CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y REDTEAM

HENRY ALLYVER FONSECA CALDERON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

CÓDIGO: 202337164

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y REDTEAM

PRESENTADO A:

EVER LUIS ARROYO BARON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

TUNJA

Tabla de Contenido

Lista Imágenes

Resumen

En la actividad, se identificaron infracciones legales relacionadas con la ley 1273 de 2009, específicamente en los artículos 269A, 269C y 269F, que sancionan accesos no autorizados, interceptación de datos y violaciones de privacidad. Estas acciones comprometieron principios éticos como la confidencialidad, integridad y transparencia, exponiendo a la organización a riesgos legales y reputacionales.

La implementación de normas, buenas Prácticas Adoptar estándares internacionales como ISO 27001, NIST CSF y OWASP para garantizar el cumplimiento normativo y la mejora continua. Incluir herramientas como Nessus, Metasploit y OWASP ZAP para auditorías y pruebas de seguridad.

Fortalecer la seguridad es un proceso perenne que requiere responsabilidad, inversión y un enfoque integral. Estas medidas ayudan a proteger los activos organizacionales frente a amenazas internas y externas, mejorando la confianza y resiliencia de la organización.

Glosario

Ciberseguridad: Contiguo de habilidades, tecnologías y metodologías diseñadas para resguardar sistemas, redes y datos contra ataques, daños o accesos no autorizados.

Red Team: Equipo que simula ataques reales contra una organización para identificar vulnerabilidades y optimizar la postura de seguridad.

Blue Team: Equipo encargado de defender y proteger la infraestructura de una organización ante ataques cibernéticos, utilizando herramientas de monitoreo y análisis.

Ley 1273 de 2009: Legislación colombiana que protege la información y los datos en sistemas informáticos, estableciendo sanciones para delitos como acceso abusivo, daño a sistemas y violación de datos personales.

Confidencialidad: Principio de seguridad que certifica que los datos solo estén disponibles para personas acreditadas.

Integridad: Asevera que los datos no sean alterados o modificados sin autorización durante su almacenamiento o transmisión.

Pentesting: Pruebas de penetración diseñadas para identificar vulnerabilidades de seguridad en sistemas y redes mediante simulación de ataques controlados.

SIEM: Solución tecnológica que colecciona, analiza y gestiona sucesos de seguridad en tiempo real, ayudando en la detección y respuesta ante incidentes.

Autenticación **multifactor (MFA)**: Método de autenticación que requiere múltiples verificaciones (como contraseñas, biometría o códigos) para garantizar la identidad del usuario.

NIST CSF: Marco de trabajo que ayuda a las empresas a tramitar y reducir los riesgos cibernéticos.

OWASP (Open Web Application Security Project): Proyecto que proporciona estándares y herramientas para mejorar la seguridad de las aplicaciones web.

Vulnerabilidad: fallo en un sistema, red o programa que es atacada, por terceros para su uso personal.

Auditoría de seguridad: Evaluación sistemática de una infraestructura tecnológica para identificar posibles brechas y comprobar el desempeño de la seguridad.

Endurecimiento de seguridad: Conjunto de técnicas para reforzar sistemas y redes, minimizando las vulnerabilidades y reduciendo la superficie de ataque.

Logs: Registros de actividades y eventos generados por sistemas o aplicaciones, útiles para auditorías y análisis forenses.

ISO 27001: Norma que permite verificar las políticas de seguridad de una organización, guiado por los requerimientos de dicha norma.

Reputación organizacional: Percepción pública sobre la credibilidad y confianza en una organización, que puede verse afectada por incidentes de seguridad.

Firewalls: Hardware o software que vigilan y infiltran el tráfico de red, sitiando accesos no autorizados.

Segmentación de redes: Práctica de dividir una red en secciones más pequeñas y seguras para limitar el acceso y contener posibles ataques.

Pruebas de intrusión: Métodos utilizados para evaluar la seguridad de un sistema intentando explotarlo de modo controlado.

1. Introducción

La seguridad de los datos es una columna primordial para garantizar el funcionamiento de cualquier empresa en el día a dia. Los crecientes ataques cibernéticos y las amenazas internas y externas exigen una gestión proactiva que integre tecnología, procesos y conciencia humana. En este contexto, la ciberseguridad se posiciona como un campo crítico, destinado a proteger los activos digitales frente a riesgos que pueden comprometer la seguridad de la información.

Este trabajo aborda los conceptos clave relacionados con la seguridad de la información y la ciberseguridad, explorando técnicas como pruebas de penetración (pentesting), auditorías y estrategias de defensa activa mediante equipos Red Team y Blue Team. Asimismo, se analizan las normativas y estándares internacionales, como la Ley 1273 de 2009, que establecen un marco jurídico para proteger los datos y sistemas informáticos.

La finalidad es comprender la importancia de implementar estrategias de seguridad robustas, que no solo fortalezcan las defensas de la organización, sino que también minimicen los riesgos reputacionales y económicos asociados a posibles vulnerabilidades. Este análisis se convierte en un recurso para fomentar la cultura de ciberseguridad en un mundo interconectado.

2. Objetivos

2.1. Objetivo General

Endurecer la seguridad de la información en organizaciones mediante la implementación de estrategias integrales que combinen técnicas de evaluación de vulnerabilidades, cumplimiento normativo, y buenas prácticas en ciberseguridad, garantizando la protección de los activos y el cumplimiento de estándares éticos y legales.

2.1.1. Objetivos Específicos

Realizar pruebas de penetración controladas para detectar y documentar fallos en la infraestructura tecnológica antes de que sean explotados por agentes malintencionados.

Cumplir con leyes nacionales e internacionales, como la Ley 1273 de 2009 y la ISO/IEC 27001, para garantizar la protección de datos y sistemas informáticos.

Diseñar medidas de protección como autenticación multifactor (MFA), cifrado de datos y segmentación de redes para minimizar el impacto de posibles ataques cibernéticos.

Desarrollar programas de formación continua para empleados y equipos técnicos en el uso ético de herramientas, detección de amenazas y respuesta a incidentes.

Integrar tecnologías avanzadas como sistemas SIEM para la descubrimiento, análisis y amortiguamiento de eventos de seguridad en tiempo real.

3. DESARROLLO DE LA ACTIVIDAD

3.1. Aspectos que aportan al desarrollo en las estrategias de red team y blue team.

3.1.1. Identificación de Infracciones Legales:

se evidenció que CyberFort Technologies facilitó y justificó accesos no autorizados a sistemas informáticos. Estas prácticas constituyen un claro ejemplo de acceso abusivo prohibido por la ley **1273 de 2009**

3.1.2. Según la ley 1273 de 2009:

Se evidencia infracciones sobre esta. Dentro de las cuales se pueden identificar las siguientes:

De acuerdo con el artículo 269A sobre acceso desmedido a los sistemas informáticos, se evidencia que CyberFort Technologies está infringiendo esta ley en su proceder. En una de sus cláusulas, se manifiesta permisible respecto a prácticas como la interceptación de datos, chuzadas, accesos no autorizados a sistemas informáticos y otras actividades ilícitas relacionadas con la vulneración de información.

3.1.3. Según el artículo 269C sobre la toma de datos informáticos:

CyberFort Technologies, a través de la aplicación del contrato elaborado por el abogado que ya no forma parte de la organización, muestra la intención de interceptar datos sin la debida autorización, lo cual constituye una clara violación de la ley.

3.1.4. Artículo 269F:

Violación de datos personales, ya que se comparte información a terceros. "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual

intervenga la apropiación de información de terceros.". obteniendo un beneficio propio y para terceros. La intención de interceptar datos sin autorización explícita, incluida en los términos contractuales, es una grave infracción que muestra intenciones ilícitas de espionaje y vigilancia no consentida. Compartir información confidencial a terceros sin consentimiento constituye una violación directa a la privacidad, derivando en un aprovechamiento indebido para beneficio propio o de terceros. Como equipo Red Team y Blue Team, se identifica que el análisis ético vulnero principios como confidencialidad, integridad, transparencia, además cada profesional, se expone a riesgos legales, reputacionales y profesionales. Estas prácticas no solo ponen en peligro su integridad, sino también su libertad y bienestar. Por lo tanto, es recomendable como equipos estratégicos RedTeam y BlueTeam, Asegurar que las pruebas de intrusión estén limitadas al alcance autorizado, garantizando el respeto a la privacidad y los términos contractuales, implementar monitoreos en tiempo real sobre el uso de herramientas avanzadas para evitar accesos indebidos. Registrar todas las actividades realizadas durante ejercicios de RedTeam, facilitando la revisión y mitigación de comportamientos indebidos. Implementación de controles preventivos, garantizando que las auditorías incluyan evaluaciones físicas y lógicas de los sistemas, sin necesidad de acceder directamente a datos sensibles. Capacitación en ética, incluir formación periódica sobre leyes de ciberseguridad, manejo ético de información y consecuencias legales del incumplimiento. Sistemas de supervisión, integrar monitoreos automatizados para detectar actividades inusuales que puedan indicar abuso de privilegios por parte de los empleados. Definición clara de cláusulas contractuales, limitar el alcance de los acuerdos de confidencialidad y garantizar que incluyan disposiciones específicas para la protección de datos personales y reportes obligatorios de actividades sospechosas.

Implementación de auditorías internas, realizar revisiones regulares para garantizar el cumplimiento de normativas legales y éticas. Segregación de funciones, separar los roles de acceso, manejo y auditoría de datos para evitar conflictos de interés y abuso de poder. Las estrategias de RedTeam y BlueTeam deben alinearse con estándares éticos y legales para proteger tanto los activos de información como la confianza de los clientes. Solo así será posible establecer un entorno seguro y transparente en el ámbito de la ciberseguridad.

4. Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

4.1. Pentesting ético:

Es un proceso controlado y autorizado en el cual se evalúa la seguridad de sistemas, redes y aplicaciones al simular ataques reales que podrían ser llevados a cabo por ciberdelincuentes. Con este se identifican y explotan vulnerabilidades de forma segura, documentarlas y proponer soluciones para mitigar riesgos antes de que sean aprovechados por atacantes maliciosos.

4.1.1. Características principales:

4.1.2. Autorizado:

Se realiza con el consentimiento del propietario del sistema o la organización involucrada.

4.1.3. Controlado:

Se lleva a cabo siguiendo procedimientos establecidos para evitar daños no deseados al entorno evaluado.

4.1.4. Proactivo:

Ayuda a detectar debilidades antes de que sean explotadas.

4.1.5. Orientado a la mejora:

No solo se identifican vulnerabilidades, sino que se brindan recomendaciones para solucionarlas.

4.1.6. Etapas de un Pentesting Ético:

4.1.7. Reconocimiento:

Recolectar datos importantes para el atacante, como IPs, nombres de dominio, y servicios disponibles.

4.1.8. Escaneo:

Identificar puertos abiertos, servicios en ejecución y versiones del software.

4.1.9. Enumeración:

Obtener detalles más profundos, como usuarios, directorios, o configuraciones específicas.

4.1.10. Explotación:

Intentar aprovechar vulnerabilidades detectadas para acceder al sistema.

4.1.11. Post-explotación:

Evaluar el impacto, como la escalación de privilegios o el acceso a datos sensibles.

4.1.12. Reporte:

Documentar los hallazgos, sus implicaciones y las recomendaciones de seguridad.

figura 1Etapas Pentesting

4.1.13. Importancia del Pentesting Ético:

Identificar vulnerabilidades críticas antes de que sean explotadas, cumplir con estándares de seguridad como PCI-DSS, ISO 27001 o NIST, optimizar la seguridad de la organización al identificar brechas en procesos, tecnologías y personal, generar confianza con clientes y partes interesadas al demostrar un compromiso con la seguridad.

4.1.14. Las herramientas utilizadas para las etapas de pentesting:

Reconocer los elementos físicos y lógicos, que permitan tener un primer contacto con el objetivo, para ello usamos la herramienta nmap, la cual permite identificar las vulnerabilidades del sistema.

4.1.15. Trabajando con nmap, buscando puertos abiertos y servicios instalados en estos, además de sistema operativo.

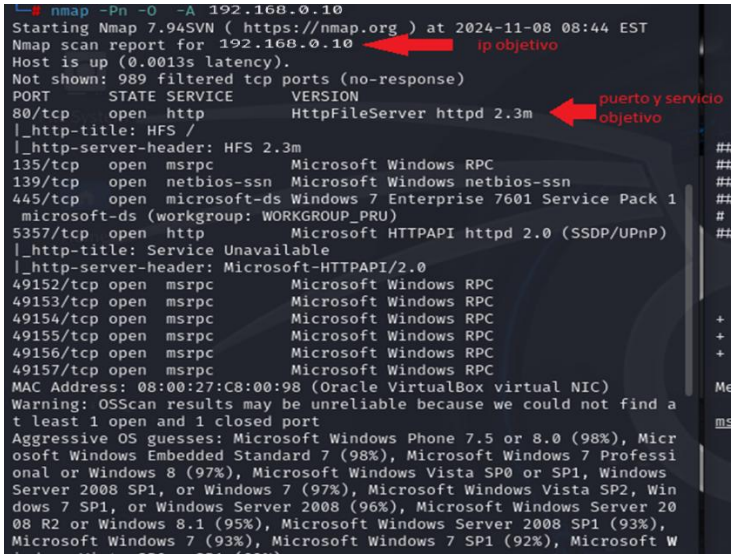

figura 2 escaneo del sistema con nmap

Este comando buscará servicios en la dirección IP 192.168.0.10, tratará de identificar el sistema operativo y la versión de los servicios que están activos, y usará scripts para obtener información adicional (como posibles vulnerabilidades).

Este tipo de escaneo es útil en la fase de reconocimiento de una prueba de penetración o auditoría de seguridad.

4.1.16. Metsploit:

Plataforma de software libre o GPL, manipulado en pruebas de penetración y auditorías de seguridad. Está diseñado para detectar, explotar y validar vulnerabilidades en sistemas y redes. Permite simular ciberataques en un entorno controlado.

4.1.17. Características y Funcionalidades de Metasploit:

4.1.18. Explotación de Vulnerabilidades:

Tiene módulos de explotación que permiten aprovechar las vulnerabilidades de sistemas para obtener acceso, probar configuraciones de seguridad, o simular ciberataques.

4.1.19. Cargas Útiles (Payloads):

Utiliza payloads, como *Meterpreter*, que permite realizar acciones dentro de un sistema después de una explotación exitosa. Meterpreter es un shell interactivo avanzado que permite ejecutar comandos en la máquina objetivo.

4.1.20. Módulos de Escaneo y Exploración:

Cuenta con módulos que pueden hacer reconocimientos y escaneos de red, como el escaneo de puertos y la detección de servicios, para identificar potenciales vulnerabilidades en el sistema.

4.1.21. Escalación de Privilegios:

Incluye herramientas para intentar elevar los privilegios del usuario comprometido, como los intentos de getsystem, lo cual intenta obtener permisos administrativos.

Herramientas de Post-Explotación: Después de comprometer un sistema, Metasploit permite realizar tareas de post-explotación como descargar archivos, realizar movimientos laterales, mantener persistencia, e incluso activar cámaras web o registrar contraseñas.

5. El endurecimiento de la seguridad en una organización requiere un enfoque integral que abarque tecnologías, procesos y personas. A continuación, se mostrarán estrategias claves para mejorar la seguridad de la información.

5.1. Gestión de Acceso y Autenticación

Principio de mínimo privilegios: Usuarios tengan únicamente los permisos necesarios para desempeñar sus funciones.

Autenticación multifactor (MFA): Realizar MFA para permitir ingresar a sistemas críticos.

Gestión de cuentas: Auditar y eliminar cuentas inactivas o duplicadas. Usar contraseñas robustas y un gestor de contraseñas.

5.1.1. Endurecimiento de Infraestructura:

Actualizar y parchear sistemas: Mantener software y sistemas operativos actualizados para evitar la explotación de vulnerabilidades conocidas.

Deshabilitar servicios innecesarios: Reducir la superficie de ataque al desactivar servicios o aplicaciones no utilizados.

Configurar firewalls: Implementar reglas estrictas para controlar el tráfico entrante y saliente.

Segmentación de red: Separar las redes críticas de las menos seguras mediante VLANs y firewalls.

5.1.2. Monitoreo y Respuesta a Incidentes

Implementación de SIEM: Monitoreo en tiempo real y crear alertas ante comportamientos sospechosos.

Logs centralizados: Centralizar los registros de eventos y establecer retención de datos adecuada.

5.1.3. Planes de respuesta a incidentes (IRP):

implementar y tratar plan para responder a incidentes de seguridad.

5.1.4. Protección de Datos

5.1.4.1. Cifrado de datos:

Cifrar datos en tránsito (SSL/TLS) y en reposo.

Usar discos duros y bases de datos cifradas.

Clasificación de datos:

Identificar datos sensibles y clasificarlos según su nivel de confidencialidad.

Implementar controles más estrictos para información crítica.

Copia de seguridad (backups): Realizar copias de seguridad regulares y verificar su integridad.

6. Controles Físicos

6.1. Acceso restringido: Asegurar áreas críticas mediante tarjetas de acceso, biometría o claves.

6.1.1. Supervisión física:

Usar cámaras de seguridad y vigilancia en áreas sensibles.

6.1.2. Pruebas Regulares de Seguridad

6.1.2.1. Pruebas de penetración:

Realizar pentests para identificar vulnerabilidades técnicas.

6.1.2.2. Auditorías de cumplimiento:

Evalúar regularmente la adherencia a regulaciones y estándares de seguridad (ISO 27001, NIST, etc.).

7. Adopción de Normas y Buenas Prácticas

7.1. Frameworks de seguridad:

Implementar estándares como ISO 27001, NIST CSF o CIS Controls.

Usar herramientas como OWASP para evaluar la seguridad de aplicaciones web.

7.1.1. Gestión de riesgos:

Identificar, analizar y mitigar riesgos en toda la organización. Fortalecer la seguridad no es un evento único, sino un asunto incesante que solicita compromiso organizacional, una inversión adecuada y una combinación de medidas técnicas, operativas y humanas. El éxito radica en adoptar un enfoque proactivo en lugar de reactivo.

8. VirtualBox:

Es el software de virtualización utilizado para crear y gestionar las máquinas virtuales. Con VirtualBox, se pueden ejecutar varios sistemas operativos simultáneamente en una sola máquina física, facilitando pruebas sin comprometer el sistema principal.

figura 3 Máquina virtual

9. Máquina virtual con Kali Linux:

Sistema operativo: Kali Linux, distribución de Linux 2024 específicamente diseñada para pruebas de penetración y análisis de seguridad. Kali Linux contiene herramientas como Metasploit, Nmap, y otros programas de pentesting que permiten identificar, analizar y explotar vulnerabilidades en sistemas objetivos.

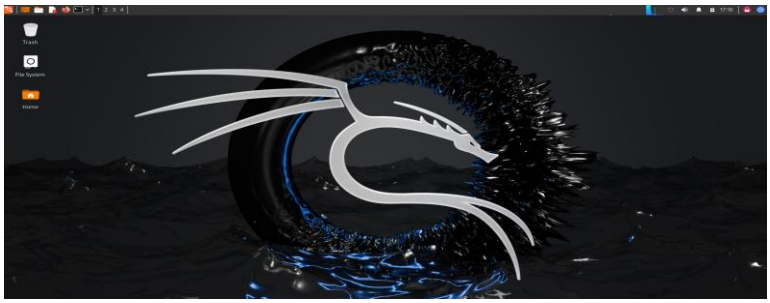

figura 4 SO Kali Linux

9.1. Máquina virtual con Windows 7:

figura 5 SO Windows 7

Sistema operativo: Windows 7, que representa el sistema objetivo en esta prueba de vulnerabilidad.

10. Uso de la Base de Datos CVE:

Catálogo público de vulnerabilidades conocidas en software y hardware.

10.1. Cómo implementarlo:

Monitorear regularmente el sitio oficial de CVE.

Implementar sistemas de gestión de parches para abordar rápidamente las vulnerabilidades críticas.

Priorizar las vulnerabilidades según su puntuación en CVSS (Common Vulnerability Scoring System).

Si un CVE relevante para la infraestructura aparece (como CVE-2017-0144, relacionado con EternalBlue), aplicar el parche correspondiente de inmediato.

10.1.1. Aplicación de las Normas OWASP

Un conjunto de estándares de seguridad para aplicaciones web y software.

10.1.2. OWASP Top 10:

Se enfoca en mitigar las vulnerabilidades más comunes, como inyección SQL, autenticación rota, o exposición de datos sensibles.

10.1.3. Herramientas útiles:

OWASP ZAP (Zed Attack Proxy): Para pruebas de seguridad mecanizadas en aplicaciones web.

10.1.4. Cheatsheets OWASP:

Guías prácticas para desarrolladores sobre seguridad.

10.1.5. Cómo implementarlo:

Realizar auditorías de seguridad periódicas para cumplir con OWASP.

Adoptar principios de Secure Coding en el desarrollo de software.

11. Adopción de Normas Internacionales

11.1. ISO/IEC 27001:

Marco global para implementar sistemas de gestión de la seguridad de la información (SGSI).

Incluye la gestión de riesgos, políticas de acceso y protección de datos.

11.1.1. NIST Cybersecurity Framework:

Un marco adoptado ampliamente, que incluye cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar.

Ideal para organizaciones que deseen estructurar su programa de seguridad.

Uso de Herramientas de Seguridad Automatizadas

11.1.2. Escáneres de Vulnerabilidades:

Nessus, Qualys o OpenVAS: Para identificar vulnerabilidades en servidores, aplicaciones y redes.

12. Análisis de tráfico y detección de intrusos:

12.1. Wireshark:

Para análisis de paquetes.

12.2. Snort o Suricata:

Para detección de intrusiones (IDS).

Gestión de Identidades y Accesos (IAM):

Implementa herramientas como Okta o Microsoft Azure AD.

13. Adopción de Buenas Prácticas

13.1. CIS Controls:

Un conjunto de 18 controles prioritarios para mitigar riesgos comunes, como la gestión de inventario, defensa perimetral y monitoreo continuo.

13.2. Zero Trust Architecture:

No confíar en ningún usuario o dispositivo por defecto; verificar siempre su identidad y acceso.

13.2.1. Principios DevSecOps:

Integrar la seguridad desde el desarrollo hasta la operación.

14. Monitoreo y Respuesta

14.1. SIEM (Security Information and Event Management):

Usar herramientas como Splunk, Elastic Security, o QRadar para monitorear eventos de seguridad en tiempo real.

15. Respuesta a incidentes:

15.1. Diseñar un plan de respuesta a incidentes (IRP) que incluya roles claros y un protocolo para contener, erradicar y recuperar de incidentes.

15.1.1. Pruebas regulares:

Realizar simulaciones de ataques (Red Team/Blue Team) y revisar la preparación ante incidentes.

Formación y Concienciación

15.1.2. Entrenamiento continuo:

Formar al personal en detección de phishing, uso seguro de contraseñas, y políticas de uso de dispositivos.

15.1.3. Certificaciones en ciberseguridad:

16. Considerar capacitarce o capacitar al equipo en estándares globales como CEH, CompTIA Security+, o CISSP.

16.1. Fortalecimiento de Infraestructura

16.1.1. Cifrado fuerte:

Implementar TLS 1.2 o superior para proteger datos en tránsito.

Usar soluciones de cifrado para datos en reposo, como discos cifrados con BitLocker.

16.1.2. Endurecimiento del sistema operativo:

Aplicar configuraciones seguras siguiendo guías como las de CIS Benchmarks.

17. Auditorías Regulares

Realizar auditorías internas y externas de seguridad.

Usar herramientas de evaluación de cumplimiento normativo.

Adoptar las estrategias indicadas anteriormente ayudara a proteger la organización de manera integral frente a ataques internos o externos.

Conclusiones

La protección de sistemas y datos no recae exclusivamente en los departamentos de TI. Cada miembro de una organización, desde el personal operativo hasta los directivos, juega un papel crucial en la implementación de buenas prácticas de seguridad.

Las amenazas cibernéticas evolucionan constantemente. Por ello, se requiere un enfoque proactivo basado en análisis de riesgos, pruebas de penetración periódicas y monitoreo continuo.

Cumplir con estándares internacionales como ISO/IEC 27001 o NIST Cybersecurity Framework no solo protege los sistemas, sino que también genera confianza entre clientes, socios y partes interesadas.

Las herramientas y tecnologías, por avanzadas que sean, no bastan si no están respaldadas por una estrategia clara de gestión de riesgos y respuesta a incidentes.

La ciberseguridad no se logra de manera definitiva, sino que requiere ajustes y actualizaciones constantes frente a nuevas vulnerabilidades y amenazas.

Los equipos internos y externos deben colaborar para compartir conocimientos, recursos y experiencias, lo que permite una defensa más sólida.

Si bien la tecnología avanzada habilita nuevas defensas, también crea vectores de ataque más sofisticados.

Todo conocimiento aplicado en ciberseguridad debe regirse por principios éticos y legales para garantizar su impacto positivo.

Bibliografía

- *Políticas de Privacidad y Condiciones de Uso - PolÃticas de Privacidad y Condiciones de Uso*. (s.f.). MINTIC Colombia. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

- **Cita en el texto:**(Políticas de Privacidad y Condiciones de Uso - PolÃticas de Privacidad y Condiciones de Uso, s.f.)

- *Securing the Network: A Red and Blue Cybersecurity Competition Case Study*. (s.f.). MDPI. https://www.mdpi.com/2078-2489/14/11/587

- **Cita en el texto:**(Securing the Network: A Red and Blue Cybersecurity Competition Case Study, s.f.).

- APLICATIVO PARA ESCANEO DE RED Y VULNERABILIDAD Y AUTOGENERACIÓN DE INFORMES DE AUDITORIA. (s.f.). BURJCDigital. https://burjcdigital.urjc.es/handle/10115/34510

- Effective penetration testing with Metasploit framework and methodologies. (s.f.). IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7028682

- Tabatabaei, F., & Wells, D. (2016, 15 de octubre). OSINT in the Context of Cyber-Security. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-319-47671-1_14

- Vulnerabilities Mapping based on OWASP-SANS: a Survey for Static Application Security Testing (SAST). (s.f.). arXiv.org. https://arxiv.org/abs/2004.03216

- Blue team red team approach to hardware trust assessment. (s.f.). IEEE Xplore. https://ieeexplore.ieee.org/document/6081410
- CIS Benchmarks™. (s.f.). CIS. https://www.cisecurity.org/cis-benchmarks
- (s.f.). CCN-CERT - Inicio. https://www.ccn-cert.cni.es/es/pdf/guias/series-ccnstic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-enipv6/file?format=html
- Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield – IJSREM. (s.f.). IJSREM – International Journal of Scientific Research in Engineering and Management. https://ijsrem.com/download/red-teaming-vs-blue-teaming-acomparative-analysis-of-cybersecurity-strategies-in-the-digital-battlefield/ (s.f.). https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tussistemas
- Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. (s.f.). Revista. Seguridad |. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantesexplotando-una-vulnerabilidad-con-metasploit-fra

Anexos

- **Video sustentación informe técnico https://1drv.ms/v/c/5fcdd22634d25ad8/EQPfbSIT525FmXie8_rkYBABTLpMletPAuTvmJsP2NBTPA?e=YHK3Am**