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

Tamaño de letra: 12

Tipo de letra: Arial

Interlineado: Sencillo

Borrar letra de color gris*

Fecha de Realización:	03/10/2021
Programa:	Seguridad informática
Línea de Investigación:	Monografía
Título:	Diseño de un sistema de seguridad de prevención y gestión de riesgo para el Instituto de Investigaciones Ambientales del Pacifico John Von Neumann que minimice los ataques cibernéticos y asegure los activos de información a partir de la norma ISO 27001
Autor(es):	Paz Lagarejo Libia Yisseth
Palabras Claves:	Seguridad, activos de información, ataques, vulnerabilidad, controles
Descripción:	Este proyecto fue desarrollado con el propósito de diseñar un sistema de seguridad de prevención y gestión de riesgo a partir de la norma ISO 27001 para una entidad del sector público, buscando minimizar los ataques cibernéticos y asegurar los activos de información. Por consiguiente, se desarrollan 4 estrategias para el diseño del sistema de seguridad. Como primero se realiza un inventario de activos de información para determinar los riesgos y fallas a los que están expuestos; Luego, se evaluarán los riesgos de acuerdo con la probabilidad de ocurrencia e impacto utilizando herramientas como encuestas análisis para la detección de amenazas, Lo que permitirá definir los controles y dominios de acuerdo con

	la norma ISO 27001 para el tratamiento efectivo de riesgos y vulnerabilidades. Por último, establecer políticas de seguridad informática donde se definan responsables, actividades y procesos a seguir.

Fuentes bibliográficas destacadas:

BLOG ESPECIALIZADO EN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA. Componentes de los sistemas de gestión de seguridad de la información. 2020.

CAMELO, L. Seguridad de la Informacion en Colombia. Colombia: Marco legal de Seguridad de la Información. 2010.

ECHEVERRY, F. (s.f.). Inicio y evolucion de la seguridad informatica en el mundo. Colombia: Universidad Piloto Colombia.

EUGENE SPAFFORD. y JAMES P. ANDERSON. Un pionero en seguridad de la información. Security&privacy, 2008. 9 Vol. 6.

INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO. Pacifico, I. d. Nosotros

INSTITUTO NACIONAL DE ESTANDARES Y TECNOLOGIA. 2019.

JYCELL-NUMAEL. Seguridad Informática. Historia de la seguridad informatica. 2017.

Contenido del documento:

	DE LA INFORMACION PARA EL INSTITUTO DE INVESTIGACIONES AMBIENTALES DEL PACIFICO JOHN VON NEUMANN ..... ¡Error! Marcador no definido. **9. CONCLUSIONES....** ¡Error! Marcador no definido. **10. RECOMENDACIONES** ¡Error! Marcador no definido. **11. BIBLIOGRAFÍA.....** ¡Error! Marcador no definido. **12. ANEXOS ..** ¡Error! Marcador no definido.
Marco Metodológico:	La metodología por utilizar para conocer el estado actual de la seguridad de los activos de información frente a vulnerabilidades o ataques. Se procura identificar, vulnerabilidades y amenazas, a las que se expone la información institucional a la hora de procesar, transportar, almacenar y la disposición final de la información. Para emprender esta metodología se tiene cuenta 3 aspectos: • Diagnóstico • Análisis con Magerit • Escaneo de vulnerabilidades **DIAGNÓSTICO.** Tiene como principio realizar una evaluación del estado de seguridad informática a todos los activos de la institución En concordancia, se toma como referencia los controles de la norma Técnica Colombiana NTC ISO/IEC 27001:2013, diagnóstico de la seguridad de la información y el resultado de las encuestas. (ver anexo G) El Instituto de Investigaciones Ambientales del pacifico en el ámbito de seguridad, no cuenta con políticas que respalden la seguridad de la

	información como activo más importante de la misma. Los equipos de cómputo no cuentan con seguridad lógica es decir cualquier usuario puede ingresar y manipular la información. No cumple con la definición de roles y responsabilidad para atender casos de incidencias en cuanto a la seguridad. Se propone realizar cada una de las actividades para asegurar los activos y tener un plan de seguridad informática como lo exige el Ministerio de las TIC a nivel nacional lo que contribuye a la seguridad digital. ANÁLISIS – MAGERIT. Existen 4 pasos para el análisis de riesgos 1. Identificar los riesgos 2. Determinar al nivel de criticidad de cada riesgo 3. Clasificar los riesgos, donde se toma como referencia el proceso Magerit 4. Determinar las acciones necesarias. ESCANEO DE VULNERABILIDADES. Se utilizan las herramientas wappalyzer y OWASP ZAP versión 2.11 para identificar las posibles vulnerabilidades que afectan a los activos de información y definir controles de acuerdo a la ISO 27001. Resultados: Se realizo una prueba de escaneo de seguridad al sitio web del Instituto de Investigaciones Ambientales del Pacifico con las siguientes herramientas: • Con la herramienta wappalyzer instalada en el explorar de Google Chrome.

	“Wappalyzer es una extensión del navegador que descubre las tecnologías utilizadas en los sitios web. Detecta sistemas de administración de contenido, tiendas web, servidores web, marcos de JavaScript, herramientas de análisis y muchos más.” En resumen, el sitio web tiene apache 2.4.29, sistema operativo Ubuntu con una tipografía de Google Font API que admite archivos de código abierto para su diseño. por consiguiente y analizar más de fondo las vulnerabilidades del servidor utilizado por la página web del IIAP apache 2.4.29 se encontraron 4 vulnerabilidades con el análisis de CVI METRI con los siguientes resultados: Gravedad de vulnerabilidad alta con 8.1 lo que indica que está en riesgo la página Co unas métricas de impacto en Confidencialidad, integridad y disponibilidad altos. También, se realizó un análisis de vulnerabilidades con la herramienta OWASP ZAP versión 2.11 la herramienta owasp zap es un escáner de seguridad con la intención de realizar pruebas de penetración para comprobar si existen vulnerabilidades. Efectivamente el resultado fueron 10 alertas encontradas en el sitio web del IIAP dos con riesgo alto, dos riesgos medios y el demás riesgo bajo. Lo que indica que si hay riesgo de información en el sitio web y de autenticación. El Instituto de Investigaciones Ambientales del Pacifico cuenta con un entorno físico de 2 plantas, cuanta con 1 servidor donde se almacena información solamente institucional, una UPC para regular la energía eléctrica y con 30 equipos de cómputo.
Conceptos adquiridos :	Inventario de activos de información, manejo de controles según la ISO 27001
Conclusiones:	El diseño de un sistema de seguridad, prevención y gestión del riesgo bajo el contexto

	de la norma ISO 27001, tiene como objeto minimizar los ataques cibernéticos y la complejidad en que se encuentra la seguridad de la información. Este sistema incorpora herramientas expuestas por la normatividad ISO 27001 en cuanto a la confidencialidad, integridad y disponibilidad de la información. En el presente proyecto se describe la importancia de la gestión del riesgo que se presentan en la seguridad de la información, los estándares y metodología para el desarrollo del análisis de vulnerabilidades en la entidad como la ISO 27001, Magerit, y escaneo de vulnerabilidades con la herramienta OWASP ZAP versión 2.11. Todas las metodologías y normas mencionadas en este proyecto permitieron realizar un análisis evaluativo en referencia a los activos, amenazas, controles y procedimientos para finalmente obtener un tratamiento efectivo de los riesgos y vulnerabilidades de acuerdo con la ISO 27001 cuyo objeto sea la protección de los activos y recursos de la información. La dificultad de la inseguridad informática no solamente se trata de identificar los riesgos, es también mantener en constante actualización todas las herramientas que ayuden a minimizar los ataques, la disponibilidad del personal de seguridad, los reporte o alertas de todos los casos posibles de riesgo, el continuo desarrollo de nuevas aptitudes y ética profesional. Un Sistema de Gestión de Seguridad de la Información no se implementa por llenar requisitos, al contrario, se implementa buscando objetivos que agreguen valía a la organización. También, determinar los activos de información, los riesgos y fallas de seguridad que están presentes en la infraestructura tecnológica del Instituto de Investigaciones Ambientales del Pacifico.

	Una vez se realiza la evaluación y análisis de riesgo, la entidad tiene una herramienta clave para el tratamiento de vulnerabilidades, diagnóstico sobre el estado de seguridad informática y activos de información. En base a la evaluación es posible actualizar o tener en cuenta las políticas que ayudan a la corrección de vulnerabilidades detectados y la gestión de seguridad a lo largo del tiempo, para corroborar y avalar que las vulnerabilidades encontradas anteriormente no sean un problema o generen más dificultad para el desarrollo de las actividades, investigación, misión y visión de la institución.