MEDIDAS DE PREVENCIÓN Y DETECCIÓN DE INTRUSOS

OSCAR DIAZ AMARO

M.C. Ana Claudia Zenteno

Benemérita Universidad Autónoma de Puebla | Av San Claudio s/n, Cd Universitaria, La Hacienda, 72592 Heroica Puebla de Zaragoza, Pue.

Tabla de contenido

INDICE DE FIGURAS

1. Introducción

En la era digital actual, la seguridad cibernética se ha convertido en un aspecto indispensable para la protección de datos y la continuidad de las operaciones empresariales. La prevención y detección de intrusos en redes y sistemas informáticos son fundamentales para garantizar la integridad, confidencialidad y disponibilidad de la información frente a las crecientes amenazas cibernéticas.

En México, al igual que en muchas partes del mundo, el aumento exponencial de ciberataques ha generado una preocupación generalizada entre las empresas y organizaciones. Se estima que, solo en el último año, se detectaron cerca de 80,000 millones de ciberataques dirigidos a empresas que carecen de estrategias efectivas para defenderse de estas amenazas. Estos ataques no solo buscan afectar, alterar o destruir los activos de las empresas, sino que también impactan negativamente en sus operaciones y relaciones con diversos grupos de interés.

Cuando nos referimos a un ciberataque, hablamos de acciones ofensivas y perjudiciales para los sistemas de información de personas, empresas o entidades gubernamentales. Estos sistemas incluyen redes informáticas, bases de datos y todos los activos que almacenan datos e información confidencial y de valor para la organización.

A pesar de los avances en tecnología de seguridad, los sistemas y redes informáticas siguen siendo vulnerables a intrusos malintencionados. Factores como la sofisticación de los ataques, la falta de conciencia de seguridad, la complejidad de las infraestructuras de red, las limitaciones de las soluciones tradicionales y la escasez de talento en seguridad cibernética agravan esta situación.

En este contexto, surge la necesidad imperante de abordar este problema de manera integral. Esta investigación se propone evaluar la efectividad y eficiencia de las medidas de prevención y detección de intrusos en redes y sistemas informáticos. A través de objetivos específicos, se buscará identificar las deficiencias actuales en la seguridad cibernética, analizar las tendencias y evolución de las amenazas cibernéticas, y proponer soluciones innovadoras para mejorar la protección de las organizaciones frente a estas amenazas emergentes.

2. Planteamiento del problema

La prevención y deteccion de intrusos en redes es impresindible hoy en día para las empresas, tan solo en México se han detectado cerca de 80,000 millones de ciberataques a empresas que no cuentan con estrategias efectivas para defenderse de los ataques, los ciberdelicuentes al cometer estos ataques no solo buscan afectar, alterar o destruir a las empresas o personas, si no también impactar negativamente en sus operaciones y las relaciones d elas empresas y/o personas con sus diversos grupos de interes.

Cuando hablamos de un ciberataque nos referimos a las acciones ofensivas y perjudicales para los sistemas de información de personas, empresas o entidades gubernamentales, Estos sistemas pueden ser las redes informáticas, las bases de datos y todos los activos que almacenen datos e información confidencial y de valor de la organización.

A pesar de los avances en tecnología de seguridad, los sistemas y redes informáticas siguen siendo vulnerables a intrusos malintencionados que buscan acceder de manera no autorizada, comprometer la

integridad de los datos o interrumpir las operaciones normales. Este problema se agrava debido a varios factores:

1. Sofisticación de los ataques: Los intrusos emplean técnicas cada vez más avanzadas y sofisticadas, como ataques de día cero, ingeniería social y ataques dirigidos, lo que dificulta su detección y prevención.

2. Falta de conciencia de seguridad: Muchas organizaciones carecen de una cultura de seguridad sólida, lo que resulta en una falta de conciencia entre los empleados sobre las mejores prácticas de seguridad cibernética y la importancia de adherirse a las políticas de seguridad establecidas.

3. Complejidad de las infraestructuras de red: Con la adopción de tecnologías como la nube, el IoT (Internet de las cosas) y la movilidad, las infraestructuras de red se vuelven más complejas, lo que dificulta la implementación y gestión efectiva de medidas de seguridad.

4. Limitaciones de las soluciones tradicionales: Las soluciones de seguridad tradicionales, como los firewalls y los sistemas de detección de intrusiones (IDS), pueden no ser adecuadas para hacer frente a las amenazas cibernéticas modernas, especialmente aquellas que evolucionan rápidamente.

5. Escasez de talento en seguridad cibernética: Existe una escasez de profesionales capacitados en seguridad cibernética, lo que dificulta a las organizaciones implementar y mantener medidas de seguridad efectivas.

3. Justificación

La necesidad de abordar el problema de la prevención y detección de intrusos en redes y sistemas informáticos se fundamenta en varios aspectos críticos que reflejan la urgencia de tomar medidas efectivas:

1. Magnitud de los ataques: La cantidad alarmante de ciberataques registrados en México es un indicativo claro de la escala del problema. Estos ataques van en aumento y abarcan una amplia gama de sectores industriales y organizaciones de todos los tamaños. La cifra de 80,000 millones de ciberataques es alarmante y subraya la urgencia de implementar medidas efectivas para proteger los activos de información crítica de las empresas.

2. Impacto en las operaciones: Los ciberataques no solo representan una amenaza para la seguridad de los datos, sino que también tienen un impacto significativo en las operaciones normales de las empresas. Interrumpen los procesos comerciales, causan pérdidas financieras debido a tiempos de inactividad y costos de recuperación, y dañan la reputación de la organización ante sus clientes y socios comerciales.

3. Vulnerabilidades persistentes: A pesar de los avances en tecnología de seguridad, las redes informáticas siguen siendo vulnerables a intrusos malintencionados. La sofisticación de los ataques, que incluyen técnicas como los ataques de día cero y la ingeniería social, representa un desafío constante para la seguridad cibernética. Además, la falta de conciencia de seguridad en muchas organizaciones contribuye a la explotación de estas vulnerabilidades.

4. Complejidad de las infraestructuras de red: La adopción de tecnologías emergentes como la computación en la nube y el Internet de las cosas (IoT) ha aumentado la complejidad de las infraestructuras de red. La expansión de la superficie de ataque y la diversidad de dispositivos conectados plantean desafíos adicionales para la implementación y gestión efectiva de medidas de seguridad.

5. Limitaciones de las soluciones tradicionales: Las soluciones de seguridad tradicionales, como los firewalls y los sistemas de detección de intrusiones (IDS), pueden no ser suficientes para hacer frente a las amenazas cibernéticas modernas. Los intrusos están evolucionando constantemente y emplean tácticas cada vez más sofisticadas, lo que destaca la necesidad de adoptar enfoques más avanzados y adaptativos para la protección de redes y sistemas informáticos.

6. Escasez de talento en seguridad cibernética: Existe una escasez significativa de profesionales capacitados en seguridad cibernética, lo que dificulta a las organizaciones implementar y mantener medidas de seguridad efectivas. La demanda de expertos en seguridad supera con creces la oferta, lo que agrava aún más el problema y resalta la necesidad urgente de abordar esta brecha de habilidades en el campo de la ciberseguridad.

4. Objetivos

4.1. Objetivo general:

- Evaluar la efectividad y la eficiencia de las medidas de prevención y detección de intrusos en redes y sistemas informáticos, identificando sus limitaciones actuales y proponiendo soluciones innovadoras para mejorar la protección cibernética de las organizaciones frente a las amenazas emergentes.

4.2. Objetivos específicos:

- Evaluar las técnicas de intrusión más recientes y sus métodos de evasión.
- Analizar las deficiencias en las medidas de seguridad existentes.
- Identificar las mejores prácticas y tecnologías emergentes en seguridad cibernética.
- Diseñar un marco integral de seguridad que integre medidas de prevención y detección de intrusos.
- Evaluar la efectividad del marco propuesto mediante pruebas y simulaciones.
- Proponer recomendaciones para la implementación exitosa de las mejoras propuestas en organizaciones reales.

5. Metodología

La seguridad cibernética es un aspecto crucial en el entorno digital actual, donde la protección de redes y sistemas de información se vuelve cada vez más indispensable debido al aumento constante de amenazas y ataques informáticos. Las medidas de prevención y detección de intrusos juegan un papel fundamental en la protección de la integridad, confidencialidad y disponibilidad de los datos. Esta investigación profundizará en las medidas más relevantes en este campo y analizará su efectividad y aplicación práctica.

1. **Firewalls:**
   - Prevención: Los firewalls son sistemas de seguridad que controlan y filtran el tráfico de red según reglas predefinidas. Ayudan a prevenir intrusiones bloqueando el tráfico no autorizado y protegiendo los sistemas de información contra accesos no deseados.
   - Detección: Los firewalls pueden detectar intentos de acceso no autorizado a través de registros de eventos y alertas generadas por patrones de tráfico sospechoso.

2. **Sistemas de Detección de Intrusos (IDS):**
   - Prevención: Los IDS monitorean el tráfico de red o las actividades del sistema en busca de comportamientos anómalos que puedan indicar intrusiones. Pueden detectar y responder a ataques en tiempo real.
   - Detección: Los IDS generan alertas cuando detectan actividades sospechosas, como intentos de intrusión, escaneos de puertos o comportamientos inusuales en la red.

3. **Sistemas de Prevención de Intrusos (IPS):**
   - Prevención: Los IPS van más allá de la detección y pueden bloquear o mitigar activamente amenazas en tiempo real. Utilizan reglas predefinidas para bloquear tráfico malicioso o realizar acciones correctivas automáticamente.
   - Detección: Al igual que los IDS, los IPS pueden detectar y generar alertas sobre actividades sospechosas, pero también pueden tomar medidas proactivas para prevenir intrusiones.

4. **Análisis de Comportamiento de Red (NBA):**
   - Prevención: NBA utiliza algoritmos avanzados para analizar el comportamiento normal de la red y detectar desviaciones significativas que puedan indicar actividades maliciosas.
   - Detección: Al identificar anomalías en el comportamiento de la red, NBA puede generar alertas para que los administradores de seguridad investiguen posibles intrusiones.

5. **Sistema de Gestión de Eventos e Información de Seguridad (SIEM):**
   - Prevención: Los SIEM recopilan, correlacionan y analizan registros de eventos de seguridad de múltiples fuentes para proporcionar una visión integral de la postura de seguridad de una organización.
   - Detección: Los SIEM pueden detectar patrones y tendencias en los registros de eventos que pueden indicar intrusiones o actividades maliciosas. Además, pueden generar alertas y notificaciones para acciones de respuesta.

6. **Autenticación Multifactor (MFA):**
   - Prevención: MFA añade una capa adicional de seguridad al requerir múltiples formas de autenticación para verificar la identidad de un usuario antes de permitir el acceso a sistemas o redes.
   - Detección: Si un intruso intenta acceder a un sistema utilizando credenciales robadas, MFA puede detectar la actividad inusual y requerir verificaciones adicionales antes de conceder el acceso.

7. **Actualizaciones y Parches de Seguridad:**
   - Prevención: Mantener actualizados los sistemas y aplicar parches de seguridad regularmente ayuda a cerrar vulnerabilidades conocidas y a prevenir la explotación por parte de intrusos.
   - Detección: Los sistemas de gestión de parches pueden detectar y notificar la falta de actualizaciones o parches críticos, lo que puede indicar un riesgo potencial de seguridad.

8. **Educación y Concienciación del Usuario:**
   - Prevención: Capacitar a los usuarios sobre las mejores prácticas de seguridad cibernética, como la creación de contraseñas seguras y la identificación de correos electrónicos de phishing, puede ayudar a prevenir intrusiones causadas por errores humanos.
   - Detección: Los usuarios educados pueden ser más conscientes de las señales de posibles amenazas y pueden informar rápidamente a los equipos de seguridad sobre actividades sospechosas.

6. Mapa general de herramientas y metodologías

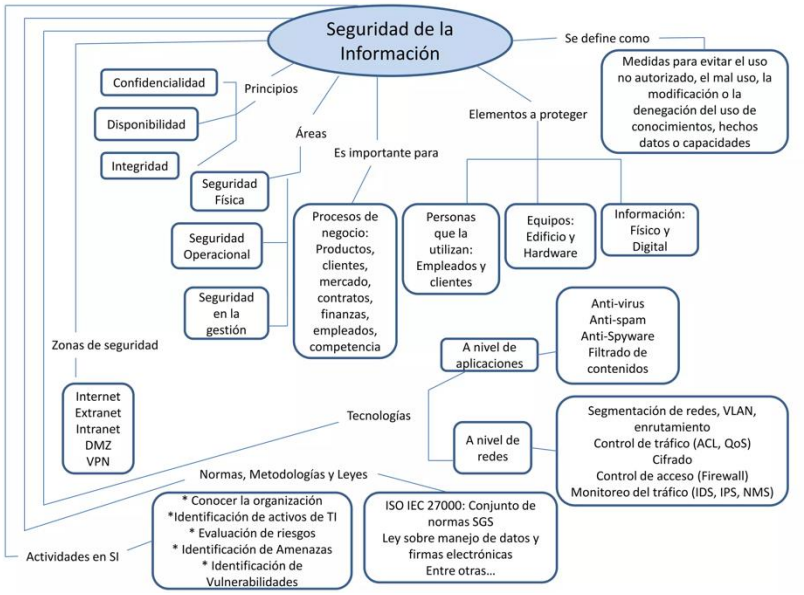

Figura 1: Mapa conceptual sobre Seguridad de la Información. (2015, November 22). [Slide show]. SlideShare. https://es.slideshare.net/jmarquez23/mapa-conceptual-sobre-seguridad-de-la-informacin

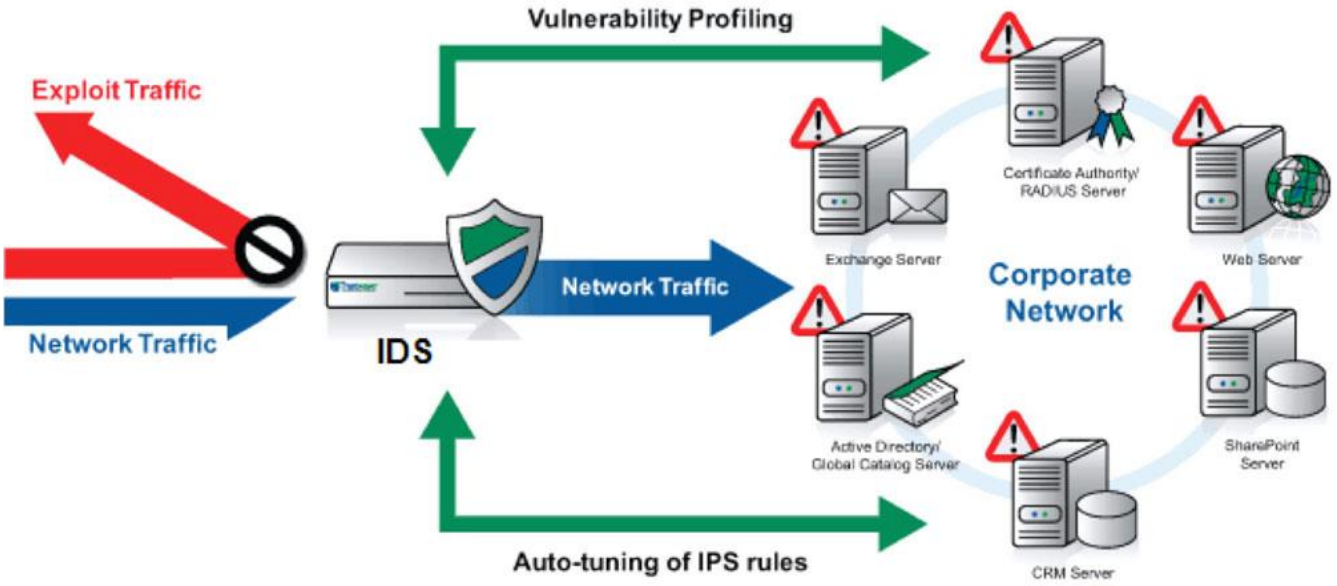

Figura 2: Centenoseo LLC. (2024, February 24). Sistema de deteccion de intrusos y prevencion de intrusos (IDS/IPS). CentenoSeo. https://centenoseo.com/ciberseguridad/ids-ips/

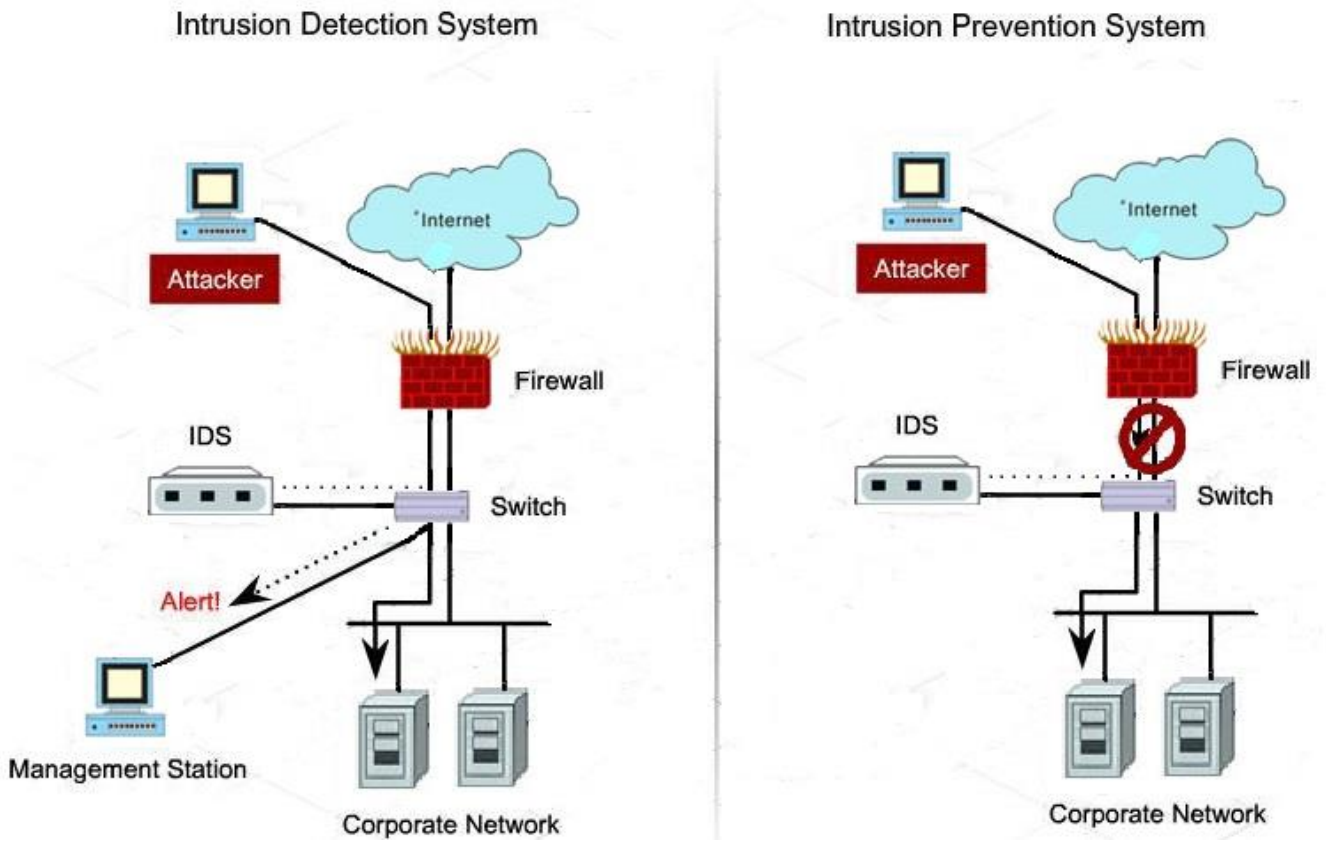

Figura 3: colaboradores de Wikipedia. (2024, February 14). Sistema de prevención de intrusos. Wikipedia, La Enciclopedia Libre. https://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos

Figura 4: ZonaIT. (n.d.). Proteger mi empresa de intrusiones - Consultoría & Consultores. https://consultoria-consultores.es/articulos/articulo-consultoria-proteger-mi-empresa-de-intrusiones/

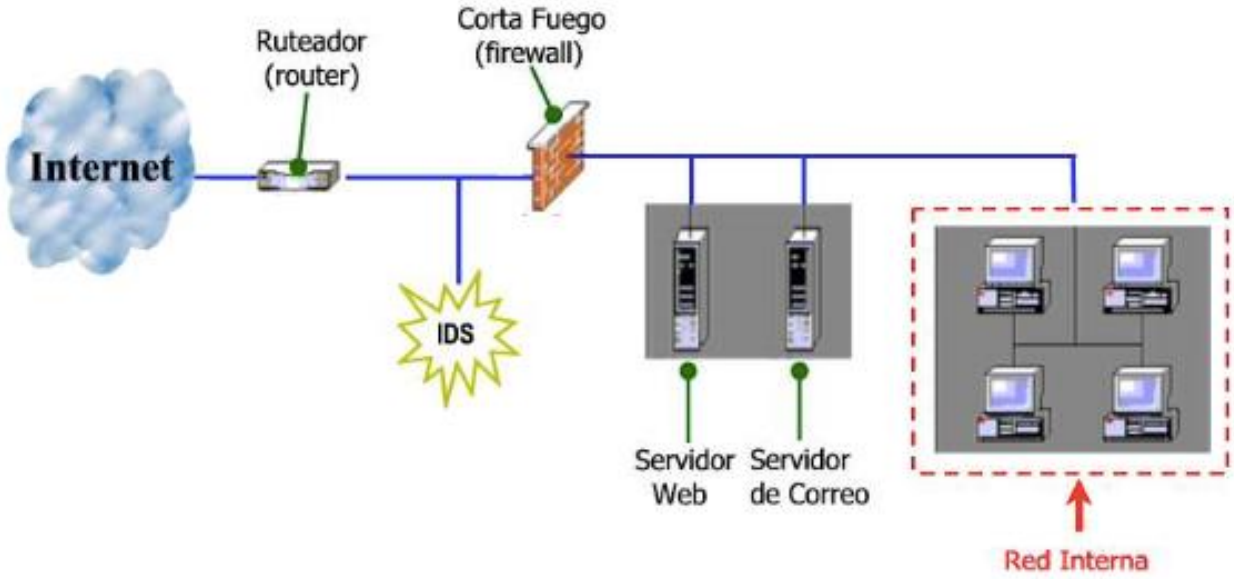

Figura 5: Red con IDS simple Fuente: Carlos Jojoa3

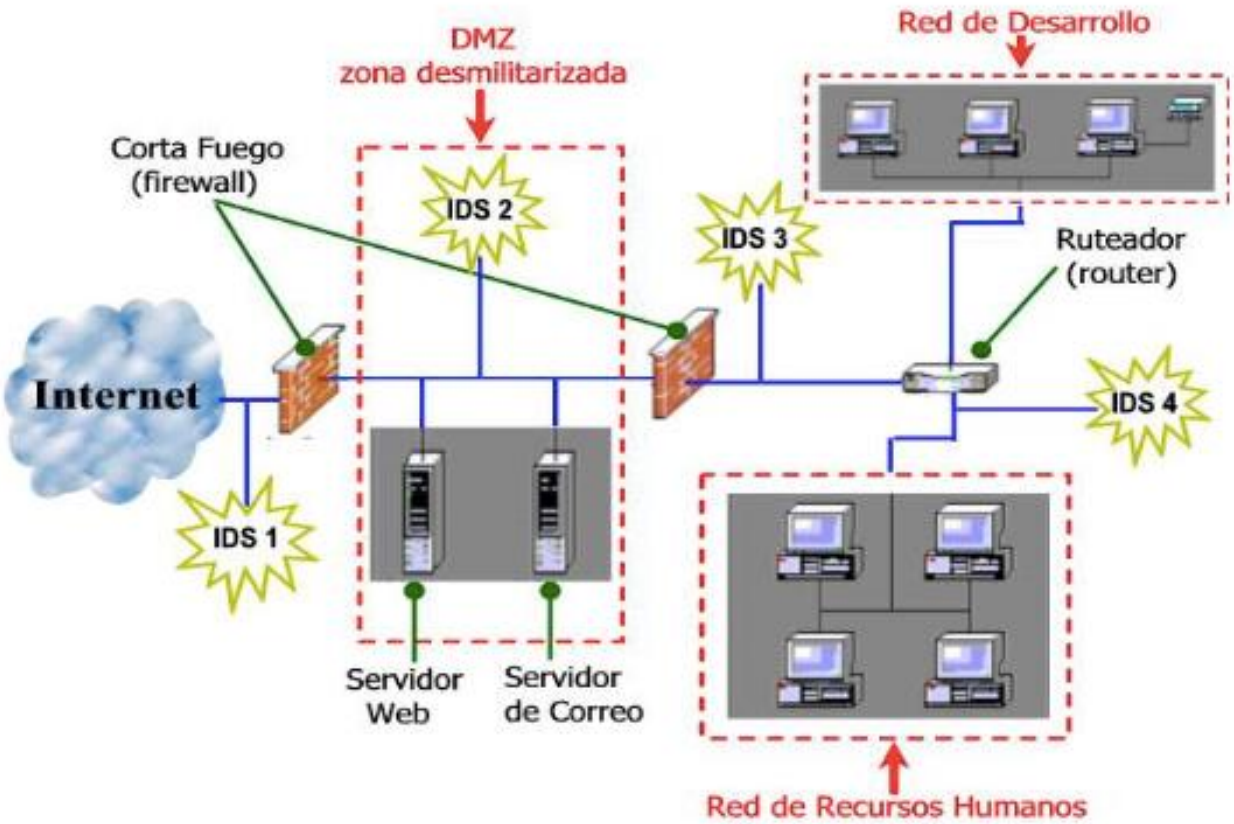

Figura 6: Red completa con IDS Fuente: Carlos Jojoa[4]

7. Alcances o metas

Los alcances o metas de esta investigación son los siguientes:

1. Análisis de las tecnologías y metodologías actuales utilizadas en la prevención y detección de intrusos en redes y sistemas informáticos.
2. Evaluación de la efectividad de las medidas de seguridad implementadas en organizaciones de diferentes sectores industriales.

3. Identificación de las vulnerabilidades más comunes en redes y sistemas informáticos que pueden ser explotadas por intrusos malintencionados.

4. Investigación sobre las tendencias y evolución de las amenazas cibernéticas para comprender los desafíos actuales en la seguridad informática.

5. Análisis de la legislación y regulaciones relacionadas con la protección de datos y la seguridad cibernética para asegurar el cumplimiento normativo en las soluciones propuestas.

6. Desarrollar un marco de referencia integral para la evaluación de la seguridad cibernética en organizaciones.

7. Proporcionar recomendaciones específicas para mejorar la prevención y detección de intrusos en redes y sistemas informáticos.

8. Proponer soluciones tecnológicas innovadoras que aborden las vulnerabilidades identificadas y fortalezcan la seguridad de la información.

9. Realizar pruebas y simulaciones para validar la efectividad de las medidas de seguridad propuestas en entornos controlados.

8. Conclusión

En un entorno digital cada vez más interconectado y dependiente de la tecnología, la prevención y detección de intrusos en redes y sistemas informáticos se han vuelto aspectos críticos para la seguridad cibernética de las organizaciones. A lo largo de esta investigación, hemos explorado la importancia de estas medidas en la protección de la integridad, confidencialidad y disponibilidad de la información frente a las crecientes amenazas cibernéticas.

Hemos evidenciado que, a pesar de los avances en tecnología de seguridad, las organizaciones siguen enfrentando una serie de obstáculos que dificultan la protección efectiva de sus activos de información. Desde la magnitud alarmante de los ciberataques hasta la persistencia de vulnerabilidades y la escasez de talento en seguridad cibernética, los desafíos son numerosos y requieren una atención prioritaria.

No obstante, esta investigación también ha revelado oportunidades significativas para mejorar la seguridad cibernética mediante la adopción de enfoques más avanzados y adaptativos. La evaluación de tecnologías emergentes, el análisis de tendencias en ciberataques y la propuesta de soluciones innovadoras son pasos fundamentales para fortalecer la resiliencia de las organizaciones ante las amenazas digitales.

Es crucial reconocer que la seguridad cibernética es un desafío continuo que requiere un enfoque proactivo y colaborativo. Solo mediante el compromiso conjunto de la comunidad académica, la industria y los organismos reguladores será posible hacer frente a las crecientes amenazas cibernéticas y garantizar un entorno digital seguro y confiable para todos.

En última instancia, esta investigación sienta las bases para futuros avances en el campo de la seguridad cibernética. Las recomendaciones propuestas y las lecciones aprendidas pueden guiar a las organizaciones en la implementación efectiva de medidas de prevención y detección de intrusos, contribuyendo así a la protección de sus activos de información y la continuidad de sus operaciones comerciales.

9. Glosario

1. Seguridad Cibernética: Campo de estudio y práctica que se centra en proteger sistemas informáticos, redes y datos contra accesos no autorizados, ataques cibernéticos y daños.
2. Prevención de Intrusos: Conjunto de medidas y técnicas diseñadas para evitar que intrusos no autorizados accedan a sistemas informáticos, redes o datos sensibles.
3. Detección de Intrusos: Proceso de identificar y responder a actividades maliciosas o no autorizadas dentro de sistemas informáticos o redes.
4. Ciberataque: Acción ofensiva y perjudicial dirigida a sistemas informáticos, redes o datos, con el objetivo de comprometer su integridad, confidencialidad o disponibilidad.
5. Intruso: Persona o entidad que intenta acceder de manera no autorizada a sistemas informáticos, redes o datos sensibles.
6. Red Informática: Infraestructura compuesta por dispositivos interconectados que permiten la comunicación y el intercambio de datos entre usuarios y sistemas.
7. Sistema de Información: Conjunto de componentes interrelacionados que recopilan, procesan, almacenan y distribuyen datos para apoyar las operaciones de una organización.
8. Ataque de Día Cero: Ataque informático que aprovecha una vulnerabilidad de seguridad recién descubierta y aún no corregida por el fabricante del software.
9. Ingeniería Social: Técnica utilizada por los intrusos para manipular a individuos y obtener información confidencial mediante la persuasión o el engaño.
10. Firewall: Dispositivo o software que controla y filtra el tráfico de red según reglas predefinidas, con el fin de prevenir accesos no autorizados y proteger la red de intrusiones.
11. Sistema de Detección de Intrusos (IDS): Herramienta de seguridad que monitorea el tráfico de red o las actividades del sistema en busca de comportamientos anómalos que puedan indicar intrusiones.
12. Sistema de Prevención de Intrusos (IPS): Dispositivo de seguridad que va más allá de la detección y puede bloquear o mitigar activamente amenazas en tiempo real.
13. Análisis de Comportamiento de Red (NBA): Método que utiliza algoritmos avanzados para analizar el comportamiento normal de la red y detectar desviaciones significativas que puedan indicar actividades maliciosas.
14. Sistema de Gestión de Eventos e Información de Seguridad (SIEM): Plataforma que recopila, correlaciona y analiza registros de eventos de seguridad de múltiples fuentes para proporcionar una visión integral de la postura de seguridad de una organización.
15. Autenticación Multifactor (MFA): Método de autenticación que requiere múltiples formas de verificación de identidad antes de permitir el acceso a sistemas o datos sensibles.
16. Actualizaciones y Parches de Seguridad: Proceso de aplicar correcciones y mejoras a sistemas y software para cerrar vulnerabilidades conocidas y prevenir la explotación por parte de intrusos.
17. Educación y Concienciación del Usuario: Práctica de capacitar a los usuarios sobre las mejores prácticas de seguridad cibernética y fomentar una cultura de seguridad en una organización.

10. Bibliografía

- De DocuSign, C. (2022, December 28). Conoce los 7 mejores métodos de seguridad informática para tu empresa. DocuSign. https://www.docusign.com/es-mx/blog/seguridad-informatica
- Prevención y detección de intrusiones. (n.d.). https://www.fortra.com/es/soluciones/ciberseguridad/infraestructura/deteccion-prevencion-intrusiones
- Seguridad informatica. (n.d.). https://www.uacj.mx/CGTI/CDTE/JPM/Documents/IIT/infseguridad/U6-2.html
- ¿Qué es un sistema de detección de intrusiones (IDS)?| IBM. (n.d.). https://www.ibm.com/mx-es/topics/intrusion-detection-system
- Joel, C. V. (2018, June 18). Definición de un sistema de detección y prevención de intrusos en una red para el control de vulnerabilidades usando software libre. https://repository.unad.edu.co/handle/10596/40138
- Jiménez, M. M. (n.d.). Ataques cibernéticos: causas, tipos y consecuencias. https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias