HACKING ETICO Y CIBERCULTURA: IMPACTO EN EL ENTORNO LABORAL

Cristian David Jiménez Calderón[1], Diego Alberto Mendoza Tuay[2], Sebastián Rodríguez Sánchez[3], Héctor Manuel Herrera[4]

[1]Fundación Universitaria Los Libertadores – Estudiante Especialización
[2]Fundación Universitaria Los Libertadores – Estudiante Especialización
[3]Fundación Universitaria Los Libertadores – Estudiante Especialización
[4]Fundación Universitaria Los Libertadores – Director Proyecto de Aplicación

RESUMEN

Este artículo aborda la problemática de la falta de preparación y conocimiento frente a los diversos tipos de ciberincidentes en las empresas. Se destaca cómo el personal puede convertirse en una brecha de seguridad, dado que los empleados pueden tener acceso a datos confidenciales de la empresa o compartirlos sin las precauciones necesarias. Por lo tanto, es crucial capacitarlos y fomentar una cultura de ciberseguridad. Los métodos preferidos por los ciberdelincuentes incluyen la explotación de aplicaciones públicas, el phishing, el ransomware y el acceso no autorizado a servidores de diversas compañías.

Para lograr el objetivo de la investigación, primero se identificarán vulnerabilidades específicas en los sistemas de información de las empresas, especialmente pymes, utilizando herramientas de hacking ético y pentesting. Se evaluará la conciencia de seguridad cibernética y las vulnerabilidades de la empresa mediante el envío de un archivo malicioso. Posteriormente, se analizarán las vulnerabilidades encontradas utilizando metodologías de hacking ético para comprender su impacto y los riesgos asociados. Finalmente, se propone una metodología basada en la norma ISO 27001:2013 y el ciclo PHVA (planificar, hacer, verificar y actuar) para mejorar la postura de seguridad cibernética de las organizaciones. Esta metodología incluirá medidas como la actualización de software, fortalecimiento de políticas de contraseñas, deshabilitación de servicios innecesarios, reducción de privilegios de usuario, capacitación en ciberseguridad e implementación de cabeceras de seguridad. Las recomendaciones buscan fomentar una cultura de seguridad cibernética robusta y continua en las empresas, incentivando la adopción de buenas prácticas y la realización de evaluaciones periódicas de seguridad.

Palabras clave: Seguridad cibernética, ciberincidentes, cultura de ciberseguridad, hacking ético, pentesting, ISO 27001:2013, PHVA (Planificar, Hacer, Verificar, Actuar), vulnerabilidades, conciencia de seguridad cibernética, capacitación en ciberseguridad, pymes.

ABSTRACT

This article addresses the issue of lack of preparation and knowledge regarding various types of cyber incidents in companies. It highlights how personnel can become a security breach, as employees may have access to confidential company data or share it without necessary precautions. Therefore, it is crucial to train them and promote a cybersecurity culture. Preferred methods by cybercriminals include exploiting public applications, phishing, ransomware, and unauthorized access to servers of various companies.

To achieve the research objective, specific vulnerabilities in companies' information systems, especially SMEs, will first be identified using ethical hacking tools and pentesting. The company's cybersecurity awareness and vulnerabilities will be assessed through the delivery of a malicious file. Subsequently, vulnerabilities found will be analyzed using ethical hacking methodologies to understand their impact and associated risks. Finally, a methodology based on the ISO 27001:2013 standard and the PDCA cycle (Plan, Do, Check, Act) is proposed to enhance organizations' cybersecurity posture. This methodology will include measures such as software updates, strengthening password policies, disabling unnecessary services, reducing user privileges, cybersecurity training, and implementing security headers. The recommendations aim to foster a robust and continuous cybersecurity culture in companies, encouraging the adoption of best practices and conducting regular security assessments.

Keywords: Cybersecurity, cyber incidents, cybersecurity culture, ethical hacking, pentesting, ISO 27001:2013, PDCA (Plan, Do, Check, Act), vulnerabilities, cybersecurity awareness, cybersecurity training, SMEs.

1. INTRODUCCIÓN

El hacking ético, a diferencia de su contraparte maliciosa, busca identificar vulnerabilidades en sistemas informáticos para fortalecer su seguridad y prevenir ataques cibernéticos. En este sentido, es crucial anticiparse a las amenazas latentes antes que a los potenciales atacantes para mejorar la seguridad y evitar la pérdida de datos. Normativas como la ISO 27001 establecen requisitos fundamentales para implementar, mantener y mejorar sistemas de gestión de seguridad de la información, priorizando la integridad, confidencialidad y disponibilidad de los datos.

La unión entre el hacking ético y la cibercultura plantea interrogantes sobre prácticas y mentalidades que impactan en el entorno laboral moderno, como la capacitación y concientización de los empleados. La investigación se enfoca en el

ámbito laboral frente al riesgo de amenazas cibernéticas, examinando la cibercultura desde una perspectiva ética de hacking. El objetivo principal es analizar cómo la implementación de prácticas de hacking ético puede influir en la cultura de seguridad cibernética de una organización.

1.1 JUSTIFICACION

El propósito de la investigación es enfocarse directamente en el ámbito laboral frente al riesgo de amenazas en cuanto ataques cibernéticos, haciendo énfasis en la cibercultura laboral examinada desde una perspectiva de hacking ético. Es crucial comprender temas de ciberseguridad puesto que se debe asimilar el

funcionamiento de un ataque cibernético y que es requerido para actuar con sensatez frente a esta problemática. Cada procedimiento definirá comportamientos clave, ya sea la realización del ataque, ejecución de procesos, entre otros factores determinantes que ayudaran a entender el propósito de la investigación. Donde se realiza un análisis frente a las posibles vulnerabilidades en un entorno laboral, evaluando la forma en que se presenta la victimización, sin indagar en alternativas para reforzar las brechas de seguridad a partir de las deficiencias del caso. Es importante aclarar que, a partir de los resultados obtenidos en este análisis, se determinaran elementos cruciales para tener en cuenta para evitar próximos ataques.

1.2 PREGUNTA PROBLEMICA

¿Cómo puede la implementación de prácticas de hacking ético y pentesting influir en la cultura de ciberseguridad de una organización?

1.3 OBJETIVOS

1.3.1 Objetivo general

Analizar el impacto del hacking ético en la cultura de seguridad cibernética en el entorno laboral de empresas pymes fomentando mejores prácticas en materia de seguridad informática, basados en la normativa ISO 27001: 2013

1.3.2 Objetivos específicos

- Identificar las vulnerabilidades específicas que podrían ser explotadas mediante técnicas de pentesting (Hacking ético).
- Evaluar el nivel de conciencia de seguridad cibernética entre los empleados de una organización.
- Proponer recomendaciones para mejorar la cultura de seguridad cibernética y fortalecer la protección de los activos digitales en el entorno laboral basados en la norma ISO 27001: 2013.

1.4 ALCANCE

El alcance del artículo se enfoca en las empresas pymes, siendo objetivos principales de ataques de hacking gracias a las vulnerabilidades de sus sistemas de seguridad. Dichas organizaciones manejan información sensible, lo que resalta la importancia de la sensibilización y capacitación respecto a las brechas de seguridad necesarias en un entorno laboral. Este enfoque no solo busca proteger la información fundamental de las empresas, sino también identificar y abordar el eslabón más débil en su cadena de seguridad: Los usuarios poco familiarizados con posibles ataques cibernéticos. Por lo tanto, se busca proporcionar orientación capacitada basada en su contenido para enfrentar eficazmente esta problemática.

A partir del análisis de impacto del hacking ético, se propondrán recomendaciones específicas para mejorar la seguridad cibernética en las pymes. Estas recomendaciones incluirán la implementación de prácticas de hacking ético, la adopción de normativas como ISO 27001:2013, y la capacitación continua de los empleados para fortalecer la postura de seguridad de las organizaciones.

2. REFERENTES TEÓRICOS

2.1 Marco teórico

Amenazas cibernéticas: Los ataques cibernéticos, como el phishing, malware, ransomware y suplantación de identidad, son amenazas comunes en el ámbito empresarial. Estudios anteriores han documentado casos de grandes corporaciones afectadas por brechas de seguridad. (Antonio, Retos y oportunidades

en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior, 2021)

Impacto económico: Las investigaciones han demostrado que los ciber incidentes pueden tener un impacto financiero significativo en las empresas, incluyendo pérdida de ingresos, daños a la reputación y sanciones legales. ((INCIBE), 2023)

Políticas de seguridad: La literatura previa destaca la importancia de implementar políticas de seguridad cibernética sólidas en las organizaciones, incluyendo la gestión de accesos y la capacitación del personal. (Tecnología, 2018)

Respuesta ante incidentes: Además de la prevención, es crucial contar con planes de respuesta ante incidentes bien definidos. Esto implica establecer procedimientos para detectar, contener y mitigar los efectos de posibles brechas de seguridad, así como para comunicarse con las partes interesadas internas y externas de manera efectiva durante y después de un incidente. (Cruz, 2021).

Tecnologías emergentes: La adopción de tecnologías emergentes como el Internet de las cosas (IoT), la computación en la nube y la inteligencia artificial también introduce nuevos desafíos de seguridad. Estas tecnologías pueden ampliar la superficie de ataque y generar nuevos puntos de vulnerabilidad que deben ser abordados mediante medidas de seguridad proactivas. (CORDIS, 2017).

Herramientas y tecnologías: Las últimas tendencias en ciberseguridad incluyen el uso de tecnologías avanzadas como la inteligencia artificial y el hacking ético para detectar y responder a amenazas de manera proactiva.

2.2 Estado del Arte

Capacitación y concienciación: La investigación se basó en la necesidad de fortalecer el eslabón humano en la ciberseguridad. Se realizó debido a la alta incidencia de incidentes de seguridad que involucran errores humanos. Los autores implementaron programas de capacitación para mejorar la conciencia y las prácticas de seguridad entre los empleados. Como resultado, lograron una reducción en la vulnerabilidad a ataques cibernéticos y un aumento en la cultura de seguridad proactiva en las organizaciones. (Muncaster, 2022).

Legislación y normativas vigentes: La investigación se centró en analizar las carencias de América Latina en políticas de ciberseguridad y capacidad para enfrentar ciber amenazas que impactan la seguridad nacional y política exterior, lo realizaron para abordar el aumento global de ciber amenazas y cómo afectan a América Latina, una región con limitadas ciber capacidades, con esto lograron un análisis comparativo de ciber capacidades entre América Latina y otras regiones, evaluando los esfuerzos de los países latinoamericanos en desarrollar políticas de ciberseguridad y construir capacidades. Se identificaron oportunidades de mejora para fortalecer la seguridad cibernética en la región. (Antonio, Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior, 2021).

Cultura de ciberseguridad: El artículo examina la seguridad de la información en Colombia frente a amenazas cibernéticas globales. A través de una investigación cualitativa, se revisa la situación actual del país, destacando la importancia de la ciberseguridad durante la pandemia de COVID-19. Se analizan los riesgos para empresas y sociedad, y se evalúan las políticas gubernamentales y estándares de calidad en seguridad informática. El estudio concluye enfatizando

los retos de Colombia en la protección de la información ante las amenazas cibernéticas1. (Rangel, 2020).

Colaboración y compartición de información: El artículo destaca la importancia de la colaboración y el intercambio de información como factores esenciales para el avance de la ciberseguridad. Se basa en la evolución histórica de las amenazas informáticas y cómo la cooperación entre investigadores y la industria ha sido crucial para desarrollar contramedidas efectivas. La investigación resalta que, a pesar de la accesibilidad de la información, es la colaboración la que permite una evolución constante en la defensa contra el cibercrimen, lo que ha llevado a un progreso significativo en la ciberseguridad (Harán, 2022).

Hacking ético y pruebas de penetración: El artículo de Nordstern Technologies se centra en la práctica del hacking ético y los diferentes tipos de pruebas de penetración (pentesting). La investigación se basó en la creciente curiosidad y demanda de información sobre el hacking ético, así como en la necesidad de identificar y descubrir vulnerabilidades en las redes y aplicaciones de las organizaciones. Se realizó para informar y educar sobre las metodologías de pentesting, incluyendo las pruebas de caja blanca, caja gris y caja negra, y su relevancia en la simulación de ataques cibernéticos. Como resultado, se logró proporcionar una guía clara sobre cómo estas pruebas pueden ayudar a reforzar la seguridad y tomar medidas preventivas contra posibles ciberdelincuentes (Nordstern, 2021).

Ciberseguridad en la nube: El estudio “Seguridad en la nube, evolución indispensable en el siglo XXI” de la Universidad Distrital Francisco José de Caldas se basó en una revisión de literatura para identificar la seguridad aplicada a la infraestructura, software y plataformas de la computación en la nube. La investigación se realizó con el fin de entender las inquietudes sobre la seguridad de la información y la privacidad de datos en la nube, enfocándose en los modelos de servicio IaaS, PaaS y SaaS. Como resultado, se destacó que los modelos de servicio de computación en la nube son más vulnerables a medida que se externalizan, y se propusieron estrategias para fortalecer la seguridad, especialmente en los modelos SaaS. (Ximena Galindo Ramírez)

Privacidad y protección de datos: La investigación Se realizó debido a la rápida evolución tecnológica, la globalización económica y la digitalización de las relaciones humanas, que han creado disparidades en los niveles de protección de datos personales a nivel mundial. Los autores analizaron la sentencia del Tribunal de Justicia de la Unión Europea sobre la invalidez del Acuerdo de Puerto Seguro UE-EE. UU. como un caso representativo de estas diferencias. El objetivo fue contribuir a la generación de estándares internacionales para la protección de datos personales. (María Solange Maqueo Ramírez, 2017).

Educación y desarrollo profesional en ciberseguridad: La investigación de Cisco se centró en la importancia crítica de la educación en ciberseguridad debido a la digitalización acelerada y la necesidad de cubrir 3.5 millones de empleos en el sector para 2021. La motivación detrás de la investigación fue la brecha de talento existente y la oportunidad de capacitar a más profesionales, especialmente mujeres en STEM. Cisco y la OEA lanzaron cursos gratuitos y crearon los Cybersecurity Innovation Councils para promover la educación y una mentalidad de “ciberseguridad primero”. Como resultado, se proporcionaron soluciones educativas para satisfacer la demanda de talento y se abrieron oportunidades de crecimiento en la industria de la ciberseguridad (Mario de la Cruz, 2020).

3. METODOLOGÍA

En este artículo se desarrollará la metodología PHVA (planificar, hacer, verificar y actuar) ya que permitirá que las organizaciones mejoren proactivamente su postura frente a incidentes de seguridad identificando y abordando vulnerabilidades antes de que sean explotadas y se conviertan en un riesgo para la compañía, fomentando una cultura de la seguridad informática sólida.

Ilustración 1 Pasos de la metodología Fuente: elaboración propia

3.1 Planificar: En esta fase se requiere establecer los objetivos principales y el alcance que tendrá el proceso de hacking ético, donde se definen los sistemas que se van a evaluar se identifican las herramientas que se van a utilizar y un plan detallado de lo que se va a ejecutar.

3.2 Hacer: En esta etapa se realizan las actividades de hacking ético, donde se identifican vulnerabilidades, la explotación de estas recopilando información importante que se obtenga para demostrar las falencias con las que cuenta la compañía.

3.3 Verificar: Una vez completado el hacking realizado se busca analizar detalladamente los resultados obtenidos con el fin de identificar las vulnerabilidades existentes y evaluar la eficiencia de las medidas de seguridad existentes documentando los hallazgos obtenidos

3.4 Actuar: En base a los resultados obtenidos se tomas las acciones correspondientes para mitigar estas vulnerabilidades identificadas con el fin de mejorar y cubrir las brechas de seguridad encontradas.

Este proceso debe ser periódico, ya que con el tiempo se descubren nuevas vulnerabilidades que es imprescindible abordar para mejorar continuamente nuestras medidas de seguridad establecidas.

4. ANÁLISIS Y RESULTADOS

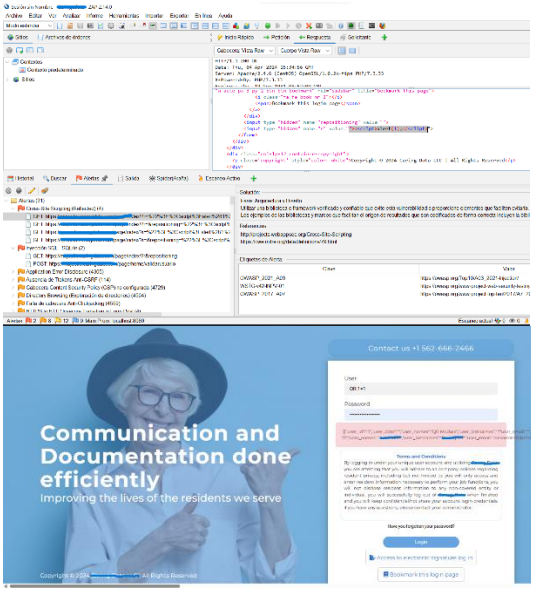
4.1 Identificación de vulnerabilidades mediante técnicas de Pentesting y Hacking Ético

El proceso de pentesting y hacking ético llevado a cabo en esta investigación reveló varias vulnerabilidades en los sistemas de información de la organización. A continuación, se detallan los hallazgos más significativos:

4.1.1 Vulnerabilidades Identificadas:

1. **Configuraciones Débiles de Seguridad en Aplicaciones Web:**

   Se identificaron aplicaciones web con configuraciones de seguridad inadecuadas, lo que permitió la explotación de vulnerabilidades como inyección SQL y Cross-Site Scripting (XSS). Estas vulnerabilidades podrían permitir a un atacante obtener acceso no autorizado a datos sensibles.



lustración 2 Vulnerabilidades aplicación WebFuente: elaboración propia

2. **Falta de Actualizaciones y Parches:**

Varios servidores y aplicaciones no contaban con las actualizaciones de seguridad más recientes, exponiendo a la organización a amenazas conocidas. La falta de parches en el software aumentó la superficie de ataque disponible para los ciberdelincuentes.

Ilustración 3: Vulnerabilidades Fuente: elaboración propia

3. **Contraseñas Débiles y Políticas de Autenticación:**

Se encontraron políticas de autenticación deficientes, incluyendo el uso de contraseñas débiles y la falta de implementación de autenticación multifactor (MFA). Esto facilitó el acceso no autorizado a cuentas de usuario.

4. **Exposición de Servicios Innecesarios:**

Se descubrieron servicios de red innecesarios que estaban habilitados y accesibles desde el exterior, aumentando el riesgo de ataque. La eliminación de estos servicios redujo significativamente la superficie de ataque.

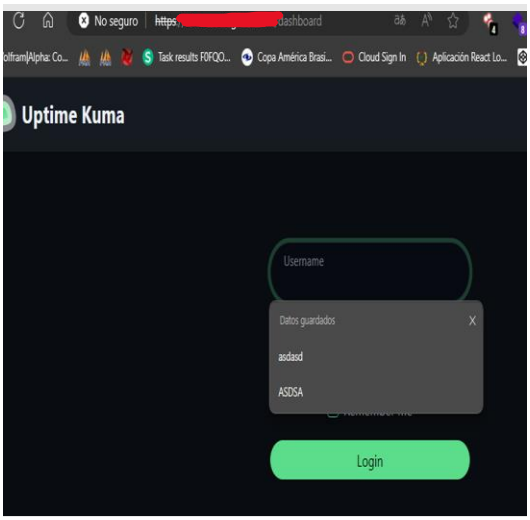


Ilustración 4 Servicios expuestos Fuente: elaboración propia

5. **Privilegios de Usuario Excesivos:**

Algunos usuarios contaban con privilegios excesivos que no eran necesarios para sus roles. La reducción de estos privilegios a lo mínimo necesario ayudó a limitar el impacto potencial de una cuenta comprometida.

6. **Bibliotecas Vulnerables:**

Se encontraron bibliotecas de software desactualizadas y vulnerables, lo que podría permitir a un atacante explotar fallos conocidos para comprometer el sistema.

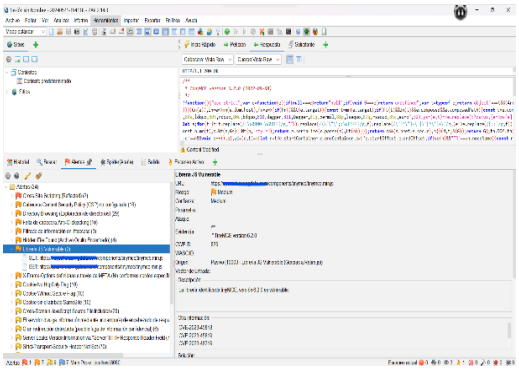


Ilustración 5 Bibliotecas Vulnerables Fuente: elaboración propia

7. **Directorios Accesibles:**

Se descubrieron directorios accesibles públicamente donde se subían imágenes y documentos. Estos directorios permitieron la visualización de información sensible de los usuarios, como números de cédula y otros documentos personales.

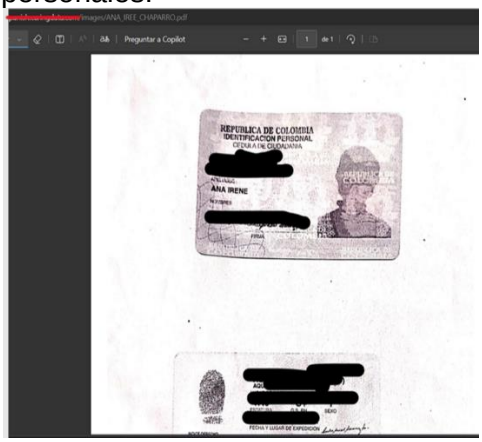


Ilustración 6 Documentos personales Fuente: elaboración propia

8. **Contraseñas y Correos en el Código Fuente:**

Se encontraron contraseñas y direcciones de correo electrónico incrustadas en el código fuente de algunas aplicaciones, lo que expone esta información a cualquier persona con acceso al código.

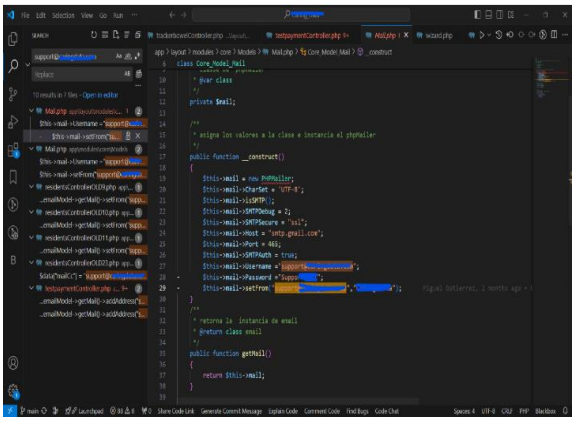


Ilustración 7 Información en código fuente Fuente: elaboración propia

9. **Ausencia de Cabeceras de Seguridad:**

La falta de cabeceras de seguridad como anti-CSRF, CSP (Content Security Policy) y anti-clickjacking, dejó las aplicaciones vulnerables a ataques como Cross-Site Request Forgery, Clickjacking y otros ataques basados en el navegador.

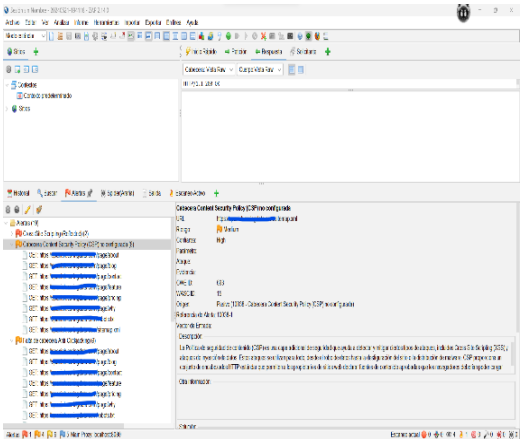


Ilustración 8 Ausencia de cabeceras Fuente: elaboración propia

4.2 Evaluación del nivel de conciencia de la seguridad cibernética

Envío de Archivo Malicioso

Se realizó un ejercicio práctico mediante el envío de un archivo malicioso a los empleados a través del chat del grupo de

la empresa. Este archivo, creado con Kali Linux utilizando msfvenom, permitía el acceso al computador de los empleados. Los resultados fueron los siguientes:

Tasa de Apertura: Se constató que un 75% de los empleados abrió el archivo malicioso enviado en la campaña de phishing. Esta alta tasa de apertura indica una vulnerabilidad significativa en la conciencia y prácticas de seguridad cibernética entre el personal de la empresa.

Tasa de Ejecución: De manera alarmante, el 40% de los empleados procedió a ejecutar el archivo malicioso en sus equipos. Esta acción representa un riesgo considerable para la integridad de los sistemas y datos de la organización, ya que la ejecución de archivos de origen desconocido puede resultar en la instalación de software malicioso o la explotación de vulnerabilidades.

Tasa de Compromiso: Como resultado directo de la ejecución del archivo malicioso, el 20% de los empleados inadvertidamente permitió el acceso no autorizado a sus equipos. Este nivel de compromiso pone en peligro la seguridad de la red corporativa, ya que los ciberdelincuentes podrían aprovechar esta puerta trasera para realizar actividades maliciosas, como robo de datos o sabotaje.

Estas métricas subrayan la necesidad urgente de implementar medidas de seguridad cibernética más rigurosas, así como de mejorar la conciencia y capacitación del personal en materia de phishing y otras amenazas cibernéticas.

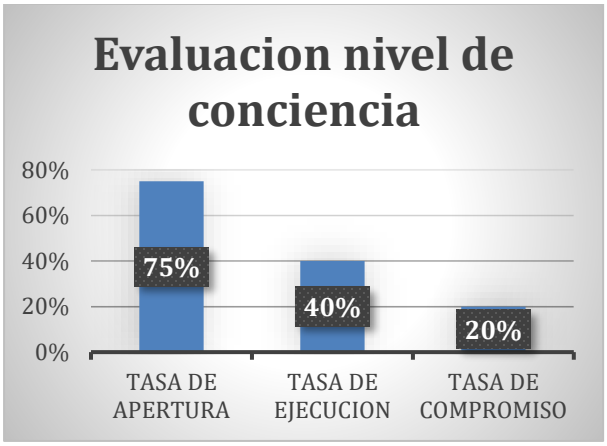


Ilustración 9 Evaluación nivel de conciencia
Fuente: elaboración propia

4.3 Análisis de Equipos Afectados

Los equipos de los empleados que ejecutaron el archivo malicioso fueron analizados para recopilar información relevante sobre las vulnerabilidades explotadas. Se descubrieron las siguientes deficiencias:

Archivos de Contraseñas: Se validó que varios equipos contenían archivos de texto o blocs de notas con contraseñas de servidores, bases de datos e información crítica de la empresa, exponiendo estos datos a posibles accesos no autorizados.

Antivirus Desactualizado: En varios equipos, el software antivirus no estaba actualizado, lo que permitió que el malware evadiera la detección. Usuarios antes del hacking ético y recomendaciones

Falta de Conciencia de Seguridad: Los empleados que ejecutaron el archivo malicioso mostraron una falta de conciencia sobre las prácticas seguras de ciberseguridad, lo que subraya la necesidad de una capacitación continua y efectiva.

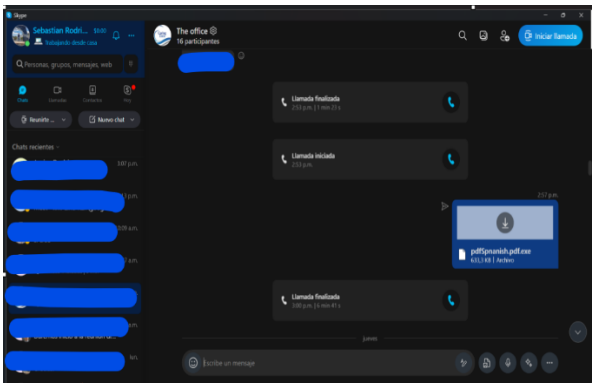


Ilustración 10 Envió del archivo malicioso al chat de la empresa. Fuente: elaboración propia

Ilustración 11 Evidencia archivo .txt
Fuente: elaboración propia.

Ilustración 12 Evidencia archivos sql y php
Fuente: elaboración propia

4.4 Propuesta para mejorar la cibercultura basado en la norma ISO 27001/2013

Basados en la norma ISO 27001/2013 se realizan las siguientes propuestas:

Implementación de Políticas de Seguridad: De acuerdo con la norma ISO27001:2013 en su numeral 4.4 se debe establecer, implementar, mantener el sistema de gestión de seguridad de la información; cabe resaltar la mejora continua en el numeral 10.2. Para este caso puntual se incluye la gestión de accesos y la actualización continua de software.

Capacitación Permanente: Establecer un programa continuo de capacitación en ciberseguridad para todos los empleados de acuerdo con la norma ISO 27001:2013 en el ANEXO A numeral A.7.2.2 *"Toma de conciencia, educación y formación de la seguridad de la información*", con énfasis en la identificación y prevención de ataques comunes como el malware.

Evaluaciones Periódicas: Respecto a la norma ISO 27001: 2013 en el Anexo A numeral A. 17.1.3 *"Verificación, revisión y evaluación de la continuidad de la seguridad de la información"* Se propone la realización de evaluaciones de seguridad periódicas mediante prácticas de hacking ético para asegurar que las medidas de seguridad sean efectivas y eficaces durante situaciones adversas.

Adopción de Normativas: Promover el sistema de seguridad de la información de acuerdo con la norma ISO 27001: 2013 su numeral 5.1 *"LIDERAZGO Y COMPROMISO*" en todos sus ítems que garantice la integridad, confidencialidad y disponibilidad de los datos, así como la comunicación asertiva de todas las partes interesadas.

Buen manejo de contraseñas: Insistir en el manejo y mejora del uso de contraseñas señalado en la norma ISO 27001: 2013 en el Anexo A: en su numeral A.9.4.3 *"Sistema de gestión de contraseñas"* y que a su vez se valida como vulnerabilidad en el desarrollo de las pruebas.

Visualización de resultados: De acuerdo con la norma ISO:27001: 2013 en su numeral 9.1 *"9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN"* La investigación no solo ha permitido conocer las vulnerabilidades existentes en los

sistemas de información, sino también ha proporcionado un camino claro para fortalecer la postura de seguridad cibernética de la organización. Con la adopción de las recomendaciones propuestas, la empresa estará mejor preparada para enfrentar las amenazas emergentes en el entorno digital.

4.4.1 Herramientas Utilizadas

Para el pentesting y el hacking ético, se utilizaron las siguientes herramientas:

Kali Linux: Distribución de Linux especialmente diseñada para pruebas de penetración y auditorías de seguridad.

NMAP: Herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red.

ZAP (Zed Attack Proxy): Herramienta de prueba de penetración de aplicaciones web que ayuda a encontrar vulnerabilidades de seguridad en aplicaciones web.

Shodan: Motor de búsqueda que permite encontrar dispositivos conectados a Internet y sus vulnerabilidades.

Wappalyzer: Extensión de navegador que identifica tecnologías utilizadas en sitios web.

4.4.2 Medidas de Mitigación Implementadas

Con base en los hallazgos del pentesting y el ejercicio del archivo malicioso, se implementaron las siguientes medidas de mitigación:

Actualización de Software: Se actualizaron todos los sistemas y aplicaciones a las últimas versiones disponibles, aplicando todos los parches de seguridad necesarios.

Fortalecimiento de Políticas de Contraseña: Se implementaron políticas de contraseña más robustas y se introdujo la autenticación multifactor para todas las cuentas de usuario.

Deshabilitación de Servicios Innecesarios: Se deshabilitaron los servicios de red no esenciales y se restringió el acceso a los servicios críticos.

Reducción de Privilegios de Usuario: Se revisaron y ajustaron los privilegios de usuario para asegurarse de que cada empleado tuviera únicamente los permisos necesarios para su rol.

Capacitación en Ciberseguridad: Se inició un programa continuo de capacitación en ciberseguridad para todos los empleados, enfocándose en la concienciación sobre amenazas como el malware y otras prácticas de seguridad.

Implementación de Cabeceras de Seguridad: Se añadieron cabeceras de seguridad como anti-CSRF, CSP y anti-clickjacking para proteger las aplicaciones web contra ataques comunes basados en el navegador.

5. Conclusiones

La investigación logra contestar la pregunta problemática: "¿Cómo puede la implementación de prácticas de hacking ético y pentesting influir en la cultura de ciberseguridad de una organización?". La implementación de estas prácticas influye positivamente en la cultura de ciberseguridad al fomentar una mentalidad de prevención y preparación entre los empleados, incrementar la conciencia sobre la seguridad, y proporcionar un enfoque estructurado y continuo para identificar y mitigar vulnerabilidades. La adopción de normativas como ISO 27001:2013 respalda este proceso, creando una cultura organizacional que valora y prioriza la ciberseguridad.

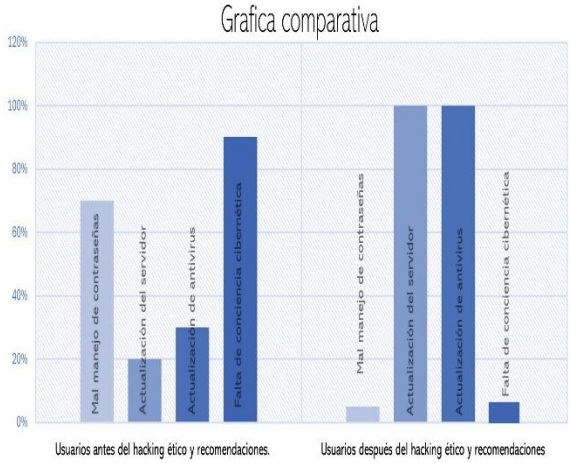
En resumen, la adopción de prácticas de hacking ético y pentesting no solo fortalece la postura de ciberseguridad de una organización, sino que también transforma su cultura, promoviendo un entorno más consciente y resiliente frente a los riesgos cibernéticos.

Impacto del Hacking Ético

Fortalecimiento de la Seguridad: El hacking ético ha permitido identificar y corregir múltiples vulnerabilidades, mejorando significativamente la seguridad de los sistemas de información.

Mejora Continua: La metodología PHVA aplicada ha demostrado ser efectiva para el ciclo continuo de identificación, corrección y prevención de vulnerabilidades.

Concienciación y Capacitación: La realización de ejercicios prácticos como el envío de archivos maliciosos ha resaltado la necesidad de una mayor concienciación y capacitación de los empleados en ciberseguridad.



Gráfica 1 Comparativa entre antes de realizar el Hacking Etico y después.Fuente: elaboración propia

REFERENCIAS

(ICONTEC), I. C. (2013). *NORMA TÉCNICA NTC-ISO-IEC 27001.* Bogotá: ICONTEC.

(INCIBE), I. (01 de 08 de 2023). *incibe*. Obtenido de https://www.incibe.es/empresas/blog/como-reducir-el-impacto-financiero-de-los-incidentes-de-ciberseguridad

Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *scielo*, 169–197.

Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Scielo*, 169–197.

CORDIS. (1 de 08 de 2017). Obtenido de https://cordis.europa.eu/article/id/85979-security-risks-of-emerging-technologies/es

Cruz, N. J. (2021). La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. *scielo*, 2021.

Giraldo, H. G. (12 de 2023). *Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001: 2022.* Obtenido de Universidad Cooperativa de Colombia: https://repository.ucc.edu.co/handle/20.500.12494/54002

Harán, J. M. (03 de 06 de 2022). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2022/06/09/colaboracion-divulgacion-informacion-ciberseguridad/

Mansur, S. M., & Salinas, S. I. (2018). *Ventajas del hacking ético para las organizaciones.* Nuevo Leon Mexico: Latindex.

María Solange Maqueo Ramírez, J. M. (2017). "La protección de datos personales, como un derecho fundamental autónomo del derecho a la vida privada, ha tenido un desarrollo asimétrico en los diferentes sistemas de derechos humano. *scielo*, 77-96.

Mario de la Cruz, P. B. (2020). *cisco*. Obtenido de https://news-blogs.cisco.com/americas/es/2020/07/29/la-educacion-en-ciberseguridad-es-una-necesidad-y-una-oportunidad-para-todos/

Muncaster, P. (22 de 06 de 2022). Programas de capacitación en ciberseguridad: por qué son tan importantes y qué funciona mejor. *welivesecurity*.

Nordstern, E. (18 de 10 de 2021). *nordsterntech*. Obtenido de https://www.nordsterntech.com/post/infograf%C3%ADa-hacking-%C3%A9tico-tipos-de-pentesting-o-pruebas-de-penetraci%C3%B3n

Rangel, M. R. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *scielo*, 199-217.

Staff, F. (28 de 02 de 2024). *Forbes*. Obtenido de https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica

Tecnología, I. N. (2018). *Marco para la mejora de la seguridad cibernética en .* Institute of Standards and Technology.

Ximena Galindo Ramírez, M. A. (s.f.). Seguridad en la nube, evolución indispensable en el siglo XXI. *udistrital*.