//UCIENCIA/23
CONVENCIÓN CIENTÍFICA INTERNACIONAL

Temática: Construcción / personalización de Sistemas Operativos basados en fuentes abiertas

Mecanismo de prevención de intrusos para Nova Servidores

Intrusion Prevention Mechanism for Nova Servidores

Michel Pedrera Suen [1*], Darelys Peña Castellanos [2], Yaniel Antonio Sánchez Domínguez [3]

[1] Universidad de las Ciencias Informáticas. Km 2 ½ carretera a San Antonio de los Baños, reparto Torrens, La Lisa, La Habana. mpedrera96@gmail.com
[2] Universidad de las Ciencias Informáticas. Km 2 ½ carretera a San Antonio de los Baños, reparto Torrens, La Lisa, La Habana. dcastellanos@uci.cu
[3] Universidad de las Ciencias Informáticas. Km 2 ½ carretera a San Antonio de los Baños, reparto Torrens, La Lisa, La Habana. yanielsanchez930316@gmail.com

[*] Autor para correspondencia: mpedrera96@gmail.com

Resumen
La Distribución Cubana de GNU/Linux Nova Servidores es un sistema que permite el trabajo con servidores. En este sistema la prevención de intrusos se ha convertido en un reto. En esta investigación tiene como objetivo definir un mecanismo de prevención de intrusos para Nova Servidores. Esto mediante el empleo de un Sistema de Prevención de Intrusos que sea seleccionado a través de la información proporcionada por los especialistas que desarrollan Nova Servidores y de la aplicación del método QSOS. De ello resulta una propuesta que implica la utilización de Fail2ban y su administración de forma remota. Esta investigación puede servir como base para definir un modelo que garantice la prevención de intrusos en este tipo de sistemas.

Palabras clave: distribuciones de GNU/Linux, Nova Servidores, seguridad de Sistemas Operativos basados en fuentes abiertas, seguridad en software libre, sistema de prevención de intrusos.

Abstract
The Cuban Distribution of GNU/Linux Nova Servidores is a system that allows working with servers. In this system, intruder prevention has become a challenge. The objective of this research is to define an intrusion prevention mechanism for Nova Servidores. This through the use of an Intrusion Prevention System that is selected through the information provided by the specialists who develop Nova Servidores and the application of the QSOS method. This results in a proposal that implies the use of Fail2ban and its administration remotely. This research can serve as a basis for defining a model that guarantees the prevention of intruders in this type of system.

Keywords: *free software security, GNU/Linux distributions, intrusion prevention system, Nova Servidores, security of operating systems based on open sources.*

Introducción

Las tecnologías de software libre y código abierto también conocido como *open source* prevalecen relevantes en la actualidad, y están en constante evolución. Cada vez más empresas están adoptándolas para reducir costos, aumentar la flexibilidad y mejorar la seguridad. También está impulsando los avances en inteligencia artificial (IA) y aprendizaje automático. La comunidad de software libre y *open source* sigue siendo muy activa y comprometida. Los proyectos de código abierto a menudo cuentan con una gran cantidad de contribuyentes y usuarios que trabajan juntos para mejorar y ampliar las capacidades de las herramientas. La privacidad y la seguridad son preocupaciones cada vez más importantes en la era digital, y las tecnologías de software libre están respondiendo a esta necesidad (Ferraz & Santos, 2021; Fitzgerald et al., 2006)

Dentro de este tipo de tecnologías, los sistemas operativos van a la delantera, los cuales han avanzado significativamente en los últimos años. Los sistemas operativos de software libre, como GNU/Linux, se han vuelto cada vez más populares. Cada vez más empresas, organizaciones y gobiernos están utilizando GNU/Linux debido a su flexibilidad, seguridad y bajo costo. Sobre ello es necesario mencionar que hay muchas distribuciones de GNU/Linux disponibles, pero en los últimos años ha habido una tendencia hacia la consolidación. Las distribuciones más grandes, como Debian, Ubuntu, Fedora y CentOS, han ganado una gran cantidad de usuarios y desarrolladores, y están liderando el camino en términos de innovación y desarrollo de nuevas características (Jaiswal, 2021). Incluso en Cuba se ha desarrollado una distribución de GNU/Linux hecha por cubanos y para los cubanos, llamada Nova, la cual es desarrollada por el Centro de Software Libre (CESOL) de la Universidad de las Ciencias Informáticas (UCI). Esta fue presentada por primera vez en la Feria Internacional Informática 2009, y cuenta actualmente con varios productos como Nova Ligero, Nova Escritorio o Nova Servidores (Albo Castro & Rodriguez Jimenez, 2020; *Nova*, 2023).

Este último es una “Variante orientada a la administración de servicios telemáticos a través de la herramienta nova-manager mediante una interfaz en consola” según se declara en (*Nova*, 2023). Esta distribución, cuya última versión descargable es la 8.0 y que puede ser manejada de forma remota, cuenta con diferentes funciones propios de los sistemas operativos para para la configuración y manejo de servidores. Tras una entrevista con los especialistas que desarrollan esta distribución, y una revisión de la misma por parte de los investigadores, se puede asegurar que se intentó alcanzar

la mejor calidad de prestación de servicios en cuando a escalabilidad, gestión remota y soporte. Además, mantiene la seguridad en todos los procesos que pueda realizar la computadora como servidor. Es necesario entender que debe haber facilidades tanto para el manejo de sistemas operativos de computadoras de uso personal como de ordenadores destinados a realizar funciones de servidores con Nova Servidores. Para ello es imprescindible además la implementación de sistemas de seguridad que resguarden la integridad, no solo de dichos equipos si no de la información que en ellos se maneja de forma independiente o en su interacción.

Sobre lo anterior, es necesario mencionar que la prevención y tratamiento de intrusos crea retos dentro de la seguridad de los sistemas y Nova Servidores no queda exento de estos peligros. Entre los mecanismos preventivos están los sistemas de prevención de intrusos (IPS), también conocidos como sistemas de detección y prevención de intrusos (IDPS), los cuales son dispositivos de seguridad de red que monitorean las actividades de la red o del sistema en busca de actividad maliciosa. Las funciones principales de los sistemas de prevención de intrusos son identificar actividades maliciosas, registrar información sobre esta actividad, informarla e intentar bloquearla o detenerla (Vallejo de la Torre et al., 2018). En este contexto es prudente abrir un paréntesis para aclarar las diferencias entre los IPS y los Sistemas de Detección de Intrusos (IDS). El reconocido autor Robert Newman en Computer Security: Protecting Digital Resources explica que “los sistemas de prevención de intrusos se consideran extensiones de los sistemas de detección de intrusos(...)” porque ambos monitorean el tráfico de la red y/o las actividades del sistema en busca de actividad maliciosa. Las principales diferencias son que, contrario a los sistemas de detección de intrusos, los sistemas de prevención de intrusos se colocan en línea y pueden prevenir o bloquear activamente los ataques maliciosos que se detectan (Newman, 2009).

Debido a que los IPS pueden tomar medidas como enviar una alarma, descartar paquetes maliciosos detectados, restablecer una conexión o bloquear el tráfico desde la dirección IP infractora (Vallejo de la Torre et al., 2018), son usados para la seguridad en muchas entidades entre las que se encuentra CESOL. A pesar de que otras distribuciones trabajen su seguridad con IDS, Nova Servidores carece de un mecanismo integrado al sistema que prevenga los posibles intrusos, lo cual provoca vulnerabilidad en los servicios y protocolos con los que se trabaja en el servidor mientras no se instale y configure manualmente un mecanismo externo al sistema. En esta investigación, moviéndose en el campo de acción de las herramientas de prevención de intrusos para sistemas operativos orientados a la gestión de servidores, se realiza un estudio que permita determinar un mecanismo de prevención de intrusos para Nova Servidores en sus versiones venideras.

Materiales y métodos o Metodología

Para esta investigación fue imprescindible la recaudación de información a través de una entrevista no estructurada que permitiera de forma flexible (Díaz-Bravo et al., 2013) consultar a los especialistas encargados del desarrollo de Nova Servidores y otros que usen dicha distribución en la producción. para comprender el funcionamiento especializado del mismo. Entre las preguntas más repetidas se encuentra ¿Qué mecanismo de prevención de ataques o intrusiones tiene integrado el SO del servidor?". Sobre ello se obtuvieron las siguientes estadísticas:

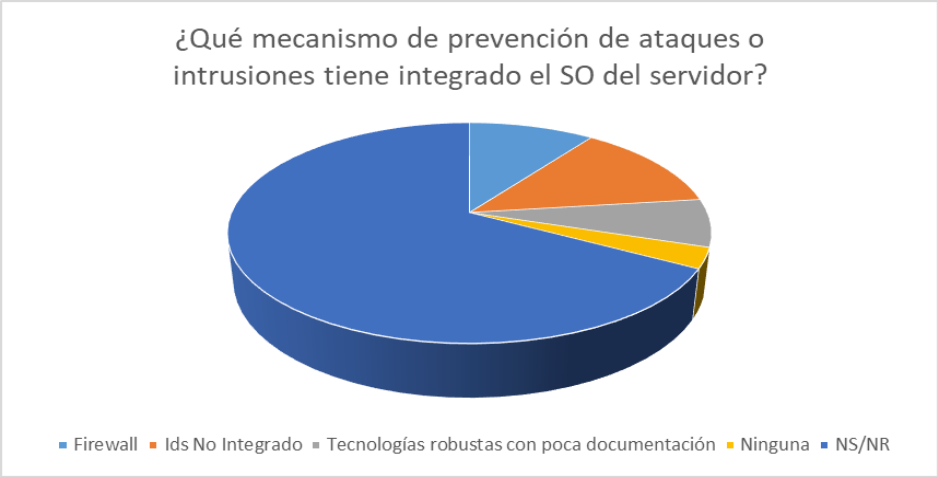

Figura 1 ¿Qué mecanismo de prevención de ataques o intrusiones tiene integrado el SO del servidor? Entrevista no estructurada a especialistas que interactúan con Nova (Fuente: Elaboración propia)

Además, para poder determinar un mecanismo de prevención de intrusos adecuado es imprescindible la implantación de un IPS en el sistema que desee asegurarse (de la O, 2021). Es por ello que también se realiza un estudio de las herramientas de prevención de intrusos existentes, de más significación o uso internacional, y para su selección como criterio fundamental se determina que sean de software libre y/o código abierto en orden de sostener los intereses de CESOL y la UCI en cuanto a estas tecnologías libres. Para este estudio se empleó el método Calificación y Selección de Código Abierto (QSOS, del inglés Qualification and Selection of Open Source software) (Semeteys, 2008). La finalidad de este análisis tiene como objetivo conocer si las aplicaciones analizadas cumplen con las necesidades existentes para la prevención de intrusos en sistemas operativos para servidores y específicamente Nova Servidores en

su versiones actuales y futuras. Para el análisis individual de cada IPS se empleó el método histórico lógico de manera que permita buscar elementos que los caractericen y permitan llegar a una conclusión una vez realizada la comparación.

Definición del método Calificación y Selección de Código Abierto

El método propone cuatro etapas: definición, evaluación, calificación y selección. Se establece un método de calificación de software para cuantificar y medir las posibilidades reales de implantación del software ofreciendo posibilidad de comparación al establecer criterios ponderados, en base a los cuales calificar el software y hacer una selección final de la manera más objetiva y beneficiosa (Semeteys, 2008).

1. Etapa de definición: se establece el marco de referencia para la búsqueda de la información relacionada con las necesidades existentes en el proyecto de software a desarrollar.
2. Etapa de evaluación: consiste en realizar una caracterización del software.
3. Etapa de Calificación: consiste en la ponderación de los criterios definidos para realizar la comparación de las herramientas analizadas.
4. Fase de Selección: El objetivo de este paso es identificar el software que cumple los requisitos del usuario o, más generalmente, comparar el software de la misma familia. Para esta fase se usa la selección estricta que está basada en la eliminación directa tan pronto como el software no cumpla con los requisitos formulados en la fase anterior (Semeteys, 2008).

Resultados y discusión

Aplicación del método Calificación y Selección de Código Abierto

A continuación, se expone el desarrollo de las diferentes correspondiente a la práctica del método Calificación y Selección de Código Abierto. Como se mencionó en epígrafes anteriores, estas herramientas que pueden ser consideradas IPS, son una selección de las más eficientes y/o más usadas a nivel mundial según (Lai et al., 2021).

Aplicación de las etapas de definición y evaluación

- Splunk ES: Splunk Enterprise Security (ES) es el centro neurálgico del ecosistema de seguridad, brindando a los equipos la información para detectar y responder rápidamente a ataques internos y externos, simplificar la gestión de amenazas y minimizar el riesgo. ES ayuda a los equipos a obtener visibilidad de toda la organización e inteligencia de seguridad para monitoreo continuo, respuesta a incidentes, operaciones de Centro de

Operaciones de Seguridad (SOC) y brinda a los ejecutivos una ventana al riesgo comercial. Además este presenta revisión y clasificación de incidentes, está construido sobre una plataforma de Big Data para inteligencia de seguridad con búsquedas ad hoc que permiten a los equipos de seguridad comprender rápidamente qué ataques están ocurriendo en su entorno para determinar el mejor curso de acción (*Splunk Enterprise Security*, 2023).

- Fail2Ban: Fail2Ban puede realizar múltiples acciones siempre que se detecte una dirección IP abusiva y actualizar las reglas de cortafuegos y de las *iptables*[1], rechazar la dirección IP de un abusador, o cualquier acción definida por el usuario que pueda ser realizada por un *script*. Funciona monitoreando archivos de registro para las entradas seleccionadas y ejecutando *scripts* basados en ellas. Con mayor frecuencia, esto se usa para bloquear direcciones IP seleccionadas que pueden pertenecer a Dispositivo que conectados a la red que intentan violar la seguridad del sistema. Puede prohibir cualquier dirección IP que haga demasiados intentos de inicio de sesión o realice cualquier otra acción no deseada dentro de un marco de tiempo definido por el administrador. Incluye soporte para IPv4 e IPv6.La configuración estándar se envía con filtros para Apache, SSH , vsftpd , qmail, Postfix y Courier Mail Server (*Fail2ban*, 2023; *Protegerse de ataques de fuerza bruta con Fail2ban*, 2023).
- DenyHosts: DenyHosts es un script destinado a ser ejecutado por los administradores del sistema Linux para ayudar a frustrar los ataques al servidor SSH (también conocidos como ataques basados en diccionario y ataques de fuerza bruta). Es una herramienta de seguridad de prevención de intrusos basada en registros para servidores SSH escrita en Python. Su objetivo es evitar ataques de fuerza bruta en servidores SSH mediante el monitoreo de intentos de inicio de sesión no válidos en el registro de autenticación y el bloqueo de las direcciones IP de origen. Está restringido a conexiones que usan IPv4. No funciona con IPv6. Puede ejecutarse manualmente, como un demonio[2]. Registra todos los intentos fallidos de inicio de sesión para el usuario y el host infractor. Por cada host que exceda un recuento de umbral, se registra como malvado. También sigue a cada infractor e inicios de sesión sospechosos (es decir, inicios de sesión exitosos para un dispositivo que tuvo muchos errores de inicio de sesión) (*DenyHosts*, 2023; *SourceForge*, 2023).

[1] Iptables: es un programa de utilidad de espacio de usuario que permite al administrador del sistema configurar las tablas proporcionadas por el cortafuego.
[2] demonio: (de sus siglas en inglés Disk And Execution MONitor), es un tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario

- OSSEC: es un sistema de detección de intrusos (HIDS) gratuito y de código abierto. Realiza análisis de registros, verificación de integridad, monitoreo del registro de Windows, detección de *rootkits*[3], alertas basadas en el tiempo y respuesta activa. Proporciona detección de intrusos para la mayoría de los sistemas operativos, incluidos Linux, OpenBSD, FreeBSD, OS X, Solaris y Windows. OSSEC tiene una arquitectura centralizada y multiplataforma que permite que múltiples sistemas sean monitoreados y administrados fácilmente. Ofrece la posibilidad de definir las adaptaciones específicas en un servidor para la definición de políticas propias más finas. Posibilita monitorizaciones basadas en agentes, pero también sin agentes como los componentes de red, enrutadores y cortafuegos (*OSSEC HIDS*, 2023).

Aplicación de la etapa de calificación

Para la confección de este análisis se establecen los parámetros a analizar siguientes:

- Monitoreo constante: Se establece “Sí” si se monitorea la red ante posibles prevencion
- es constantemente, y “No” en caso de que no se haga.
- Bloqueo de ataques en tiempo real: Se establece “Sí” en caso de que sea capaz de bloquear ataques en tiempo real y “No” en cualquier otro caso.
- Funcionalidad para diferentes servicios: Se establece “Sí” en caso de que la herramienta pueda ser configurada para más de un servicio o protocolo, y “No” si no puede hacerlo.
- Mecanismo de notificación: Se establece “Sí” en caso de que la herramienta presente mecanismos que notifiquen de los ataques, o posibles ataques y “No” en caso de que no los posea.

Se le otorga mayor peso a la Funcionalidad en Diferentes Servicios pues es de mayor interés para el cliente que el Sistema de Prevención de intrusos de Nova Servidores pueda configurarse en la mayor cantidad de servicios o protocolos posible.

Aplicación de la etapa de selección

En la Tabla 1 se muestra la comparación y demás aspectos referentes al proceso de selección en esta fase atendiendo a todo el estudio reflejado anteriormente.

[3] rootkit: es un conjunto de software que permite un acceso de privilegio continuo a un ordenador, de forma oculta al control de los administradores.

Tabla 1 Tabla comparativa de los sistemas de prevención de intrusos estudiados

IPS	Monitoreo constante	Bloqueo de ataques en tiempo real	Diferentes servicios	Mecanismo de notificación
Splunk	Sí	Sí	No (Está pensado para situaciones específicas)	Sí
Fail2Ban	Sí	Sí	Sí	Sí
DenyHosts	No(Debe ser ejecutado)	Sí	No(Solo funciona para SSH)	Sí
Ossecs	Sí	Sí	Sí	No

Luego de realizado el análisis comparativo mediante el método QSOS se definió como solución Fail2Ban por cumplir con la mayor cantidad de parámetros de selección posible.

Fail2Ban es un marco de software de prevención de intrusos y un IPS que protege los servidores de la computadora de ataques de fuerza bruta. Escanea los archivos de registro y prohíbe las IP que muestran signos maliciosos: demasiadas fallas de contraseña, búsqueda de vulnerabilidades, etcétera. En general, Fail2Ban se usa para actualizar las reglas del cortafuego para rechazar las direcciones IP durante un período de tiempo específico, aunque cualquier otro arbitrario puede aceptarse. También se puede configurar la acción (por ejemplo, enviar un correo electrónico). Fail2Ban viene con filtros para varios servicios (Apache, Samba, SSH, etcétera.). Puede reducir la tasa de intentos de autenticación incorrectos, sin embargo, no puede eliminar el riesgo que presenta una autenticación débil. Configure los servicios para usar solo dos factores o mecanismos de autenticación públicos/privados si realmente desea proteger los servicios (Carles, 2018).

Fail2ban es una solución flexible y eficaz para prevenir acciones de *bots*[4], scripts u otro tipo de ataques informáticos a un servidor. Este hace posible el seguimiento de archivos de registro con patrones sospechosos y permite bloquear o desbloquear sus direcciones IP temporal o indefinidamente. El usuario es libre a la hora de determinar aquellos aspectos que deben ser controlados, así como los parámetros exactos que se aplicarán durante la búsqueda (de la O, 2021). Para

[4]bot: es un programa informático que efectúa automáticamente tareas repetitivas a través de Internet, cuya realización por parte de una persona sería imposible o muy tediosa

instalación y configuración, Fail2ban cuenta con documentación muy clara y constantes actualizaciones de software (Carles, 2018; *Fail2ban*, 2023).

Definición de una herramienta para el manejo del mecanismo de prevención de intrusos para Nova Servidores

Para una implementación que permita un manejo más usable –según lo planteado por (Sanchez, 2011)– en Nova Servidores, se recomienda el desarrollo de una herramienta visual de acceso remoto a partir de una computadora con el sistema Nova, ello teniendo en cuenta que en Nova Servidores se trabaja directamente en consola de comandos y que Fail2ban tampoco cuenta con una interfaz de usuario. El siguiente modelo conceptual muestra los conceptos asociados a lo anterior. Un concepto para este caso, es un objeto del mundo real, es decir, es la representación de cosas del mundo real y no de componentes de software. En él no se definen operaciones.

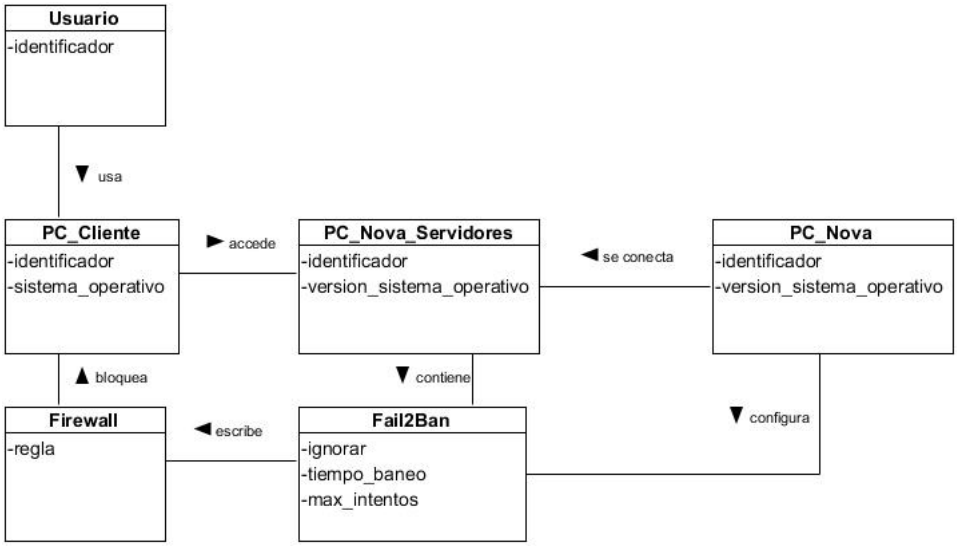

Figura 2 Modelo conceptual para implementar el mecanismo de prevención de intrusos para nova Servidores

A continuación, se detallan los diferentes objetos y relaciones que conforman el proceso.

- Usuario: persona que intenta acceder a PC_Nova_Servidores con una PC_cliente.
- PC_cliente: computadora que se conecta a Nova Servidores.

- PC_Nova_Servidores: computadora que recibe la conexión de la PC_cliente, y que tiene el sistema Nova Servidores, el cual permite el alojamiento de servidores.
- PC_Nova: Computadora que se conecta a PC_Nova_Servidores, y que mediante la administración remota trabaja con Fail2Ban.
- Fail2Ban: Sistema de prevención de intrusos que se encarga del bloqueo de acceso de los clientes al servidor a partir de reglas, y que es administrada remotamente por PC_Nova en PC_Nova_Servidores (debe estar instalada en esta última).
- Firewall: (o cortafuegos) en un sistema o una red permite bloquear el acceso no autorizado (del Usuario en el caso de este modelo conceptual), permitiendo al mismo tiempo comunicaciones autorizadas mediante reglas. Fail2Ban puede actualizar estas reglas.

Validación de la propuesta de Mecanismo de prevención de intrusos para Nova Servidores

Para validar lo que en esta investigación se propone teóricamente, se realizó la evaluación de la satisfacción de los usuarios, teniendo en cuenta los postulados teóricos de (Campistrous & Rizo, 2006) cuando expresan que la técnica de criterio de usuarios, aplicando técnica de IADOV, debe usarse como vía para valorar resultados en aquellos casos en que los evaluadores son usuarios de lo que se propone, es decir que además de tener dominio del problema en estudio, están “contextualizados”, inmersos en el contexto en el que se aplica el resultado.

La técnica de IADOV se compone de cinco preguntas claves: tres cerradas y dos abiertas, es utilizada para determinar el nivel de satisfacción individual y grupal de los usuarios a partir de una encuesta elaborada según las exigencias pertinentes. La aplicación de esta técnica constituye una vía indirecta para el estudio de satisfacción, ya que los criterios que se utilizan se fundamentan en las relaciones que se establecen entre las tres preguntas cerradas.

Las preguntas 2,3 y 4 de la encuesta se relacionan a través de lo que se denomina el Cuadro Lógico de IADOV que se muestra en la Tabla 2. Cada encuestado recibe una evaluación individual en dependencia de las respuestas que dé a las preguntas cerradas. Para facilitar el procesamiento posterior, en el diseño de la encuesta se debe tener en cuenta que a estas preguntas deben estar respondidas de la forma prevista en el cuadro lógico de IADOV. La encuesta fue aplicada a 7 trabajadores de CESOL, por ser el centro que más cerca está del producto Nova Servidores.

Tabla 2 Cuadro Lógico de IADOV

4. Luego de haber mostrado los resultados de la solución refleje en qué medida le gusta la solución diseñada.	2. ¿Considera usted correcta la forma en que se realiza la prevención de intrusos en Nova Servidores 7?								
	No			**No sé**			**Sí**		
	3. ¿Considera usted factible la implantación de fail2ban como sistema que prevenga de los intrusos en Nova Servidores 7?								
	Sí	**No sé**	**No**	**Sí**	**No sé**	**No**	**Sí**	**No sé**	**No**
Me gusta mucho	1	2	6	2	2	6	6	6	6
Me gusta más de lo que me disgusta	2	2	3	2	3	3	6	3	6
Me da lo mismo	3	3	3	3	3	3	3	3	3
Me disgusta más de lo que me gusta	6	3	6	3	4	4	3	3	4
No me gusta nada	6	6	6	6	4	4	6	4	5
No sé qué decir	2	3	6	3	3	3	6	3	4

Para obtener el índice de satisfacción grupal (ISG) se trabaja con los diferentes niveles de satisfacción que se expresan en la escala numérica que oscila entre +1 y – 1. El número resultante de la interrelación de las tres preguntas que indica la posición de cada encuestado en la siguiente escala de satisfacción:

1. Clara satisfacción +1
2. Más satisfecho que insatisfecho 0.5
3. No definido y contradictorio 0
4. Más insatisfecho que satisfecho -0.5
5. Clara insatisfacción -1

El índice de satisfacción grupal (ISG) se expresa en una escala numérica que va desde 1 (máxima satisfacción), hasta -1 (máxima insatisfacción). El ISG se calcula mediante la siguiente fórmula:

$$\mathrm{ISG} = \frac{\mathrm{A}(+1) + \mathrm{B}(+0.5) + \mathrm{C}(0) + \mathrm{D}(-0.5) + \mathrm{E}(-1)}{\mathrm{N}}$$

En esta fórmula A, B, C, D, E, representan la cantidad de encuestados colocados respectivamente en las posiciones de satisfacción 1; 2; 3 o 6; 4; 5 y donde N representa la cantidad total de encuestados (Fernández de Castro Fabre & López Padrón, 2014). Los resultados obtenidos de la aplicación de la encuesta se presentan en la Tabla 3.

Tabla 3 Resultados obtenidos de los encuestados

Categorías grupales de satisfacción	**N = 7**	**Escala**
Clara satisfacción	4	A
Más satisfecho que insatisfecho	3	B
No definido	0	C
Más insatisfecho que satisfecho	0	D
Clara insatisfacción	0	E
Contradictorio	0	-

De esta forma se obtiene el cálculo del ISG

$$\mathrm{ISG} = \frac{\mathrm{A}(+1) + \mathrm{B}(+0.5)}{\mathrm{N}}$$

$$\mathrm{ISG} = \frac{4(+1) + 3(+0.5)}{7} = 0.92$$

El proceso de evaluación del objetivo de la investigación mediante la técnica de IADOV confirmó su factibilidad de uso, expresando cuantitativamente en el alto ISG (0.9) y cualitativamente en los criterios emitidos en el centro de desarrollo CESOL, lo que refleja la aceptación de la propuesta, y el reconocimiento a su utilidad.

Conclusiones

De manera general se puede concluir sobre la presente investigación que existe una necesidad de desarrollar un mecanismo que permita la prevención de intrusos en la distribución Nova Servidores y otros sistemas operativos de software libre para la gestión de servidores, ello evidenciado en el análisis de los referentes bibliográficos y de las herramientas informáticas que implementan mecanismos de prevención de intrusos estudiadas. Por ello se define como propuesta efectiva para solucionar dicha necesidad, la implementación de una herramienta que permita la gestión de forma remota del IPS fail2ban. A pesar de que la aplicación de la técnica de IADOV permitió obtener un índice de satisfacción grupal elevado respecto al diseño de un Mecanismo de prevención de intrusos para Nova Servidores, es imprescindible tener en cuenta que la herramienta debe ser desarrollada, por lo que se recomienda el empleo de la

presente como referente teórico y principio de diseño para la misma. Esta investigación puede servir como base para el desarrollo de un modelo de seguridad que garantice la prevención de intrusos en los productos de software desarrollados por CESOL.

Referencias

Albo Castro, M. M., & Rodríguez Jiménez, A. (2020). La importancia de la calidad de la distribución GNU/Linux Nova para un desarrollo económico y social sostenible del país. *Serie Científica de la Universidad de las Ciencias Informáticas*, *13*(2), Artículo 2.

Campistrous, L., & Rizo, C. (2006). *El Criterio de Expertos como Método en la Investigación Educativa* [Doctoral]. Instituto Superior de Cultura Física "Manuel Fajardo".

Carles, J. (2018, mayo 6). *Instalar configurar y usar fail2ban para evitar ataques de fuerza bruta*. geekland. https://geekland.eu/instalar-configurar-y-usar-fail2ban-para-evitar-ataques-de-fuerza-bruta/

de la O, M. (2021). *Mecanismo de bloqueo a conexiones remotas que intentan accesos por fuerza bruta para nova-ltsp*. https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=2265&path%5B%5D=995

DenyHosts. (2023). [Python]. denyhosts. https://github.com/denyhosts/denyhosts (Obra original publicada en 2009)

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., & Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Investigación en educación médica*, *2*(7), 162-167.

Fail2ban. (2023). [Python]. Fail2Ban. https://github.com/fail2ban/fail2ban (Obra original publicada en 2011)

Fernández de Castro Fabre, A., & López Padrón, A. (2014). Validación mediante criterio de usuarios del sistema de indicadores para prever, diseñar y medir el impacto en los proyectos de investigación del sector agropecuario. *Revista Ciencias Técnicas Agropecuarias*, *23*(3), 77-82.

Ferraz, I. N., & Santos, C. D. dos. (2021). Organization of Free and Open Source Software Projects: In-between the Community and Traditional Governance. *BBR. Brazilian Business Review*, *18*(3), 334-352.

Fitzgerald, B., Scacchi, W., Feller, J., Hissam, S., & Lakhani, K. (2006). Understanding Free/Open Source Software Development Processes. *Software Process: Improvement and Practice*, *11*(2), 95-105. https://doi.org/10.1002/spip.255

Jaiswal, A. (2021). *Linux-the Operating System: Journal of Advances in Shell Programming*. *7*, 1-5. https://doi.org/10.37591/JoASP

Lai, C., Chavez, A., Jones, C., Jacobs, N., Hossain-McKenzie, S., Johnson, J., & Summers, A. (2021). *Review of Intrusion Detection Methods and Tools for Distributed Energy Resources* (SAND2021-1737, 1769265, 694253; pp. SAND2021-1737, 1769265, 694253). https://doi.org/10.2172/1769265

Newman, R. C. (2009). *Computer Security: Protecting Digital Resources.* Jones & Bartlett Learning.

Nova. (2023). https://www.nova.cu/

OSSEC HIDS. (2023). https://www.ossec.net/

Protegerse de ataques de fuerza bruta con Fail2ban. (2023). IONOS Ayuda. https://www.ionos.es/ayuda/seguridad/servidor-dedicado/protegerse-de-ataques-de-fuerza-bruta-con-fail2ban/

Sanchez, W. (2011). *La usabilidad en Ingeniería de Software: Definición y características*. *2*. https://core.ac.uk/download/pdf/47264961.pdf

Semeteys, R. (2008). Method for Qualification and Selection of Open Source Software. *Open Source Business Resource*, *May 2008*.

SourceForge. (2023). https://sourceforge.net/

Splunk Enterprise Security. (2023). https://www.splunk.com/en_us/products/enterprise-security.html

Vallejo de la Torre, C., Marcillo Sánchez, P. M., & Vélez, M. (2018). *Sistemas de Prevención de Intrusos (IDS) en la Gestión de la Información*. https://doi.org/10.29018/978-9942-792-39-6