RESUMEN ANALITICO EDUCATIVO
RAE

Título del texto	APROVECHAMIENTO DE SOLUCIONES DE SOFTWARE LIBRE EN EL MONTAJE Y PUESTA EN MARCHA DE UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA ORGANIZACIONES COLOMBIANAS
Nombres y Apellidos del Autor	ALEJANDRO BERNAL CASTIBLANCO
Año de la publicación	2024

Resumen del texto:

A través del tiempo la evolución en la administración de la información, adquisición de infraestructura, plataformas y servicios de información, diferentes organizaciones colombianas se han preocupado en implementar políticas, procesos y procedimientos enfocados en mitigar los diferentes ataques de ciberseguridad que se han presentado en el año 2020. De acuerdo con diferentes organizaciones dedicadas a la ciberseguridad y a la situación actual por la emergencia sanitaria COVID-19, la organización FORTINET, multinacional estadounidense, identificó 5.400 millones de intentos de ataque por ciberdelincuentes en el primer semestre del presente año.

Por consiguiente, este proyecto aplicado tiene como objetivo presentar a la comunidad interesada, las estrategias y alternativas de aprovechamiento de herramientas informáticas bajo licencia open source en el establecimiento de las operaciones de un CSIRT (Centro de Respuestas a Incidentes Informáticos), a partir de procesos de identificación, evaluación y análisis para el monitoreo, analítica de datos, explotación de información, detección y defensa de incidentes informáticos que pueden ocasionar grandes pérdidas de información en las diferentes organizaciones**.**

Palabras Claves	cibercrimen, gestión de la información, gobierno electrónico, protección de datos, seguridad.

Problema que aborda el texto:
Aumento de ataques cibernéticos, Preparación insuficiente de las organizaciones, Pérdidas económicas, Brechas de seguridad y amenazas cibernéticas en América Latina, Necesidad de un Centro de Respuesta a Incidentes Informáticos (CSIRT)

Objetivos del texto:
OBJETIVO GENERAL
Estructura un documento guía que brinde información de herramienta de software libre que puedan ser usadas en un centro de respuesta a incidentes informáticos para pequeñas y medianas empresas colombianas

OBJETIVOS ESPECÍFICOS

●Examinar documentación de herramientas de seguridad informática de software libre que puedan ser usadas en las actividades de un centro de respuestas a incidentes informáticos.

●Evaluar la usabilidad de herramientas de software libre que puedan servir como infraestructura tecnológica para respuesta a un evento o incidente informático

●Proponer la integración de herramientas de software libre para soportar las actividades de un centro de respuestas a incidentes informáticos

Hipótesis planteada por el autor:

Considerando el contexto de la creciente digitalización impulsada por la emergencia sanitaria del COVID-19, se plantea la hipótesis de que la integración de herramientas de software libre en un Centro de Respuesta a Incidentes Informáticos (CSIRT) para pequeñas y medianas empresas (PYMEs) en Colombia ofrecerá una solución viable y eficaz para abordar los desafíos de seguridad cibernética a los que se enfrentan estas organizaciones.

Se espera que la implementación de estas herramientas de software libre, con un enfoque en la detección, análisis y respuesta a incidentes informáticos, permita una mayor agilidad y eficiencia en la gestión de la seguridad de la información. La utilización de herramientas opensource específicamente adaptadas al entorno colombiano posibilitará una mejor adaptación a las necesidades y recursos de las PYMEs, al tiempo que minimizará los costos asociados con la adquisición y mantenimiento de soluciones propietarias.

Se anticipa que la evaluación de la usabilidad y funcionalidad de estas herramientas, así como su capacidad para integrarse con el entorno tecnológico existente de las PYMEs, será fundamental para determinar su efectividad en la práctica. Además, se espera que la propuesta de integración de herramientas de software libre como parte de la infraestructura tecnológica del CSIRT permita una respuesta más proactiva y eficiente ante posibles amenazas cibernéticas, fortaleciendo así la resiliencia y seguridad de las PYMEs colombianas en un entorno digital cada vez más complejo y dinámico.

Tesis principal del autor:

Proyecto Aplicado

Argumentos expuestos por el autor:

Respuesta efectiva a incidentes:

Dado por el crecimiento de los ataques cibernéticos, es fundamental que las organizaciones cuenten con mecanismos sólidos de respuesta a incidentes para proteger sus activos de información y mantener la confianza de sus clientes.

La capacidad de identificar, analizar y mitigar rápidamente los incidentes informáticos es crucial para minimizar el impacto negativo en la operación del negocio y evitar posibles repercusiones legales y financieras.

Viabilidad con la integración de herramientas de software libre:

Las herramientas de software libre ofrecen una alternativa atractiva para las organizaciones colombianas debido a su costo reducido en comparación con las herramientas licenciadas.

Al optar por herramientas de código abierto, las empresas pueden acceder a una amplia variedad de recursos de seguridad informática sin incurrir en gastos significativos de licencias de software.

Además, la comunidad de código abierto ofrece soporte continuo, actualizaciones y mejoras, lo que garantiza que las herramientas permanezcan actualizadas y relevantes para las necesidades cambiantes de seguridad.
Evaluación de usabilidad y funcionalidad:

Es importante que cada organización evalue las herramientas a implementar, de acuerdo a la lógica del negocio de cada empresa, con esto se garantizará que las herramientas seleccionadas sean intuitivas y fáciles de usar para el personal de la empresa, lo que minimizará la curva de aprendizaje y facilitará su adopción.

Además, se debe asegurar que las herramientas satisfagan los requisitos específicos de seguridad y cumplimiento de la empresa, así como su integración con el entorno tecnológico existente.

Conclusiones del texto:

En Con la implementación de un CSIRT en una organización, las diferentes herramientas articuladas ayudan a recopilar información para un análisis, con el fin de establecer un plan de acción y mitigar los riesgos, para proteger la información de una organización

Por otra parte, se pueden realizar toma de acciones preventivas para mitigar riesgos antes de que se produzca un incidente; como también tomar acciones preventivas para mitigar riesgos antes de que se produzca un incidente.

Proporcionar informes y estadísticas sobre la actividad de seguridad, para aumentar la eficiencia y eficacia de la respuesta a al incidente de seguridad, para una mejora continua en el monitoreo y detección de la amenaza. primer lugar, en el desarrollo de este artículo se logró investigar las diferentes herramientas de software libre para la integración de un CSIRT.

Por otra parte, se realiza un análisis y se seleccionan los componentes para la conformación de un CSIRT.

Finalmente, se realiza la integración de las herramientas aprovechando las bondades de cada herramienta para la puesta en marcha de un CSIRT para las organizaciones colombianas

Bibliografía citada por el autor:

POPULAR. [En Línea]. NETTIX. 20 septiembre 2020. Disponible en: https://www.nettix.com.pe/documentacion/administracion/vpn/que-es-pfsense-y-porque-es-un-firewall-tan-popular/

CAPTERA. Papertrail. [En Línea]. 2022. Disponible en: https://www.capterra.co/software/180057/papertrail

CENTRO CIBERNETICO POLICIAL. Balance Cibercrimen 2020. [En Línea]. PONAL. 2020. 2p. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

CENTRO CRIPTOLOGICO NACIONAL. GUÍA DE SEGURIDAD (CCN-STIC-810): GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En Línea]. España: CONPES. 2011. 60p. Sin Clasificar. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. [En Línea]. Bogota D.C.: CONPES. 2021. 43p. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

CORRAL, Yolanda. Construye y gestiona un SOC con herramientas Open Source. [En Línea]. YolandaCorral. 12 octubre 2020. Disponible en: https://www.yolandacorral.com/construye-y-gestiona-un-soc-con-herramientas-open-source/

CSIRT; ASOBANCARIA. QUIÉNES SOMOS: CSIRT Financiero – Equipo de apoyo para la respuesta a incidentes de Ciberseguridad para el sector financiero colombiano. [En Línea]. CSIRT Financiero. 2022. Disponible en: https://csirtasobancaria.com/quienes-somos

CYPHON. FULL STACK DETECTION AND RESPONSE. [En Línea]. 2022. 1p. Disponible en: https://cyphn.io/

DATAMEDIA. ¿Qué es Tableau?. [En Línea]. 2022. Disponible en: https://datademia.es/blog/que-es-tableau

DUPLICATI. Duplicati 2.0: Free backup software to store encrypted backups online For Windows, macOS and Linux. [En Línea]. 2022. Disponible en: https://www.duplicati.com/

EL ESPECTADOR. Detectan más de 5.400 millones de intentos de ciberataques en Colombia. En: El Espectador. [En Línea]. 21 agosto 2020. Disponible en: https://www.elespectador.com/tecnologia/detectan-mas-de-5400-millones-de-intentos-de-ciberataques-en-colombia-article/

ELASTIC. ¿Qué es el ELK Stack?. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/what-is/elk-stack

ELASTIC. El corazón del Elastic Stack, gratuito y abierto. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/elasticsearch/

ELASTIC. Logstash. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/logstash/

ELASTIC. Tu ventana al Elastic Stack. [En Línea]. 2022. Disponible en: https://www.elastic.co/es/kibana/

EveBox. EveBox. [En Línea]. EveBox. 2922. Disponible en: https://www.ibm.com/mx-es/cloud/learn/docker

GARCIA, Hernan. Suricata — IDS/IPS — Introduccion — Parte 1. [En Línea]. 24 octubre 2020. Disponible en: https://hernangarciawolf.medium.com/suricata-ids-ips-introducction-parte-1-486972a3ed22

Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Resumen de vulnerabilidades para la semana anterior. [En Línea]. COLCERT. 6 de febrero de 2022. Disponible en: http://www.colcert.gov.co/?q=acerca-de

IBM. ¿Qué es Docker?. [En Línea]. IBM Cloud Education. 23 junio 2021. Disponible en: https://www.ibm.com/mx-es/cloud/learn/docker

IMAGICLE. Faxes a un clic, no importa la ubicación. [En Línea]. 2022. Disponible en: https://www.imagicle.com/es/products/digital-fax/

INCiBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?. [En Línea]. 20 marzo 20217. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INSTITUTO NACIONAL DE CIBER SEGURIDAD. Glosario de términos de ciber seguridad: una guía de aproximación para el empresario. [En Línea]. INCIBE. 2017. 41p. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

KINSTA. ¿Qué Es Apache Web Server? Una Mirada Básica a lo que Es y Cómo

Funciona. [En Línea]. 2022. 1p. Disponible en: https://kinsta.com/es/base-de-conocimiento/que-es-apache/

LinkSYS. LinkSYS. [En Línea]. 2022. Disponible en: https://www.linksys.com/hn/p/P-WRT3200ACM/

LINUBE. LOGGLY. [En Línea]. 2022. Disponible en: https://linube.com/blog/loggly-ayuda-registros-en-orden/

MANCOMUN. OSSEC: Sistema de detección de intrusos. [En Línea]. 3 noviembre 2017. Disponible en: https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES, . Servicios CSIRT Gobierno. [En Línea]. COLCERT. 26 julio 2022. Disponible en: https://colcert.gov.co/800/w3-article-208774.html#:~:text=El%20objetivo%20principal%20del%20CSIRT%20Gobierno%2C%20es%20ofrecer,todos%20los%20funcionarios%20y%20encargados%20de%20seguridad%20digital

MORALES GONZÁLEZ, Carlos; MORENO SÁMCHEZ, Omar y ORTIGOZA PÉREZ, Johanna. PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONS DE SEGURIDAD (SOC) PARA FUERZA AÉREA COLOMBIANA. [En Línea]. Bogota D.C.: Universidad Piloto de Colombia. 2014. 94p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2786/trabajo%20de%20grado1627.pdf?sequence=1n

MVWARE. ¿Qué es vSphere Hypervisor?. [En Línea]. 2022. 1p. Disponible en: https://www.vmware.com/co/products/vsphere-hypervisor.html

NAGIOS. Nagios Enterprises. [En Línea]. 2022. Disponible en: https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

OPENWEBINARS. Qué es OpenVAS. [En Línea]. 2022. Disponible en: https://openwebinars.net/blog/que-es-openvas/

OPNSENCE. Welcome to OPNsense’s documentation!. [En Línea]. 2022. Disponible en: https://docs.opnsense.org/

OPS; OMS. COVID-19 y el rol de los sistemas de información y las tecnologías en el primer nivel de atención. [En Línea]. 23 mayo 2020. Disponible en: https://iris.paho.org/bitstream/handle/10665.2/52205/OPSEIHISCOVID19200022_spa.pdf?sequence=9

PANDA. ¿Qué es Threat Hunting y por qué es necesario. [En Línea]. PANDA SECURITY. 15 noviembre 2018. Disponible en: https://www.pandasecurity.com/es/mediacenter/adaptive-defense/threat-hunting-por-que-

necesario/

PANDORA FMS. Pandora FMS: Monitorización como servicio (MaaS). [En Línea]. 2022. Disponible en: https://pandorafms.com/es/#

PÉREZ PÉREZ, Yulis. IMPORTANCIA DE LA CIBERSEGURIDAD EN COLOMBIA. [En Línea]. Bucaramanga: Universidad Piloto de Colombia. 2014. 9p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

QUILORA VALERAZO, Lisbeth. Análisis de Vulnerabilidades de Seguridad Informática, del Sistema de Gestión Médica SISMEDICALEC, de la empresa Incomsis... [En Línea]. Ambato Ecuador: Universidad Técnica de Ambato. 2019. 135p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31771/alsantillanm.pdf?sequence=1&isAllowed=0079

RAMIREZ NAVIA, Fernando. CACTI: Monitoreo de Red y Reportes Gráfico Opensource. [En Línea]. ITSOFTWARE. 21 septiembre 2017. Disponible en: https://www.mancomun.gal/es/artigo-tic/ossec-sistema-de-deteccion-de-intrusos/

REDCANARY. 2021 Gartner Market Guide for MDR Services: Behind the research. [En Línea]. 10 diciembre 2021. 1p. Disponible en: https://redcanary.com/blog/gartner-2021-market-guide-to-mdr/

REDHAT. ¿Qué es el open source?(CCN-STIC-810): GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En Línea]. RedHat. 24 ictubre 2019. Disponible en: https://www.redhat.com/es/topics/open-source/what-is-open-source

REPUBLICA. Sphinx, motor de búsqueda de texto OpenSource. [En Línea]. 24 JULIO 2007. Disponible en: https://www.republica.com/gizmos/sphinx-motor-de-busqueda-de-texto-opensource-20070724-14061523187/

RETIREMENT. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. [En Línea]. 23 enero 2018. Disponible en: https://blog.rch1.com/blog/the-crucial-role-of-the-csirt

ROUNDCUBE. About the Roundcube webmail project. [En Línea]. 2022. 1p. Disponible en: https://roundcube.net/about/

SANTILLÁN MOSQUERA, Angela. IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN EMPRESARIAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA JARDINES CRISTO REY LTDA. [En Línea]. PASTO: Universidad Nacional Abierta Y A Distancia. 2019. 140p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31771/alsantillanm.pdf?sequence=

1&isAllowed=0079

SAOUT. dm-crypt: a device-mapper crypto target. [En Línea]. 2022. Disponible en: https://www.saout.de/misc/dm-crypt/

SECURITY ONION SOLUTIONS. Security Onion: Visión General. [En Línea]. 2022. Disponible en: https://securityonionsolutions.com/software/

SEMANA. La tecnología ha sido clave en estos momentos de crisis. En: SEMANA. [En Línea]. 20 abril 2020. ISSN 2745-2794. Disponible en: https://www.dinero.com/tecnologia/articulo/columna-la-tecnologia-ha-sido-clave-en-estos-momentos-de-crisis-por-eliseo-barcas-20-de-abril/284442

SERVICIOS DE RED NOONA. Sistema de Monitoreo Zenoss 4.2. [En Línea]. 2022. Disponible en: https://serviciosderednoona.wordpress.com/sistema-de-monitoreo-zenoss-4-2/

SOLR TUTORIAL. Qué es Solr. [En Línea]. 2022. Disponible en: https://solrtutorial.es/que-es-solr.html

SOURSEFORGE. AlienVault OSSIM. [En Línea]. 2022. Disponible en: https://sourceforge.net/projects/os-sim/

SQUID. Squid: Optimising Web Delivery. [En Línea]. 2022. Disponible en: http://www.squid-cache.org/

THEHIVE PROYECT. THEHIVE: A 4-IN-1 SECURITY INCIDENT RESPONSE PLATFORM. [En Línea]. THEHIVE. 2022. Disponible en: https://thehive-project.org/
UCLG-CGLU. Tecnologías digitales y la pandemia de COVID-19. [En Línea]. 2022. 17p. Disponible en: https://www.uclg.org/sites/default/files/eng_briefing_technology_es.pdf

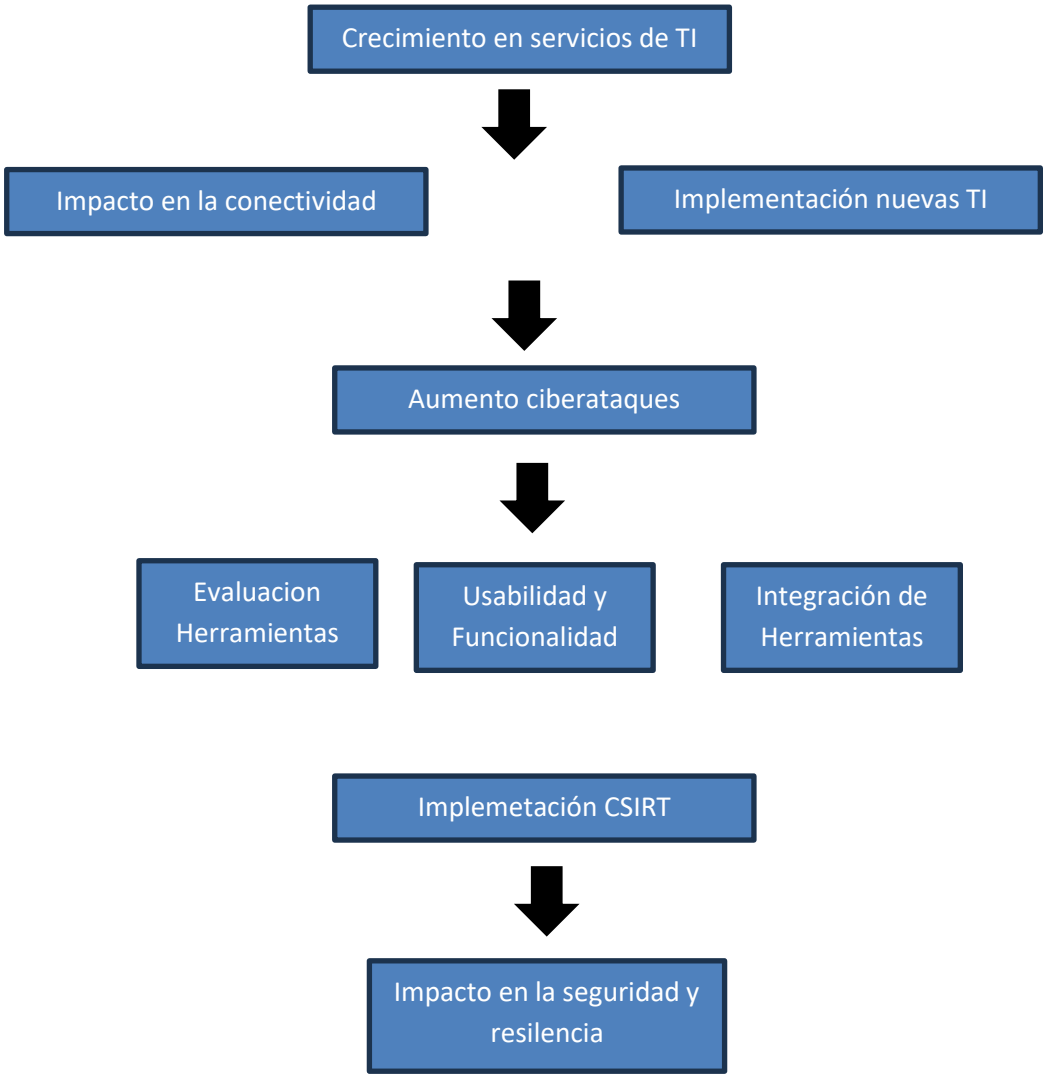
WELIVESECURITY. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. [En Línea]. 18 mayo 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/#:~:text=Dado%20este%20escenario%20de%20evoluci%C3%B3n,Computer%20Security%20Incident%20Response%20Team

ZABBIX. Zabbix technical demo video: Explora el resumen técnico rápido de las funciones de Zabbix.. [En Línea]. 2022. Disponible en: https://www.zabbix.com/la/demo

Nombre y apellidos de quien elaboró este RAE	Alejandro Bernal Castiblanco

Fecha en que se elaboró este RAE	15/06/2024

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:



Comentarios finales:

La adopción de herramientas de software libre en un CSIRT no solo ofrece una solución costo-efectiva para las PYMEs colombianas, sino que además proporciona una mayor flexibilidad y personalización en la implementación de medidas de seguridad cibernética.

En consecuencia, la naturaleza de código abierto de estas herramientas brinda la oportunidad de acceder a comunidades activas de desarrollo y contribuir a la mejora continua de la seguridad informática.

Por lo tanto, al adaptarse así a las necesidades específicas de cada organización, estas herramientas garantizan una respuesta eficiente y adaptada a las amenazas emergentes en el entorno digital actual.