Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	05/03/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de sistemas
Título:	DISEÑO TÉCNICO DEL EQUIPO DE RESPUESTA ANTE INCIDENCIAS DE SEGURIDAD INFORMÁTICAS (CSIRT) EN LA EMPRESA "CYBERSECURITY DE COLOMBIA LTDA"
Autor(es):	Durán Granados José Enrique
Palabras Claves:	CSIRT, Seguridad, Información, Incidentes, Tecnología
Descripción:	Desarrolla acciones encaminadas en la puesta en funcionamiento inicial de un CSIRT tales como revisión de herramientas tecnológicas para el desarrollo de funciones, selección de las herramientas de acuerdo al tipo de licenciamiento, uso y disponibilidad, la propuesta de estructura organizacional con referente a diferentes casos de éxito y finalmente la construcción de un laboratorio basado en la formulación de un escenario problema que atienda a necesidades cercanas a las presentadas en la realidad usando un entorno controlado y verificable.

Fuentes bibliográficas destacadas:

CCIT-POLICIA NACIONAL DE COLOMBIA. 2020. Informe de las tendencias del cibercrimen en Colombia (2019-2020). [En línea] 20 de 10 de 2020. [Citado el: 28 de 11 de 2020.] https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf.

ESPAÑA. CENTRO CRIPTOLÓGICO NACIONAL. 2011. Guía de Creación de un CERT/CSIRT. [En línea] 09 de 2011. [Citado el: 27 de 11 de 2020.] 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.

GARCÍA, Mónica Alexandra. 2014. Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea] 2014. [Citado el: 28 de 11 de 2020.] http://repositorio.espe.edu.ec/bitstream/21000/8063/1/T-ESPE-047639.pdf.

OSPINA JARRO, Eduardo Andres. 2018. Modelo de protección de activos de información estratégica: una lectura desde la dirección y gerencia de la seguridad de la información. [En línea] 2018. [Citado el: 28 de 11 de 2020.]

<table>
<tr><td colspan="2">https://repository.urosario.edu.co/bitstream/handle/10336/20003/UR-ArtInvestigacion-EduardoAndresOspinaJarro.pdf?sequence=1&isAllowed=y.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). 2016. Buenas prácticas para establecer un CSIRT nacional. [En línea] 04 de 2016. [Citado el: 6 de 1 de 2020.] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

SÁNCHEZ, Héctor Mauricio y RODRÍGUEZ PARRA, Alexander. 2019. Constitución de un CSIRT para una Entidad Financiera en Colombia. [En línea] 12 de 2019. [Citado el: 28 de 11 de 2020.] https://proyectosmaestrias.virtual.uniandes.edu.co/images/TNQzugjz0p1d26AM6aQVaAs8MbHg9RzfnHBnKmhf.pdf.</td></tr>
<tr><td>Contenido del documento:</td><td>Definición del problema
antecedentes del problema
formulación del problema
justificación
objetivos
objetivos general
objetivos específicos
Marco referencial
Marco teórico
Marco conceptual
Marco histórico
Antecedentes o estado actual
Marco legal
Diseño metodológico
Desarrollo de los objetivos
Fase 1: recopilación información relacionada con herramientas de software que permitan desarrollar las actividades del CSIRT, teniendo presente que sus servicios son reactivos y proactivos.
Fase 2: definición del mapa de la estructura ti del CSIRT teniendo como base las mínimas dependencias para su correcto funcionamiento</td></tr>
</table>

	Fase 3: consolidación de la información necesaria acerca de las herramientas software necesarias para que el CSIRT pueda ejecutar sus actividades correctamente. Fase 4: desarrollo del diseño de un laboratorio controlado por medio del uso de máquinas virtuales que permita la ejecución de pruebas del software que se utilizara en el CSIRT. Conclusiones Recomendaciones Bibliografía Anexos
Marco Metodológico:	El desarrollo del proyecto se lleva a cabo usando la Metodología Aplicada, debido a que esta se caracteriza principalmente por la aplicación de conocimientos adquiridos previamente y la obtención de otros complementarios durante el desarrollo del proceso.
Conceptos adquiridos :	Construcción de equipos técnicos orientados las TI, desarrollo de laboratorios controlados de seguridad informática, selección y clasificación de herramientas software.
Conclusiones:	El diseño técnico el equipo de respuesta ante incidencias de seguridad informática (CSIRT) en La Empresa “Cybersecurity de Colombia LTDA” generó como resultado una experiencia altamente favorable para la empresa ya que de esta forma se preparó el camino en el marco de la consolidación tanto de las actividades como de las necesidades el CSIRT teniendo en cuenta la perspectiva técnica y administrativa.