

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

DISEÑO Y EVALUACIÓN DE PROYECTOS - NRC 16504

INTEGRANTES:

ANDRANGO JESSICA
FALCONI SEBASTIAN

IMPLEMENTACIÓN DE UN AMBIENTE DE
PRUEBAS PARA LOS SISTEMAS DE
TOLERANCIA A FALLOS DE UNA
EMPRESA (BRG) UTILIZANDO TÉCNICAS
DE CIBERSEGURIDAD.

PROBLEMÁTICA

Deficiencia de controles de seguridad de la información y la escasez medidas de prevención de ciberataques en el país.

OBJETIVO

Asegurar la integridad y la confidencialidad de los datos sensibles y críticos de la organización mediante técnicas de ciberseguridad.

Luis, M. B. J. (2019, 1 febrero). Diseño de un modelo de seguridad de la información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de educación: caso de estudio Universidad Regional Autónoma de los Andes, extensión Tulcán.
<https://repositorio.uisek.edu.ec/handle/123456789/3260>

INVESTIGACIÓN

CIBERATAQUES EN ECUADOR

El 11 de abril del 2019 representa una fecha importante para los ataques de ciberseguridad en Ecuador, debido al asilo a Julian Assange se registraron más de 40 millones de ciberataques a sitios web de entidades como la Presidencia, el SRI, y el Banco Central, entre otras instituciones importantes, por lo que el ministerio de defensa activó su protocolo de seguridad, aunque su funcionamiento no se ha dado a conocer.

Chang, J. E. (2020). Análisis de ataques ciberneticos hacia el Ecuador. Revista Científica Aristas, 18-27. https://revistacientificaistjba.edu.ec/images/joomgallery/details/gallery_2/gallery_1_9/Edicion_Mayo_2020_COMPLETO-c.pdf#page=19

Morán Maldonado, N. M. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática (Bachelor's thesis). <https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf>

INVESTIGACIÓN

“Las universidades ecuatorianas, tienen el gran reto de promover carreras en el ámbito de ciberseguridad, de impulsar cursos cortos de capacitación continua relacionadas a este tema, de fomentar en sus alumnos la cultura de prevención de riesgos tecnológicos especialmente en las redes sociales.” (Villacís, 2022)

“Ecuador está en el puesto 82 del NCSI, clasificado como un país con ciberseguridad deficiente en general, que coincide con la percepción de los usuarios.” (Chang, 2020)

En base a datos de Kaspersky Lab, Ecuador ocupa el primer lugar en América del Sur en la cantidad de amenazas en tiempo real reportado por esta organización.

Morán en su trabajo del 2021 menciona que en 2019 existieron 5048 casos de denuncias de ciberseguridad en el Ecuador, lo que evidencia la falta de mecanismos efectivos de seguridad implementados en el país.

Morán Maldonado, N. M. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática (Bachelor's thesis).

EVALUACIÓN Y ANÁLISIS DE RIESGOS

Esta etapa implica identificar y comprender las vulnerabilidades y amenazas potenciales que podrían afectar las áreas críticas de TI del BGR (La empresa). Se lleva a cabo una evaluación exhaustiva de los sistemas y activos de información para determinar sus vulnerabilidades y evaluar los posibles impactos de las amenazas. Vamos a utilizar estándares internacionales reconocidos, como ISO 27001, NIST SP 800-30 o el Marco de Ciberseguridad del NIST, como guías para este proceso de evaluación y análisis de riesgos.

Luis, M. B. J. (2019, 1 febrero). Diseño de un modelo de seguridad de la información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de educación: caso de estudio Universidad Regional Autónoma de los Andes, extensión Tulcán.
<https://repositorio.uisek.edu.ec/handle/123456789/3260>

La ISO/IEC 27001 proporciona un marco para que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un SGSI. Este sistema se centra en garantizar la confidencialidad, integridad y disponibilidad de la información crítica de la organización, así como en gestionar los riesgos relacionados con la seguridad de la información de manera efectiva

NIST SP 800-30 es una publicación especial del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Este documento proporciona orientación sobre la gestión de riesgos de seguridad de la información. Específicamente, detalla el proceso de evaluación y gestión de riesgos de seguridad de la información en sistemas de tecnología de la información. Ofrece pautas detalladas sobre cómo identificar, evaluar y mitigar los riesgos de seguridad de la información en una organización.

El Marco de Ciberseguridad del NIST es una guía de buenas prácticas, se ha convertido en un recurso ampliamente adoptado por organizaciones de diversos sectores y tamaños como una herramienta para mejorar la resiliencia cibernética y la capacidad de respuesta ante amenazas digitales.

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Una vez identificados los riesgos y amenazas, se procede a implementar medidas de seguridad adecuadas para mitigarlos y proteger las áreas críticas de TI del BGR. Esto incluirá la implementación de controles de seguridad técnicos, como firewalls, sistemas de detección de intrusiones, y autenticación multifactor, así como la adopción de políticas y procedimientos de seguridad robustos.

Sistemas de Detección de Intrusos (IDS): Estos sistemas monitorean el tráfico de red o los eventos en los sistemas informáticos en busca de patrones o comportamientos sospechosos que puedan indicar un intento de intrusión. Los IDS pueden ser basados en red, que analizan el tráfico de red, o basados en host, que supervisan la actividad en sistemas individuales.

PRUEBAS

ATAQUES DE FUERZA BRUTA

Un IDS puede detectar intentos repetidos de acceso no autorizado mediante ataques de fuerza bruta, donde un atacante intenta adivinar contraseñas o credenciales de acceso.

ATAQUES DE DENEGACIÓN DE SERVICIO (DOS) Y DISTRIBUIDOS (DDOS)

Un IDS puede detectar patrones de tráfico anormal asociados con ataques de denegación de servicio, como un aumento repentino en el tráfico o la aparición de patrones de tráfico malicioso.

PHISHING

Algunos IDS pueden integrarse con sistemas de prevención de phishing para identificar y bloquear los correos electrónicos de phishing entrantes, así como las comunicaciones salientes que podrían contener información confidencial, ayudando a prevenir la divulgación de datos sensibles como resultado de ataques de phishing.

Áreas críticas



SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Area Gestión de Aplicaciones
Seguridad de la información

INFRAESTRUCTURA TECNOLÓGICA

Area de Infraestructura.
Gestión de redes

GESTIÓN DE LA SEGURIDAD CIBERNÉTICA

Infraestructura de redes

REFERENCIAS

- Chang, J. E. (2020). Análisis de ataques cibernéticos hacia el Ecuador. Revista Científica Aristas, 18-27. https://revistacientificaistjba.edu.ec/images/joomgallery/details/gallery_2/gallery_1_9/Edicion_Mayo_2020_COMPLETO-c.pdf#page=19
- Morán Maldonado, N. M. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática (Bachelor's thesis).
- Morán Maldonado, N. M. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática (Bachelor's thesis). <https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf>

DESARROLLO DE UN SISTEMA DE DETECIÓN DE ATAQUES CIBERNÉTICOS A TRAVÉS DEL USO DE MACHINE LEARNING

DESARROLLO

Recopilación de datos: Para entrenar un modelo de machine learning, se necesitará datos relevantes. Esto puede incluir registros de eventos de red, datos de tráfico de red, registros de servidores, entre otros. Es esencial contar con un conjunto de datos amplio y representativo para que el modelo pueda aprender correctamente los patrones de los ataques.

Una vez que los datos estén preparados, se puede seleccionar el algoritmo de machine learning más adecuado. Algunas opciones comunes para la detección de ataques cibernéticos incluyen árboles de decisión, bosques aleatorios, SVM (Support Vector Machines) y redes neuronales.

Entrenando así el modelo utilizando el conjunto de datos preparado y ajustando los hiperparámetros según sea necesario para optimizar el rendimiento.

REFERENCIAS

Chang, J. E. (2020). Análisis de ataques cibernéticos hacia el Ecuador. Revista Científica Aristas, 18-27.
https://revistacientificaistjba.edu.ec/images/joomgallery/details/gallery_2/gallery_1_9/Edicion_Mayo_2020_COMPLETO-c.pdf#page=19

Morán Maldonado, N. M. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática (Bachelor's thesis).

Morán Maldonado, N. M. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática (Bachelor's thesis).
<https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf>