de evaluar un sistema, red o aplicación para identificar y clasificar las debilidades de seguridad que podrían ser explotadas por atacantes".

2.3.5 Auditor

"Persona encargada de realizar la auditoría y verificar que los requisitos establecidos por una empresa o los que dicta una norma se cumplen" (Asensi, 2019).

2.3.6 Auditoría de Seguridad

Estudio y análisis independiente del historial y las actividades de un sistema de información, para verificar la idoneidad de los controles del sistema, garantizar el cumplimiento de la estructura de seguridad establecida y los procedimientos operativos, identificar vulnerabilidades y recomendar cambios en los procedimientos, controles y estructuras de seguridad (Correa, 2019).

2.3.7 Confidencialidad

Roa (2015)señala que "la confidencialidad intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas".

2.3.8 Cracker

Son individuos que buscan acceso a un sistema buscando una brecha o vulnerabilidad de seguridad, una vez dentro del sistema extraen la información para fines ilegales o delictivos (Murillo, 2017).

2.3.9 CSF (Framework de Ciberseguridad)

El CSF es un marco especializado de ciberseguridad que incluye la prevención, detección y respuesta a las amenazas digitales. Este marco puede adaptarse a los requisitos específicos de cada organización, lo que permite una mayor flexibilidad en la implementación de sus mecanismos de protección (Silva, 2023).

2.3.10 Disponibilidad

Roa (2015) menciona que "La disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido".

2.3.11 Gusanos

Es un virus que se activa y se transmite a través de la red. El objetivo es multiplicarse hasta agotar el espacio en el disco o la RAM. Por lo general, este es uno de los ataques más destructivos, ya que generalmente conduce a la interrupción de la red (Murillo, 2017).

2.3.12 Hacker

El término hacker hace referencia a los individuos con un gran conocimiento de las tecnologías de la información y la comunicación, dominan el hardware, el software, los lenguajes de programación, los protocolos, etc. Están interesados en el funcionamiento los sistemas de información. Su clasificación se lleva a cabo de acuerdo con sus actividades (Coronel Suárez & Quirumbay Yagual, 2022).

2.3.13 Hackers de sombrero blanco (White hat hackers)

Coronel Suárez & Quirumbay Yagual (2022) definen a los hackers de sombrero blanco como "profesionales de la seguridad informática, realizan investigaciones en busca de vulnerabilidades y fallos, pero bajo un contrato y previa autorización de la organización que se evalúa. Buscan salvaguardar los pilares de la seguridad informática, confidencialidad, integridad y disponibilidad".

2.3.14 Hackers de sombrero negro (Black hat hackers)

Estas personas, conocidas como ciberdelincuentes, tienen un nivel de conocimiento similar al de los expertos en seguridad. Pero la diferencia es que usan su capacidad para obtener acceso no autorizado a los sistemas informáticos para robar o secuestrar información. Por regla general, buscan obtener beneficios económicos vendiendo datos robados o exigiendo un rescate por su devolución (Coronel Suárez & Quirumbay Yagual, 2022).

2.3.15 Hackers de sombrero gris (Gray hat hackers)

Estos híbridos de hackers de sombrero blanco y negro no utilizan sus conocimientos para obtener ganancias financieras, realizan intervenciones de seguridad no autorizadas para exponer a ciertas organizaciones, brindan servicios a empresas y luego venden sus servicios para eliminar deficiencias (Coronel Suárez & Quirumbay Yagual, 2022).

2.3.16 Integridad

Roa (2015) indica que "El objetivo de la integridad es que los datos queden almacenados tal y como espera el usuario: que no sean alterados sin su consentimiento".

2.3.17 ISO 27002

La Norma ISO 27002 proporciona pautas y mejores prácticas para administrar la seguridad de la información dentro de una organización. Su aplicación abarca la identificación de activos de información, el análisis de riesgos, la implementación de controles de seguridad, así como el fortalecimiento y mejora continua del sistema de gestión de la seguridad de la información (Silva, 2023).

2.3.18 Malware

Chavez et al. (2018) definen al malware como "códigos diseñados por ciberdelincuentes cuyo objetivo es el de variar el funcionamiento de cualquier sistema informático, sobre todo sin el usuario se dé cuenta".

2.3.19 No Repudio

Mantilla (2018) menciona que el no repudio "garantiza que quien genere un evento de forma válida no pueda retractarse, pues se puede probar la ocurrencia de un evento y quien lo origina".

2.3.20 Pishing

El phishing es un delito electrónico en forma de fraude, consiste en capturar información altamente confidencial (nombres de usuario, contraseña, tarjetas de crédito, etc) a través de correos electrónicos, redes sociales y sitios web (Fauzan Imam et al., 2023).

2.3.21 Riesgo Informático

Es la combinación de la probabilidad de que ocurra un incidente relacionado con la seguridad de la información y el impacto o consecuencias que dicho evento podría generar (National Quality Assurance, 2022).

2.3.22 SGSI

"Sistema de Gestión de la Seguridad de la Información. Parte del sistema de gestión general empleado para mantener y mejorar la seguridad de la información" (Asensi, 2019).

2.3.23 Spam

También conocido como correo no deseado, aunque no está estrictamente clasificado como un ataque, actualmente está causando un daño significativo a empresas y organizaciones (Murillo, 2017).

2.3.24 Virus

Estos son programas diseñados para cambiar o eliminar información que puede ingresar al sistema a través de dispositivos externos o a través de una red (por ejemplo, correo electrónico) sin la intervención directa de los atacantes (Murillo, 2017).

2.3.25 Vulnerabilidad

Cruz Lucas et al. (2023) señalan que "La vulnerabilidad de la seguridad informática se trata de una debilidad en un sistema de información que abre la puerta para que

un atacante o situación no prevista pueda comprometer la integridad, disponibilidad o confidencialidad de los datos"

2.4. Legal

2.4.1 Constitución de la República del Ecuador

De acuerdo a la Constitución de La República Del Ecuador (2008), numeral 19 menciona lo siguiente: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

2.4.2 Ley Orgánica de Protección de Datos Personales

El artículo 44 de la Ley Orgánica de Protección de Datos Personales hace mención que las autoridades públicas y el personal responsable de la seguridad informática (Equipos de respuesta de emergencias informáticas, equipos de respuesta a incidentes de seguridad informática, centros de operaciones de seguridad, prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad) tienen la facultad para acceder y tratar los datos personales involucrados en notificación de vulneración a las seguridades específicamente para la detección, análisis, protección y respuesta ante cualquier tipo de riesgo o incidente (Ley Orgánica de Protección de Datos Personales, 2021).

2.4.3 Ley Orgánica de Telecomunicaciones

Artículo 76.- Medidas técnicas de seguridad e invulnerabilidad

El artículo 76 establece que los prestadores de servicios de telecomunicaciones tienen la 0responsabilidad de adoptar medidas técnicas en cuanto a la seguridad y protección de las redes y los datos que se transmiten a través de ellas (Ley Orgánica de Telecomunicaciones, 2015, art 76).

En caso de que exista un riesgo de violación de la seguridad de la red, el prestador de servicios de telecomunicaciones tiene la obligación de notificar a sus abonados

o clientes, además deberá proponer posibles soluciones si ese riesgo no está bajo su control.

Artículo 77.- Interceptaciones

El artículo 77 regula la interceptación de comunicaciones y constituye que solo puede realizarse bajo una orden judicial emitida por un juez competente, en el marco de una investigación de un delito o por razones de seguridad pública, cumpliendo con las leyes y el debido proceso (Ley Orgánica de Telecomunicaciones, 2015, art 77).

Bajo este contexto los prestadores de servicios están obligados cooperar en este proceso proporcionando toda la información solicitada, se garantizará que las comunicaciones y los datos personales que sean objeto de interceptación se manejen bajo los más altos estándares de confidencialidad establecidos por la ley.

2.4.4 Código Orgánico Penal (COIP)

Artículo. 178.- Violación a la intimidad

Según el artículo 178 del COIP menciona que la persona que sin consentimiento o sin autorización legal acceda, grabe, publique o difunda información privada de otra persona contenida en sistemas informáticos, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal, 2014, art 178).

Artículo. 190.- Apropiación fraudulenta por medios electrónicos

El artículo 190 del COIP establece sanciones con pena privativa de uno a tres años de libertad a quienes manipulen o alteren de manera fraudulenta sistemas informáticos, redes electrónicas o telecomunicaciones con la finalidad de apropiarse de bienes ajenos o realizar transferencias no consentidas de bienes o valores (Código Orgánico Integral Penal, 2014, 190).

Artículo. 229.- Revelación ilegal de base de datos

El artículo 229 del COIP sanciona con pena privativa de uno a tres años de libertad a la persona que de manera intencional vulnera la privacidad, el secreto y la intimidad de las personas mediante la revelación ilegal de información contenida en una base de datos o medios semejantes a través o dirigidas a un sistema informático o de telecomunicaciones.

Si este delito es cometido por un servidor público, empleadas o empleados bancarios o personas implicadas en la intermediación financiera, la pena aumenta de tres a cinco años de privación de libertad (Código Orgánico Integral Penal, 2014, art 229).

Artículo. 230.- Interceptación ilegal de datos

De acuerdo al artículo 230 del COIP, numerales 1,2,3 y 4 menciona que la interceptación ilegal de datos será sancionada con pena privativa de tres a cinco años de libertad para quienes, sin autorización judicial previa, intercepten y/o manipulen datos informáticos con fines fraudulentos (Numeral 1). Por otro lado, el pishing (Numeral 2), la clonación de tarjetas (Numeral 3) y la producción y distribución de herramientas destinadas a estos fines (numeral 4) también son acciones sujetas a sanción (Código Orgánico Integral Penal, 2014, art 230).

Artículo. 231.- Transferencia electrónica de activo patrimonial

El artículo 231 del COIP sanciona a la persona que altere, manipule o modifique el funcionamiento de un sistema informático o telemático con el fin de procurar la transferencia o apropiación no consentida de activos patrimoniales. Además, será sancionada la persona que facilite o proporcione datos bancarios para recibir de manera ilegítima un activo patrimonial. La pena por estos delitos es de tres a cinco años de privación de libertad (Código Orgánico Integral Penal, 2014, art 231).

Artículo. 232.- Ataque a la integridad de sistemas informáticos

En el artículo 232 del COIP se sanciona el ataque a la integridad de sistemas informáticos, que engloba acciones como destruir, dañar, borrar, deteriorar, alterar o generar un mal funcionamiento en sistemas informáticos o de telecomunicaciones.

En los numerales 1 y 2 de este artículo se menciona que también se sanciona la creación o distribución de programas maliciosos y la alteración de infraestructura tecnológica sin autorización (Código Orgánico Integral Penal, 2014, art 232).

La pena para estos delitos es de tres a cinco años de privación de libertad.

Artículo. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

El artículo 234 del COIP declara que la persona que acceda de manera no autorizada a sistema informático, telemático o de telecomunicaciones, ya sea para modificar portales web, desviar tráfico de datos u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con una pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014, art 234).

Artículo. 476.- Interceptación de las comunicaciones o datos informáticos

El artículo 476 del COIP regula interceptación de comunicaciones y datos informáticos bajo autorización judicial, estableciendo procedimientos estrictos para su uso en investigaciones. Solo puede ser solicitado por un fiscal y aprobado por un juez cuando existan indicios relevantes para la investigación. Se detallan reglas específicas, como la duración de la interceptación, el manejo de la información obtenida y las garantías sobre el secreto profesional y religioso, entre otros aspectos (Código Orgánico Integral Penal, 2014, art 476).

2.4.5 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

De acuerdo a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002, art 57) menciona lo siguiente: "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.".

2.4.6 Esquema Gubernamental de Seguridad de la Información

De acuerdo con el artículo 1 del Acuerdo Ministerial No. 166, el uso de las normas NTE INEN-ISO/IEC 27000 es de carácter obligatorio para todas las instituciones públicas, siendo el SGSI una política prioritaria para la preservación de la información pública y la confianza de los ciudadanos en los sistemas tecnológicos del estado ecuatoriano (MINTEL, 2013).

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

3.1.1 Investigación Descriptiva

La información se recopiló de investigaciones previas que se enfocan en el análisis de uso del Pentesting (Pruebas de Penetración) y su aporte en el cumplimiento de la Norma ISO 27001 en la Gestión de la Seguridad de la Información. Mediante la descripción de los procesos y controles que ofrece la Norma ISO 27001, se identificó como el Pestesting se integra a la norma y qué impacto tendrá en garantizar la seguridad de la información en las organizaciones.

3.2. Enfoque de la investigación

3.2.1 Enfoque Cualitativo

Se adoptó un enfoque cualitativo para realizar una exploración profunda sobre el rol que desempeña el Pestesting dentro de las organizaciones que buscan adherirse a la Norma ISO 27001. Este enfoque permite comprender, desde una perspectiva interpretativa, la percepción y experiencia de los expertos en ciberseguridad sobre cómo el Pentesting contribuye a la identificación de vulnerabilidades y al fortalecimiento de los controles de seguridad.

3.3. Métodos de Investigación

3.3.1 Método Deductivo

Se empleó el método inductivo para investigar los principios generales establecidos en la ISO 27001 para la Gestión de la Seguridad de la Información para realizar el análisis de como el Pentesting puede cumplir con ciertos controles del estándar. Partiendo de los requisitos de la norma se realizó la investigación de cómo las organizaciones implementan el Pentesting en base a los lineamientos de la ISO 27001.

3.3.2 Método Inductivo

Se usó el método inductivo para extraer conclusiones a partir de la observación de casos específico, donde el pentesting ha sido implementado en la Norma ISO 27001. A través de un previo análisis de casos documentados.

3.4. Técnicas e Instrumentos de Recopilación de Datos

3.4.1 Documental

La recopilación de datos fue de tipo documental, basándonos en la revisión exhaustiva del Estándar ISO 27001, procesos de informes de auditoría, documentación técnica sobre el pentesting (Pruebas de Penetración) y estudios e investigaciones previas que aborden la seguridad de la información. El análisis documental permitió obtener información relevante para entender el marco regulador (en este caso la ISO 27001) y la aplicación del Pentesting.

3.5. Procesamiento de la Información

3.5.1 Análisis documental

El procesamiento de la información partió de un análisis documental, mismo que permitió tener un resumen detallado de los documentos revisados, lo que facilitó extraer información esencial para relacionar el uso del Pentesting con los requisitos y controles de seguridad de la Norma ISO 27001. A través de un análisis sistemático de estos documentos se identificarán los controles de seguridad donde el Pentesting juega un rol fundamental.

Artículos elegidos para la investigación

Tabla 6

Instrumento de Investigación

N°	Título	Autor(es)	Año de Edición	País	Base de Datos	Resumen
1	El Papel del informático como auditor en la "iso 27001:2017 tecnología de la información. técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. requisitos."	• Jorge Asensi Shaw	2019	España	Universitat Politècnica de València	El documento aborda el rol del informático como auditor en la implementación de la norma ISO/IEC 27001:2017, ofreciendo una guía para formar a nuevos profesionales en la auditoría de sistemas de gestión de la seguridad de la información. Incluye conceptos clave sobre auditoría, certificación y formación necesarios para cubrir la creciente demanda de expertos en ciberseguridad.
2	Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001.Orientado a los medios de comunicación	• Esteban Fernando Castillo Durán • Fernando Illescas Peña • Andrés Sebastián Quevedo Sacoto	2023	Ecuador	Conciencia Digital	La falta de un Plan de Gestión de la Seguridad de la Información en la mayoría de las empresas, sumado al desconocimiento de la importancia de una adecuada gestión de la seguridad de la información (TI), representa un problema para las organizaciones Castillo Durán et al. (2023).

3	ISO 27001 PARA PYMES Trabajo	• Ángela María Parra Giraldo	2014	Colombia	Universidad Internacional de La Rioja	Esta tesis propone una metodología práctica para implementar un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001, adaptado a las limitaciones de presupuesto, personal, personal y conocimiento de las pequeñas y medianas empresas (Parra, 2014).
4	Planificación de la implementación de un esquema de seguridad basada en la Norma ISO 27001:2013, para el proceso de administración del sistema de información geográfica en el Gobierno Autónomo Descentralizado del Cantón Samborondón	• Víctor Manuel Sánchez Mera	2019	Ecuador	Escuela Superior Politécnica del Litoral	La presente investigación tiene como objetivo implementar un esquema de seguridad basado en la norma ISO 27001 para el proceso de gestión del sistema de información geográfica en el Gobierno Autónomo Descentralizado de Samborondón. La investigación tiene como objetivo establecer políticas, procedimientos y proyectos para garantizar la integridad, confidencialidad y disponibilidad de la información proporcionada. La importancia de este trabajo radica en mejorar la seguridad de los sistemas de información gubernamentales, alineándolos con los estándares internacionales para la protección efectiva de datos confidenciales (Sánchez, 2019).

5	Adaptación de una empresa tecnológica a UNE-ISO/IEC 27001 (versión 2013)	• Javier Donoso Morán	2015	España	Universidad Carlos III de Madrid	El proyecto profundiza en la definición de objetivos, recomendaciones y requisitos, destacando la importancia de las políticas de seguridad en los sistemas de gestión de seguridad de la información (SGSI). Explora aspectos críticos del sistema de la CIA y su papel en el ISMS. Además, el proyecto incluye un marco estructurado que abarca capítulos sobre introducción, objetivos, declaración de aplicabilidad, planificación, presupuesto, conclusiones, referencias y un modelo PDCA para los procesos de toma de decisiones. Proporciona información sobre la planificación, la ejecución, la verificación y los procedimientos de toma de decisiones para una implementación efectiva en las organizaciones (Donoso, 2015).
6	Gestión de Seguridad Informática en una dependencia gubernamental	• Elvia Lorena Gómez Bravo • Gustavo Durán Cruz	2022	México	Universidad Nacional Autónoma de México	El proyecto propone la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en base a la Norma ISO/IEC 27001, con aplicación a una organización

						gubernamental. El estudio identifica y analiza los riesgos relacionados con la seguridad de la información y propone políticas, procedimientos y controles para garantizar la confidencialidad, integridad y disponibilidad de los activos de información (Gómez & Durán, 2022).
7	Evaluación de vulnerabilidades de seguridad en la Empresa Booknowledge. Soluciones para mitigar las vulnerabilidades encontradas bajo la Norma ISO 27001:2013. caso: Empresa Booknowledge.	• Andrea Verónica Murillo Chiriboga	2017	Ecuador	Universidad de las Américas	Esta tesis propone un Sistema de Gestión de Seguridad de la Información para proteger los activos de informáticos de la empresa. Se hizo un análisis de riesgos utilizando el método cualitativo, identificando amenazas humanas, tecnológicas y naturales. (Murillo, 2017)
8	Manual de políticas de Seguridad de la Información basado en la Norma ISO 27001 en el GAD Intercultural de el Tambo	• Carlos Francisco Chimborazo Quzhpi	2021	Ecuador	Universidad Católica de Cuenca	Esta investigación propone el diseño e implementación de un manual de políticas de seguridad de la información para el GAD Municipal Intercultural El Tambo. La finalidad es garantizar la confidencialidad, integridad y disponibilidad de la información institucional. La propuesta se basa en el estándar ISO/IEC 27001:2013, con la finalidad de establecer los controles adecuados

						y fortalecer la seguridad de la información en la institución (Chimborazo, 2021).
9	Propuesta para implementación de controles establecidos por la Norma ISO/IEC 27001:2013 - Anexo A, aplicables en el centro de diagnóstico automotor – CEDAC - LTDA., ubicado en la zona industrial de la ciudad de Cúcuta	• Martin Javier Diez Contreras	2018	Colombia	Universidad Abierta y a Distancia	Esta tesis propone una estrategia para mejorar la seguridad de la información de CEDAC Ltda., mediante la aplicación de controles específicos de la ISO 27001:2013. El trabajo identifica riesgos y vulnerabilidades en los procesos y plantea políticas y controles de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información, protegiendo los datos sensibles y asegurando la continuidad del negocio (Diez, 2018).
10	Diseño de un Sistema de Gestión de Seguridad de la Información basado en la Norma Técnica Peruana NTP ISO 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco	• Victor Hugo Cuba Gamarra • Marco Emerson Solis Cano	2024	Perú	Universidad Nacional de San Antonio Abad del Cusco	Esta tesis tiene como objetivo fortalecer la seguridad de la información en la Unidad de Trámite Documentario de la UNSAAC. Propone un modelo de gestión que mitiga riesgos, garantiza la confidencialidad, integridad y disponibilidad de la información y asegura el cumplimiento normativo conforme a la NTP ISO/IEC 27001:2014 (Cuba & Solis, 2024).

11	Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la Empresa Plasticaucho Industrial S.A	• Jorge Luis Tige Moposita	2020	Ecuador	Universidad Técnica de Ambato	Esta tesis propone un sistema de gestión de seguridad de gestión de seguridad de la información que garantice la confidencialidad, integridad y disponibilidad de los datos de la empresa Plasticaucho. La propuesta incluye el diseño e implementación de políticas y procedimientos de seguridad alineados a las Norma ISO 27001 (Tigse, 2020).
12	Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino	• Lisbet Odelly Monteza Mera	2019	Perú	Universidad Peruana de Ciencias Aplicadas	Esta investigación propone el diseño de un SGSI para proteger los activos de información relacionados con el proceso de recaudación tributaria de la municipalidad. Siguiendo el ciclo PDCA y la Norma ISO 27001 el proyecto identifica los riesgos, define controles y establece políticas para garantizar la confidencialidad, integridad y disponibilidad de la información (Monteza Mera, 2019)
13	Diseño de un esquema de auditoría de seguridad informática en los controles de acceso a los activos de información bajo los lineamientos de la Norma ISO	• Angela Mercedes Yance Saltos	2024	Ecuador	Escuela Superior Politécnica del Litoral	Este trabajo de titulación tiene la finalidad de diseñar un esquema de auditoría en seguridad informática para los controles de acceso a los activos de información, alineado a la Norma ISO 27001 en una

	27001 para una empresa de industria automotriz					empresa de la industria automotriz. Esta investigación busca garantizar la confidencialidad, integridad y disponibilidad de la información mediante la formulación de recomendaciones de seguridad y controles adecuados (Yance, 2024).
14	Adaptación de las Normas ISO 27001 e HIPPA para la reducción de riesgos en la seguridad en hospitales nivel I del IESS	• Christian Fernando Barragán Quizhpe	2017	Ecuador	Escuela Superior Politécnica de Chimborazo	Este proyecto de investigación busca mejorar la seguridad de la información en el Hospital Básico del IESS Guaranda. La propuesta incluye una adaptación de las Normas ISO 27001 e HIPPA para garantizar la confidencialidad, integridad y disponibilidad del historial clínico digital (Barragán, 2017).

Elaborado por: Jair Cachipuendo, 2024

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y Discusión de Resultados

4.1.1 Análisis

En base a los artículos revisados en el instrumento de investigación se realizó un análisis exhaustivo de los siguientes dominios de seguridad:

A.9 Control de Accesos

A.12 Seguridad de las Operaciones

A.13 Seguridad de las Comunicaciones

A14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

En el cumplimiento de estos dominios, el rol que juega el pentesting resulta ser crucial, a continuación, se muestra el análisis de la aplicabilidad del pentesting en los dominios antes mencionados y sus respectivos controles.

4.1.1.1 A.9 Control de Accesos

Tabla 7

Análisis de los Controles del Dominio A.9

A.9 Control de Accesos				
A.9.1 Requisitos de negocio para el control de accesos		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.9.1.1	Política de control de accesos		X	Es un control orientado a la documentación de políticas, por lo tanto, es inviable la evaluación de este control mediante pruebas de penetración.
A.9.1.2	Control de acceso a las redes y servicios asociados	X		Permite determinar si usuarios no autorizados pueden acceder a redes o servicios mediante técnicas como escaneos de redes o intentos de acceso no autorizado.
A.9.2 Gestión de acceso de usuarios		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**

A.9.2.1	Gestión de altas/bajas en el registro de usuarios		X	Es un control administrativo y de gestión de registro de usuarios.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios		X	Es un control administrativo y de auditoría, por lo tanto, no requiere la implementación de pentesting.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	X		Permite la identificación de configuraciones incorrectas y escalación de privilegios.
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	X		Mediante la ejecución de ataques de fuerza bruta, ingeniería social e intentos de acceso no autorizad, permite validar si los datos de autenticación están protegidos adecuadamente.
A.9.2.5	Revisión de los derechos de acceso de los usuarios		X	Es un control administrativo donde no involucra pruebas de penetración.
A.9.2.6	Retirada o adaptación de los derechos de acceso		X	Es un control administrativo donde no involucra pruebas de penetración.
A.9.3 Responsabilidades de los usuarios		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.9.3.1	Uso de información confidencial para la autenticación	X		Se pueden realizar ataques como pruebas de fuerza bruta o phishing para validar si los usuarios gestionan adecuadamente sus credenciales.
A.9.4 Control de acceso a sistemas y aplicaciones		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.9.4.1	Restricción del acceso a la información	X		Se puede implementar pruebas de penetración para identificar accesos no autorizados.

A.9.4.2	Procedimientos seguros de inicio de sesión	X		Mediante la implementación de ataques de fuerza bruta o bypass de autenticación es factible testear la fortaleza de estos procedimientos
A.9.4.3	Gestión de contraseñas de usuario		X	Es un control administrativo, por lo tanto, no requiere pentesting.
A.9.4.4	Uso de herramientas de administración de sistemas	X		Las pruebas pueden incluir intentos de acceso a herramientas administrativas para verificar controles como segmentación y autenticación.
A.9.4.5	Control de acceso al código fuente de los programas	X		Se pueden realizar intentos de acceso al código fuente, por ejemplo, probando vulnerabilidades en repositorios como Git.

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de investigación

4.1.1.2 A.12 Seguridad de las operaciones

Tabla 8

Análisis de los Controles del Dominio A.12

A.12 Seguridad de las operaciones				
A.12.1 Responsabilidades y procedimientos de operación		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.1.1	Documentación de procedimientos de operación		X	Es un control administrativo y documental donde no involucra pruebas de penetración.
A.12.1.2	Gestión de cambios		X	Este control va dirigido a procesos administrativos y gestión de cambios.
A.12.1.3	Gestión de capacidades		X	Este control está orientado a monitorización y planificación de recursos, por lo que no es viable la aplicación de pentesting.
A.12.1.4	Separación de entornos de desarrollo, prueba y producción		X	Al ser un control relacionado con la gestión operativa, no requiere una evaluación mediante pentesting.

A.12.2 Protección contra código malicioso		Aplicabilidad del Pentesting		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.2.1	Controles contra el código malicioso	X		Se pueden realizar ataques con malware controlado para evaluar la seguridad de un sistema.
A.12.3 Copias de seguridad		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.3.1	Copias de seguridad de la información		X	Al ser un control relacionado con la gestión operativa, no requiere una evaluación mediante pentesting.
A.12.4 Registro de actividad y supervisión		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.4.1	Registro y gestión de eventos de actividad	X		Se puede probar la capacidad del sistema para registrar un evento crítico, simulando accesos no autorizados o actividades sospechosas.
A.12.4.2	Protección de los registros de información	X		Puede evaluar la seguridad de los registros intentando modificar o eliminar los eventos registrados.
A.12.4.3	Registros de actividad del administrador y operador del sistema	X		Simula las acciones de los usuarios privilegiados para asegurarse de que las acciones se registran correctamente.
A.12.4.4	Sincronización de relojes		X	Este es un control técnico relacionado con la configuración del sistema, pero no está directamente relacionado con el pentesting.
A.12.5 Control del software en explotación		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.5.1	Instalación del software en sistemas en producción	X		Para probar la eficacia de los controles, se puede simular intentos de instalación de software no autorizado.
A.12.6 Gestión de la vulnerabilidad técnica		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.6.1	Gestión de las vulnerabilidades técnicas	X		Realizar pruebas de vulnerabilidad y simulaciones de explotación para identificar fallas en la gestión de vulnerabilidades.

A.12.6.2	Restricciones en la instalación de software	X		Se pueden realizar pruebas para intentar instalar software no autorizado y verificar las restricciones.
A.12.7 Consideraciones de las auditorías de los sistemas de información		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.12.7.1	Controles de auditoría de los sistemas de información		X	Este control es de contexto administrativo y no puede ser evaluado mediante pentesting.

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

4.1.1.3 A.13 Seguridad de las Comunicaciones

Tabla 9

Análisis de los Controles del Dominio A.13

A.13 Seguridad de las Comunicaciones				
A.13.1 Gestión de la seguridad en las redes		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.13.1.1	Controles de red	X		Se pueden realizar pruebas como escaneo de puertos, pruebas de intrusión y validación de la segmentación para evaluar la seguridad de la infraestructura de red.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	X		Pruebas como el análisis de configuración, las pruebas de túneles VPN y el modelado de ataques MITM (man-in-the-middle) nos permiten evaluar la seguridad de estos mecanismos.
A.13.1.3	Segregación de redes	X		Pruebas como la exploración de rutas y simulaciones de accesos entre redes pueden verificar si la segregación está correctamente implementada.
A.13.2 Intercambio de información con partes externas		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.13.2.1	Políticas y procedimientos de intercambio de información		X	Se trata de un control administrativo destinado a documentar las directrices y que no incluye componentes técnicos que puedan evaluarse mediante pentesting.

A.13.2.2	Acuerdos de intercambio		X	Este control es contractual y administrativo, no técnico.
A.13.2.3	Mensajería electrónica	X		Se puede realizar pruebas de seguridad, como intentos de intercepción (MITM) y phishing, para verificar las medidas de protección de los servicios de mensajería.
A.13.2.4	Acuerdos de confidencialidad y secreto		X	Es un control administrativo y legal, por lo tanto, no es susceptible a una evaluación técnica.

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

4.1.1.4 A14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Tabla 10

Análisis de los Controles del Dominio A.14

A.14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información				
A.14.1 Requisitos de seguridad de los sistemas de información		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.14.1.1	Análisis y especificación de los requisitos de seguridad		X	Es un control enfocado a la planificación y documentación de requisitos de seguridad, por lo tanto, el pentesting no es aplicable a este control.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	X		Se pueden realizar ataques Man-in-the-Middle para testear la resistencia de los métodos de cifrado y autenticación ante amenazas reales.
A.14.1.3	Protección de las transacciones por redes telemáticas	X		Mediante ataques de replay, interceptación de datos y manipulación de transacciones se puede validar la seguridad de este control.
A.14.2 Seguridad en los procesos de desarrollo y soporte		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.14.2.1	Política de desarrollo seguro de software		X	Es un control administrativo, por lo tanto, no es aplicable el pentesting.
A.14.2.2	Procedimientos de control de cambios en los sistemas		X	Es un control administrativo, por lo tanto, no es aplicable el pentesting.

A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	X		Se puede aplicar pentesting para identificar vulnerabilidades introducidas tras los cambios en el sistema operativo.
A.14.2.4	Restricciones a los cambios en los paquetes de software		X	Es un control administrativo y preventivo orientado a la gestión de cambios.
A.14.2.5	Uso de principios de ingeniería en protección de sistemas		X	Es un control conceptual, por lo tanto, no es aplicable el pentesting.
A.14.2.6	Seguridad en entornos de desarrollo	X		Pruebas para validar la protección de entornos de desarrollo frente a accesos no autorizados.
A.14.2.7	Externalización del desarrollo de software		X	Es un control administrativo, por lo tanto, no es aplicable el pentesting.
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	X		Las pruebas de penetración específicas en las etapas de desarrollo permiten identificar fallos de seguridad.
A.14.2.9	Pruebas de aceptación	X		Las pruebas de aceptación pueden incluir pentesting para garantizar la seguridad del sistema antes de la implementación.
A.14.3 Datos de prueba		**Aplicabilidad del Pentesting**		
N°	**Control**	**Si**	**No**	**Motivo**
A.14.3.1	Protección de los datos utilizados en pruebas	X		Pruebas de acceso a los datos en entornos de prueba pueden validar que estos estén debidamente protegidos.

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

4.1.2 Interpretación

El análisis de los dominios A.9, A.12, A.13 y A.14 de la Norma ISO 27001 permitió evaluar el rol del pentesting en los controles de los dominios antes mencionados. Los resultados e interpretación de los mismos se detallan a continuación:

4.1.2.1 Dominio A.9 Control de Accesos

Este dominio hace enfoque a la protección del acceso a los recursos de información, durante el análisis de este dominio y sus respectivos controles, se pudo evidenciar que el pentesting tiene un rol importante dentro de este dominio. Los controles

como el A.9.1 están orientados a la gestión administrativa, en consecuencia, el pentesting poca o nula incidencia dentro de estos controles administrativos.

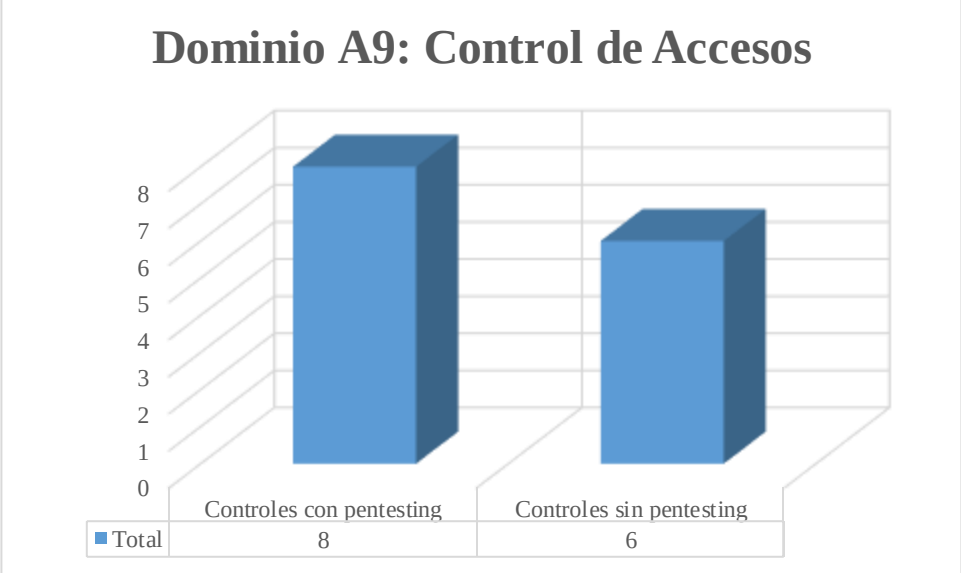

Ilustración 2: Controles con o sin Pentesting del Dominio A.9
Fuente: Elaboración propia

4.1.2.2 Dominio A.12 Seguridad Operacional

El pentesting juega un papel decisivo en este dominio. Controles como el A.12.6 están directamente relacionados con la identificación y mitigación de vulnerabilidades técnicas en los sistemas operativos. Además, pentesting permite evaluar la efectividad de las medidas de protección contra malware y las pruebas de vulnerabilidad y proporciona evidencia concreta del nivel de seguridad en la operación diaria.

Ilustración 3: Controles con o sin Pentesting del Dominio A.12
Fuente: Elaboración propia

4.1.2.3 Dominio A.13 Seguridad de las Comunicaciones

El análisis muestra que el pentesting también es relevante en este dominio. Un control como el A.13.2 ofrece una garantía de seguridad de la transmisión de datos. Las pruebas de penetración permiten evaluar la configuración y el rendimiento de los protocolos de cifrado, así como identificar vulnerabilidades que pueden afectar la confidencialidad e integridad de los datos en tránsito.

El análisis de los controles demuestra que el pentesting no desempeña un papel crucial dentro de este dominio, los controles que se derivan del objetivo A.13.1.

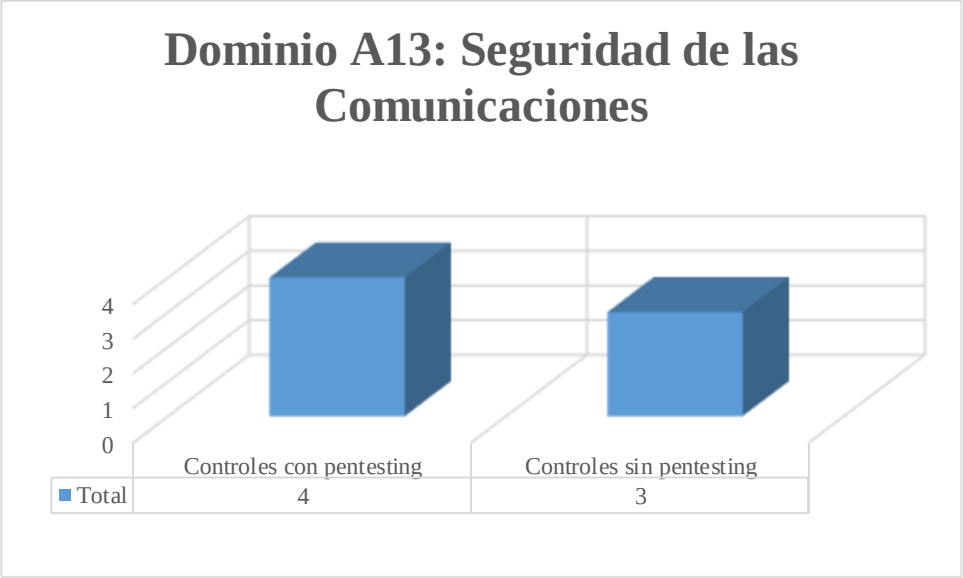

Ilustración 4: Controles con o sin Pentesting del Dominio A.13
Fuente: Elaboración propia

4.1.2.4 Dominio A14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

El pentesting es importante en este dominio, especialmente para controles como el A.14.2, diseñado para evaluar sistemas y aplicaciones antes de su implementación. Las pruebas de penetración permiten identificar fallas de diseño y desarrollo y garantizar que el sistema cumpla con los requisitos de seguridad desde la etapa inicial hasta el mantenimiento.

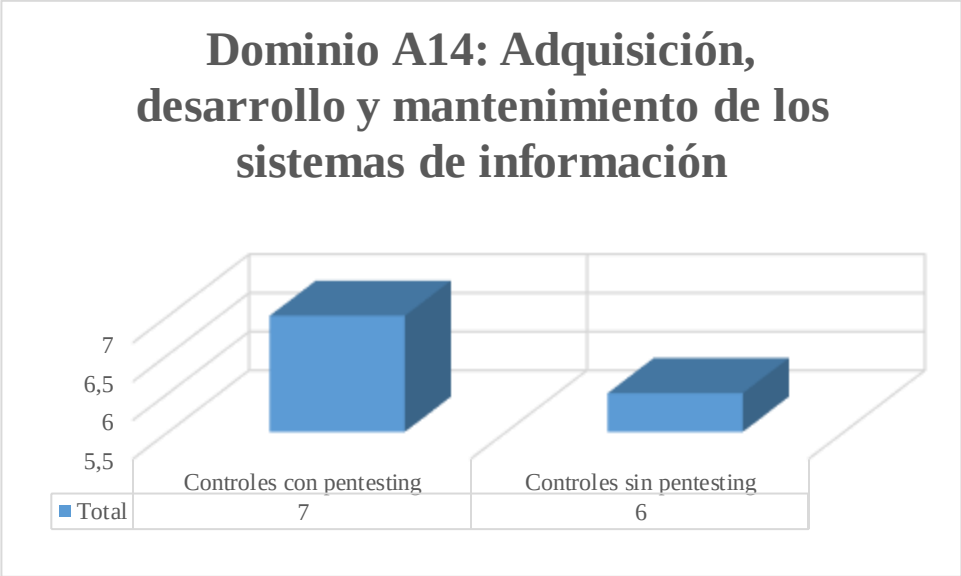

Ilustración 5: Controles con o sin Pentesting del Dominio A.14
Fuente: Elaboración propia

4.1.3 Discusión de Resultados

4.1.3.1 Relación con el cumplimiento de la ISO 27001

En base al análisis y la interpretación de resultados, se puede destacar la relevancia del pentesting dentro del Anexo A de la ISO 27001 en los dominios A.9, A12, A.13 Y A.14. La capacidad del pentesting para identificar vulnerabilidades reales contribuye un aporte significativo en el cumplimiento de la norma al proporcionar evidencia objetiva. Sin embargo, en el caso de los controles dirigidos a la parte administrativa, su efecto es limitado, lo que indica claramente que estos controles dependen de medidas complementarias, como las políticas organizativas.

4.1.3.2 Implicaciones para las organizaciones

Estos resultados son importantes para las organizaciones que buscan obtener la certificación ISO 27001. La integración del pentesting en su estrategia de seguridad no solo mejora la evaluación de los controles técnicos, sino que también proporciona un enfoque proactivo para amenazas potenciales. Sin embargo, un enfoque excesivo en las pruebas técnicas sin tener en cuenta las medidas administrativas puede dejar áreas vulnerables, especialmente en áreas como el dominio A. 9.

4.1.3.3 Limitaciones del pentesting

Es indiscutible la efectividad del pentesting en la evaluación de vulnerabilidades técnicas, sin embargo, presenta limitaciones en la identificación de riesgos que van en relación con políticas organizativas y configuraciones administrativas. Esto resalta la necesidad de un enfoque integral que combine el pentesting con revisiones y políticas administrativas.

4.1.3.4 Complementariedad del Pentesting con Métodos Tradicionales de Auditoría

El estudio muestra que el pentesting complementa significativamente los métodos tradicionales de auditoría de acuerdo con la norma ISO 27001. Las auditorías internas y las revisiones administrativas generalmente se centran en verificar el cumplimiento de políticas y la implementación correcta de los controles administrativos. Sin embargo, carecen de la capacidad para identificar vulnerabilidades técnicas específicas en sistemas y aplicaciones.

Por otro lado, el pentesting proporciona una perspectiva técnica que evalúa la robustez de los controles en escenarios de ataque del mundo real. Esta capacidad permite verificar no solo la implementación, sino también la efectividad práctica de los controles, especialmente en áreas como A. 12, A. 13 y A. 14. Por ejemplo, si bien una auditoría tradicional puede verificar la presencia de políticas de seguridad para la transmisión de datos, la pentesting identifica vulnerabilidades técnicas en los protocolos de cifrado utilizados.

CAPITULO V

PROPUESTA

5.1. Guía de aplicación sugerida del pentesting en aplicación a los controles de la Norma ISO/IEC 27001:2013

5.1.1 Introducción

Esta guía proporciona una metodología detallada para la realización de pruebas de penetración (pentesting) enfocadas en los controles de los Dominios A.9 (Control de Accesos), A.12 (Seguridad en la Operativa), A.13 (Seguridad de las Comunicaciones) y A.14 (Seguridad en la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información) de la norma ISO/IEC 27001:2013. Su propósito es facilitar la evaluación técnica de los controles de acceso implementados por una organización, apoyando tanto los procesos de auditoría como el fortalecimiento de la seguridad de la información.

El enfoque está basado en una estructura de trabajo profesional que sigue las fases clásicas del pentesting y establece su aplicabilidad en cada control analizado. Se consideran las siguientes fases estándar de una prueba de penetración:

- Reconocimiento
- Escaneo y Enumeración
- Explotación
- Mantenimiento del Acceso
- Borrado de Huellas
- Elaboración del Informe

5.1.2 Objetivo de la Guía

- Facilitar el proceso de evaluación técnica de los controles aplicables al pentesting de los dominios ya definidos en la norma ISO/IEC 27001:2013,
- Establecer procedimientos claros y herramientas específicas para la ejecución de pruebas de penetración.
- Proporcionar recomendaciones concretas para mitigar vulnerabilidades detectadas durante el proceso de pruebas.

5.1.3 Alcance

Esta guía cubre exclusivamente los controles de los Dominios A.9 (Control de Accesos), A.12 (Seguridad de las Operaciones), A.13 (Seguridad de las Comunicaciones) y A.14 (Seguridad en la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información) que permiten su validación mediante pruebas de penetración. No se incluyen controles que solo puedan ser evaluados a través de gestiones administrativas y revisión documental.

5.1.4 Guía de aplicación sugerida de Pentesting – Dominio A.9 (Control de Accesos) ISO/IEC 27001:2013

Tabla 11

Controles Aplicables al Pentesting Dominio A.9

Controles	Pentesting Aplicable
A.9.1.2 Control de acceso a las redes y servicios asociados	Si
A.9.2.3 Gestión de los derechos de acceso con privilegios especiales	Si
A.9.2.4 Gestión de información confidencial de autenticación de usuarios	Si
A.9.3.1 Uso de información confidencial para la autenticación	Si
A.9.4.1 Restricción del acceso a la información	Si
A.9.4.2 Procedimientos seguros de inicio de sesión	Si
A.9.4.4 Uso de herramientas de administración de sistemas	Si
A.9.4.5 Control de acceso al código fuente de los programas	Si

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

5.1.4.1 Control A.9.1.2 – Control de acceso a las redes y servicios asociados

Tabla 12

Guía de Aplicación Sugerida Control A.9.1.2

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Es clave para identificar la superficie de ataque y servicios expuestos en redes.
Escaneo	Aplicable	Es fundamental para obtener información sobre los servicios que se exponen y su configuración.
Explotación	Aplicable	Se busca validar que los controles de acceso resistan intentos no autorizados.
Mantenimiento del acceso	Opcional	Es aplicable si el escenario incluye validación de persistencia tras la explotación.
Borrado de huellas	Opcional	Se puede realizar si el pentesting requiere demostrar evasión de controles de monitoreo.
Elaboración del informe	Opcional	Esta fase está dirigida a la documentación y reporte de vulnerabilidades encontradas. Sin embargo, se pueden realizar más pruebas técnicas de ser necesario.

Elaborado por: Jair Cachipuendo, 2024

Tabla 13

Herramientas a Utilizar Control A.9.1.2

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Shodan, Censys, Recon-ng, WHOIS, NSLookup
Escaneo	Nmap, Netcat
Explotación	Metasploit, Hydra
Mantenimiento del acceso	Meterpreter, SSH tunnels

Borrado de huellas	Auditpol (Windows), LogCleaner (Linux)
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.2 Control A.9.2.3 Gestión de los derechos de acceso con privilegios especiales

Tabla 14

Guía de Aplicación Sugerida Control A.9.2.3

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Permite identificar dónde existen cuentas privilegiadas
Escaneo	Aplicable	Requiere mapear usuarios y sus roles dentro de los sistemas.
Explotación	Aplicable	Se intenta escalar privilegios hacia cuentas administrativas.
Mantenimiento del acceso	Aplicable	Una vez con privilegios elevados, es lógico mantener el acceso para futuras acciones.
Borrado de huellas	Opcional	Se puede aplicar si el control requiere evaluar la detección de actividades indebidas.
Elaboración del informe	Aplicable	Se debe evidenciar la escalada y los riesgos derivados.

Elaborado por: Jair Cachipuendo, 2024

Tabla 15

Herramientas a Utilizar Control A.9.2.3

Fase	Herramientas de pentesting a utilizar
Reconocimiento	BloodHound y LDAPDomaindump
Escaneo	PowerView y NetView
Explotación	Mimikatz y Metasploit
Mantenimiento del acceso	Empire y Meterpreter

Borrado de huellas	Auditpol y Clear-EventLog (PowerShell)
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.3 Control A.9.2.4 Gestión de información confidencial de autenticación de usuarios

Tabla 16

Guía de Aplicación Sugerida Control A.9.2.4

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Busca información sobre credenciales expuestas (repositorios, leaks).
Escaneo	Aplicable	Verificación de almacenamiento y transmisión de credenciales.
Explotación	Aplicable	Intento de obtener credenciales y validarlas en servicios reales.
Mantenimiento del acceso	No Aplica	El objetivo es evaluar la gestión de credenciales, no la persistencia en el sistema.
Borrado de huellas	No aplica	En este control se busca el manejo seguro de autenticación, no cubrir rastros.
Elaboración del informe	Aplicable	Documentación del manejo inseguro de autenticación.

Elaborado por: Jair Cachipuendo, 2024

Tabla 17

Herramientas a Utilizar Control A.9.2.4

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Google Dorking y GitLeaks
Escaneo	Wireshark y Burp Suite
Explotación	Hydra, Hashcat y John the Ripper
Mantenimiento del acceso	No Aplica

Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.4 Control A.9.3.1 Uso de información confidencial para la autenticación

Tabla 18

Guía de Aplicación Sugerida Control A.9.3.1

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Revisión de métodos de autenticación y credenciales en tránsito.
Escaneo	Aplicable	Análisis de tráfico y protocolos usados para autenticación.
Explotación	Aplicable	Simulación de ataques como phishing y MITM para obtener credenciales.
Mantenimiento del acceso	No Aplica	El objetivo es probar autenticación, no mantener acceso.
Borrado de huellas	No Aplica	No hay persistencia ni necesidad de ocultar acceso en este control.
Elaboración del informe	Aplicable	Documentación de vulnerabilidades en el proceso de autenticación.

Elaborado por: Jair Cachipuendo, 2024

Tabla 19

Herramientas a Utilizar Control A.9.3.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Wireshark, SSLScan y Burp Suite
Escaneo	ZAP y SSLyze
Explotación	SET y Bettercap
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.5 Control A.9.4.1 Restricción del acceso a la información

Tabla 20

Guía de Aplicación Sugerida Control A.9.4.1

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Para identificar posibles objetivos y recursos protegidos.
Escaneo	Aplicable	Para enumerar permisos y derechos de acceso en archivos y bases de datos.
Explotación	Aplicable	Para intentar acceder a la información sin autorización, rompiendo las restricciones.
Mantenimiento del acceso	Opcional	Solo si el objetivo incluye demostrar persistencia tras obtener el acceso a datos sensibles.
Borrado de huellas	No Aplica	El objetivo es validar control de acceso, no ocultar la explotación de datos.
Elaboración del informe	Aplicable	Documentación de accesos indebidos y debilidades en las restricciones de acceso.

Elaborado por: Jair Cachipuendo, 2024

Tabla 21

Herramientas a Utilizar Control A.9.4.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap
Escaneo	PowerView y BloodHound
Explotación	SQLMap, Nmap y Dirbuster
Mantenimiento del acceso	SSH Tunnels (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.6 Control A.9.4.2 Procedimientos seguros de inicio de sesión

Tabla 22

Guía de Aplicación Sugerida Control A.9.4.2

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Para identificar portales de autenticación accesibles.
Escaneo	Aplicable	Analizar el mecanismo de inicio de sesión y sus características.
Explotación	Aplicable	Intentar ataques de fuerza bruta y bypass de autenticación.
Mantenimiento del acceso	No Aplica	El control se limita al proceso de autenticación, no a la persistencia.
Borrado de huellas	No Aplica	No es el objetivo del control.
Elaboración del informe	Aplicable	Documentar mecanismos débiles en el inicio de sesión.

Elaborado por: Jair Cachipuendo, 2024

Tabla 23

Herramientas a Utilizar Control A.9.4.2

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap y Google Dorking (búsqueda de portales de login)
Escaneo	Burp Suite, OWASP ZAP y SSLScan
Explotación	Hydra y Medusa
Mantenimiento del acceso	No Aplica
Borrado de huellas	No aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.7 Control A.9.4.4 Uso de herramientas de administración de sistemas

Tabla 24

Guía de Aplicación Sugerida Control A.9.4.4

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Para identificar herramientas expuestas o accesibles.
Escaneo	Aplicable	Para descubrir interfaces administrativas disponibles.
Explotación	Aplicable	Intentar acceso no autorizado a estas herramientas.
Mantenimiento del acceso	Opcional	Solo si se requiere demostrar persistencia tras comprometer herramientas de administración.
Borrado de huellas	Opcional	Se aplica si el control requiere validar la respuesta ante el ocultamiento de accesos.
Elaboración del informe	Aplicable	Documentar accesos no autorizados y recomendaciones.

Elaborado por: Jair Cachipuendo, 2024

Tabla 25

Herramientas a Utilizar Control A.9.4.4

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap
Escaneo	Gobuster y Dirb
Explotación	Hydra, Metasploit
Mantenimiento del acceso	Empire y Meterpreter
Borrado de huellas	Auditpol
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.4.8 Control A.9.4.5 Control de acceso al código fuente de los programas

Tabla 26

Guía de Aplicación Sugerida Control A.9.4.5

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificar repositorios expuestos o accesibles públicamente.
Escaneo	Aplicable	Análisis de políticas de acceso en los repositorios.
Explotación	Aplicable	Intentar obtener código fuente mediante accesos indebidos.
Mantenimiento del acceso	No Aplica	El control se centra en la protección del acceso, no en la persistencia.
Borrado de huellas	No Aplica	No se trata de acceso a sistemas críticos con necesidad de ocultar rastros.
Elaboración del informe	Aplicable	Documentar accesos indebidos y recomendaciones.

Elaborado por: Jair Cachipuendo, 2024

Tabla 27

Herramientas a Utilizar Control A.9.4.5

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Google Dorking y GitLeaks
Escaneo	GitMiner
Explotación	Wget y Burp Suite
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.5 Guía de aplicación sugerida de Pentesting – Dominio A.12 (Seguridad en la Operativa) ISO/IEC 27001:2013

Tabla 28

Controles Aplicables al Pentesting Dominio A.12

Controles	Pentesting Aplicable
A.12.2.1 Controles contra el código malicioso	Si
A.12.4.1 Registro y gestión de eventos de actividad	Si
A.12.4.2 Protección de los registros de información	Si
A.12.4.3 Registros de actividad del administrador y operador del sistema	Si
A.12.5.1 Instalación del software en sistemas en producción	Si
A.12.6.1 Gestión de las vulnerabilidades técnicas	Si
A.12.6.2 Restricciones en la instalación de software	Si

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

5.1.5.1 Control A.12.2.1 Controles contra el código malicioso

Tabla 29

Guía de Aplicación Sugerida Control A.12.2.1

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplica	Revisión de las medidas de defensa frente a malware.
Escaneo	Aplica	Identificación de los mecanismos de protección activos.
Explotación	Aplica	Evaluar la efectividad mediante intento de ejecución de malware de prueba.
Mantenimiento del acceso	Opcional	Puede usarse malware persistente para validar protección en tiempo real.
Borrado de huellas	No Aplica	No es el foco del control, salvo si se desea ocultar la ejecución del malware.

Elaboración del informe	Aplicable	Documentar las detecciones y respuesta del sistema de protección.

Elaborado por: Jair Cachipuendo, 2024

Tabla 30

Herramientas a Utilizar Control A.12.2.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Sysinternals Suite
Escaneo	Powershell y AppLocker Tools
Explotación	Metasploit y Veil-Evasion
Mantenimiento del acceso	Metasploit (Opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis y Faraday Security

Elaborado por: Jair Cachipuendo, 2024

5.1.5.2 Control A.12.4.1 Registro y gestión de eventos de actividad

Tabla 31

Guía de Aplicación Sugerida Control A.12.4.1

Fase	Aplicabilidad	Justificación
Reconocimiento	Opcional	Identificar si los logs están habilitados es relevante, pero no siempre prioritario.
Escaneo	Aplicable	Revisar logs expuestos o accesibles sin autenticación.
Explotación	Aplicable	Intentar generar eventos maliciosos y validar su registro.
Mantenimiento del acceso	No Aplica	El foco es validar el registro, no persistencia.
Borrado de huellas	Opcional	Se puede intentar la eliminación de registros para validar controles de protección.
Elaboración del informe	Aplicable	Documentar si los registros existen y son efectivos.

Elaborado por: Jair Cachipuendo, 2024

Tabla 32

Herramientas a Utilizar Control A.12.4.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	OSINT y Nmap
Escaneo	Log Parser
Explotación	Nmap y Hydra
Mantenimiento del acceso	No Aplica
Borrado de huellas	Auditpol
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.5.3 Control A.12.4.2 Protección de los registros de información

Tabla 33

Guía de Aplicación Sugerida Control A.12.4.2

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Verificar la ubicación y protección de los logs.
Escaneo	Aplicable	Revisar las políticas de permisos sobre los registros.
Explotación	Aplicable	Intentar modificar o eliminar los registros.
Mantenimiento del acceso	No Aplica	No es un control que requiera persistencia.
Borrado de huellas	Aplicable	Se intenta eliminar o manipular registros para probar protección.
Elaboración del informe	Aplicable	Documentar la integridad de los registros y protección efectiva.

Elaborado por: Jair Cachipuendo, 2024

Tabla 34

Herramientas a Utilizar Control A.12.4.2

Fase	Herramientas de pentesting a utilizar

Reconocimiento	Sysinternals
Escaneo	auditctl
Explotación	Metasploit
Mantenimiento del acceso	No Aplica
Borrado de huellas	Auditpol
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.5.4 Control A.12.4.3 Registros de actividad del administrador y operador del sistema

Tabla 35

Guía de Aplicación Sugerida Control A.12.4.3

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Revisar cómo se controlan y monitorean las acciones de los administradores.
Escaneo	Aplicable	Verificar la existencia y protección de los registros de actividad.
Explotación	Aplicable	Probar si es posible realizar acciones privilegiadas sin ser registrado.
Mantenimiento del acceso	Opcional	Puede usarse si se desea mantener acceso oculto como administrador.
Borrado de huellas	Aplicable	Intentar eliminar registros para validar su protección.
Elaboración del informe	Aplicable	Documentar la falta de registro o controles inadecuados.

Elaborado por: Jair Cachipuendo, 2024

Tabla 36

Herramientas a Utilizar Control A.12.4.3

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Auditpol, Event Viewer (Windows) y auditd (Linux)
Escaneo	Log Parser
Explotación	PowerShell (Windows), Linux sudo (Linux)

Mantenimiento del acceso	Meterpreter (opcional)
Borrado de huellas	Auditpol
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.5.5 Control A.12.5.1 Instalación del software en sistemas en producción

Tabla 37

Guía de Aplicación Sugerida Control A.12.5.1

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificar sistemas y usuarios con permisos de instalación.
Escaneo	Aplicable	Enumerar permisos y aplicaciones instaladas.
Explotación	Aplicable	Intentar instalar software sin la debida autorización.
Mantenimiento del acceso	Opcional	Si se busca persistencia a través de software malicioso.
Borrado de huellas	No Aplicable	No se busca ocultar la instalación en este control.
Elaboración del informe	Aplicable	Documentar instalaciones no autorizadas o riesgos derivados.

Elaborado por: Jair Cachipuendo, 2024

Tabla 38

Herramientas a Utilizar Control A.12.5.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Windows AppLocker, Linux SELinux
Escaneo	PowerShell
Explotación	Meterpreter
Mantenimiento del acceso	Meterpreter (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.5.6 Control A.12.6.1 Gestión de las vulnerabilidades técnicas

Tabla 39

Guía de Aplicación Sugerida Control A.12.6.1

Fase	Aplicabilidad	Descripción
Reconocimiento	Aplicable	Identificación de software y versiones expuestas a vulnerabilidades.
Escaneo	Aplicable	Escaneo activo de vulnerabilidades conocidas.
Explotación	Aplicable	Explotar vulnerabilidades no corregidas para demostrar riesgo real.
Mantenimiento del acceso	Opcional	Si se compromete el sistema, mantener el acceso para pruebas posteriores.
Borrado de huellas	No Aplica	No es el foco principal de este control.
Elaboración del informe	Aplica	Documentar hallazgos, priorización y recomendaciones.

Elaborado por: Jair Cachipuendo, 2024

Tabla 40

Herramientas a Utilizar Control A.12.6.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap y Shodan
Escaneo	OpenVAS y Nessus
Explotación	Metasploit y ExploitDB
Mantenimiento del acceso	Meterpreter (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis y Faraday Security

Elaborado por: Jair Cachipuendo, 2024

5.1.5.7 Control A.12.6.2 Restricciones en la instalación de software

Tabla 41

Guía de Aplicación Sugerida Control A.12.6.2

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificación de políticas de control de software.

Escaneo	Aplicable	Verificación del software instalado y permitido.
Explotación	Aplicable	Intento de instalación de software no autorizado.
Mantenimiento del acceso	Opcional	En caso que se busque implantar un software para acceso persistente.
Borrado de huellas	No Aplica	No es el enfoque del control.
Elaboración del informe	Aplicable	Documentar resultados y recomendaciones.

Elaborado por: Jair Cachipuendo, 2024

Tabla 42

Herramientas a utilizar Control A.12.6.2

Fase	Herramientas de pentesting a utilizar
Reconocimiento	AppLocker
Escaneo	PowerShell
Explotación	Metasploit payloads
Mantenimiento del acceso	SSH tunnels (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.6 Guía de aplicación sugerida de Pentesting – Dominio A.13 (Seguridad de las Comunicaciones) ISO/IEC 27001:2013

Tabla 43

Controles Aplicables al Pentesting Dominio A.13

Controles	Pentesting Aplicable
A.13.1.1 Controles de red	Si
A.13.1.2 Mecanismos de seguridad asociados a servicios en red	Si
A.13.1.3 Segregación de redes	Si
A.13.2.3 Mensajería electrónica	Si

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

5.1.6.1 Control A.13.1.1- Controles de red

Tabla 44
Guía de Aplicación Sugerida Control A.13.1.1

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Descubrir la superficie expuesta y los accesos externos e internos.
Escaneo	Aplicable	Identificar los servicios activos y las reglas de red aplicadas.
Explotación	Aplicable	Intentar eludir los controles de red, acceso a segmentos no autorizados.
Mantenimiento del acceso	Opcional	En caso que se logre acceso a la red interna, la persistencia puede aplicarse.
Borrado de huellas	No Aplica	Este control no busca evidenciar la eliminación de rastros.
Elaboración del informe	Aplicable	Documentar los accesos indebidos a la red y bypass de controles.

Elaborado por: Jair Cachipuendo, 2024

Tabla 45
Herramientas a utilizar Control A.13.1.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap
Escaneo	Nmap y ARP-Scan
Explotación	Ettercap
Mantenimiento del acceso	VPN tunnels (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis y Faraday Security

Elaborado por: Jair Cachipuendo, 2024

5.1.6.2 Control A.13.1.2 Mecanismos de seguridad asociados a servicios en red

Tabla 46
Guía de Aplicación Sugerida Control A.13.1.2

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificación de los servicios expuestos.

Escaneo	Aplicable	Determinación de las configuraciones inseguras en protocolos y servicios.
Explotación	Aplicable	Explotar los servicios vulnerables, MITM en conexiones no seguras.
Mantenimiento del acceso	Opcional	Si se explotan servicios para obtener acceso, se puede mantener persistencia.
Borrado de huellas	No Aplica	El control se enfoca en la seguridad de los servicios, no en el ocultamiento de accesos.
Elaboración del informe	Aplicable	Documentar configuraciones inseguras o vulnerabilidades explotadas.

Elaborado por: Jair Cachipuendo, 2024

Tabla 47

Herramientas a Utilizar Control A.13.1.2

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap y SSLScan
Escaneo	Dig y DNSenum
Explotación	Metasploit y Bettercap
Mantenimiento del acceso	VPN y Reverse SSH (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.6.3 Control A.13.1.3- Segregación de redes

Tabla 48

Guía de Aplicación Sugerida Control A.13.1.3

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificación de diferentes segmentos de red.
Escaneo	Aplicable	Determinar si la segregación es efectiva.
Explotación	Aplicable	Intentar acceder a redes restringidas o realizar VLAN hopping.

Mantenimiento del acceso	Opcional	En caso que se logre acceder a una red restringida, mantener el acceso puede ser relevante.
Borrado de huellas	No aplica	El control no incluye el ocultamiento de acciones.
Elaboración del informe	Aplicable	Documentar la falta de segregación o bypass de segmentación.

Elaborado por: Jair Cachipuendo, 2024

Tabla 49

Herramientas a Utilizar Control A.13.1.3

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap y ARP-Scan
Escaneo	Ping Sweep
Explotación	Metasploit y ProxyChains
Mantenimiento del acceso	Reverse tunnels y SSH pivoting
Borrado de huellas	No Aplica
Elaboración del informe	Dradis y Faraday Security

Elaborado por: Jair Cachipuendo, 2024

5.1.6.4 Control A.13.2.3- Mensajería electrónica

Tabla 50

Guía de Aplicación Sugerida Control A.13.2.3

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificar los servidores de correo y políticas aplicadas.
Escaneo	Aplicable	Verificar los protocolos usados y autenticación.
Explotación	Aplicable	Pruebas de spoofing, phishing y explotación de servicios.
Mantenimiento del acceso	No Aplica	No es el enfoque de este control mantener acceso persistente.
Borrado de huellas	No Aplica	No corresponde ocultar acciones en pruebas de mensajería.

Elaboración del informe	Aplica	Documentar los riesgos y pruebas exitosas.

Elaborado por: Jair Cachipuendo, 2024

Tabla 51

Herramientas a Utilizar Control A.13.2.3

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Dig y MXToolbox
Escaneo	DNSenum
Explotación	SET y GoPhish
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7 Guía de aplicación sugerida de Pentesting – Dominio A.14 (Seguridad en la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información) ISO/IEC 27001:2013

Tabla 52

Controles Aplicables al Pentesting Dominio A.14

Controles	Pentesting Aplicable
A.14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes Públicas	Si
A.14.1.3 Protección de las transacciones por redes telemáticas	Si
A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Si
A.14.2.6 Seguridad en entornos de desarrollo	Si
A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	Si
A.14.2.9 Pruebas de aceptación	Si
A.14.3.1 Protección de los datos utilizados en pruebas	Si

Elaborado por: Jair Cachipuendo, 2024

Fuente: Instrumento de Investigación

5.1.7.1 Control A.14.1.2 - Seguridad de las comunicaciones en servicios accesibles por redes públicas

Tabla 53
Guía de Aplicación Sugerida Control A.14.1.2

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificar los activos expuestos en redes públicas.
Escaneo	Aplicable	Analizar las configuraciones y servicios expuestos.
Explotación	Aplicable	Evaluar la seguridad de los servicios públicos.
Mantenimiento del acceso	Opcional	En caso que se explote un servicio público, mantener el acceso puede aplicarse.
Borrado de huellas	No Aplica	No es el foco principal del control.
Elaboración del informe	Aplicable	Documentar las vulnerabilidades en servicios públicos.

Elaborado por: Jair Cachipuendo, 2024

Tabla 54
Herramientas a Utilizar Control 14.1.2

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Amass y Shodan
Escaneo	Nmap, Masscan
Explotación	Burp Suite, OWASP ZAP y SQLMap
Mantenimiento del acceso	Reverse Shells y SSH tunnels (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7.2 Control A.14.1.3 - Protección de las transacciones por redes telemáticas

Tabla 55
Guía de Aplicación Sugerida Control A.14.1.3

Fase	Aplicabilidad	Justificación

Reconocimiento	Aplicable	Identificar los servicios transaccionales y su cifrado.
Escaneo	Aplicable	Evaluar la seguridad de los protocolos y certificados.
Explotación	Aplicable	Pruebas de ataques MITM, downgrade y manipulación de transacciones.
Mantenimiento del acceso	No Aplica	No se busca persistencia, sino seguridad en la transacción.
Borrado de huellas	No Aplica	No es el objetivo de la prueba.
Elaboración del informe	Aplicable	Documentar los riesgos en la protección de las transacciones.

Elaborado por: Jair Cachipuendo, 2024

Tabla 56

Herramientas a Utilizar Control A.14.1.3

Fase	Herramientas de pentesting a utilizar
Reconocimiento	SSL Labs
Escaneo	SSLScan y Nmap
Explotación	Bettercap, Burp Suite y OWASP ZAP
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7.3 Control A.14.2.3 - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Tabla 57

Guía de Aplicación Sugerida Control A.14.2.3

Fase	Aplicabilidad	Justificación
Reconocimiento	Opcional	Revisar los cambios recientes en SO aplicados en entornos de prueba.
Escaneo	Aplicable	Identificar las configuraciones inseguras tras cambios.

Explotación	Aplicable	Explotar las vulnerabilidades o cambios introducidos por el nuevo SO.
Mantenimiento del acceso	No Aplica	No se busca persistencia en este control.
Borrado de huellas	No Aplica	No es relevante en la revisión de compatibilidad y seguridad.
Elaboración del informe	Aplicable	Documentar problemas técnicos introducidos tras la actualización.

Elaborado por: Jair Cachipuendo, 2024

Tabla 58

Herramientas a Utilizar Control A.14.2.3

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Sysinternals y Wazuh (opcional)
Escaneo	Nmap, Nessus y OpenVAS
Explotación	Metasploit y Burp Suite
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7.4 Control A.14.2.6 - Seguridad en entornos de desarrollo

Tabla 59

Guía de Aplicación Sugerida Control A.14.2.6

Fase	Aplicabilidad	Justificación
Reconocimiento	Aplicable	Identificar el nivel de segregación entre entornos.
Escaneo	Aplicable	Enumerar accesos, configuraciones y políticas en entornos de DEV y QA.
Explotación	Aplicable	Validar si se puede escalar de un entorno de prueba a producción o acceder a datos sensibles.
Mantenimiento del acceso	Opcional	Si se logra explotar una vulnerabilidad, se puede buscar mantener el acceso a

		través de puertas traseras o cuentas ocultas (esto se simula respetando la ética).
Borrado de huellas	No Aplica	El control es sobre segregación y acceso, no ocultamiento.
Elaboración del informe	Aplicable	Se documentan los hallazgos detallados, se presentan las vulnerabilidades explotadas, el riesgo asociado y recomendaciones específicas para mitigarlas.

Elaborado por: Jair Cachipuendo, 2024

Tabla 60

Herramientas a Utilizar Control A.14.2.6

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap, Shodan (si son accesibles públicamente)
Escaneo	BloodHound
Explotación	Metasploit y SSH pivoting
Mantenimiento del acceso	Reverse shells, Empire (opcional)
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7.5 Control A.14.2.8 - Pruebas de funcionalidad durante el desarrollo de los sistemas

Tabla 61

Guía de Aplicación Sugerida Control A.14.2.8

Fase	Aplicabilidad	Justificación
Reconocimiento	Opcional	Revisión de políticas y procedimientos de pruebas.
Escaneo	Aplicable	Análisis del código y los procesos de desarrollo.

Explotación	Aplicable	Pruebas de las vulnerabilidades en aplicaciones en desarrollo (pentesting de aplicaciones).
Mantenimiento del acceso	No Aplica	Enfoque en seguridad de código y aplicaciones, no persistencia.
Borrado de huellas	No Aplica	No aplica en pruebas de desarrollo.
Elaboración del informe	Aplicable	Documentar vulnerabilidades funcionales en el código.

Elaborado por: Jair Cachipuendo, 2024

Tabla 62

Herramientas a Utilizar Control A.14.2.8

Fase	Herramientas de pentesting a utilizar
Reconocimiento	OSINT y Revisión documental (opcional)
Escaneo	SonarQube, Semgrep, OWASP ZAP
Explotación	Burp Suite, Postman (para APIs) y OWASP ZAP
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7.6 Control A.14.2.9 - Pruebas de aceptación

Tabla 63

Guía de Aplicación Sugerida Control A.14.2.9

Fase	Aplicabilidad	Justificación
Reconocimiento	Opcional	Validar si el sistema tiene procedimientos de aceptación.
Escaneo	Aplicable	Identificar las vulnerabilidades pendientes en el sistema antes de la aceptación.
Explotación	Aplicable	Pruebas de pentesting de caja negra o gris sobre el sistema a aceptar.
Mantenimiento del acceso	No Aplica	No es el objetivo de las pruebas de aceptación.

Borrado de huellas	No Aplica	No corresponde en la fase de aceptación.
Elaboración del informe	Aplicable	Documentar resultados de las pruebas de aceptación de seguridad.

Elaborado por: Jair Cachipuendo, 2024

Tabla 64

Herramientas a utilizar Control A.14.2.9

Fase	Herramientas de pentesting a utilizar
Reconocimiento	OSINT y Revisión documental (opcional)
Escaneo	OWASP ZAP, Nessus y Nmap
Explotación	Burp Suite, Metasploit y Postman (APIs)
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

5.1.7.7 Control A.14.3.1 - Protección de los datos utilizados en pruebas

Tabla 65

Guía de Aplicación Sugerida Control A.14.3.1

Fase	Aplicabilidad	Descripción
Reconocimiento	Aplicable	Identificar si los entornos de prueba contienen datos sensibles.
Escaneo	Aplicable	Verificar el contenido de las bases de datos y archivos en entornos de prueba.
Explotación	Aplicable	Acceso y extracción de datos sensibles desde entornos de prueba.
Mantenimiento del acceso	No Aplica	El enfoque es en la protección de datos, no en la persistencia.
Borrado de huellas	No Aplica	No es parte de la evaluación de este control.
Elaboración del informe	Aplicable	Documentar los datos expuestos o las prácticas inadecuadas.

Elaborado por: Jair Cachipuendo, 2024

Tabla 66

Herramientas a Utilizar Control A.14.3.1

Fase	Herramientas de pentesting a utilizar
Reconocimiento	Nmap y Shodan
Escaneo	DBeaver y SQLMap
Explotación	SQLMap
Mantenimiento del acceso	No Aplica
Borrado de huellas	No Aplica
Elaboración del informe	Dradis

Elaborado por: Jair Cachipuendo, 2024

CONCLUSIONES

La presente investigación determinó que el pentesting complementa y fortalece el cumplimiento de los controles en los dominios A.9 (Control de accesos), A.12 (Seguridad operacional), A.13 (Seguridad en las comunicaciones) y A.14 (Adquisición, desarrollo y mantenimiento de los sistemas de información).

Se identificaron los controles de la Norma ISO 27001 que se benefician de la implementación del pentesting, se detalla el motivo de cumplimiento del pentesting en cada control de los dominios A.9, A.12, A.13 y A.14 y se demuestra la importancia de esta herramienta en el cumplimiento de la Norma ISO 27001

La investigación determinó las barreras y desafíos que enfrenta la implementación del pentesting en el cumplimiento de la Norma ISO 27001, principalmente en los controles orientados a la parte administrativa y documental, donde no se requiere de pruebas técnicas y en donde el pentesting juega un rol limitado o nulo en cada uno de estos controles.

Finalmente, el pentesting es una herramienta determinante para la detección e identificación de vulnerabilidades, no obstante, no sustituye a métodos tradicionales de auditoría dentro de la Norma ISO 27001. Es necesario combinar las auditorías documentales (tradicionales) con las pruebas técnicas (pentesting) para lograr un mejor enfoque en la gestión de la seguridad de la información

RECOMENDACIONES

- Se recomienda implementar el pentesting como una práctica recurrente dentro de un Sistema de Gestión de Seguridad de la Información. Esto permitirá detectar vulnerabilidades a tiempo y reducir el riesgo de incidentes de seguridad.
- Desarrollar políticas y procedimientos claros para la ejecución del pentesting, definidos dentro del SGSI. Estas políticas deben incluir alcances, metodologías, autorización, protección de datos y tratamiento de hallazgos, en concordancia con los requisitos legales y contractuales aplicables.
- Considerar la combinación de pentesting con otras prácticas de seguridad como análisis de vulnerabilidades automatizados y simulaciones Red Team/Blue Team. Esto permitirá una visión más completa de las amenazas, mejorando la postura de seguridad de la organización.
- Es recomendable complementar los métodos tradicionales de auditoría (documentales) con pruebas técnicas de pentesting para obtener una visión integral del estado de la seguridad de la información.
- Se recomienda a los estudiantes de la Carrera de Software de la Universidad Estatal de Bolívar que deseen continuar con esta línea de investigación, tomar como base la guía de pentesting propuesta en este proyecto, enfocándose en un solo dominio de la Norma ISO 27001 a la vez, esto permitirá un análisis más profundo, una implementación práctica mas viable y evitará la sobrecarga de trabajo en el desarrollo de futuros proyectos de tesis.

BIBLIOGRAFÍA

Agalit Mohamed, A., El Mostapha, C., Taqafi, I., & Youness Idrissi, K. (2023). A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. *International Journal of Safety and Security Engineering*, *13*, 1109–1116. https://doi.org/10.18280/ijsse.130614

Argudo Vera, H. (2024). Optimización y colaboración en ciberseguridad: diseño y desarrollo de una plataforma de soporte para equipos de pentesting. In *Sergioguillen.Com* (Issue 710). Universitat Politècnica de Catalunya.

Asensi, J. (2019). *El Papel Del Informático Como Auditor En La "Iso 27001:2017 Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos."* [Universitat Politècnica de València]. https://m.riunet.upv.es/bitstream/handle/10251/126076/Asensi - El papel del informático como auditor en la ISO 27001%3A2017 Tecnología de la información....pdf?sequence=1&isAllowed=y

Barragán, C. F. (2017). *Adaptación de las Normas ISO 27001 e HIPPA para la reducción de riesgos en la seguridad en Hospitales Nivel I del IESS*. Escuela Superior Politécnica de Chimborazo.

Byte-Mind. (2019). *Dradis para recolectar información de un pentest*. Byte-Mind.Net. https://byte-mind.net/dradis-para-recolectar-informacion-de-un-pentest/

Castillo Durán, E. F., Fernando Illescas Peña, F., & Quevedo Sacoto, A. S. (2023). Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001. Orientado a los medios de comunicación. *ConcienciaDigital*, *6*(4.1), 31–50. https://doi.org/10.33262/concienciadigital.v6i4.1.2725

Chavez, G., Galdamez, J., & Viera, K. (2018). *Guía de implementación del área de seguridad de la información como un servicio de TI basado en las buenas prácticas de COBIT 5, ISO 27001 E ITIL* [Universidad Don Bosco]. https://rd.udb.edu.sv/items/09d5463d-039e-42ee-951d-a65f177c714b

Chimborazo, C. (2021). Manual de políticas de Seguridad de la Información basado en la Norma ISO 27001 en el GAD Intercultural de el Tambo [Universidad Católica de Cuenca]. In *Universidad Católica de Cuenca*. https://dspace.ucacue.edu.ec/handle/ucacue/9712

Cilleruelo, C. (2024). *Fases de un pentest*. Keepcoding.Io. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

Código Orgánico Integral Penal. (2014).

Constitución de la República del Ecuador. (2008).

Contero, W. (2019). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL*

SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR. Universidad Internacional SEK Ecuador.

Coronel Suárez, I., & Quirumbay Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*, *9*(2), 97–108. https://doi.org/10.26423/rctu.v9i2.672

Correa, J. (2019). *TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (MISTIC) Plan de Implementación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 : 2013 Estudiante : Jorge Andrés Correa Morales Director : Antonio José Segovia Hena*. Universidad Oberta de Catalunya.

Cruz Lucas, G. I., Figueroa Rodríguez, E. L., Cruz Lucas, N. I., & Abad Parrales, W. M. (2023). Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001. *Journal TechInnovation*, *2*(2), 54–59. https://doi.org/10.47230/journal.techinnovation.v2.n2.2023.54-59

Cuba, V., & Solis, M. (2024). *Siseño de un Sistema de Gestión de Seguridad de la Información basado en la Norma Técnica Peruana NTP ISO 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco* (Vol. 15, Issue 1). Universidad Nacional de San Antonio Abad del Cusco.

Curcio, R. (2023). *Strengthening Cybersecurity in the Digital Age The Synergy of Penetration Testing and ISO / IEC 27001*. Alma Mater Studiorum – Università di Bologna.

De La Cruz Rodríguez, G. R., Méndez Fernández, R. A., & Mendoza De Los Santos, A. C. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Innovación y Software*, *4*(1), 219–236. https://doi.org/10.48168/innosoft.s11.a79

Diez, M. (2018). *Propuesta para la implementación de controles establecidospor la Norma ISO/IEC 27001:2013 - Anexo A, aplicables en el centro de diagnóstico automotor - CEDAC LTDA., ubicado en la zona industrial de la ciudad de Cúcuta*. Universidad Nacional Abierta y a Distancia.

Donoso, J. (2015). *Adaptación de una empresa tecnológica a UNE-ISO/IEC 27001 (versión 2013)*. Universidad Carlos III de Madrid.

Escrivá Gascó, G., Romero, R., Ramada, D., & Onrubia, R. (2013). *Seguridad Informática*. Macmillan Iberia, S.A.

Fadhli, M. (2024). *Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities*. *4*(June), 15–22. https://doi.org/https://doi.org/10.57152/ijeere.v4i1 15

Fauzan Imam, Iqbal Aditya Ferryanto, & Hardika Khusnuliawati. (2023). Sosialisasi Pishing Guna Mengedukasi Ibu-Ibu Pkk Dukuh Brajan Dalam Antisipasi Kejahatan Siber. *Jurnal Pengabdian Masyarakat Sains Dan Teknologi*, *2*(4), 189–195. https://doi.org/10.58169/jpmsaintek.v2i4.289

Felipe Redondo, A. M., & Núñez Cárdenas, F. de J. (2024). Criterios de selección de herramientas para pentesting. *Ciencia Huasteca Boletín Científico de La Escuela Superior de Huejutla*, *12*(24), 31–35. https://doi.org/10.29057/esh.v12i24.12763

Filippov, I. (2018). *SISTEMA DE PRUEBAS PARA REALIZAR AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA BASADAS EN ESTÁNDARES INTERNACIONALES*. Universidad Estatal Pedagógica Vocacional de Rusia.

Garza, L. (2024). *Secure Scan 360 , herramienta de pentesting automatizado Tesis para la obtención del título de Universidad Catolica de Cordoba Facultad de Ingeniería Carrera de Ingeniería de Documento de Proyecto Integrador* [Universidad Católica de Córdova]. https://pa.bibdigital.ucc.edu.ar/

Gómez, E., & Durán, G. (2022). *Gestión de Seguridad Informática en una dependencia gubernamental*. Universidad Nacional Autónoma de México.

Herrero Pérez, L. (2022). *Hacking Ético* (1st ed.). RA-MA Editorial.

Hung-Hsiou, H., & Jyun-Rong, S. (2023). *ISO 27001 Information Security Survey of Medical Service Organizations*. 19. https://doi.org/10.3390/engproc2023055019

Jiménez, C., Mendoza, D., Rodríguez, S., & Herrera, H. (2024). *Hacking Etico Y Cibercultura : Impacto En El Entorno Laboral*.

Laprovittera, C. (2024). *Cómo Iniciarse como Pentester en 2025*. Achirou.Com. achirou.com

Laseca, M. (2019). *Auditing the IoT or how to tame the botnet of things*. Universidad Autónoma de Madrid.

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2002). https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf?fbclid=IwAR2PhfFJMvEU4S0R_nYNE2--YV9mjaGvZ-eTb0efkBpKn5QEgmnrIwJeGMA

Ley Orgánica de Protección de Datos Personales. (2021). In *Asamblea Nacional del Ecuador* (Vol. 43, Issue 3). https://doi.org/10.1007/bf02189201

Ley Orgánica de Telecomunicaciones. (2015). https://www.telecomunicaciones.gob.ec/ley-organica-de-telecomunicaciones/

Mantilla, A. (2018). Gestión de seguridad de la información con la norma ISO 27001:2013. *Revista Espacios*, *39*.

Ministerio de Salud y Protección Social. (2023). *Declaración de aplicabilidad - iso/iec 27001:2013*.

MINTEL. (2013). Esquema Gubernamental De Seguridad De La Informacion. In *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. https://www.telecomunicaciones.gob.ec

Monteza Mera, L. O. (2019). Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino [Universidad Peruana de Ciencias Aplicadas]. In *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://repositorioacademico.upc.edu.pe/handle/10757/652121

Moreno, A. (2022). *Assessing web applications security*. Universitat Politècnica de Catalunya.

Murillo, A. (2017). *Evaluacion De Vulnerabilidades De Seguridad De La Empresa Booknowledge, Soluciones Para Mitigar Las Vulnerabilidades Encontradas Bajo La Norma Iso 27001:2013. Caso: Empresas Booknowledge*. Universidad de las Américas.

Muyón, C., & Montaluisa, F. (2020). Information security methods to protect rest web services communication and data in http requests using json web token and keycloak red hat single sign on | Métodos de seguridad de la información para proteger la comunicación y los datos de servicios web. *Risti, 2020*(E29), 198–213.

National Quality Assurance. (2022). *ISO 27001:2022 GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish QRFs and PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Ogechi, M. (2019). *Software Testing , Data Security and GDPR*. Universidad del Sureste de Noruega.

Palacio, J. (2025). *Las 5 fases del Pentesting | Todo lo que necesitas saber*. Ransomwarehelp.Com. https://www.ransomwarehelp.com/es/riesgos-y-necesidades/pentesting/

Parra, Á. (2014). *Iso 27001 para pymes* [Universidad Internacional de la Rioja]. http://reunir.unir.net/handle/123456789/3128

Pérez, A. (2024). *No Title*. OBS Business School. https://www.obsbusiness.school/blog/cuales-son-los-tipos-de-pentesting-mas-utilizados

Pilleux, G. (2021). *Sistemas de Pruebas de Penetración automatizadas para aplicaciones web*. Universidad de Chile.

Ramírez, E., & Rinconc, M. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*. https://doi.org/10.17013/risti.46.87–99

Ředina, M. (2021). *Uso de pruebas de penetración para aumentar la seguridad de los equipos informáticos.* Universidad de Pardubice.

Roa, B. J. F. (2015). *Seguridad informática - Ciclo formativo grado medio*. www.mhe.es/cf/informatica

Sánchez, V. (2019). *Planificación de la implementación de un esquema de seguridad basada en la Norma ISO 27001:2013, para el proceso de administración del sistema de información geográfica en el Gobierno Autónomo Descentralizado del Cantón Samborondón*. Escuela Superior Poltécnica del Litoral.

Silva, E. (2023). Propuesta de seguridad informática en los aspectos organizativos de un sistema informático, aplicando ISO 27002 y CSF. *Revista Ingeniería e Innovación Del Futuro*, *2*(1), 31–40. https://doi.org/10.62465/riif.v2n1.2023.9

Svatá, V. (2023). The Significance of Soc2 Type 2 and ISO 27001 Regulations for CC Service Providers in the Czech Republic. *IDIMT 2023: New Challenges for ICT and Management - 31st Interdisciplinary Information Management Talks*, 227–234. https://doi.org/10.35011/IDIMT-2023-227

Tigse, J. (2020). *Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la empresa Plasticaucho Industrial S.a* [Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec/handle/123456789/30696

Vanegas, R., & Alfonso, Y. (2019). *Pentesting, ¿Porque es importante para las empresas?*

Yance, A. (2024). *Diseño de un esquema de auditoría de seguridad informática en los controles de acceso a los activos de información bajo los lineamientos de la Norma ISO 27001 para una empresa de industria automotriz*. Escuela Superior Politécnica del Litoral.

ANEXO 1

Cronograma (Gantt)

Proyecto de Investigación

Nombre de tarea	Fecha de inic	Fecha final
	02/09/2024	**19/01/2025**
Presentación del Tema	02/09/2024	08/09/2024
Presentación del Anteproyecto	09/09/2024	13/10/2024
Introducción	14/10/2024	20/10/2024
Formulación General del Proyecto	21/10/2024	27/10/2024
Marco Teórico	28/10/2024	03/11/2024
Metodología	04/11/2024	17/11/2024
Resultados y Discusión	18/11/2024	01/12/2024
Propuesta (Comprobación)	02/12/2024	22/12/2024
Conclusiones, recomendaciones, r...	23/12/2024	19/01/2025

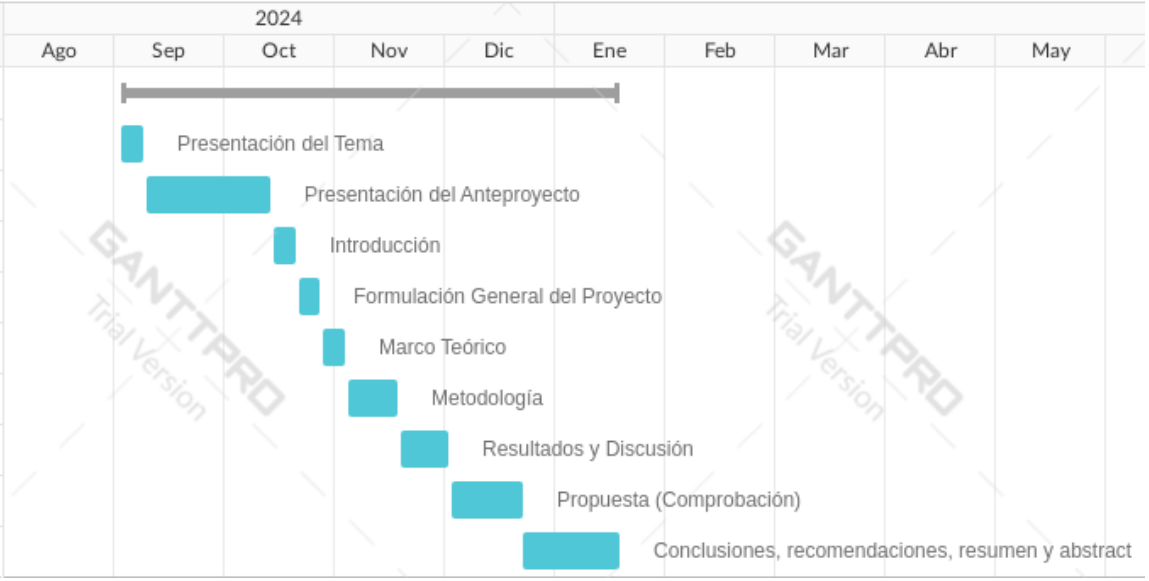

Ilustración 6: Cronograma Tentativo de Gantt
Fuente: Elaboración propia

ANEXO 2

Presupuesto Ejecutado

Tabla 67

Presupuesto del Proyecto de Investigación

N°	Recursos	Cantidad	Precio Unitario	Total
1	Portátil Hp I7 8GB RAM	1	$ 1.250,00	$ 1.250,00
2	Portátil Dell I5 8GB RAM	1	$ 400,00	$ 400,00
3	Impresiones, anillado y empastado	1	$ 150,00	$ 150,00
4	Internet	5	$ 25,00	$ 125,00
Total				**$ 1.925,00**

Elaborado por: Jair Cachipuendo, 2024

ANEXO 3

Certificado Antiplagio

ING. DARWIN CARRIÓN EN CALIDAD DE DIRECTOR(A) DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "ROL DEL PENTESTING EN EL CUMPLIMIENTO DE LA NORMA ISO 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, 2024", presentado por CACHIPUENDO AGUIAR JAIR ALEXANDER estudiante de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta TURNITIN, reflejando un **porcentaje de similitud del 6%**, como se puede evidenciar en el documento adjunto.

Guaranda, 25 de marzo del 2025

Atentamente,

Ing. Darwin Carrión
Director

Jair Cachipuendo

Tesis.docx

My Files
My Files
Universidad Estatal de Bolivar

Detalles del documento

Identificador de la entrega
trn:oid:::3117:440829636

Fecha de entrega
19 mar 2025, 2:31 p.m. GMT-5

Fecha de descarga
19 mar 2025, 2:46 p.m. GMT-5

Nombre de archivo
Tesis.docx

Tamaño de archivo
696.2 KB

107 Páginas

21.588 Palabras

128.136 Caracteres

turnitin Página 1 of 112 - Portada Identificador de la entrega trn:oid:::3117:440829636

6% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 15 words)

Exclusions

- 1 Excluded Source
- 29 Excluded Matches

Top Sources

5% Internet sources
1% Publications
5% Submitted works (Student Papers)

Integrity Flags

1 Integrity Flag for Review

Hidden Text
4702 suspect characters on 41 pages
Text is altered to blend into the white background of the document.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

ANEXO 4

Link del repositorio digital de biblioteca donde fue subido el proyecto