Herramienta de Ciberseguridad para la auditoría de una línea base de buenas prácticas de seguridad informática en Pymes a través de un prototipo funcional de Chatbot que ofrezca recomendaciones para la mitigación de vulnerabilidades en servidores Windows y Linux

John Jairo Giraldo Ramírez

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Medellín, Colombia
2022

Herramienta de Ciberseguridad para la auditoría de una línea base de buenas prácticas de seguridad informática en Pymes a través de un prototipo funcional de Chatbot que ofrezca recomendaciones para la mitigación de vulnerabilidades en servidores Windows y Linux

John Jairo Giraldo Ramírez

Trabajo de investigación presentado como requisito para optar al título de:
Magister en Seguridad Informática

Director: Msc. Julián Ramírez
Codirector: Msc. Miguel Ángel Roldan

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Medellín, Colombia
2022

Dedicatoria

A mi hermosa madre, siempre elevando las virtudes de sus hijos, a mi esposa Ana María, mis hijos Tomas y Mariana, a quienes les he dedicado menos tiempo durante la realización de este proyecto. Son ellos mi fuente de motivación y la razón para hacer las cosas bien en mi vida.

Agradecimientos

Al ITM, una gran institución dedicada a hacer hombres más capaces, dotada de personas en su mayoría centradas en la construcción de un mejor futuro para nuestra ciudad formando profesionales íntegros.

Resumen

Las amenazas de ciberseguridad son de igual magnitud para grandes empresas y para pequeñas como la Pymes, pero los riesgos y la metodología de prevención/mitigación, no lo son. En el caso de las grandes organizaciones, cuentan con equipos robustos para prevenir y solucionar eventos generados por los delincuentes informáticos, mientras las Pymes por su tamaño y cultura solo tienen un técnico dedicado al manejo de incidentes informáticos. Es por esta razón que se elabora una herramienta de ciberseguridad que brinda recomendaciones por medio de un Chatbot, orientadas al endurecimiento de la seguridad en los servidores Windows y Linux, esto disminuirá la probabilidad de ataques informáticos, mejorará la estabilidad de los servicios prestados por los servidores, ayudando de esta manera al crecimiento de la empresa.

Palabras clave: Auditoría, Chatbot, Ciberseguridad, Mitigación, Pymes, Servidores, Vulnerabilidades.

Abstract

Cybersecurity threats are of the same magnitude for large companies and for small ones such as SMEs, but the risks and the prevention/mitigation methodology are not. Large organizations have robust teams to prevent and solve events generated by computer criminals, while SMEs, due to their size and culture, only have one technician dedicated to handling computer incidents. It is for this reason that a cybersecurity tool is developed that provides recommendations through a Chatbot, aimed at hardening security on Windows and Linux servers, this will reduce the probability of computer attacks, improve the stability of the services provided by the servers, thus helping the growth of the company.

Keywords: Audit, Chatbot, Cybersecurity, Mitigation, SMEs, Servers, Vulnerabilities.

Contenido

Pág.

Índice de gráficas

Índice de tablas

Introducción

El ser humano está encaminado a sobrevivir haciendo cada vez su ambiente más seguro y propicio para el crecimiento, a su vez la necesidad de evolución propicia el cambio de condiciones que derivan en nuevos retos que representan riesgos. De igual manera, en el mundo de las tecnologías, se encuentran una serie de ambientes amenazados por diversos factores que encuentran en las debilidades de algunos ecosistemas, la posibilidad de lucrarse económicamente, manifestar una posición política o solo por mostrar estatus. Esto lo hacen robando cuentas, cifrando información, borrando registros y muchas otras actividades que terminan por hacer más complicado el crecimiento emprendedor o inclusive desaparecer una organización.

Debido a lo anterior, se precisa necesario tomar cartas en el asunto y propiciar, por diferentes métodos un ambiente más seguro en el cual operar, quitarles escenarios de interacción a los delincuentes informáticos, proteger al más débil ante muy bien preparados adversarios. Todo esto equiparando fuerzas, fortaleciendo la defensa y propiciando el crecimiento sin las inclemencias de un mundo hostil proveniente de Internet.

En el día a día de un analista informático, se experimentan o se escuchan por parte de colegas, sobre empresas que fueron permeadas por ataques cibernéticos y diversas vulnerabilidades materializadas. Lo más relevante del tema es que corresponden a infraestructuras, políticas o ajustes mal manejados y que se pudieron haber evitado o mitigado en gran medida. Con el fin de obtener más información sobre vulnerabilidades y su modo de mitigarlas, se emplea la metodología de estudio de caso, en la cual se procede a la configuración de un ambiente controlado en VirtualBox en el cual se instalan varios sistemas operativos Windows y Linux tipo servidor. Este ambiente se asemeja a una infraestructura básica de una empresa de mediano tamaño.

Para el área de las Pymes se maneja un nivel de soporte técnico informático a servidores de bajo nivel, quien opera y administra estas infraestructuras y sus servidores son técnicos básicos sin profundidad en temas especialmente de seguridad, escasos protocolos ni herramientas con soporte profesional. Esto pone en desventaja a este tipo de empresas, ya que el Ciberdelito no discrimina por tamaño de organización a la hora de realizar sus complejos ataques, dejando, a la hora de materializarse, a las Pymes en estado crítico con información cifrada, borrada, alterada o inutilizable. Por su lado, las grandes organizaciones cuentan con modelos de soporte especializado para cada subrama de la seguridad, equipos como el SOC, CCIRT, Mesas de ayudas, analistas preparados y armados con software de prestigiosas casas, además de compleja infraestructura para cada segmento y tipo de amenaza.

Situaciones como las descritas en el párrafo anterior, propician que empresas tipo Pyme con actividades económicas promisorias se vean amenazadas o frenadas en su crecimiento debido a eventos desafortunados para los cuales están expuestas con gran nivel de probabilidad de ocurrencia, algunas veces por desconocimiento, otras, por negligencia en la toma de decisiones que, por austeridad, salen más costosas y hacen difícil el panorama de crecimiento.

Por esta razón se propone la elaboración un Chatbot que brinde recomendaciones de buenas prácticas con el fin de mejorar la seguridad en servidores Windows y Linux, con técnicas avanzadas que se aplican algunas de forma manual, otras automatizadas, además de scripts o programas y que dificultarán la acción de los criminales informáticos, teniendo como resultado servidores más seguros y estables para la continuidad y crecimiento de las operaciones en la empresa. Para ello es necesario recopilar información de diversas fuentes científicas fiables, complementadas con conocimiento propio y algunas referencias tomadas de la web, bases de datos institucionales y trabajos similares elaborados con afinidad a los objetivos del presente trabajo.

Para la elaboración de este proyecto, se establece como objetivo principal "*Diseñar una herramienta de Ciberseguridad que ayude a los técnicos de las PYMES a preparar una auditoría basándose en buenas prácticas de seguridad informática a través de un Chatbot que brindará recomendaciones para endurecer las configuraciones en servidores Windows y/o Linux* además de los siguientes objetivos específicos:

- Caracterizar cuáles son los ataques cibernéticos más ejecutados en servidores con sistemas Windows y Linux.
- Elaborar línea base de buenas prácticas de acuerdo a la caracterización de los ataques debido a las débiles configuraciones más frecuentes.
- Desarrollar un Chatbot para la interacción con el personal técnico de las PYMES.
- Validar la herramienta desarrollada de acuerdo a su funcionalidad, a través de un caso de estudio, prueba de escritorio o simulación.

El resultado final busca ser la mejora en los niveles de seguridad en los servidores y los componentes que lo rodean, poniendo a la altura las configuraciones de un servidor de las Pymes con relación a los servidores configurados por personal experto en el área SOC de empresas de gran magnitud.

1. Estado del Arte

Este apartado contiene el marco teórico, marco conceptual y el marco referencial, orientados a familiarizar al lector con los conceptos técnicos empleados en el medio anteriormente, ahora y los que son tendencia.

1.1 Marco teórico.

De acuerdo a estudios realizados por la Universidad Piloto de Colombia [1], las Pymes no toman en cuenta la magnitud de afectación que puede tener la materialización de una Amenaza Persistente Avanzada, se realizó una encuesta con el fin de determinar si estaban familiarizados con el término, pero la respuesta es simple, no se conoce el término ni la dimensión real del problema. Todo ello a razón de no contar con personal técnico debidamente entrenado para enfrentar amenazas del tipo mencionado, personal con lo que, si cuentan las grandes empresas, quienes tienen robustos equipos tipo SOC, CERT, CCIRT, Mesa de ayuda, analistas e ingenieros especializados en todas las áreas y gran parte de ellos con actividad de 7 x 24.

Según otro estudio reciente en el 2021 y realizado por Google sobre la seguridad cibernética de las pequeñas empresas en España, indica que un 87% de las pequeñas y medianas empresas no cuentan con un sistema de seguridad para los equipos móviles. Por otro lado, también se identificó que el 33% de estas no ejecutan una copia de seguridad o un sistema de respaldo, y solamente el 33% cuenta con un plan de continuidad de negocio [2]. Para complementar las estadísticas, de acuerdo a la Asociación Colombiana de Ingenieros de Sistemas - ACIS, en su encuesta anual de seguridad, estableció que solo el 33% de las empresas tienen una inversión en los temas de monitoreo y gestión de la seguridad, así mismo, se indica que el 48% de las organizaciones, hacen una evaluación al año y el 16% ninguna, un tema preocupante dadas las crecientes amenazas de Ciberseguridad. Establecer un proceso de auditoria o revisión de vulnerabilidades se vuelve fundamental para el apoyo a la industria en sus operaciones para garantizar la continuidad del negocio.

Finalmente, las vulnerabilidades a nivel mundial reportadas, se siguen presentando y evolucionan a través de los años. En el portal CVE del 2021 (figura 1) se registraron 20141 tipos de vulnerabilidades (identificadas o reportadas), siendo este el tercer año consecutivo que se supera con más de 15.000 y se prevé que se seguirá la tendencia. Éste aumento debe ser considerado por las organizaciones como una alerta temprana para validar si dichas vulnerabilidades (dependiendo del sistema o las plataformas tecnológicas que se tengan) pudieran afectar negativamente su negocio en caso de ser explotadas.

A continuación, se relacionan en la Gráfica 1, las vulnerabilidades más frecuentes según el portal CVE Details.

Gráfica 1.

Vulnerabilidades por año según la base de datos de CVE Details.

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	894	177	112	172			2	7		25	16	103			2
2000	1020	257	208	206	1	2	4	20		48	19	139			
2001	1677	403	403	297		7	34	124		83	36	220		2	2
2002	2156	498	553	435	2	41	200	103		127	76	199	2	14	1
2003	1527	381	477	372	2	50	129	60	1	62	69	144		16	5
2004	2451	580	614	408	3	148	291	111	12	145	96	134	5	38	5
2005	4935	838	1627	657	21	604	786	202	15	289	261	221	11	100	14
2006	6610	893	2719	664	91	967	1302	322	8	267	272	184	18	849	30
2007	6520	1101	2601	955	95	706	883	338	14	267	326	242	69	700	45
2008	5632	894	2310	699	128	1101	807	362	7	288	268	188	83	170	76
2009	5736	1035	2185	698	188	963	851	323	9	337	302	223	115	138	738
2010	4653	1102	1714	676	342	520	605	276	8	234	284	238	86	73	1501
2011	4155	1221	1334	734	351	294	470	108	7	197	411	206	58	17	557
2012	5297	1425	1459	833	423	243	759	122	13	344	392	250	166	14	623
2013	5191	1455	1186	853	366	156	650	110	7	352	512	274	123	1	206
2014	7939	1599	1572	841	420	304	1103	204	12	457	2106	239	264	2	403
2015	6504	1793	1830	1084	749	221	784	151	12	577	753	366	248	5	129
2016	6454	2029	1496	1311	717	94	498	99	15	444	870	602	86	7	1
2017	14714	3155	3004	2490	745	508	1518	279	11	629	1657	459	327	18	6
2018	16557	1853	3041	2121	400	517	2048	545	11	708	1236	247	461	31	4
2019	17344	1342	3201	1264	488	551	2392	469	10	710	942	202	535	57	13
2020	18325	1351	3248	1564	409	462	2179	406	14	966	1279	310	402	37	62
2021	20141	1837	3844	1680	484	738	2703	503	5	874	842	260	505	46	
2022	2403	393	420	238	18	106	269	47		83	71	11	56	3	

Nota. La figura 1 muestra el incremento en la cantidad de tipos diferentes de vulnerabilidades detectadas o reportadas, lo que podría hacer pensar entre otras cosas, que es un negocio rentable. Fuente: Tomado de [3].

Para concluir se puede decir que las Pymes son empresas familiares, constituidas por personas con conocimiento comercial y con pocas bases tecnológicas, esto hace que sus esfuerzos se centren en la producción, descuidando uno de los elementos más valiosos en la actualidad, su información, los datos; sin un tratamiento adecuado de los mismos, la producción se puede ver seriamente amenazada.

1.2 Marco conceptual

Para adentrarnos en los temas que competen a esta tesis, es necesario tener claros los siguientes conceptos:

- Que son los servidores informáticos

- Servidores Windows
- Servidores Linux
- En que consiste una auditoría
- ¿En qué consiste una auditoría?
- ¿Qué es una auditoría a los servidores?
- ¿Qué son vulnerabilidades y ataques informáticos a servidores Windows y Linux?
- ¿Cuáles son los más frecuentes y peligrosos?
- ¿Qué son los controles/remediaciones y cómo mitigarlos?
- ¿En qué consiste una línea base?
- ¿Qué es un Chatbot?

Servidor:

Sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, también conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos equipos que comparten recursos con otras máquinas cliente. Existen muchos tipos de servidores, como son los servidores web, los servidores de correo, los servidores virtuales, entre otros [1].

Servidores Windows:

Es similar al sistema operativo Microsoft Windows que se conoce de toda la vida, solo que éste está enfocado al de área de servidores, es muy parecido y a la vez muy diferente a la versión de escritorio, sobre todo las versiones más recientes. También se puede reconocer fácilmente como un servidor Windows ofrece herramientas incorporadas con el fin de proveer funcionalidad a una operación las cuales son especiales para su rol [2].

Servidores Linux:

Este es un sistema operativo de código abierto que permite a las organizaciones tener una alternativa de menor costo para suplir las necesidades de aplicaciones y servicios en un entorno corporativo, además de brindar mayor estabilidad [4].

Auditoria (Servidores):

Consiste en un servicio llevado a cabo por profesionales ajenos a la organización y tiene la finalidad de descubrir posibles vulnerabilidades tras revisiones exhaustivas de software, redes de comunicación, servidores, estaciones de trabajo, dispositivos móviles. En el caso de una auditoría de seguridad informática es una evaluación de los sistemas informáticos cuyo fin es detectar errores y fallas y que, por medio de un informe detallado, se entregan reportes sobre hallazgos y sus debidas recomendaciones [6]. Además, una auditoría consiste en un proceso de verificación o validación del cumplimiento de una actividad de acuerdo a lo planeado y las normas estipuladas. La finalidad de una auditoría es diagnosticar; identificar qué actividades se desarrollan según lo esperado, cuales no y aquellas a las cuales es necesario realizarle mejoras. [9]

En el caso de auditorías a servidores Windows o Linux, no es como una auditoría fiscal o de cumplimiento, es una forma de rastrear y revisar las actividades en su servidor. El proceso comienza con la creación de una política de auditoría como guía. Estas políticas definirán los eventos que desea monitorear y registrar, los cuales, luego puede examinar en busca de posibles amenazas a la seguridad. Por ejemplo, si esta política identifica y registra los intentos equivocados de inicio de sesión, esto le permitirá detectar las acciones delictivas de los piratas informáticos que intentan acceder a la red.
Todas las empresas deben definir la mejor política de auditoría para ellas de acuerdo a los tipos de amenazas que enfrentan, además deben tener en cuenta su tolerancia al riesgo.
La auditoría del servidor es altamente importante para mejorar la seguridad, además ayuda a mantener las operaciones en funcionamiento en una empresa brindando estabilidad y confiabilidad. Los servidores se utilizan normalmente para actividades de trabajo pesadas y grandes volúmenes de tráfico de información, y cualquier impacto en ellos puede derivar en tiempo de inactividad, información imprecisa o una brecha de inseguridad, todo esto puede afectar negativamente.

Por medio de una política de auditoría definida, los gerentes de TI pueden realizar un seguimiento de los cambios o intentos de acceder a la información crítica a través de la auditoría del servidor de Windows, la auditoría del servidor de archivos de Windows y la auditoría de SQL Server. Los resultados brindan a los administradores información sobre la dimensión del impacto del cambio (degradación del rendimiento, por ejemplo) y la capacidad de identificar el nivel de amenaza.
La auditoría también es importante desde la orientación al cumplimiento, muchas organizaciones utilizan SQL Server para almacenar información confidencial y estos datos pueden estar sujetos a los requisitos de HIPAA y SOX, entre otros. Si tiene una política de auditoría de SQL Server para monitorear cambios y

modificaciones, puede crear informes basados en esta información y demostrar el cumplimiento normativo [6].

Ataques a servidores informáticos

Consisten en la explotación de algunas vulnerabilidades detectadas dentro de un sistema informático, con un propósito desconocido por el administrador del sistema y que pueden causar daño, estos procedimientos se realizan remotamente o por medio de dispositivos de hardware conectados a la red local. [7]

Ataques más frecuentes y peligrosos:

A continuación, se relacionan vulnerabilidades más comunes según la CVE [3]:

Malware: es un término general para referirse a cualquier clase de "malicious software" (software malicioso) el cual está diseñado para infiltrarse en cualquier dispositivo que tenga acceso a la red.
DDNS-Denegación de servicio: Este ataque consiste en inundar con muchas peticiones de servicio al servidor, hasta que éste no pueda atenderlas, provocando su colapso.
Execute code-Ejecución de código: Este ataque corresponde a ejecución de scripts en diferentes lenguajes posibles que buscan desestabilizar el sistema, denegar el servicio, obtención de privilegios, además de otros.
Overflow-Desbordamiento: Consiste en un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer): Si dicha cantidad supera la capacidad preasignada, los bytes que sobran se almacenan en zonas de memoria aledañas, sobrescribiendo su contenido original, que probablemente pertenecían a datos o código almacenados en memoria. Esto representa un fallo de programación.

Gain privilege-Obtención de privilegios: ganar una consola con privilegios con el fin de manipular el sistema.
Bypass something-Evasión de algo: Evitar los controles con el fin de escalar en un sistema sin ser detectado.
Directory traversal-Salto de directorio: Un Directory traversal (o salto de directorio o cruce de directorio o path traversal) consiste en explotar una vulnerabilidad informática que ocurre cuando no existe suficiente seguridad en cuanto a la validación de un usuario, permitiéndole acceder a cualquier tipo de directorio superior sin ningún control.
Memory corruption-Corrupción de memoria: utilización de código para la desestabilización de un sistema.

Cross site scripting (XSS)-Comandos en sitios cruzados: envío de scripts entre páginas para obtener información o para dañar la estructura de un sitio.
Gain information-Obtención de información: cualquier método orientado a la recolección no autorizada de información para diversos fines.
Sql injection-Inyección SQL: La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código en un sitio web con el fin de evadir las medidas de seguridad y acceder a datos confidenciales o sensibles. Una vez dentro, puede controlar las bases de datos del sitio web y secuestrar la información de los usuarios [6].

Controles/vulnerabilidades y como mitigarlos: con el fin de controlar las vulnerabilidades en servidores, es necesario seguir 4 pasos claves explicados a continuación:

Paso 1: Entender sus activos
La proliferación de todo tipo de dispositivos tecnológicos en la mayoría de las empresas significa que la cantidad de activos crece de manera exponencial, junto con muchos más usuarios de estos dispositivos y más tipos de datos que viajan a través de ellos.

Paso 2: Perfilar a los potenciales actores de amenazas organizacionales y sus herramientas, técnicas y modo de operar.
Una vez que entendemos qué es lo que buscamos proteger, necesitamos entender mejor quién está buscando obtener acceso a nuestros activos y las capacidades que poseen.
Aquí, nuevamente, el contexto es importante. Muchos CISO creen que no pueden protegerse de los estados nación. Pero el hecho es que muchos delincuentes cibernéticos utilizan herramientas que antes se consideraban como del dominio exclusivo de los actores de estados-nación, como las comunicaciones cifradas y el malware polimórfico. Si muchos actores del tipo delincuente utilizan estas herramientas, las organizaciones no pueden ignorarlas.

Paso 3**:** Identificar las vulnerabilidades tecnológicas corporativas
Las vulnerabilidades son debilidades entre las personas, los procesos o la tecnología. ¿Por qué identificamos vulnerabilidades después de perfilar amenazas y clasificar activos? Porque vivimos en un mundo donde la seguridad absoluta simplemente no existe. Las herramientas automatizadas solo pueden llegar hasta cierto punto para identificar los puntos débiles, como encontrar vulnerabilidades técnicas en

una pila de software, pero no pueden decir si sus usuarios necesitan capacitación para que las amenazas no los superen.

El pragmatismo y la priorización son dos principios clave de la buena gestión de las vulnerabilidades. Necesitamos ver qué sistemas de sistemas de datos nos preocupan y en qué volumen. Algunas preguntas clave para hacer acerca de estos sistemas son:

- ¿Los sistemas son accesibles externamente?
- ¿Las aplicaciones que atienden los datos ejecutan sus versiones más actualizadas?
- ¿Dónde y cómo se almacenan los detalles de inicio de sesión?
- ¿Está enviando información confidencial dentro del cifrado?

Paso 4: Aplicar controles y salvaguardas

Las vulnerabilidades siempre surgirán. Sin embargo, los controles y salvaguardas pueden disminuir el impacto o la probabilidad de que ocurra un riesgo. Los controles no tienen que ser absolutos. Es inusual que un control elimine un riesgo por completo; se está buscando reducir el riesgo a un nivel aceptable. ¿Quién establece este nivel? Una vez más, es el negocio [8].

Línea base: Son un grupo de opciones de configuración recomendadas por el desarrollador del sistema operativo, que explica su impacto de seguridad. Estas opciones de configuración se basan en comentarios de los equipos de ingeniería de seguridad, los grupos de productos, los partners y los clientes.

Chatbot: Consiste en un programa que interactúa con usuarios, clientes, humanos y procesa las conversaciones escritas o verbales, brindando entendimiento entre las partes y dependiendo del nivel de inteligencia artificial del Chatbot, será tan coherente que el interlocutor humano no diferenciará si es una máquina o un agente quien está tomando su requerimiento. Los Chatbots pueden brindar soluciones al 100% o canalizar la información a un agente humano para finalizar de manera exitosa con el caso.

Existen básicamente 2 clases de Chatbots:

a. Inicialmente los orientados a tareas, también llamados declarativos, son diseñados para un solo propósito, se centran en realizar una función. Utilizando reglas, NPL y también Machine Learning, brindan respuestas automáticas, pero altamente entendibles a las consultas de los usuarios. Las interacciones con estos Chatbots son muy específicas y estructuradas y son más aplicables a las funciones de soporte y servicio: preguntas frecuentes interactivas de pensamiento sólido. Los Chatbots

orientados a tareas pueden manejar preguntas comunes, como consultas sobre horarios comerciales o sobre operaciones sencillas que no conllevan el uso de muchas o complejas variables. Aunque utilizan el NLP para que los usuarios finales puedan experimentarlos de forma conversacional, sus capacidades son bastante básicas. En la actualidad estos son los Chatbots más utilizados.

b. También existen los Chatbots basados en datos y predictivos, también denominados conversacionales, se denominan con frecuencia asistentes virtuales o asistentes digitales, los cuales son mucho más avanzados, interactivos y hechos a la medida que los Chatbots orientados a tareas. Estos Chatbots son conscientes del contexto y utilizan para su procesamiento de preguntas, la comprensión del lenguaje natural (NLU), el NLP y el ML mejorando así sus respuestas con cada uso. También aplican la inteligencia predictiva y la analítica para permitir la personalización basada en perfiles de los usuarios y el comportamiento anterior del usuario. Los asistentes digitales pueden aprender las preferencias del usuario con el tiempo, ofrecer algunas recomendaciones e incluso anticiparse a las necesidades de los usuarios. Además de supervisar los datos y las intenciones, pueden iniciar conversaciones. Proyectos como Siri de Apple y Alexa de Amazon son ejemplos de Chatbots orientados al consumidor, basados en datos y predictivos. Para comprenderlo mejor, se enumeran a continuación las ventajas de tener un sistema tipo Chatbot.

Ventajas:

- Aumentan la eficiencia operativa y reducen los costes para las empresas al tiempo que ofrecen comodidad y servicios adicionales para los empleados internos y los clientes externos. Permiten a las empresas resolver fácilmente muchos tipos de consultas y problemas de los clientes, a la vez que reducen la necesidad de interacción con humanos.

- Además, con la ayuda de un Chatbot, las empresas pueden centralizar sus operaciones de forma automatizada, esto ayuda de gran manera a mejorar la productividad y organización de la información, su escalabilidad permite atender a un número muy elevado de personas simultáneamente, esto lo hace también más rentable.

- También los Chatbots permiten a las empresas interactuar con un número ilimitado de usuarios de forma personal y pueden ampliarse o reducirse según la demanda y las necesidades empresariales. Mediante su uso, una empresa puede ofrecer un servicio proactivo, personalizado y similar al humano a millones de personas al mismo tiempo [7].

7. 2. Marco referencial

En el área de la seguridad informática orientada a servidores Windows y Linux, se encuentran amplios escritos dirigidos a los administradores de red donde se relacionan los ataques más comunes y como contrarrestarlos, en este caso el sistema de Hardenización del CIS [6] muestra un completo sistema de prevención por medio de la configuración adecuada de todo tipo de sistemas, para el propósito de este proyecto, nos centramos en la Hardenización de servidores Windows y sistemas Linux, los cuales buscan endurecer las medidas de seguridad restringiendo la mayoría de brechas que por desconocimiento o facilidad se dejan sin configurar o con configuraciones incompletas, débiles, aptas para el aprovechamiento de un atacante.

En el caso de los servidores Windows, el documento "Windows server Benchmark", ofrece un compendio de controles multiplataforma de la organización Cisecurity [7] donde reposan múltiples documentos que, según la necesidad, permiten elevar el nivel de seguridad a gran cantidad de plataformas.

En la búsqueda de trabajos similares que se enfocaran en la solución al problema de falta de capacidad para contratar especialistas en seguridad informática ante ataques cibernéticos en las Pymes, se encontró un proyecto similar el cual, por medio de un Bot, ofrece recomendaciones de cómo actuar en el momento de detectar novedades que pudieran deberse a ataques de este tipo [8].

Se lista también a continuación una serie de trabajos orientados a la Hardenización de servidores. Estos trabajos serán tenidos en cuenta para la elaboración de este proyecto, orientado a su mayor efectividad:

- Diseño de un proceso de Hardening de servidores para una institución financiera del sector público, elabora una serie de pasos lógicos para el endurecimiento de las configuraciones de seguridad a servidores Windows y Linux, comparando diferentes estándares y extrayendo lo mejor de cada uno con el fin de realizar una Hardenizacion más efectiva [14]
- Hardening a servidores críticos de la parte transaccional web de una entidad financiera [10] analiza las vulnerabilidades en los servidores de una institución financiera y plantea procesos de Hardenización basados en controles Cobit para la mitigación de los mismos.
- Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el centro técnico laboral de Tunja-Cotel (fache, 2016) [11] realiza una evaluación de riesgos en la infraestructura tecnológica de una empresa y planea el proceso de Hardening como una excelente estrategia para mejorar la seguridad en su red de equipos.

- Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net, plantea la importancia de la aplicación de procesos de Hardening a la medida buscando no afectar las aplicaciones implementadas en el servidor, considera la importancia de asegurar primero el entorno de la empresa. [17]

La tabla 1 compara cada uno de los trabajos similares encontrados y consultados, lista las falencias identificadas y propone la aplicación de mejoras:

Tabla 1.

Trabajos similares al proyecto.

TRABAJO SIMILAR	SERVICIOS	FALENCIAS	COMO MEJORARLO
Diseño de un proceso de Hardening de servidores para una institución financiera del sector publico	Elabora una serie de pasos lógicos para el endurecimiento de las configuraciones de seguridad a servidores Windows y Linux, comparando diferentes estándares y extrayendo lo mejor de cada uno con el fin de realizar una Hardenización más efectiva.	Falta automatizar el proceso con el fin de hacerlo más útil al usuario	Ofrecer una guía técnica que brinde al usuario un paso a paso de cómo aplicar el Hardening de acuerdo al caso
Hardening a servidores críticos de la parte transaccional web de una entidad financiera	Analiza las vulnerabilidades en los servidores de una institución financiera y plantea procesos de Hardenización basados en controles COBIT para la mitigación de los mismos.	No alcanza a ofrecer un plan de remediación concreto, no hay automatización	Elaborar un paso a paso de cómo realizar el Hardening y automatizar parte del proceso
Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el centro	Realiza una evaluación de riesgos en la infraestructura tecnológica de una empresa y planea el proceso de Hardening como una excelente estrategia	No incluye procesos automatizados	Automatizar el proceso para hacerlo entendible al técnico ejecutante del proceso

técnico laboral de Tunjacotel	para mejorar la seguridad en su red de equipos.		
Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net	Plantea la importancia de la aplicación de procesos de Hardening a la medida buscando no afectar las aplicaciones implementadas en el servidor, considera la importancia de asegurar primero el entorno de la empresa.	Carece de un proceso que facilite la labor a un técnico, un paso a paso para ejecutar el Hardening propuesto	Elaborar un paso a paso de cómo realizar el Hardening y automatizar parte del proceso

Nota. En la tabla 1 se detallan los trabajos similares encontrados y que se usaron como referencia para el presente trabajo. Fuente: tomado de [11], [15], [12], [16].

Acorde a lo visto en la tabla 1 y según lo que indica la Nist [17], quienes trabajan en áreas tecnológicas, son conscientes de la importancia del SOC, CSIRT y el CERT centros especializados en la prevención detección, análisis y mitigación de incidentes tecnológicos y de Ciberseguridad aplicando técnicas de Hardening. Son estos centros quienes tienen a la mano las herramientas actualizadas y conocimientos de vanguardia para enfrentar cualquier tipo de eventualidad y restaurar el servicio a su normal operación en un tiempo razonable según la severidad e impacto del daño. [13]. Para ello es necesario apoyarnos en el trabajo de investigación de Kozlovs, Cjaputa y Kirikova, (2016) [14] quienes enfatizan en la necesidad de ejecutar procesos de auditorías de seguridad a Servidores más acordes al medio, replanteando los procedimientos tradicionales, proponiendo una detección automática de patrones de seguridad, que puedan servir para la auditoria y el aseguramiento. El resultado final, es establecer procesos que puedan ahorrar tiempo en la misma ejecución de la auditoria, lo que conlleva a pensar en procesos más automáticos y holísticos [14].

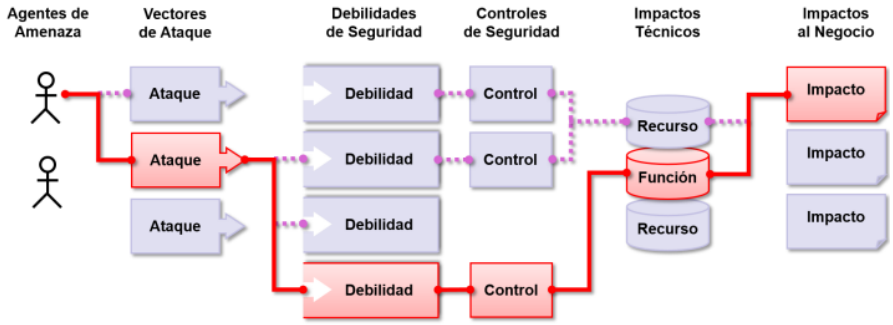
Según lo anterior, los equipos SOC, CSIRT y CERT son exclusivos de grandes organizaciones, debido a su complejidad y robusto organigrama, pero las vulnerabilidades y los ataques son generalizados, para grandes, medianas y pequeñas organizaciones, de aquí surge la necesidad de idear una estrategia que permita equilibrar las ventajas de tener el recurso y el conocimiento que se maneja en los mencionados equipos de prevención, reacción, respuesta y mitigación, solución que pueda ser aplicada de manera

efectiva en las Pymes y Micro Pymes. Según el documento “Base de conocimiento y bots: ¿cómo alcanzar la simbiosis perfecta?” [15] Debe elaborarse un documento con herramientas procedimentales tomadas de las experiencias de los grandes grupos organizados, con un modus operandi de acuerdo a cada situación, estas opciones podrían ser brindadas por un Bot que luego de ser alimentado por bases de conocimientos y matrices, ofrezcan alternativas eficientes ante ataques de todo tipo; dichas bases de datos deberán ser actualizadas constantemente con los resultados obtenidos al enfrentar nuevas variaciones de los ataques.

Acorde con lo anterior, en las empresas tipo Pymes, no se tiene capacidad para crear ambientes de prevención, tampoco cómo reaccionar de forma efectiva ante los ataques cibernéticos debido a la carencia de programas de prevención por medio de configuraciones estrictas, estructuras tecnológicas robustas y personal altamente preparado en estas áreas; son limitaciones asociadas a la falta de dinero para su conformación. Tomando en cuenta estas falencias en seguridad, sería útil también en la búsqueda del mejoramiento, tener en cuenta el modus operandi de los atacantes, como piensan, cuáles son sus técnicas organizadas para obtener su objetivo. Para eso, se relaciona la siguiente gráfica 2:

Gráfica 2.

Camino a tomar un atacante según las vulnerabilidades del entorno.



Nota. La gráfica 2 muestra una secuencia organizada empleada por los atacantes con el fin de orientar su accionar a un objetivo más próspero. Fuente: tomado de [18].

Se suma también a lo anterior y acorde al manual de seguridad en servidores desarrollado por Redhat [16], los principales errores que conducen a vulnerabilidades encontrando como más comunes los servicios

inutilizados, los puertos abiertos, servidores desactualizados además de la falta o mala administración, todo ello conlleva a un escenario óptimo para un atacante.

3. Metodología y Marco lógico

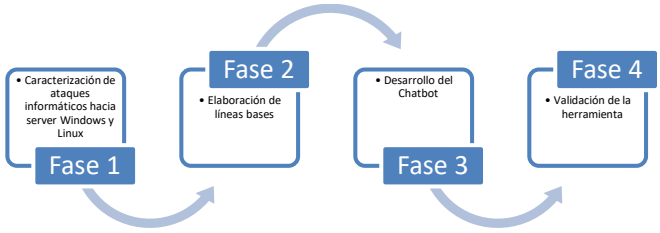
Para el curso de este proyecto se empleó el enfoque metodológico de Estudio de Caso plasmado por Robert Yin en su libro [24], acorde a sus principios, se identifican las siguientes fases elementales:

- Seleccionar el caso
- Elaborar preguntas
- Identificar las fuentes y recopilar los datos
- Analizar e interpretar la información y los resultados
- Elaborar un informe

Para el desarrollo y aplicación del método, se tomó en cuenta la experiencia con empresas tipo Pymes, la trayectoria tecnológica del autor y la confrontación del producto final (Chatbot) por parte de varios técnicos que realizarán pruebas reales en servidores y compartirán sus experiencias en busca del mejoramiento de la herramienta. Todo ello teniendo en cuenta el trabajo "El método de estudio de caso" de donde se validarán y aplicarán varias de sus teorías [24]. Este método radica básicamente en estudiar y registrar el comportamiento de un individuo o sistema con el fin de analizar patrones y posteriormente ofrecer soluciones, en este caso, el comportamiento de los ciberdelincuentes y sus herramientas, la afectación al medio tecnológico y a que nichos con mayor rigor. Es aquí donde se encontró que son las Pymes quienes tienen menos defensas a la hora de enfrentar los sofisticados ataques.

Luego de esto, y para dar claridad al objetivo general, se definieron 4 fases (gráfica 3), que corresponden a cada uno de los objetivos específicos indicados en la introducción respectivamente.

Gráfica 3.
Estructura de las fases para el desarrollo metodológico.



Nota. En la gráfica 3 se muestra de manera secuencial cada una de las fases que componen el proyecto relacionadas con sentido lógico ya que, para iniciar con una fase, es necesario haber completado la anterior.

Así mismo, en este capítulo se describe la metodología con la cual se da cumplimiento a las 4 fases propuestas en el proyecto y se entregan los resultados en el numeral 3.

3.1 Marco lógico: Metodología

Se busca con este marco lógico (tabla 2) esquematizar el proceso en pasos sencillos, fáciles de comprender para el lector, todo orientado al mejor aprovechamiento de la herramienta obtenida al juntar los objetivos.

Tabla 2.

Marco lógico.

Fases	Actividades	Entregables
Fase 1	a. Consultar cuales son los ataques más frecuentes en servidores Windows y Linux b. Determinar de acuerdo al impacto, cuáles son los más comunes o frecuentes. c. Determinar el modo de prevenirlos y detenerlos en caso de materializarse	a. Documento con listado de ataques más frecuentes, su modo de evitarlos, mitigar su impacto y remediar. b. Tablas tomadas de CVE Details con el ranking de los ataques más frecuentes c. Tabla con ataques y modo básico de prevenirlos
Fase 2	a. Determinar entidades con bases de datos tipo benchmark implementadas como líneas base de seguridad. b. Seleccionar la o las líneas base que se ajusten al propósito del proyecto.	a. Tabla comparativa con diversas opciones de líneas base, sus ventajas y desventajas b. Descripción en el documento con argumentos que justifiquen la elección de la línea base a emplear en el proyecto.

Fase 3	a. Identificación de la plataforma de Chatbot a emplear. b. Determinar el público objetivo, quienes tendrán acceso a la plataforma c. Seleccionar la estructura y lógica que tendrá la interface. d. Interfaz con presentación de respuestas y submenús. e. Calcular la cantidad de usuarios que utilizarán el Chatbot y cuantos soporta la capa gratuita de collect.chat. f. Identificar el tamaño de la base de datos límite soportada por collect.chat. g. Definir mapa con estructura de presentación h. Documentar las experiencias o lecciones aprendidas durante el proceso de elaboración y pruebas.	a. Tabla comparativa con opciones según características b. Listado con posibles usuarios, sus perfiles y posibles necesidades clave. c. Mapa con estructura a emplear d. Interfaz con presentación de respuestas y submenús e. Cálculo de posible cantidad de usuarios f. Dato exacto con tamaño de BD soportada g. Gráfico con paso a paso dentro del Chatbot h. Documento con lecciones aprendidas.
Fase 4	a. Definir caso de estudio. b. Evidencia y resultados de la ejecución. c. A través de una encuesta por medio de la sección anexa del Chatbot, sondear con los técnicos objetivos, el nivel de utilidad que esta herramienta proporcionará.	a. Documento con observaciones a prototipo inicial. b. Tabulación de resultados de encuesta en Formulario de collect.chat c. Documento con respuestas ingresadas por los técnicos luego de validar el Chatbot.

Nota: La tabla 2 corresponde a los objetivos a cumplir durante la elaboración del proyecto, considerando las actividades y entregables por fase.

A continuación, se describen cada una de las fases acorde al marco lógico:

3.2 Fase 1: Caracterización de ataques

En esta fase se ejecutaron 3 actividades que son:

a. Caracterización de los ataques/vulnerabilidades cibernéticas más ejecutados en servidores con sistemas Windows y Linux:

Se realizó una búsqueda en bases de datos institucionales y de renombre, los ataques/amenazas que representen mayor daño a los servidores en cuanto a inestabilidad o interrupción en su normal operación. Se considera el sitio CVE Details adecuado y con buena reputación para tomar como punto de inicio en la toma de información que de claridad y valor al contenido de este numeral.

b. Ataques/vulnerabilidades con mayor impacto según información de la CVE:

Se adoptó la base de datos de CVE Details como fuente idónea para realizar comparativos entre los ataques más frecuentes a servidores y el nivel de impacto negativo luego de la materialización de la amenaza, para ello se documentarán los datos estadísticos más relevantes.

c. Modo de prevenirlos o remediarlos en caso de materializarse:

Cada una de las vulnerabilidades identificadas como más frecuentes e impactantes para la infraestructura tecnológica, tienen una técnica específica de prevención y remediación como se muestra en la tabla 7 (Procedimientos básicos para prevenir algunos de los ataques más frecuentes), pero al aplicar procedimientos y políticas de seguridad inicialmente a la infraestructura, firewall, antivirus y demás, se garantiza una disminución considerable en la probabilidad de materializarse alguna de las vulnerabilidades, al disminuir el riesgo, la infraestructura y las aplicaciones contenidas en los servidores ofrecerán un nivel de estabilidad mejor.

3.3 Fase 2: Elaboración de las líneas base.

Una línea base de seguridad informática es una especificación o conjunto de parámetros sugeridos, los cuales, en caso de ser implementados, derivarán en un sistema óptimamente seguro.

Los siguientes numerales corresponden al desarrollo de las actividades y entregables propuestos para el logro del objetivo que en este caso es la elaboración de una línea base.

a. Determinar entidades con bases de datos tipo benchmark implementadas como líneas base de seguridad:

Para este caso, se realizó una tabla comparativa con diversas opciones, sus ventajas y desventajas. En ese sentido, se encuentran en el mercado diversas opciones de líneas base para aplicar en sistemas operativos Windows y Linux, algunas de ellas son la NIST, CIS, Microsoft, para cada distribución de Linux, entre otros. Se elaboró una tabla comparativa con cada uno de los entes reguladores y sus características, todo ello con el fin de identificar la que ofrecía mejores beneficios al proyecto y proceder a su implementación. Para esto se visitó cada uno de los sitios oficiales y se recopilo la información requerida para tabularla.

b. Seleccionar la o las líneas base que se ajusten al propósito del proyecto: Con la finalidad de seleccionar la línea base más acorde a las necesidades del proyecto, se realizó una tabla comparativa con características más relevantes de cada una de las líneas base encontradas.

3.4 Fase 3: Desarrollar Chatbot

En esta fase se desarrolló un Chatbot con el fin de facilitar la interacción paso a paso a los técnicos de las Pymes. Para ello, se desarrollaron 8 actividades:

a. Identificación de la plataforma a emplear:
   Para ello, se elaboró una tabla comparativa con opciones según características: en este numeral se realizó la identificación de las plataformas para la construcción de Chatbots más usadas, sus fortalezas y debilidades con el fin de realizar la mejor elección de acuerdo a las características del proyecto buscando el mejor aprovechamiento para el usuario final. Luego de ello se realizó el análisis para elegir la plataforma a emplear explicando el porqué de la decisión final. Esta selección se realizó identificando una serie de características requeridas para el proyecto y evaluadas a través de un sistema de puntos.

b. Determinar el público objetivo que tendrá acceso a la plataforma:

Se elaboró una tabla con los perfiles de posibles usuarios que tomarán provecho de la herramienta entregada, en la cual se tuvieron en cuenta sus necesidades y nivel de conocimiento para facilitar su aplicación al servidor que requieran. Esta tabla permitió dar un enfoque asertivo al producto final (Chatbot).

c. Seleccionar la estructura lógica de la interfaz:

   Se desarrolló un mapa con la estructura de presentación del Chatbot, este procedimiento facilitará la comprensión para el autor sobre la mejor forma de entregar la información al usuario. La estructura debía tener cronología y sentido escalar. Se buscó que fuera un flujo dinámico, ágil y enriquecedor para el usuario, que permitiera entregar la información que realmente fuera útil para el mejoramiento de la seguridad en su servidor. Se tuvieron en cuenta aspectos gráficos, colores, distribución de menús, entre otros.

d. Interfaz con presentación de respuestas y submenús:

   Para este paso, se identificaron los datos mas relevantes a solicitar, como información personal básica, las respuestas ofrecidas automáticamente por Auditbot e información sobre el resultado de la fase en la cuenta de correo registrada por el usuario.

e. Calcular cantidad de usuarios

   Se realizó un cálculo aproximado de cuantos usuarios empleará la herramienta con el fin de identificar cuantos soporta la plataforma, si la actual es escalable o si era necesario migrar a otra con características superiores.

f. Tamaño de la base de datos límite soportada por collect.chat:

   Se identificó el tipo y tamaño de base de datos soportada por la estructura del collect.chat con el fin de asegurar la correcta operatividad de la herramienta implementada en ella (a la cual se le denominó Auditbot). Esta actividad se desarrolló a través del contacto directo con el soporte técnico del proveedor.

g. Mapa con estructura de presentación:

   Se dio claridad al procedimiento de aplicación de los benchmarks por medio de una estructura gráfica de presentación como se muestra en la gráfica 14.

h. Documentar las experiencias o lecciones aprendidas:

   Se compilaron las experiencias positivas y negativas con el fin de tenerlas presentes para posteriores proyectos o la ampliación del presente trabajo.

Comentado [HFVM1]: Este título no esta en los resultados, esto ya lo habíamos revisado y esta en la grabación!!!! Minuto 41

Comentado [L2R1]: MODIFICADO

3.5 Fase 4: Validar el Chatbot

En esta fase se validó el Chatbot por parte de 20 técnicos informáticos con la finalidad de obtener retroalimentación y medir el nivel de aceptación, para ello, se desarrollaron las siguientes actividades:

a. Caso de estudio

Se hace una descripción básica de la organización en la cual se ejecutaron las diferentes pruebas.

b. Ejecución de prueba

Se ejecutaron las pruebas con la participación de 20 personas técnicas, evidenciando los diferentes resultados.

c. Tabulación de resultados de encuesta en Formulario de collect.chat: Fueron seleccionados 20 técnicos

Para enviarles el vínculo con acceso a Auditbot para que realizaran pruebas de la aplicación y documentaran su experiencia con percepción y sugerencias como oportunidades de mejora las cuales llegan al correo del gestor del proyecto, estos datos se tabularán para mayor comprensión, análisis y posteriores ajustes a la aplicación. Serán tabulados en Excel y presentados como apéndice 10 (Respuestas encuestas técnicos tabulada)

4. Resultados

Se presentan en este capítulo los resultados de cada una de las fases propuestas en este proyecto, estas fases desencadenan en un producto útil para la Hardenización de servidores Windows y Linux, fue probado por al menos 20 técnicos del medio quienes concluyeron que aporta al mejoramiento del escenario en pro de la seguridad. Luego de probar la herramienta se obtienen recomendaciones con oportunidades de mejora las cuales se tabulan y se entregan como como apéndice 7 (Respuestas encuestas técnicos tabuladas) del proyecto para trabajo futuro.

A continuación, se documentan los resultados por fases, de acuerdo a la metodología ya definida.

4.1 Fase 1:

Caracterizar cuáles son los ataques cibernéticos más ejecutados en servidores con sistemas Windows y Linux.

a. Con el fin de hacer los servidores Windows y Linux más seguros, es necesario tener en cuenta según estadísticas y documentación científica, los ataques o vulnerabilidades (como se muestra en la tabla 3), que se han presentado con mayor frecuencia y que generan mayor impacto negativo a las empresas tipo Pymes.

Tabla 3.

Comparativos ataques/vulnerabilidades por servidor Windows y Linux según información extraída de la base de datos de CVE Details. **[3]**

	WINDOWS SERVER			LINUX SERVER		
	2012	2016	2019	Ubuntu Server	Redhat Enterprise	Debian Server
Malware	X	X	X	X	X	X
Denial of Service	X	X	X	X	X	X
Execute Code	X	X	X	X	X	X
Overflow	X	X	X	X	X	X
Memory Corruption	X	X	X	X	X	X
Gain Privilege	X	X	X	X	X	X
Bypass Something	X	X	X	X	X	X
Gain Information	X	X	X	X	X	X
Directory Traversal	X	X	X		X	

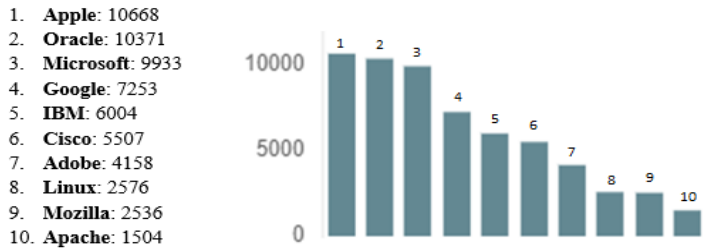
Nota. La Tabla 3 muestra que los atacantes encuentran vulnerabilidades en cualquier plataforma, independiente del sistema operativo.

b. El sitio Web *DB Vulnerabilities* [21] relaciona el comportamiento en tiempo real de las vulnerabilidades según la aplicación afectada, mostrando las de mayor afectación en un ranking de 10 marcas con variaciones de su comportamiento día a día, ayudando a mantener divulgadas las vulnerabilidades en el mismo momento que se detectan en cualquier lugar del mundo.

La gráfica 4 muestra las marcas más vulneradas en un ranking de los primeros 10 en relación a cada año.

Gráfica 4.

Top 10 cantidad de vulnerabilidades por marca.



Nota. La gráfica 4 ilustra el top 10 de marcas más vulneradas por los atacantes. Fuente: tomado de [25].

Con el fin de conocer más sobre las vulnerabilidades y amenazas que pueden afectar la infraestructura tecnológica de las Pymes, se muestra a continuación en la gráfica 5, los principales eventos que se presentan en la actualidad puntuadas según su nivel de impacto y la recomendación de como remediarla [22]:

Gráfica 5.

Principales vulnerabilidades, puntuación y remediación según el CVE.

#	CTI	Vulnerability	Base	Temp	0day	Today	Exp	Rem	CVE
1	10.00-	Apache HTTP Server Path Normalization path traversal	5.3	5.1	$10k-$25k	$5k-$10k	Not Defined	Official Fix	CVE-2021-41773
2	5.88	BIQS IT Biqs-drive index.php file inclusion	3.3	3.2	$0-$1k	$0-$1k	Not Defined	Not Defined	CVE-2021-39433
3	5.59-	Apache HTTP Server HTTP2 Request null pointer dereference	5.3	5.1	$10k-$25k	$2k-$5k	Not Defined	Official Fix	CVE-2021-41524
4	4.93-	Linux Kernel 6pack.c decode_data out-of-bounds write	8.8	8.4	$25k-$50k	$5k-$10k	Not Defined	Official Fix	CVE-2021-42008
5	3.13	Apache HTTP Server ap_escape_quotes buffer overflow	5.6	5.6	$25k-$50k	$25k-$50k	Not Defined	Not Defined	CVE-2021-39275
6	3.03	Google Chrome V8 use after free	6.3	6.0	$50k-$100k	$10k-$25k	Not Defined	Official Fix	CVE-2021-37975
7	2.89	GitHub Community Edition/Enterprise Edition apollo_upload_server Ruby Gem denial of service	5.4	5.4	$0-$1k	$0-$1k	Not Defined	Not Defined	CVE-2021-39880
8	2.75	Apache HTTP Server mod_proxy server-side request forgery	7.3	7.3	$25k-$50k	$25k-$50k	Not Defined	Not Defined	CVE-2021-40438
9	2.56	nginx request smuggling	6.9	6.9	$2k-$5k	$1k-$2k	Not Defined	Not Defined	CVE-2020-12440
10	2.52	Apache HTTP Server mod_rewrite redirect	6.7	6.7	$25k-$50k	$10k-$25k	Not Defined	Not Defined	CVE-2020-1927

Nota. La gráfica 5 muestra las vulnerabilidades por plataforma con su respectivo nivel de riesgo y su código CVE para profundizar en su estudio y posterior remediación. Esta tabla nos ayuda a evidenciar los ataques más frecuentes y, por consiguiente, los de mayor impacto para las Pymes donde se alcancen a materializar. Fuente: Tomado de [3].

Ataques más frecuentes en servidores:

Se buscó en bases de datos institucionales y sitios web registros que indicaran cuales son los ataques/vulnerabilidades a servidores Windows y/o Linux que se ejecutan con mayor frecuencia a servidores Windows y Linux, así mismo, se validó la generación de impacto negativo a las empresas. [17].

Del mismo modo se realizó una consulta en fuentes de vulnerabilidades como la CVE y la Vulndb, portales de los proveedores y otras fuentes abiertas; de dichas fuentes se extrajo la siguiente información: amenazas y vulnerabilidades a los sistemas operativos, algunas características y definiciones, posibles impactos y cantidad de eventos ocurridos, categorización o selección de los ataques, lo cuales deben ser aquellos que afecten el sistema operativo Windows o Linux.

Por cada fuente de información se obtuvo la información ya referida, luego se validaron las amenazas y vulnerabilidades en común, para seleccionar las que tienen un impacto importante en los servidores mencionados.

El sitio CVE Details [3] se enfoca en suministrar información de vulnerabilidades y su comportamiento anual permitiendo los comparativos según su comportamiento. Con respecto a los servidores Windows, se tomaron aquellos cuyo soporte y mantenimiento son vigentes por el proveedor a septiembre de 2021, los cuales son [20]:

- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

Con respecto a los sistemas Linux y como base referencial, se tomaron las siguientes distribuciones por ser las más utilizadas en el medio:

- Ubuntu server
- Redhat Enterprise

Dado lo anterior, se relacionan las gráficas con estadísticas de Ataques/Vulnerabilidades más frecuentes según las versiones y relacionadas por año, con el fin de crear comparativos, tomar decisiones y prever lo que va a pasar según el comportamiento del medio.

Windows Server 2012

En la siguiente gráfica 6 se relacionan los diferentes eventos de seguridad que han afectado la versión 2012 de Windows Server y como se puede observar, tienen lugar las vulnerabilidades más frecuentes y con incremento anual en casi todas las intrusiones.

Gráfica 6.

Comparativo cantidad y tipo vulnerabilidades en Windows server 2012 R2 por año.

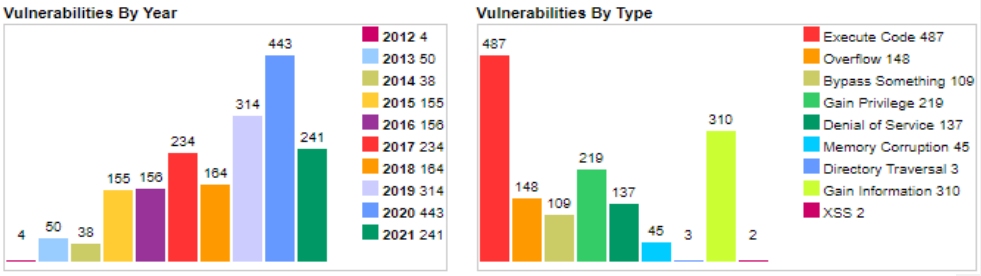
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	4		1	1						1		2			
2013	50	13	16	17	4			1		2	2	21			4
2014	38	9	11	4	3					6	6	12			4
2015	155	16	46	14	9			1		31	26	60			1
2016	156	8	42	19	7					16	28	76			
2017	234	24	50	19	4		1			6	108	15			
2018	164	11	34	6	1		1			13	25				
2019	314	25	116	1	6			1		9	33				
2020	443	13	85	67	8					9	65	33			
2021	241	18	86		3					16	17				
Total	1799	137	487	148	45		2	3		109	310	219			9
% Of All		7.6	27.1	8.2	2.5	0.0	0.1	0.2	0.0	6.1	17.2	12.2	0.0	0.0	

Nota. En la Gráfica 6 se relacionan las estadísticas de Ataques/Vulnerabilidades más frecuentes en servidores Windows 2012 R2 según las versiones y relacionadas por año, con el fin de crear comparativos, tomar decisiones y prever lo que va a pasar según el comportamiento del medio. Fuente: tomado de [3]

Así mismo, la evolución de las diferentes vulnerabilidades por tipo y año, dan a entender el aumento progresivo de las mismas (gráfica 7), con ello, los procesos de Hardening deben afrontar cada vez nuevos retos para reducir las posibles brechas de seguridad.

Gráfica 7.

Comparativo en barras cantidad y tipo de vulnerabilidades en Windows Server 2012 por año **[3]**.



Nota. La gráfica 7 muestra la evolución en cantidad desde el 2012 hasta el 2021 de cada una de las amenazas conocidas. Fuente: tomado de [3].

Windows Server 2016

La gráfica 8 tomada de los registros de la CVE Details, muestra la cantidad de vulnerabilidades presentadas en WS2016 y su incremento cada año, esto hace pensar que es un negocio lucrativo y en constante evolución.

Gráfica 8.

Comparativo cantidad y tipo vulnerabilidades en Windows server 2016 por año **[3]**.

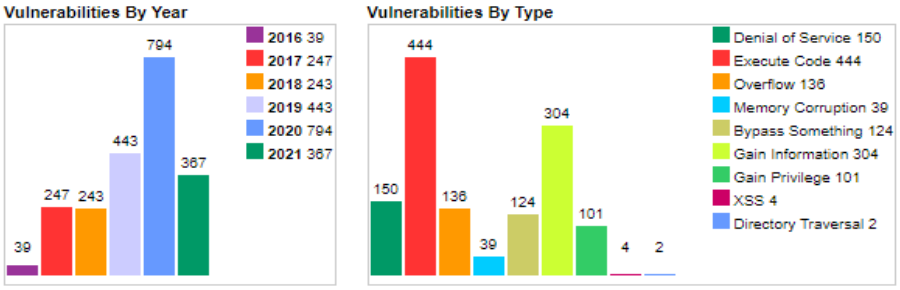
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2016	39	1	7	12	2					3	6	23			
2017	247	29	49	12	4		1			17	100	13			
2018	243	18	41	7	1		1	1		41	28				
2019	443	36	140	6	9		1	1		18	44	3			
2020	794	31	104	98	20		1			20	100	62			
2021	367	35	103	1	3					25	26				
Total	2133	150	444	136	39		4	2		124	304	101			
% Of All		7.0	20.8	6.4	1.8	0.0	0.2	0.1	0.0	5.8	14.3	4.7	0.0	0.0	

Nota. La gráfica 8 muestra la relación de vulnerabilidades por año y su variación con respecto a la cantidad de intrusiones. Fuente: tomado de [3].

La gráfica 9 muestra de manera ilustrativa las variaciones de las vulnerabilidades en cantidad e impacto para WS2016, lo que permite prever que pueda pasar para el año siguiente en temas de ataques cibernéticos.

Gráfica 9.

Comparativo en barras cantidad y tipo de vulnerabilidades en Windows Server 2016 por año.



Nota. La gráfica 9 ilustra el comportamiento para las vulnerabilidades anuales de los servidores Windows 2016. Fuente: tomado de [3].

En síntesis, para los servidores Windows 2012 y 2016 se presentan tipos similares de ataques/vulnerabilidades, con incrementos en algunos años, pero conservando la tendencia. Se encuentra en ambas versiones aumento en las intrusiones en el año 2020 a causa de la pandemia (Covid-19).

Ataques y vulnerabilidades más frecuentes en servidores Linux

Los atacantes no discriminan sistemas operativos, existen amenazas elaboradas a medida para cada uno de los sistemas operativos, para ello se muestran a continuación gráficas con el comportamiento por cantidad, tipo de amenaza y año.

Linux Ubuntu Server

La gráfica 10 permite visualizar el comportamiento de las vulnerabilidades presentadas en sistemas Ubuntu Server por año, identificando que las cantidades se incrementan al pasar el tiempo.

Gráfica 101.

Comparativo cantidad y tipo vulnerabilidades en Linux Ubuntu server por año.

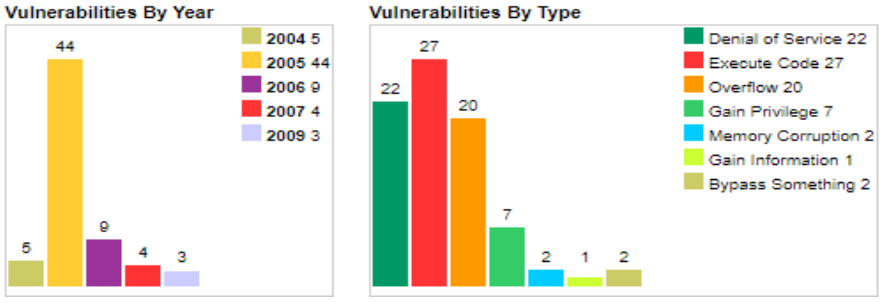
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	8	3	4	3						3					
2006	18	8	4	4	1	1	2			1		2			
2007	38	9	15	15	1		1	1		1	4	3			1
2008	61	29	19	17	11		5	2		12	4	4			
2009	37	18	4	4	3					4	6	7			3
2010	88	56	28	24	12					5	15	5			3
2011	33	20	10	8	2			2			4	3			1
2012	107	58	59	29	39		10			6	6	2	1		1
2013	161	62	56	28	18	1	3	1		18	16	8			1
2014	231	109	48	34	13		1	4		30	26	12	1		7
2015	315	172	55	98	23		3	4	2	19	25	16			
2016	314	174	46	76	18		1	4		19	33	13	2		1
2017	231	104	25	37	6		1	4		7	12	10			
2018	859	223	88	177	57	2	11	6		32	52	6	3		
2019	488	78	41	61	15		4	8		24	18	1			
2020	413	51	30	53	23		3	4	1	19	12		1		
2021	29	1	4	1						3	1	2			
2022	21	2	4	1						2		3			
Total	3452	1177	540	670	242	4	45	40	3	205	234	97	8		18
% Of All		34.1	15.6	19.4	7.0	0.1	1.3	1.2	0.1	5.9	6.8	2.8	0.2	0.0	

Nota. La gráfica 10 muestra cada uno de los ataques más comunes con las cantidades desde el 2005 hasta el 2022. Fuente: tomado de [3].

Por otro lado, la gráfica 11 muestra de manera ilustrativa la cantidad de vulnerabilidades presentadas con su respectivo impacto diferenciados por año.

Gráfica 11.

Comparativo en barras cantidad y tipo de vulnerabilidades en Linux Ubuntu Server por año.



Nota. La gráfica 11 muestra los tipos de ataque por año, se puede evidenciar su comportamiento en cuanto a Ciberseguridad. Fuente: tomado de [3].

Así mismo, la gráfica 12 relaciona el comportamiento de los ciberdelincuentes con los ataques o vulnerabilidades presentados por año. Su evolución es evidente debido a las cantidades crecientes cada año.

Gráfica 12.

Comparativo cantidad y tipo vulnerabilidades en Linux Redhat Enterprise por año.

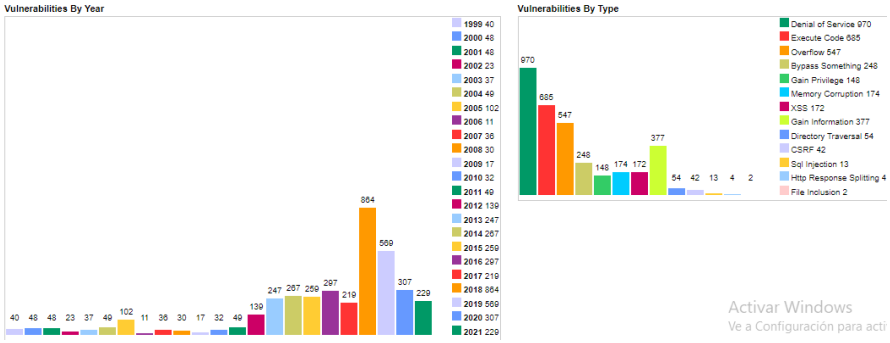
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	40	8	4	13						1		5			
2000	48	4	11	13						1		17			
2001	48	6	14	6						2		8			
2002	23	6	6	3	1					1		4			
2003	37	10	9	5			1				1	1			
2004	49	21	16	14			1	1		2	1	2			
2005	102	43	35	28	3		1	2		2	4	5			
2006	11	6	3	1						1					
2007	36	14	10	10				1		3	5	3			
2008	30	12	7	5			3			1	3	3			
2009	17	4			1		3			2	3	2			
2010	32	16	4	1	2					1	8	6	1		
2011	49	28	9	9	3					1	7	5	2		
2012	139	68	59	29	30	1	12			8	13	3	3		2
2013	247	96	54	43	24	2	11	1		17	35	20	2		6
2014	267	97	49	24	10	2	21	2	1	25	52	13	1		7
2015	259	103	48	43	22	1	9	4	1	23	28	15	3		
2016	297	90	56	40	12	1	9	1	1	25	34	5	4		
2017	219	56	44	31	6		11	2		8	27	5	4		
2018	864	131	104	136	34	3	27	16	1	57	71	7	4	1	
2019	569	77	82	47	17	1	30	12		42	39	5	11		1
2020	307	41	43	18	5	2	23	10		15	26	9	4	1	
2021	229	33	18	28	4		10	2		10	20	5	3		
Total	3919	970	685	547	174	13	172	54	4	248	377	148	42	2	16

Nota. La gráfica 12 muestra la evolución en ciberataques para Redhat por año. Fuente: tomado de [3].

La gráfica 13 permite identificar de manera ilustrativa los bajos índices de vulnerabilidades en años tempranos en Redhat server, pero un incremento importante al pasar los años.

Gráfica 13.

Comparativo en barras cantidad y tipo de vulnerabilidades en Linux Redhat Enterprise por año.



Nota. La gráfica 13 ilustra los ataques según sus características de manera anual. Fuente: tomado de [3].

Las anteriores tablas y gráficas muestran el comportamiento de los ataques por año encontrando como comportamiento habitual, que, para toda edición, hay una cantidad representativa de ataques/vulnerabilidades, lo que indica que los atacantes y los desarrolladores van de la mano. También cabe resaltar un incremento en todas las ediciones, de actividades anómalas en el año 2020, comportamiento atribuido a la pandemia del Covid-19, atacantes confinados con recursos tecnológicos a la mano y tiempo suficiente para diseñar sus estrategias intrusivas. Es importante resaltar que la gran mayoría de amenazas se pueden prevenir con la hardenización vía SCAP (*Security Content Automation Protocol*), pero antes de ello es necesario realizar un respaldo como lo indica el Apéndice 4 (respaldo previo a la hardenización nivel II Redhat)

Con el fin de hacer los servidores Windows y Linux más seguros, es necesario tener en cuenta según estadísticas y documentación científica, los ataques o vulnerabilidades (como se muestra en la tabla 6), que se han presentado con mayor frecuencia y que generan mayor impacto negativo a las empresas tipo Pymes.

Seguidamente, se muestra en la tabla 4, la consolidación de los ataques más comunes y el modo a nivel básico de cómo controlarlos.

Tabla 4.

Ataques más frecuentes y procedimientos básicos para prevenirlos.

ATAQUE	PREVENCIÓN/REMEDIACIÓN
Malware	Antivirus, políticas de acceso, separación de roles
DoS	Permitir/bloquear IP´s, políticas de acceso, bloquear servicios
Execute code	Políticas de acceso, captcha, uso de WAF, parametrización de código
Overflow	Políticas de acceso, parametrización de código, compiladores robustos
Memory corruption	Políticas de acceso, parametrización de código, compiladores robustos
Gain privilege	Políticas de acceso, separación de roles, aislamiento de Vlan
Bypass something	Políticas de acceso, separación de roles, aislamiento de Vlan
Gain information	Políticas de acceso, separación de roles, aislamiento de Vlan, bkp´s
Directory traversal	Políticas de acceso, separación de roles, aislamiento de Vlan

Nota: La tabla 4 muestra los ataques más frecuentes y la forma de prevenirlos como primera alternativa, ya que existen muchos métodos, se citan los que están a la mano de un técnico de las Pymes.

Finalmente y acorde a los datos anteriores, se puede apreciar la existencia de al menos 9 amenazas o ataques informáticos que pueden afectar los sistemas operativos, así mismo, es posible tener una forma de solucionarlo según la CVE Details y DB Vulnerabilities, todo con el fin de crear conciencia sobre la cantidad de configuraciones inexistentes, débiles o mal elaboradas en los servidores y recordar que es muy difícil garantizar que todas van a ser cubiertas en este proyecto, por esta razón se ofrecerán remediaciones a los ataques/vulnerabilidades que causan mayor daño y que son más frecuentes, de esta manera la herramienta propuesta será más útil.

A continuación (fase 2), se relaciona el procedimiento para la elaboración y definición de la línea base a aplicar al servidor de acuerdo con sus características.

4.2 Fase 2:

En esta fase, como se indicó en la metodología, se relacionan las diferentes líneas base elaboradas por cada fabricante para garantizar, luego de su aplicación, un nivel de seguridad y funcionalidad óptimos.

Se validaron varias bases de datos tipo benchmark de diferentes entidades las cuales contienen las configuraciones más útiles según su impacto en el proceso de aseguramiento de los servidores Windows y Linux con el fin de implementar la que ofrezca mejores beneficios en el proceso de hardenización.

La tabla 5 sintetiza los fabricantes y organizaciones dedicadas a la creación de líneas base para la optimización de la seguridad en diferentes sistemas.

Tabla 5.

Bases de datos tipo benchmark con sus características más representativas.

FUENTE: LINEAS BASE	VENTAJAS	DESVENTAJAS
STIG - Security Technical Implementation Guide (Disa)	- Herramienta automatizada - Efectividad probada en estudio de caso - Respaldada y utilizada por el departamento de defensa de EE.UU. - Uso libre sin pago. - Cubren Windows y Linux	
CIS	- Herramienta automatizada - Opción de pago y capa gratuita - Uso muy popular - Cubren Windows y Linux	- Capa gratuita con bajo alcance
NIST	- Tiene líneas robustas y amplias - Cubren Windows y Linux	- subcategorías muy obvias y otras irrelevantes
Microsoft security baseline	- Robustas y efectivas	- Solo Microsoft
Líneas base de seguridad Linux	- Robustas y efectivas	- Solo Linux
Líneas base de seguridad personalizadas	- Dinámicas, manejables según interés específico	- Poco confiables, sin marca prestigiosa que las respalde - Pueden contener backdoors
Programas de terceros	- Dinámicas, manejables según interés específico	- Poco confiables, sin marca prestigiosa que las respalde - Pueden contener backdoors

Nota: Cada entidad ofrece una alternativa, algunas con características favorables al proyecto que compete.

Luego de elaborar la tabla comparativa (Tabla 5) y constatar ventajas y desventajas en busca de la mejor alternativa para alcanzar óptimos resultados, se determinó que se utilizaría la base de datos tipo benchmark generada por la DISA (Defense Information System Agency), encargada de suministrar los ajustes necesarios a los sistemas tecnológicos del Departamento de Defensa de los Estados Unidos. Este benchmark se carga en la herramienta SCAP Compliance Checker con el fin de comparar los benchmarks optimizados en STIG con los ajustes de seguridad actuales del servidor en cuestión, para luego tomar decisiones sobre el método a emplear en la hardenización del mismo.

La técnica de endurecimiento para Windows consiste en la aplicación de GPO´s optimizadas con las líneas base de seguridad de Microsoft empaquetados para luego ser cargados por la línea de comandos sobrescribiendo las configuraciones existentes. Al final se puede realizar una nuevamente verificación del nivel de seguridad resultante por medio de la herramienta SCAP (Security Content Automation Protocol)

Compliance Checker obteniendo un nivel de ciberseguridad bastante mejor que el medido al inicio del proceso.

A continuación, se encuentra el consolidado de las líneas base, esto es, las configuraciones que deben tenerse en cuenta como mecanismos de seguridad en los diferentes sistemas operativos.

Línea Base de seguridad Windows Server:

Microsoft tiene un listado con las configuraciones y ajustes de seguridad recomendadas para conservar los servidores seguros. Ver Apéndice 2 hardenización nivel I Windows, para más detalle.

Se relaciona a continuación un listado de los grupos de Directivas a aplicar en los servidores Windows con el fin de mejorar su seguridad según Microsoft [26]:

- Directivas de cuenta: direccionará los permisos de acuerdo a la directiva de dominio.
- Directivas locales: configuración de permisos exclusivos para cada equipo.
- Firewall de Windows con seguridad avanzada: las características habituales mejoradas con IA.
- Directivas de Administrador de listas de red: agrupan instrucciones y permisos para un colectivo.
- Directivas de clave pública: permite sincronizar un clave de dominio relacionada a un certificado.
- Directivas de restricción de software: limita la instalación o ejecución de software en terminales que hagan parte de la directiva.
- Directivas de control de aplicaciones: permite delimitar el alcance o funcionalidad de aplicaciones con características parametrizadas en dicha directiva.
- Directivas de seguridad IP en el equipo local: permite o niega la ejecución de aplicaciones o funcionalidades de acuerdo a un rango de IP´s o una en específico.
- Configuración avanzada de directivas de auditoría: hace a un equipo o un grupo de equipos parte de una muestra para ser auditada y tomar decisiones con respecto a los demás componentes de la red.

Línea Base de seguridad Linux Server

Así mismo, se recomienda a nivel general realizar las siguientes configuraciones a los servidores Linux con la finalidad de mejorar su nivel de seguridad:

- Configuración de arranque: delimita las opciones de inicio avanzado para recuperación del sistema o de acceso sin credenciales.

- Configuración de usuarios y grupos: parametriza el tipo de usuario y su alcance de acuerdo al grupo que sean asignados.
- Configuración de acceso: asigna un alcance dentro de una organización a carpetas, horarios específicos o cualquier parametrización de acuerdo a la necesidad del usuario.
- Configuración de sudo: quitar o permitir la ejecución de procedimientos con privilegios de administrador.
- Configuración de servicios: permite delimitar permisos en servicios relacionados a puertos abiertos o cerrados.
- Configuración del sistema de ficheros: ayuda a restringir o permitir escalamientos en niveles de permisos dentro de las carpetas de usuario o del sistema.
- Configuración de red: parametriza niveles de acceso de acuerdo a un segmento de red o dirección IP específica.
- Configuración de firewall: características para permitir o denegar la ejecución de procesos que puedan dañar el sistema o la información contenida en él.
- Configuración de actualizaciones: para fines de seguridad, se permiten de forma automática o manual, esto para proteger el funcionamiento de algunas aplicaciones que podrían entrar en conflicto con nuevas reglas contenidas y aplicadas en nuevas actualizaciones.
- Configuración de registros (logs): ayuda a evidenciar los eventos de ingreso, logueo, actualización, borrado y toda la actividad que puedan orientar en la solución de algún incidente.

Para este apartado se relacionaron las líneas base más representativas de cada fabricante con sus respectivas características, por ello, se adoptaron al proceso de Hardenización del presente proyecto.

Algunos proveedores son CIS, NIST, Microsoft, Ubuntu y Redhat permiten resaltar diferentes controles a ser aplicados y con ello, se pretende prevenir o mitigar el impacto de las amenazas más frecuentes. Estos controles se pueden aplicar de forma automática con herramientas como SCAP, pero antes de ello es necesario realizar un respaldo como lo indica el Apéndice 5 (respaldo previo a la hardenización nivel II Ubuntu).

En consecuencia, la fase 2 permitió evaluar las diferentes opciones existentes para cada fabricante, determinar cuáles ofrecen mejores beneficios para el proyecto, en este caso con la ayuda de DISA (Defense Information Systems Agency) como fuente de líneas base empleadas para asegurar los sistemas

tecnológicos del departamento de defensa de los Estados Unidos y liberándolas al público. Se aprovechó este recurso implementándolo en el prototipo inicial según las etapas de Auditbot.

4.3 Fase 3. Desarrollo del Chatbot.

A continuación, se muestran los procedimientos empleados para la elaboración y configuración del Chatbot orientado a facilitar la labor del técnico de las Pymes en busca de servidores con configuración de seguridad optimizada, esto, con base en las líneas base de seguridad y la posible reducción de los ataques informáticos.

a. Plataforma Chatbot:

El resultado de este objetivo corresponde a la interacción de los objetivos anteriores configurados para obtener un resultado útil y satisfactorio para los usuarios. Para ello se realizó un comparativo entre varias plataformas para la elaboración de Chatbots, identificando diferentes características de acuerdo al objetivo concluyendo con collect.chat como la que más se ajustó al modelo requerido para este proyecto.

La tabla 6 muestra varias opciones de Chatbots a usar con el fin de identificar características favorables para el logro de los objetivos del proyecto.

Tabla 6.

Comparativo entre plataformas para la implementación de Chatbots. Información tomada de cada una de las páginas oficiales del fabricante luego de previa validación y análisis.

PLATAFORMA	VENTAJAS	DESVENTAJAS
Collect.chat	- Intuitivo - Interfaz amigable - Machine Learning integrado - Escalable - Herramientas y opciones suficientes - Capa gratuita y paga	- Capa gratuita limitada
Dialogflow	- Muy completo - Machine Learning integrado - Interfaz profesional - Chat por texto y voz	- Para desarrolladores - Máxima inversión de tiempo para su elaboración - Herramientas avanzadas, complejas
Microsoft Bot Framework	- Buena opción para principiantes - Intuitivo - Machine Learning integrado - Chat por texto y voz	- redundancia en los diálogos - dependencia de servicios en la nube de Azure - Elevado costo
Pandorabots	- Machine Learning integrado - Chat por texto y voz	- Para desarrolladores - Máxima inversión de tiempo para su elaboración

Nota: La anterior tabla relaciona las opciones más recomendadas según la literatura y puntuaciones dadas por los usuarios. Mas información sobre este tema y el prototipo inicial, se puede ampliar en al Apéndice 9 (observaciones del prototipo inicial).

Para La selección de la solución a construir en Chatbot, se definieron las siguientes características:

1. Característica 1: Intuitivo, fácil uso
2. Característica 2: Machine Learning integrado
3. Característica 3: Escalable
4. Característica 4: Capa gratuita suficiente: Asociado a cuantas características *free* pueden ser usadas.

A cada característica se le da una puntuación de la siguiente manera y se seleccionó la solución que tuvo más puntos de acuerdo con las características:

- 0 puntos: no tiene la característica
- 1 punto, la cumple parcialmente
- 2 puntos, la cumple totalmente.

La siguiente tabla busca determinar la solución que brinde mejores ventajas al proyecto de acuerdo con los criterios anteriormente seleccionados.

Tabla 7.

Puntuación de cada solución tipo Chatbot según características propuestas.

Solución	Característica 1	Característica 2	Característica 3	Característica 4	Total
Collect.chat	2	2	2	2	8
Dialogflow	1	2	2	2	7
Microsoft Bot Framework	1	2	2	1	6
Pandorabots	1	2	2	1	6

Nota: estas características fueron descritas de acuerdo con el estudio de mercado y las ventajas-desventajas de cada una de las soluciones.

Como se puede apreciar, la solución Collect.chat obtuvo el mejor puntaje, por lo cual, es la seleccionada para la construcción del Chatbot, esto, dada las ventajas y el número de características que cumple aportando a la viabilidad del proyecto.

b. Listado con posibles usuarios o públicos con acceso

Luego de realizar la validación según la aceptación de quienes lo usaron en la fase de pruebas, se llegó a la conclusión sobre los perfiles de usuarios que utilizarán la herramienta para mejorar la seguridad en sus servidores. Este análisis es de gran importancia ya que ayuda a la definición del contenido, la terminología y el contenido para hacerlo más aprovechable en su labor.

En la tabla 8, se encuentran los posibles usuarios del Chatbot y sus perfiles, además, del alcance que tendrán a la hora de hacer uso de la herramienta.

Tabla 8.

Posibles usuarios, sus necesidades y alcance debido al uso de la herramienta.

USUARIO	NECESIDADES	ALCANCE
Técnico de las Pymes	- Mejorar las condiciones de seguridad y operatividad de sus servidores	Nivel elevado de seguridad debido al uso y aplicación de la herramienta.
Estudiante	- Explorar metodologías automatizadas y ordenadas para el endurecimiento de la seguridad en servidores. - Optar a por un caso de estudio con opciones de mejora como proyecto de grado.	Conceptos mejorados sobre seguridad y conocimiento avanzado en infraestructuras estables.
Explorador tecnológico	- Identificar elementos que den valor a su infraestructura tecnológica. - Enriquecer sus conocimientos. - Buscar oportunidad de negocio y mejora.	Panorama mejorado sobre posibilidades de mejora en el campo de la seguridad informática aplicada a servidores.

Nota: Se toman en cuenta en la tabla 8 los posibles usuarios y su nivel de utilidad al emplear la herramienta para mejorar la seguridad en servidores.

c. Mapa con estructura a emplear

Se relaciona a continuación de manera gráfica la forma como está distribuida la estructura del Chatbot para la interacción con el usuario final. En la gráfica 14 se busca orientar de manera facil al usuario sobre como moverse dentro de los menus para su mejor aprovechamiento.

Gráfica 14.

Diagrama de flujo con estructura básica empleada para la interacción con el Chatbot.

Nota: Para su uso, se ingresa por medio de un navegador en el PC o dispositivo celular.

La estructura del chatbot se representa por lo siguiente:

- *Saludo presentación*: Saluda, informa que es un Chatbot y describe básicamente lo que hace.
- *Información del usuario*: Solicita datos básicos como nombre, teléfono movil y correo electrónico de quien va a utilizar el Chatbot con el fin de hacerlo mas familiar, remitirle los resultados a su correo y hacerlo mas familiar tratandolo por su nombre.
- *Presentación del proceso*: Describe lo que se va a hacer a grandes rasgos.
- *Nivel 0:* Indica las características y alcance del nivel 0.

Este nivel busca garantizar un entorno confiable a los servidores por medio de la aplicación de las 10 revisiones de seguridad, según como se muestra en la tabla 9. El técnico de las Pymes debe puntuar bajo su propio criterio ajustado a la realidad, cada ítem con el fin de garantizar un ambiente optimo y confiable para los servidores que van a ser Hardenizados.

Comentado [SAD3]: Por favor validar toda la numeración de las tablas. dado que no corresponde con las del texto

Tabla 9.

Revisiones básicas de seguridad.

Nota. La tabla 9 busca asegurar el entorno al servidor luego de garantizar el cumplimiento de los 10 ítems propuestos.

1. Gestión y control de Antivirus	6. Gestión de contraseñas
2. Actualizaciones automáticas	7. Gestión de usuarios
3. Copias de seguridad	8. Gestión de la configuración (CMDB)
4. Gestión de incidentes	9. Gestión de contratos, licencias, mantenimientos
5. Gestión de la monitorización	10.Pruebas de planes de contingencia

- *Nivel 1:* Indica las características y alcance del nivel I.

Este nivel muestra la línea base generalizada como requisitos mínimos de configuración y procedimientos para cada uno de los servidores objeto de estudio. Decálogo de seguridad, según la tabla anexa (Tabla 10)

Tabla 10.

Hardenización básica [23].

LINEAMIENTO	BENEFICIO
1. Configuración de usuario	Proteger tus credenciales
2. Configuración de red	Establecer comunicaciones
3. Características y configuración de roles	Adicionar lo que necesitas, remover lo que no
4. Instalar actualizaciones	Parchear vulnerabilidades
5. Configuración NTP	Prevenir clock drifting
6. Configuración de Firewall	Minimizar su visivilidad externa
7. Remover configuraciones de acceso	Endurecer la administración de sesiones remotas
8. Configuración de servicios	Minimizar los escenarios de ataque
9. Incrementar Hardenización	Protege el S.O. y otras aplicaciones
10. Registro y seguimiento	Conocer lo que esta pasando en su sistema

Nota. La tabla 10 permite iniciar con el proceso de Hardenización manual por parte del técnico y permitirá cerrar gran parte de las brechas básicas, de esta manera se dará lugar a la fase final de Hardenización en su mayoría automatizada por scripts o programas de uso libre. Se anexa documento "Hardenización Nivel I" con línea base de seguridad la cual contiene un paso a paso de cómo aplicar los correctivos sugeridos en la tabla 10.

- *Nivel 2:* Indica las características y alcance del nivel II.
- *Selección del sistema operativo:* Permite al usuario seleccionar el sistema operativo que va a ser hardenizado.
- *Opciones de hardening:* Ofrece al usuario varias opciones y técnicas de hardenización.

En la tabla 11 se muestra cada uno de los sistemas operativos, métodos y herramientas disponibles en la web desarrollados para endurecer la seguridad:

Tabla 11.

Opciones de Hardenización sugerido para cada sistema operativo.

S.O.	Método de Hardenización	Técnica	Accesibilidad
Windows Server 2012 y 2016	Parches de seguridad (Windows Update)	Automatizable	Free
	Windows 11 Security Baseline	Ejecutable	Free

	Microsoft System Center https://www.microsoft.com/en-us/evalcenter/evaluate-system-center-2019	Programa instalado	180 días de prueba
	Calcom Server Hardening Solution https://www.calcomsoftware.com/	Programa instalado	Trial
	SysHardener https://www.novirusthanks.org/products/syshardener/	Programa instalado	Free
	Hardentools https://github.com/securitywithoutborders/hardentools/releases	Herramienta portable	Free
	Hard Configurator https://github.com/AndyFul/Hard_Configurator	Programa instalado	Free
	CIS Cat lite	Manual asistido	Free
Ubuntu Server	Parches de seguridad	Repositorio	Free
	https://www.informaticar.net/security-hardening-ubuntu-20-04/ https://www.youtube.com/watch?v=YZnkAWdXB4s&t=657s https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/ https://linuxsecurity.expert/security-tools/linux-hardening-tools	Manual + herramientas	Free
Redhat Enterprise	Ansible https://linux-audit.com/hardening-guides-tools-red-hat-linux-rhel/	Programa instalado Herramientas	Free

Nota. La tabla 11 relaciona las diferentes herramientas encontradas en la web, diseñadas para el endurecimiento de la seguridad en servidores, algunas gratuitas, otras pagas y otras con periodo de prueba.

Comentado [SAD4]: No hay enlace…

Comentado [JG5R4]: hecho

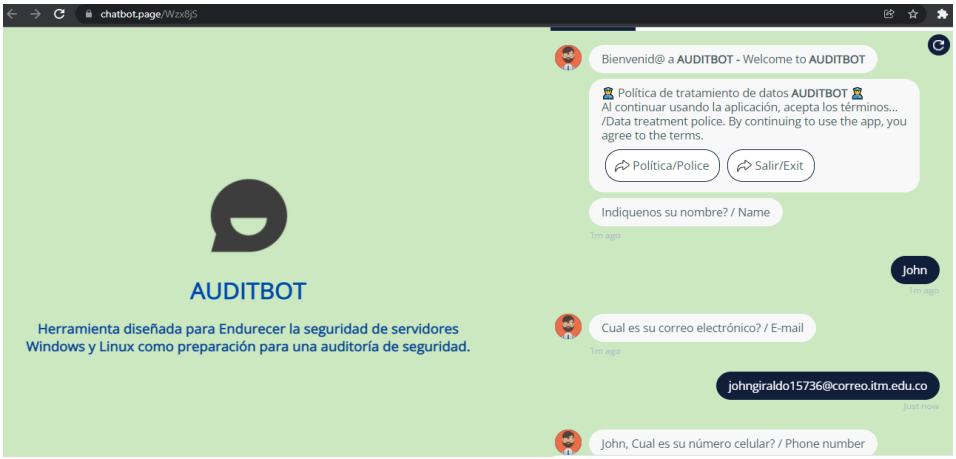
- *Encuesta de funcionalidad:* Al finalizar el proceso de hardenización, se adiciona una sección con encuesta para identificar la utilidad de la herramienta y el modo de hacerla mejor.

d. Interfaz con presentación de respuestas y submenús:

Es la interfaz gráfica con la que inicia el Chatbot recolectando de primera mano, los datos del técnico que hará uso de la herramienta. La gráfica 15 muestra la presentación inicial del chatbot donde informa qué es y solicita los datos personales a los técnicos que harán uso de la herramienta.

Gráfica 15.

Interfaz con presentación de respuestas y submenus dentro del chatbot.



Nota. Ofrece inicialmente una presentación de la herramienta y un breve saludo.

Para la elaboración y configuración del Chatbot se empleó, como se indicó, la plataforma **collect.chat** en su capa gratuita, la cual permite la parametrización de la información de acuerdo a la necesidad del Chatbot y la presenta de forma atractiva.

Así mismo, en la gráfica 16, se pueden observar varias opciones de hardenización teniendo en cuenta como actividad obligada, la creación de respaldo tipo Snapshot o imagen a su servidor. Para el caso de Windows, se detalla en el Apéndice 3.

Gráfica 16.
Nivel II, proceso de hardenización del servidor.

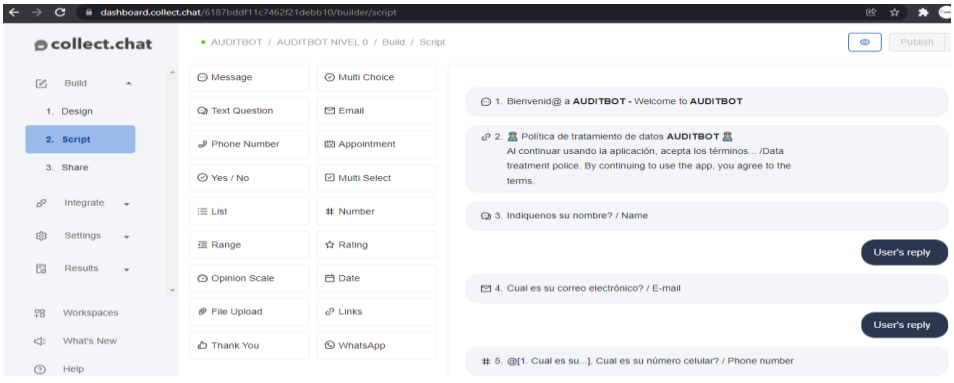
Nota: En esta fase el usuario tiene la opción de aplicar diferentes técnicas de hardenización con programas, scripts o de forma manual.

Luego de este proceso se ejecuta nuevamente el SCAP Compliance Checker para garantizar que el nivel de seguridad luego de la hardenización es mucho mejor que el nivel inicial medido (como se muestra en la gráfica 21).

La gráfica 17 muestra la consola de configuración y parametrización del Chatbot en sus diferentes opciones.

Gráfica 17.

Plataforma de parametrización collect.chat.



Nota. Collect.chat es una plataforma dinámica que permite parametrizar un Chatbot según su necesidad.

Cada uno de los elementos se encarga de enlazar la información y entregarla al usuario simulando una conversación con un agente humano, no reacciones 100% mecánicas provenientes de una máquina.

La cantidad de usuarios depende de la difusión que se le dé a la herramienta. Esta no ha sido presentada oficialmente al público en general, por el momento se ha dado a conocer (pruebas de concepto) a 20 técnicos experimentados los cuales han dado sus recomendaciones de mejora, se espera realizar las mejoras para incrementar cada día el uso de este recurso. La finalidad principal es hacer del medio tecnológico un ambiente cada vez más seguro y confiable.

La plataforma collect.chat puede soportar hasta 500 usuarios simultáneos en todas las capas (paga y gratuita). Se utilizará la capa gratuita ya que ofrece la mayoría de las características claves para la obtención de resultados. Con respecto a la base de datos de collect.chat es de alrededor de 1 Petabyte, espacio compartido entre todos los usuarios, está diseñado para soportar gran cantidad de información. Se tenía pensado utilizar la plataforma Dialogflow, pero se encontraron ventajas interesantes en la aplicación seleccionada.

e. *Cálculo de posible cantidad de usuarios*:

El ejercicio de identificar la posible cantidad de usuarios es útil para determinar si la infraestructura y configuraciones de Auditbot es suficiente para la demanda. Por estar en fase de desarrollo, no es altamente relevante, ya que en esta etapa solamente los invitados a probar la herramienta, aproximadamente 30 técnicos, son los usuarios totales con uso ilimitado de repeticiones, pero en fase de producción, luego de los ajustes debido a los comentarios aportados por los usuarios iniciales, se espera difundir su uso por medios institucionales, redes sociales y publicaciones científicas si logra la suficiente aceptación del público.

Se estima una cantidad de usuarios de aproximadamente 50 cada mes, de acuerdo con la difusión por parte de quienes utilicen la herramienta y descubran los beneficios de la misma.

f. Tamaño de BD soportada:

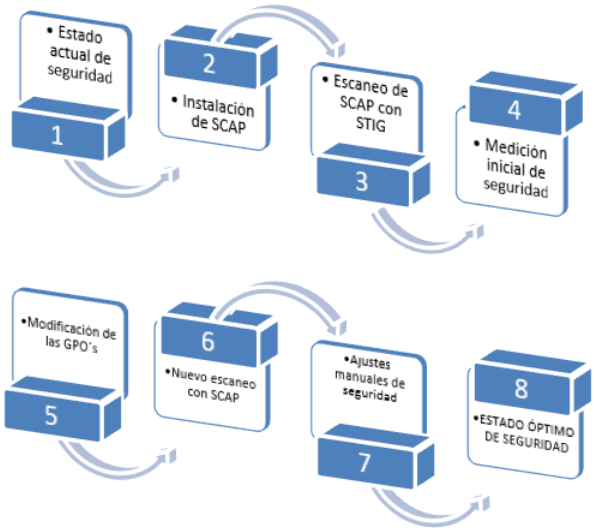
Según información suministrada por el por el proveedor de la herramienta collect.chat, tiene disponible una capacidad de base de datos ilimitada para las capas gratuita y paga, se pueden crear usuarios también sin límite según lo informa el proveedor por medio de un correo brindando confianza de ser una plataforma suficiente para la futura demanda de operaciones y almacenamiento por parte de Auditbot.

g. Mapa con estructura de presentación:

La gráfica 18 muestra el paso a paso para la utilización y aplicación de configuraciones dentro del Chatbot concluyendo en un sistema más seguro.

Grafica 18

Mapa estructural de presentación Auditbot.



Nota: Este mapa permite entender las fases de aplicación del benchmark.

A continuación, se hace una breve descripción del mapa estructural:

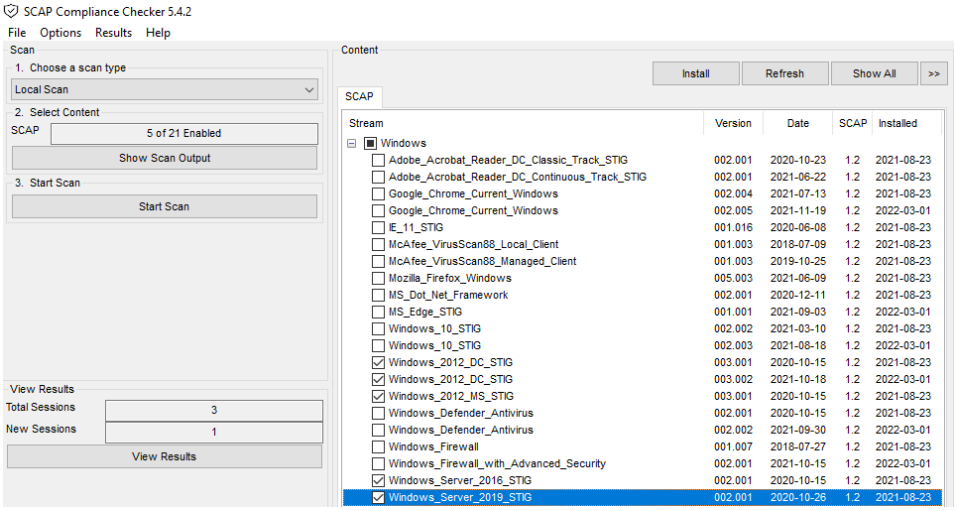
1. Estado actual de la seguridad: estado en el que se recibe el servidor.
2. Instalación de SCAP: se instala la herramienta.
3. Escaneo de SCAP con STIG: se procede al escaneo con la herramienta usando la línea base ideal de STIG y comparándola con el estado actual de seguridad.

4. Medición inicial de seguridad: ofrece una cifra porcentual del estado de seguridad luego del escaneo.
5. Modificación de las GPO´s: configuración de las líneas base de DISA para elevar el nivel de seguridad.
6. Nuevo escaneo con SCAP: nuevo resultado porcentual del estado de seguridad resultante luego de la optimización de las GPO´s.
7. Ajustes manuales de seguridad: modificaciones manuales a las vulnerabilidades que no corrige DISA.
8. Estado óptimo de seguridad: resultado final luego de la optimización de GPO´s con DISA y los ajustes manuales. Debe ser igual o cercano al 100%.

La siguiente gráfica muestra el funcionamiento de SCAP para identificar el nivel de seguridad que se mide al inicio de Auditbot y al final, luego de ejecutarse el Nivel II de Hardenización.

Gráfica 19.

Identificación del nivel de seguridad del servidor en evaluación con SCAP.



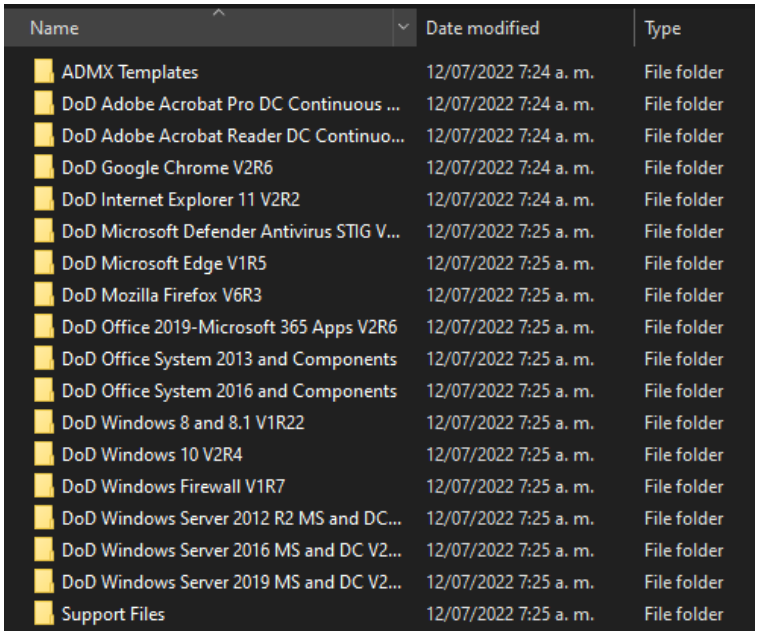
Nota: La gráfica 19 compara el estado actual de las BPO con el benchmark de SCAP.

Este procedimiento permite cargar el benchmark de SCAP acorde a cada sistema operativo y ofrece un nivel porcentual de seguridad.

La siguiente gráfica 20 muestra el paquete de GPO´s disponibles para configurar en cada sistema operativo Windows, navegador, además de otros elementos del sistema, con la finalidad de optimizarlos.

Gráfica 20.

Registros con GPO´s estandarizadas para mejorar la seguridad en Windows.



Name	Date modified	Type
ADMX Templates	12/07/2022 7:24 a. m.	File folder
DoD Adobe Acrobat Pro DC Continuous ...	12/07/2022 7:24 a. m.	File folder
DoD Adobe Acrobat Reader DC Continuo...	12/07/2022 7:24 a. m.	File folder
DoD Google Chrome V2R6	12/07/2022 7:24 a. m.	File folder
DoD Internet Explorer 11 V2R2	12/07/2022 7:24 a. m.	File folder
DoD Microsoft Defender Antivirus STIG V...	12/07/2022 7:25 a. m.	File folder
DoD Microsoft Edge V1R5	12/07/2022 7:25 a. m.	File folder
DoD Mozilla Firefox V6R3	12/07/2022 7:25 a. m.	File folder
DoD Office 2019-Microsoft 365 Apps V2R6	12/07/2022 7:25 a. m.	File folder
DoD Office System 2013 and Components	12/07/2022 7:25 a. m.	File folder
DoD Office System 2016 and Components	12/07/2022 7:25 a. m.	File folder
DoD Windows 8 and 8.1 V1R22	12/07/2022 7:25 a. m.	File folder
DoD Windows 10 V2R4	12/07/2022 7:25 a. m.	File folder
DoD Windows Firewall V1R7	12/07/2022 7:25 a. m.	File folder
DoD Windows Server 2012 R2 MS and DC...	12/07/2022 7:25 a. m.	File folder
DoD Windows Server 2016 MS and DC V2...	12/07/2022 7:25 a. m.	File folder
DoD Windows Server 2019 MS and DC V2...	12/07/2022 7:25 a. m.	File folder
Support Files	12/07/2022 7:25 a. m.	File folder

Nota: La gráfica 20 muestra un listado de las GPO´s disponibles.

Los archivos GPO se invocan desde una consola y se reemplazan por los existentes para eliminar la mayor parte de las vulnerabilidades. Al final, se realiza nuevamente la medición con SCAP para identificar el nivel porcentual de seguridad alcanzado (se evidencia en gráficas posteriores).

h. Documento con lecciones aprendidas de acuerdo a los aciertos y equivocaciones:

Durante el proceso de identificación y validación del benchmark a utilizar, se presentaron eventos favorables y desfavorables los cuales se plasman a continuación con el fin de justificar la decisión final.

Cada una de las organizaciones reguladoras adoptan y documentan técnicas orientadas a preservar la estabilidad de los sistemas por medio de estándares aplicados a la ciberseguridad. Se realizaron

validaciones de las líneas base del CIS, la NIST, Microsoft e independientes, encontrando características favorables y desfavorables en cada uno de ellos las cuales se listan a continuación:

- Algunas configuraciones pueden crear conflicto con servicios o aplicaciones, al igual que algunas actualizaciones del sistema operativo.
- Los benchmarks están diseñados como estado óptimo de seguridad, inicialmente para compararlos con el estado actual del servidor en estudio y con opción de remediación por medio de software adicional.
- La CIS y la NIST no tienen aplicación automatizada de uso libre de sus líneas base.
- Para los benchmark de Microsoft y Linux se encontró la herramienta SCAP que permite de forma automática identificar los niveles de seguridad, realizar modificaciones al registro del servidor y medir nuevamente para comprobar la mejora.
- Se encontraron benchmarks alternativos, incluidos en programas de hardenización, pero sin respaldo técnico que brinde confiabilidad, se omitieron para este proyecto ya que el resultado podría ser adverso.
- Los procedimientos automáticos de hardenización por medio de benchmarks no remedian el 100% de las brechas, es necesario realizar algunos ajustes de forma manual.
- Ningún sistema de defensa o benckmark puede garantizar seguridad absoluta, los ciberdelincuentes siempre encuentran brechas para materializar sus fines, lo que se busca es disminuir la probabilidad de ocurrencia, que les sea difícil.
- Luego de validar los diferentes benchmarks e identificar las características de cada uno de ellos, se concluye que la herramienta SCAP contiene las configuraciones que se ajustan al objetivo del proyecto y las aplica de forma automática.

Se pudo observar en el desarrollo de la fase 3 que la funcionalidad del Chatbot (prueba unitaria) es idónea y aporta a la facilitación en la configuración de seguridad de un servidor por parte de un técnico siguiendo las instrucciones entregadas por la herramienta, que además contiene textos de ayuda para garantizar el éxito del ejercicio por parte del usuario.

4.4 Fase 4. Validar el Chatbot

En esta fase se realizaron pruebas por parte de un grupo de técnicos e ingenieros con trayectoria en tecnología y conocimiento de infraestructuras, las cuales poseen como mínimo un servidor al cual aplicar las configuraciones sugeridas por la herramienta.

a. Caso de estudio:

A continuación, se hace la descripción del respectivo caso, en el cual, se ha probado el Chatbot (denominado Auditbot).

- *Objetivo del caso de estudio:*
  Ejecutar una herramienta de Ciberseguridad que ayude a los técnicos de las PYMES a preparar una auditoría, a través del uso de un Chatbot.
- *Alcance:*
  Se ejecutó en 2 empresas, una del sector industrial y la otra del sector textil.
- *Contexto de la empresa: Sector industrial:*
  El sector industrial tiene una gama amplia de empresas que permite la fabricación de productos acabados para luego comercializarlos, y es uno de los 3 sectores que componen la economía del país. Dentro de las empresas que hacen parte de este sector se pueden encontrar, entre otras, la industria de automóviles, electrónica de consumo, productos de acero, industria textil, industria del tabaco, etc.
- *Contexto de la empresa: Sector textil:*
  En lo particular, el sector textil en Colombia es un sector dedicado a la producción, fabricación y procesamiento de fibras naturales y sintéticas, hilados y telas, así como productos para la confección de ropa, lo que constituye una serie de productos masivos de amplia cobertura. En consideración de las empresas textiles hacen uso de la tecnología como mecanismo de apoyo tanto para su Core de negocio como la automatización de algunos procesos a través de las TIC, con lo cual, los procesos digitales que vienen fortaleciendo cada vez más.
  En general, las empresas Pymes del sector textil, hacen uso de sistemas de información, redes e internet para interactuar tanto interna como externamente, con lo cual, se hace necesario que, de manera periódica, se ejecuten pruebas de funcionalidad, rendimiento y de seguridad en las diferentes plataformas tecnológicas.
  En ese sentido, de forma anual un grupo de personas se enfrentan a auditorias tecnológicas que, con base de un Checklist, hacen diferentes validaciones de seguridad en los sistemas operativos que tienen al interior.

  Para el caso, se cuenta con 2 empresas una del sector industrial y otra del sector textil que poseen algunos elementos tecnológicos:

Empresa 1 (industrial): Red LAN, acceso a Internet, correo, servidor HP Blade, máquina virtual Windows Server 2012 R2. Tiene 17 usuarios para uso de aplicación contable, CRM, carpetas compartidas.

Empresa 2 (textil): Red LAN, acceso a Internet, correo, Servidor Dell, máquina virtual Windows Server 2016, tiene 24 usuarios para uso de aplicación contable y carpetas compartidas.

- *Problemática*

  Cada que se requiere una auditoría de seguridad, es necesario o bien la contratación externa de personal idóneo para su ejecución, o llevar a cabo el Checklist manual que valide el estado actual, generando con esto, en la primera actividad, costos extras para la compañía y en el segundo caso, obtener resultados que pueden no reflejar la realidad de la seguridad. En consecuencia, el problema radica en la necesidad de contar con una herramienta interna que dé un panorama de seguridad más adecuado para la Pyme, reduciendo posibles costos y generando valor en términos de ciberseguridad.
- *Expectativas*

  Contar con una herramienta funcional que permita la identificación de problemáticas en los sistemas operativos Windows y Linux y pueda aportar a las soluciones de ciberseguridad.

b. Resultados de la ejecución, evidencia:

Comentado [HFVM6]: ¿en qué apéndice quedó esta evidencia? O sea, lo pantallazos de lo ejecutado. Indicar acá eso.

Comentado [L7R6]: ESTÁN UN PARRAFO ABAJO, CADA UNO DE LOS RESULTADOS DEL ESCANEOS CON SEGURIDAD OPTIMIZADA, PARA CADA EMPRESA.

Se relaciona en el siguiente apartado, la evidencia que prueba el cumplimiento del objetivo general con la elaboración de una herramienta de ciberseguridad tipo Chatbot con recomendaciones para mejorar la seguridad empleando buenas prácticas de seguridad.

Por consiguiente, una vez definido el caso de estudio, se realizaron las siguientes actividades en los servidores de ambas empresas:

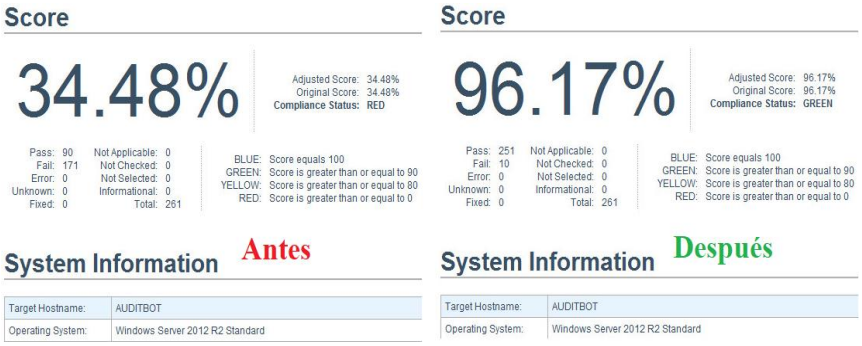
1. Identificar el sistema operativo Windows o Linux en cada una de las empresas.
2. Ingresar al servidor y abrir la URL de Auditbot para iniciar el proceso.
3. Seguir las indicaciones del nivel 0 (garantizar y ajustar el entorno tecnológico externo del servidor)
4. Seguir las indicaciones del nivel I (realizar configuraciones, ajustes del decálogo de seguridad)
5. Realizar backup a cada uno de los servidores. En caso de presentarse alguna incompatibilidad del procedimiento con las aplicaciones que corren dentro del servidor, de realizará un Rollback.

6. Iniciar con el nivel II con la instalación de la herramienta SCAP.
7. Proceder con la medición inicial del nivel de seguridad con SCAP.
8. Configurar las GPO´s de DISA por medio de comandos para optimizarlos.
9. Realizar la segunda medición para confirmar la efectividad del procedimiento anterior.
10. Revisar el informe de SCAP para realizar las modificaciones restantes de manera manual y acercar el resultado a un 100%.

La gráfica 21 muestra el estado inicial de seguridad en el servidor Windows 2012 R2 de la empresa industrial luego de instalar el programa SCAP y el resultado final luego de realizar los ajustes automatizados con las líneas base contenidas en el paquete DISA.

Gráfica 21.

Sugar CRM Server 2012 R2, Servidor en producción (empresa industrial).



Nota: el nivel de seguridad inicial de 34.48% y final optimizado de 96.17%, confirman la funcionalidad de la herramienta Auditbot en la orientación a procedimientos que mejoran sustancialmente la seguridad en los servidores. Esto queda registrado en el Apéndice 6 (registro de pruebas en servidores).

Gráfica 22.

Servidor de aplicación de contabilidad y carpetas compartidas Windows Server 2016 (empresa textil).

Nota: niveles antes y después de la aplicación del Hardening del nivel II en Windows Server 2016.

En la gráfica 22 se muestra la aplicación de las indicaciones dadas por Auditbot en su fase inicial y final después de hacer el chequeo inicial y luego aplicar los ajustes de seguridad. Para llegar a esos resultados, fue necesario instalar la herramienta SCAP en Windows Server 2012, medir para obtener el resultado inicial de 38.42 % (nivel bajo), ejecutar las configuraciones vía comandos a las GPO´s suministradas por la entidad DISA y medir nuevamente para obtener el resultado final con seguridad mejorada de 96.21% (nivel alto).

Las anteriores gráficas 21 y 22 confirman a modo de evidencia, el desarrollo del caso de estudio aplicado a dos empresas reales y operativas en las cuales, luego de ejecutar los procedimientos recomendados por Auditbot, desbordaron en un mejor nivel de seguridad con respecto a la medición inicial. Esto concluye, que sus servidores ahora son más seguros, pues la gran mayoría de las vulnerabilidades detectadas inicialmente, fueron resueltas.

Nota: para alcanzar un nivel del 100% es necesario revisar el informe final del SCAP y realizar ajustes manuales.

c. Encuesta realizada a los técnicos:

Se desarrolló una encuesta a cada uno de los técnicos, con el fin de validar el grado de utilidad de la herramienta con respecto a su uso. Para ello, se desarrollaron 2 preguntas básicas, que son:

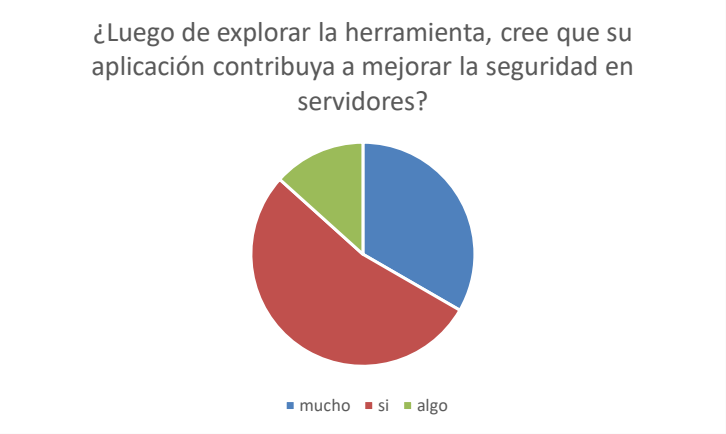
- Pregunta 1: ¿Luego de explorar la herramienta, cree que su aplicación contribuya a mejorar la seguridad en servidores?

- Pregunta 2: Que le adicionaría o cambiaría para que sea más útil?

La gráfica 23 sintetiza las opiniones de los agentes de manera ilustrativa con el fin de determinar su aceptación y efectividad en el proceso de aumentar la seguridad en su servidor.

Gráfica 23

Nivel de contribución de la herramienta a la seguridad en servidores.



Nota: luego de tabular la información consignada por los técnicos, se concluye que aporta a la seguridad de los servidores y generaría mejores resultados luego de aplicar las sugerencias documentadas por cada uno de los participantes. Para esta pregunta se obtuvieron las siguientes respuestas: MUCHO, SI, ALGO, con sus respectivos porcentajes ilustrados en la gráfica.

También se puede identificar en la gráfica, que el 53% de los encuestados respondieron "SI", 33% "MUCHO" y un 13% "algo". Esto confirma que la herramienta recibió una aprobación elevada por parte de los técnicos evaluadores, si sumamos el MUCHO y el SI, nos da una aceptación del 86% y un porcentaje restante de usuarios que no están seguros de su opinión. La posterior adición de funciones a la herramienta hará los calificativos más positivos.

Comentado [HFVM8]: ¿y qué significa esto??? Minuto 55:30

Comentado [L9R8]: NOTA ADICIONADA

Pregunta 2: ¿Que le adicionaría o cambiaría para que sea más útil?

Se obtuvieron de esta pregunta interesantes aportes los cuales serán tenidos en cuenta para mejorar la aplicación, algunos de ellos no son aplicables o pertinentes por razones técnicas. Se relacionan a continuación los más relevantes:

- "Incluir de alguna manera una pregunta o preguntas acerca de un simulacro de los posibles casos de contingencias que pueden ocurrir"
  R/se tendrá en cuenta para la versión 2.0 de Auditbot

- "Tal vez una sección de preguntas, donde el usuario pueda enviar sus inquietudes de algo que quiere profundizar o no se entendió. Excelente aplicativo"
  R/la implementación de más variables como preguntas, harían más compleja la función de automatización, pero se anexará una cuenta de correo al final para que compartan sus inquietudes o aportes al mejoramiento de la herramienta.

- "Generar un reporte con los resultados para hacer seguimiento posterior"
  R/al finalizar el proceso, se remiten las respuestas al correo relacionado al inicio de la interacción.

- "Ampliarlo a más sistemas operativos. Incluir más opciones para mejorar la seguridad"
  R/para incluir más sistemas operativos dependemos de los benchmarks que publica la DISA.

Los resultados de la gráfica anterior y las recomendaciones de los técnicos encuestados, junto con las evidencias presentadas en el numeral anterior sobre el mejoramiento de los niveles de seguridad en los servidores de las empresas en producción, confirman la efectividad de la herramienta Auditbot en la solución de la mayoría de las vulnerabilidades presentes en los sistemas operativos Windows y Linux.

En resumen, los resultados obtenidos son satisfactorios. Los comentarios adicionados por los clientes muestran la necesidad de escalar la herramienta a otros niveles para cubrir más áreas. Auditbot permite la escalabilidad no solo a otros sistemas operativos sino también a la validación en la seguridad de toda la infraestructura tecnológica en una versión 2.0 y a la gestión integral de la mayoría de los incidentes tecnológicos, mejora en las brechas de seguridad y optimización del recurso en una versión 3.0.

La dedicación de más tiempo a este proyecto podría derivar en una herramienta profesional y comercial que aportaría a la mejor calidad en la experiencia de usuario durante la interacción con el mundo de Internet.

6. Conclusiones y recomendaciones

6.1 Conclusiones

El escenario actual conocido dentro de las Pymes consiste en una infraestructura básica conformada por una conexión de internet, Mikrotik o similar, switch, servidor local, red LAN, Wifi y computadores. Todo esto administrado por un técnico informático básico, pues el tamaño de la empresa no amerita la implementación de un centro de monitoreo con subdivisiones organizativas enfocadas a la seguridad como si lo tiene una empresa de gran envergadura.

Los atacantes y sus herramientas tipo virus, malware y demás, no diferencian a sus objetivos por tamaño o tipo de empresas, son los mismos ataques para las grandes multinacionales que para las Pymes.
El anterior escenario identifica a las Pymes como pequeñas organizaciones en desventaja, las cuales no tienen una capacidad de prevención, reacción o remediación igual que los robustos equipos de las grandes empresas. Esto motivó a la creación de la herramienta Auditbot, la cual consta de una serie de configuraciones, estrategias y programas que aseguran los servidores Windows y Linux además de su infraestructura, todo ello de la mano de un Chatbot, Auditbot, de transaccionalidad ágil, al alcance de cualquier técnico básico, pero con el potencial de servir también a las grandes organizaciones.

Durante el desarrollo del proyecto escrito y la elaboración del Chatbot, se presentaron varios inconvenientes los cuales fueron bien sorteados en su momento, por ejemplo, a la hora de elegir la plataforma que albergaría el Chatbot, encontramos varias opciones, cada una con prestaciones diferentes, niveles de complejidad variados e interfaces sin las suficientes opciones o claridad para llevar nuestro contenido al usuario final de una manera ágil y entendible. Al final se optó por collect.chat, una plataforma con capa gratuita y opción de pago que permitió llevar a cabo el proyecto con opciones variadas y útiles orientadas al beneficio del usuario, en este caso, el técnico de las Pymes.

Luego de revisar varias veces el trabajo final se concluye que es un proceso altamente escalable, siempre se encuentran más oportunidades de mejora las cuales se espera poder abordar próximamente con el fin de ir perfilando el producto a una mayor utilidad. Podría ser una opción que otro estudiante retome el proceso y realice mejoras aprovechando un nuevo punto de vista y conocimientos diversos aportados por un nuevo integrante.

Es claro que los sistemas operativos no vienen ya Hardenizados debido a que se utilizan para miles de proyectos en los cuales se instalan y configuran programas con puertos o servicios que deben operar libremente. La hardenización es un asunto delicado, se corren riesgos elevados de sacar un servicio o aplicación de operación debido a un estricto proceso de optimización en la seguridad. El servidor se asemeja a una casa, está conformada por muros fuertes y gruesos, pero son necesarias las ventanas y puertas para que ingrese y salga el aire, la luz y las personas, en un servidor se requiere tener puertos abiertos por los cuales ingresan solicitudes y salen respuestas a las mismas, también ingresan potenciales amenazas que en muchos de los casos se materializan y crean lentitud, caídas de servicio o malfuncionamiento general del dispositivo.

Es imposible asegurar al 100% un sistema, lo que se hace es minimizar las probabilidades de ocurrencia de un evento con la aplicación de configuraciones de seguridad que estrechan las “puertas y ventanas” para hacer estricta la circulación.

Como apreciación de cierre se concluye que se logró diseñar la herramienta de ciberseguridad que brinda recomendaciones de buenas prácticas y que mejora la seguridad en servidores Windows y Linux según evidencia plasmada en gráficas 21 y 22 y algunos videos instructivos adicionados al Chatbot, todo esto para cumplir con el objetivo principal del presente proyecto.

6.2 Recomendaciones, Lecciones aprendidas y Trabajo futuro:

Se recomienda de forma estricta e imperativa, la creación de copias de seguridad, puntos de restauración, snapshots y respaldo a la información antes de iniciar la aplicación de instrucciones de Auditbot, ya que en muchos casos el solo hecho de actualizar un servidor con los parches o paquetes emitidos por Microsoft, se entra en conflicto con algunos servicios o puertos y deja de funcionar una aplicación critica dentro del servidor.

Para la continuación del presente proyecto se espera poder incluir módulos que puedan aprovechar la escalabilidad del sistema, es una gran oportunidad para mejorar el trabajo adicionando módulos que hagan del mismo una herramienta cada vez más útil, no solo para mejorar la seguridad en los servidores, sino también para su entorno tecnológico en general.

Se encontró durante las prolongadas búsquedas, que la información es amplia y dispersa, se requiere de gran análisis para la optimización de esta, ya que de utilizar cada una de las fuentes, se corría con el riesgo de entorpecer el proceso con datos errados o mal utilizados.

Quien se tome la tarea de escalar el proyecto con opciones más complejas y completas debe comprometerse a profundizar en cada uno de los numerales de este trabajo para comprender la lógica, detectar errores, corregirlos y enriquecer su contenido siempre enfocado en ayudar a su público objetivo.

La plataforma collect.chat soporta las operaciones actuales de Auditbot en la capa gratuita, las funcionalidades que se obtienen con la versión de pago, no son estrictamente necesarias para la presentación del presente proyecto luego de consultarlo con las autoridades respectivas de la universidad (HV). Mas detalles sobre trabajo futuro para la mejora de la herramienta Auditbot, puede ser consultada en el Apéndice 8 (trabajo futuro).

8. Apéndices

Se elaboran y se presentan 10 apéndices a este proyecto con la finalidad de servir como apoyo y dar claridad a los ítems que lo necesiten:

- Apéndice: 1 Resultados en un ambiente controlado
  Le ayudará al lector a familiarizarse con la herramienta y su mejor aprovechamiento.
- Apéndice: 2 hardenización nivel I Windows
  Servirá de guía para el endurecimiento de la seguridad del servidor Windows mediante la correcta aplicación de los procesos sugeridos.
- Apéndice: 3 respaldo previo a la hardenización nivel II Windows
  Ofrece un paso a paso de cómo realizar el respaldo a las configuraciones de los servidores Windows en caso de ser necesario un Rollback.
- Apéndice: 4 respaldo previo a la hardenización nivel II Redhat
  Ofrece un paso a paso de cómo realizar el respaldo a las configuraciones de los servidores Redhat en caso de ser necesario un Rollback.
- Apéndice: 5 respaldo previo a la hardenización nivel II Ubuntu

Ofrece un paso a paso de cómo realizar el respaldo a las configuraciones de los servidores Ubuntu en caso de ser necesario un Rollback.

- Apéndice: 6 registro de pruebas en servidores
  Recopila las pruebas realizadas junto con experiencias varias y como sortearlas.
- Apéndice: 7 resultados y tabulación de las encuestas
  Relación de los comentarios de los técnicos.
- Apéndice: 8 trabajo futuro
  Recopila las tareas a realizar en un futuro cercano por parte del gestor del proyecto o por otro ingeniero que quiera seguir mejorando la herramienta ya que es totalmente escalable.
- Apéndice: 9 observaciones a prototipo inicial Auditbot.
  Permite identificar los pasos iniciales, bases de datos consultadas y la evolución del proyecto hasta llegar al producto final.

9. Bibliografía

[1] C. F. Mora Franco, «Desconocimiento de las Pymes frente a los APT, Universidad Piloto de Colombia,» 2015. [En línea]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2957/00002030.pdf?sequence=1.

[2] Widefense, «Las principales amenazas de ciberseguridad para las pequeñas empresas (Pymes),» 2021. [En línea]. Available: https://www.widefense.com/recursos/ciberseguridad/pequenas-empresas/.

[3] «CVE Details,» 2021. [En línea]. Available: https://www.cvedetails.com/. [Último acceso: 2021].

[4] IT Explained SERVIDOR, «PAESSLER,» 2021. [En línea]. Available: https://tinyurl.com/2xbn4w4u.

[5] Hosting Diario, «Microsoft Windows Server,» 2019. [En línea]. Available: https://tinyurl.com/yckuejp7.

[6] «Platzi,» 2019. [En línea]. Available: https://platzi.com/tutoriales/1667-linux/4894-que-es-un-servidor-linux/#:~:text=Un%20servidor%20Linux%20es%20un,y%20servicios%20a%20sus%20clientes.&text=Si%20tiene%20en%20ejecuci%C3%B3n%20un,que%20sea%20en%20CentOS%C2%AE..

[7] DNSStuff, «Server Auditing Best Practices—Windows Server, SQL Server, and File Server Auditing,» 2021. [En línea]. Available: https://tinyurl.com/2p9ax74r.

[8] Tenable, «Interrumpa las rutas de ataque,» 2022. [En línea]. Available: t.ly/5Uv0

[9] Kaspersky, « Las vulnerabilidades de software,» 2020. [En línea]. Available:

[10] «Oracle OCI,» Enero 2022. [En línea]. Available: https://www.oracle.com/co/chatbots/what-is-a-chatbot/.

[11] C. CIS Benchmarks, «CIS Benchmarks,» Julio 2020. [En línea]. Available: https://www.cisecurity.org/cis-benchmarks/.

[12] Cisecurity, «CIS Benchmarks,» 2020. [En línea]. Available: https://learn.cisecurity.org/benchmarks.

[13] S. Sanchez, «An Intent-Aware Chatbot for Cibersecurity Chatbot,» Zürich, Switzerland, 2020.

[14] C. Ana, DISEÑO DE UN PROCESO DE HARDENING DE SERVIDORES PARA UNA INSTITUCIÓN FINANCIERA DEL SECTOR PUBLICO, Quito Ecuador: Universidad Internacional SEK, 2019.

[15] C. E. Frías Morales, Hardening a servidores críticos de la parte transaccional web de una entidad financiera,

Guayaquil Ecuador, 2018.

[16] J. D. Fache Montaña, Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el Centro Técnico Laboral de Tunja, Tunja Colombia: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), 2016.

[17] R. M. R. R. JAVIER HUMBERTO ROBAYO LÓPEZ, ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA, Bogota: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD, 2015.

[18] J. D. Fache Montaña, «Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el Centro Técnico Laboral de Tunja – Cotel.,» Universidad Nacional Abierta y a Distancia UNAD, Tunja, 2017.

[19] J. H. Robayo López, «Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net,» Universidad Nacional Abierta y a Distancia UNAD, Zipaquira, 2015.

[20] N. NIST 800-61, «NIST 800-61,» 2019. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs /SpecialPublications/NIST.SP.800-61r2.pdf.

[21] D. &. K. M. Kozlovs, «Auditing Security of Information Flows,» 2016. [En línea]. Available: https://doi.org/10.1007/978-3-319-45321-7.

[22] A. Casanova, «Base de conocimiento y bots: ¿cómo alcanzar la simbiosis perfecta?,» 03 Diciembre 2019. [En línea]. Available: https://automation.ctl.com.ar/blog/base-de-conocimiento-y-bots.

[23] Red Hat, «Guia de seguridad,» 2021. [En línea]. Available: https://tinyurl.com/3zfffr8d.

[24] M. Carazo, P. Cristina. «El método de estudio de caso,» 2006. [En línea]. Available: https://www.redalyc.org/pdf/646/64602005.pdf.

[25] «DB Vulnerabilities,» 2022. [En línea]. Available: https://vuldb.com/es/. [Último acceso: 2022].

[26] INCIBE, «Decálogo de buenas prácticas de seguridad en un Departamento de Informática,» 2014. [En línea]. Available: https://tinyurl.com/4jpab6j5.

[27] «Configuración de las directivas de seguridad,» Microsoft, 03 11 2021. [En línea]. Available:

https://docs.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/administer-security-policy-settings.

[28] Owasp, «Owasp,» 2017. [En línea]. Available: https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf.

[29] DoD Ciber Exchange, » 2021. [En línea]. Available: https://public.cyber.mil/stigs/.

[30] F. E. Catota Quintana, «Diseño de un proceso de Hardening de servidores para una institución financiera del sector publico,» Universidad Internacional SEK, 2019.

[31] C. E. Frías Morales, «Hardening a servidores críticos de la parte transaccional web de una entidad financiera,» Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Licenciatura en Sistemas de Información., 2018.