MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Gestión de Unidad de Seguridad de la Información y Ejecución de Pruebas de Seguridad a Sistemas de Información

Autor: Víctor Andrés León Acosta

Guía: Roque Jacinto Hernández Bustos

Presentando como parte de los requisitos para el título de magister en ciberseguridad.

Guayaquil, 4 de marzo del 2024

PROPUESTA DE CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN

Yo, LEÓN ACOSTA, VÍCTOR ANDRÉS, autor del trabajo de titulación "Gestión de Unidad de Seguridad de la Información y Ejecución de Pruebas de Seguridad a Sistemas de Información", certifico que el ensayo reflexivo es una creación de mi autoría, por lo que sus contenidos son originales, de exclusiva responsabilidad de su autor y no infringen derechos de autor de terceras personas. Con lo cual, exonero a la Universidad Casa Grande de reclamos o acciones legales.

Firmado electrónicamente por:
VICTOR ANDRES LEON ACOSTA

LEÓN ACOSTA, VÍCTOR ANDRÉS

0924439300

LEÓN ACOSTA, VÍCTOR ANDRÉS en calidad de autor y titular del trabajo de titulación "Gestión de Unidad de Seguridad de la Información y Ejecución de Pruebas de Seguridad a Sistemas de Información" para optar por la **Maestría en Ciberseguridad**, autorizo a la Universidad Casa Grande para que realice la digitalización y publicación de este trabajo de titulación en su Repositorio Digital de acceso abierto, con fines estrictamente académicos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Asimismo, autorizo a la Universidad Casa Grande a reproducir, distribuir, comunicar y poner a disposición del público mi documento de trabajo de titulación en formato físico o digital y en cualquier medio sin modificar su contenido, sin perjuicio del reconocimiento que deba hacer la Universidad sobre la autoría de dichos trabajos.

Firmado electrónicamente por:
VICTOR ANDRES LEON ACOSTA

LEÓN ACOSTA, VÍCTOR ANDRÉS

0924439300

Gestión de Unidad de Seguridad de la Información y Ejecución de Pruebas de Seguridad a Sistemas de Información

Introducción

En el presente trabajo de titulación detalla cómo la Maestría en Ciberseguridad de la Universidad Casa Grande facilita la incursión en el desafiante y apasionante mundo de la ciberseguridad. Abordando dos perspectivas: la gestión (gobernanza) y las técnicas y tácticas para proteger el activo más preciado de toda organización: la información.

Un activo de información, es todo aquello que tiene información y valor para la empresa y que por lo tanto debe ser protegido, implementando las medidas más acordes a la relevancia que tiene el activo para el llevar a cabo las diferentes operaciones de la empresa (Borrero, 2019)

El enfoque de gestión que cuenta la Maestría en Ciberseguridad nos permite evaluar los controles mínimos necesarios para garantizar o minimizar el impacto de un posible ataque.

El enfoque técnico se incluye técnicas y tácticas que pueden ser implementadas para proteger la información, como son:

- Criptografía
- Seguridad de redes
- Análisis forense digital
- Gestión de riesgos
- Políticas de seguridad

Cada materia de la maestría, contribuye de manera positiva al desarrollo profesional del maestrante, permitiéndole:

- Comprender las normas de seguridad ISO 27001 la cual establecen marco de referencia para la implementación de un sistema de gestión de seguridad de la

información.

- Proponer actualizaciones a los procesos internos de seguridad de la información,
- Cumplimiento normativo.

En el entorno laboral en el cual el maestrante se ha venido desenvolviendo es el sector financiero tanto público como privado sector que por su naturaleza debe cumplir con normativa legal en temas relacionados con la seguridad informática la cual esta contantemente en evolución.

En un mundo cada vez más interconectado es necesario estar actualizado y preparado para afrontar los desafíos que se presentan. Según datos de la Asobanca la banca ecuatoriana es uno de los sectores con mayor crecimiento en la digitalización de sus productos, a través de página web, aplicaciones móviles, asistentes virtuales tipos chatbots, los sistemas de pago sin contacto entre otros.

El aumento de estos servicios o canales digitales supone un reto en temas de ciberseguridad ya que la adaptación de estos nuevos modelos de negocios bancarios para satisfacer la demanda de los clientes, ya que estos servicios se traducen en aumentar el número de activos de la información publicados y por ende un aumento en la superficie de expuesta a posibles ataques.

La Maestría en Ciberseguridad ha ayudado al maestrante a desempeñarse de mejor manera en el rol de gestos como especialista de riesgo operativo las materias que aportaron la visión de la gobernanza de la ciberseguridad como son:

- Gerencia, Operación y Planificación de la Ciberseguridad.
- Estrategias y Políticas Multilaterales para la Ciberseguridad

En el rol técnico como ingeniero de ciberseguridad las materias que aportaron el apartado técnico son:

- Tecnología, Modelos y Técnicas de Ciberseguridad
- Seguridad de Aplicaciones y Bases de Datos
- Hacking Ético y Análisis del Ciberataque

Desarrollo

Gerencia, Operación y Planificación de la Ciberseguridad, fue el punto inicial para comprender la necesita de realizar la planificación estratégica en el área de seguridad de la información y así dar cumplimento al marco normativo, a los estándares de seguridad como son la ISO 27001 y la mejora en las políticas y procedimientos del área.

Estrategias y Políticas Multilaterales para la Ciberseguridad, se abordaron temas de vital importancia para la gestión de la seguridad de la información además de entender lo importante del cumplimento normativo como lo es en el sector financiero.

La Codificación de las Normas de Superintendencia de Bancos establece en el Libro, Título IX.- De la Gestión y Administración de Riesgos, Capítulo V, Norma de Control para la Gestión de Riesgo Operativo, Sección VIII.- Seguridad de la Información como en la cual se indica la necesidad de contar con un comité de seguridad de la información que se encargara de evaluar y supervisar el sistema de gestión de seguridad de la información.

Tecnología, Modelos y Técnicas de Ciberseguridad, ha permitido la actualizar los conceptos referentes a la ciberseguridad y destacar la importancia de tomar medidas preventivas a nivel técnico que disminuya el riesgo de sufrir un ataque informático.

Seguridad de Aplicaciones y Bases de Datos, Se prioriza la importancia de asegurar las aplicaciones ya sean estas web , escritorio o móvil esto se logra con la aplicación de prueba de seguridad de aplicaciones estáticas (SAST) el cual es un método que permite realizar pruebas para asegurar una aplicación y revisa el código fuente, por otro lado la prueba de seguridad de aplicaciones dinámicas (DAST) es un método de prueba que utiliza un enfoque de caja negra, es decir los probadores no tiene conocimiento o acceso del código fuente de la aplicación o a su funcionalidad interna.

Hacking Ético y Análisis del Ciberataque, Esta materia nos brindó la oportunidad de comprender la ejecución de un ciberataque y así poder preparar nuestra defensa ya que si conocemos como trabaja nuestro adversario los ciberdelincuentes, El ciberdelincuente es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware. (incibe, 2020).

También los permitió conocer los tipos de ataques y las herramientas que estos utilizan para cometer actividades ilícitas. Esto ayudo a dar recomendaciones de mejores prácticas para los controles ya implementados y así mitigar las consecuencias de sufrir un ataque informático.

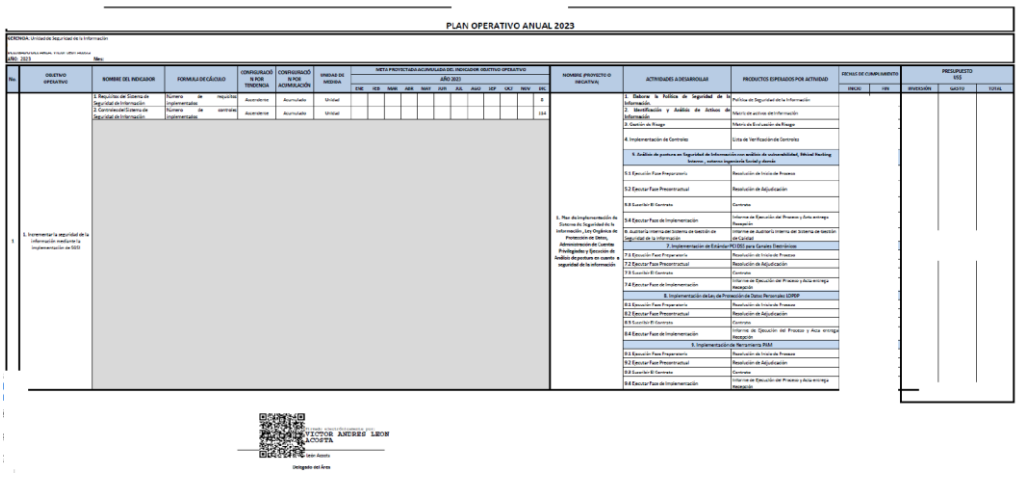
Implementación

Dentro el sector financiero público y privado sector donde se puso en práctica los conocimientos adquiridos en la Maestría en Ciberseguridad de la Universidad Casa Grande, en la primera organización del sector financiero ámbito público donde se desempeñó un rol de Gestos en temas relacionados a la seguridad de la información.

Como parte de la Gestión de Unidad de Seguridad de la Información y Ejecución de Pruebas de Seguridad a Sistemas de Información se aplicó lo aprendido en la Materia de **Gerencia, Operación y Planificación de la Ciberseguridad** lo cual fue la Planeación Operativa Anual (POA) de la Unidad de Seguridad de la Información todo esto alineado a los objetivos estratégicos de la institución.

Figura 1

1. Plan Operativo Anual – POA



El POA 2023 se propone el Plan de implementación de Sistema de Seguridad de la Información donde se detallan las actividades macros que se deben desarrollar para concepción de la implementación de un sistema de seguridad de la Información.

Luego de definir las actividades macros que se van a desarrollar en la unidad de seguridad de la información se elabora un documento donde se asignan tareas y responsabilidades.

Figura 2

2. Asignación de tareas Unidad de Seguridad de la Información

No.	TAREA	FRECUENCIA	CATEGORIA	ÁREA
1	Matriz de Roles	ÚNICA	Levantamiento de Información	USI
2	Levantar Activos de Información	SEMESTRAL	Levantamiento de Información	USI
3	Seguimiento de Matriz de Riesgo	MENSUAL	Seguimiento y Control	USI
4	Depuración Active Directory AD	SEMESTRAL	Seguimiento y Control	USI
5	Depuración Cobis	SEMESTRAL	Levantamiento de Información	USI
6	Llamar a Comité SIG	ÚNICA	Documentación	USI
7	Revisión de Documentación de TIC	BAJO DEMANDA	Documentación	USI
8	Elaborar Manual de Roles	ÚNICA	Documentación	USI
9	Revisión de implementación de observaciones Riesgo Operativo	MENSUAL	Seguimiento y Control	USI
10	Investigación de SharePoint Capacidades	ÚNICA	Levantamiento de Información	USI
11	Elaboración de Informe Cartera	ÚNICA	Documentación	USI
12	Ejecución de Remediación cartera	ÚNICA	Documentación	USI
13	Elaboración de Informe Banca Electrónica	ÚNICA	Documentación	USI
14	Administración de Credenciales Banca Electrónica	MENSUAL	Seguimiento y Control	USI
15	Tarjeta MasterCard Administración	MENSUAL	Seguimiento y Control	USI
16	Canales Seguro DINARDAP	BAJO DEMANDA	Seguimiento y Control	USI
17	Reclamos BANRED	BAJO DEMANDA	Seguimiento y Control	USI
18	Depuración de Exchange	MENSUAL	Seguimiento y Control	USI
19	Revisión de Documentación Reservada	SEMESTRAL	Documentación	USI
20	Mesa de Ayuda	DIARIO	Seguimiento y Control	USI
21	Gestión de Observaciones de la Súper de Cía.	MENSUAL	Seguimiento y Control	USI
22	Ética Hacking	ÚNICA	Proceso de Compra	USI
23	Contratación PAM	ÚNICA	Proceso de Compra	USI
24	Elaboración de Informe Horas Extras	MENSUAL	Documentación	USI
25	Elaboración de Informe de Incompatibilidad de Roles	MENSUAL	Documentación	USI
26	Legalización y Custodia de Actas entrega recepción de Credenciales	MENSUAL	Seguimiento y Control	USI
27	Implementación de PCI DSS	ÚNICA	Proceso de Compra	USI
28	Actualización de documento MAP-GSI-01 Seguridad de la Información v01.01	ÚNICA	Documentación	USI
29	Revision de Documentacion de TI	ÚNICA	Documentación	USI
30	Seguimiento para designacion de nuevo presidente del Comité de Seguridad	Unica	Seguimiento y Control	USI

A la fecha la Unidad de seguridad de la Información no se encuentra normada ya que no existe en el Organigrama empresarial. para cubrir esta deficiencia la gerencia general realiza delegación de funciones a personal de otras áreas. en virtud de lo cual y para el cumplimento normativo se realiza una participa en la propuesta de creación de la Gerencia de Seguridad de la Información la cual tendría la siguiente estructura.

Figura 3

3. Estructura orgánica propuesta

Se define la Misión de la Nueva Gerencia de Seguridad de la Información: “Fortalecer el nivel de confidencialidad, disponibilidad e integridad de la información, así como la protección de ciberamenazas y protección de datos personales mediante la implementación de mecanismos, estrategias y controles para su cumplimiento en la institución”.

Con la información adquirida en la materia de **Estrategias y Políticas**

Multilaterales para la Ciberseguridad y con el firme objetivo del cumplimiento normativo tal como lo indica el “Las entidades controladas deben establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información que incluya, al menos, lo siguiente, pero sin limitarse a: (…) 2. Políticas, objetivos, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación, alineados a los objetivos y actividades de la entidad, así como las consecuencias de su incumplimiento. Las políticas, procesos, procedimientos y metodologías de seguridad de la información deben ser revisados y aceptados por el comité de seguridad de la información; y, propuestos para la posterior aprobación del directorio; así como, ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento.” (SuperIntendencia de Bancos, 2018)., con esta primicia y los conocimientos adquiridos se toma participación en la revisión y posterior aprobación de la actualización de la "Políticas de Seguridad de la Información“ la política que se encontraba vigente data del 2019, la actualización tiene como objetivo establecer el marco de referencia en el ámbito de Seguridad de la Información para la entidad financiera con base en las buenas prácticas y estándares internacionales actuales, así como en la normativa legal vigente para salvaguardar y preservar la información institucional considerando los principios de confidencialidad, integridad y disponibilidad.

Para la aprobación de la Políticas de Seguridad de la Información fue necesario seguir una serie de pasos para posterior presentación en el Comité de seguridad de la Información cuerpo colegiado encargado de aprobar las actualizaciones de dicho documento.

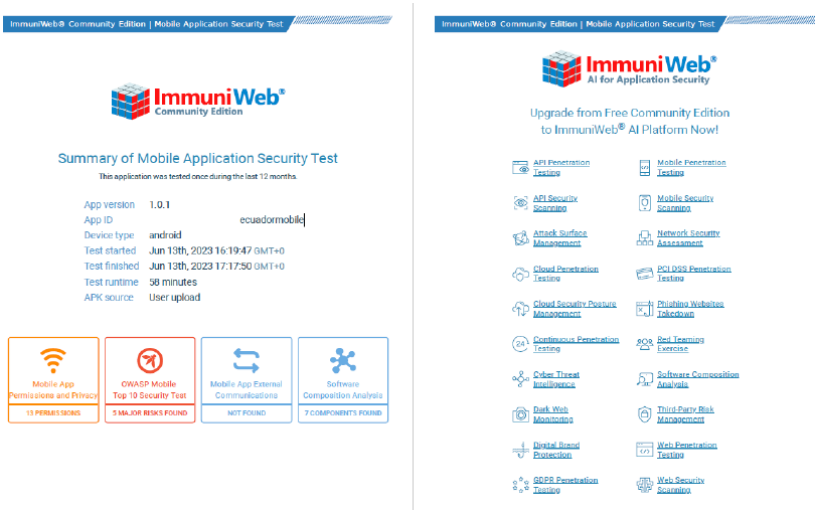
por necesidad institucional y los conocimientos adquiridos en la materia **Tecnología, Modelos y Técnicas de Ciberseguridad** se emiten informes técnicos con recomendaciones en cuanto al desarrollo de aplicaciones móviles y la aplicación de

codificación segura.

Como parte final de este proyecto y con la ayuda de las materias **Seguridad de Aplicaciones y Bases de Datos** y **Hacking Ético y Análisis del Ciberataque** con el uso de herramientas online se ejecuta prueba de seguridad de aplicaciones estáticas (SAST) y remite informe con recomendaciones para mitigar las vulnerabilidades detectadas.

Figura 4

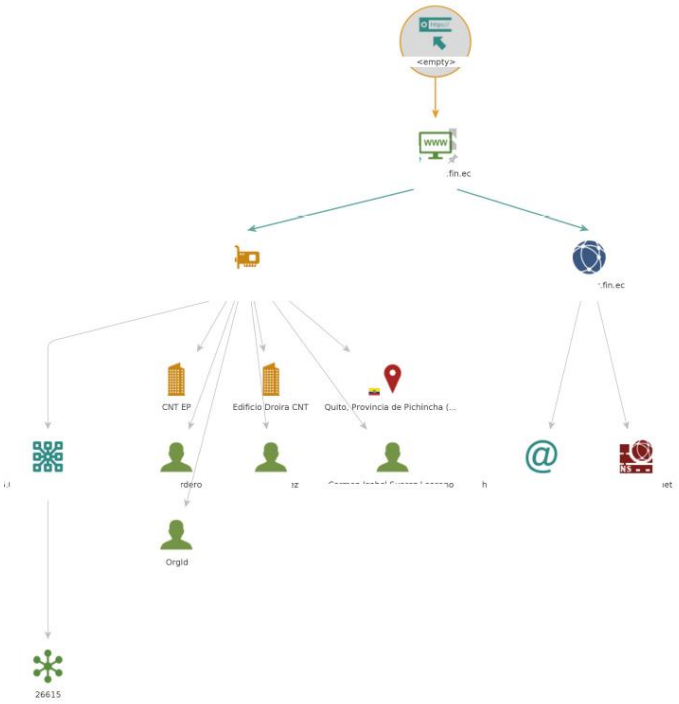
4. Pruebas de seguridad de aplicaciones estáticas – SAST



Así mismo se ejecuta un análisis de dominio público de la institución con el objetivo de tener mapeada nuestra superficie de ataque y así aplicar controles de seguridad de la información de una manera más eficiente.

Figura 5

5. Descubrimiento de Superficie de Ataque - Maltego



Además de esto se realizó una búsqueda en la Dark Web para identificar posibles brechas de seguridad poder así tomar los recaudos necesarios para garantizar la confidencialidad, disponibilidad e integridad de la información.

Figura 6

6. Búsqueda de información de la DarkWeb

SOCRadar Dark Web Test Results

The following Dark Web Report presents security findings in the dark web detected by SOCRadar.

The report uncovers where/how your organization is exposed to deep and dark web threats. To find out the compromised credentials of your employees and possible sensitive data exposures, massive data collected from thousands of underground hacker forums, black markets, onion sites, Telegram channels, and Russian and English dark web marketplaces have been analyzed.

We highly recommend you request and run a free 14-day demo to see SOCRadar in action. The platform's alerts will be supported by certified Threat Intelligence analysts and the remediation actions will be provided instantly..

HIGH
Threat Severity

Today
Latest exposure finding

531+
Data from Infected Machine

107
Data for Sale in Blackmarket

87
Compromised Credentials of Employees in the Last 1 Year
In **5** Leak Sources

0
Dark Web Mentions
8 Different Sources

Conclusiones

La gestión de la Unidad de Seguridad de la información es un proceso dinámico y en constante evolución que requiere un profundo conocimiento del marco legal y normativo para garantizar el cumplimiento y proteger a la organización de riesgos legales.

El equipo de seguridad debe contar con habilidades técnicas y administrativas necesarias para proponer, revisar, implementar y gestionar las medidas de seguridad de forma eficaz.

Limitaciones

El no contar con una unidad o gerencia dentro de la estructura organizacional limita en campo de acción y la toma de decisiones en materia de seguridad de la información.

Falta de personal para ejecutar a cabalidad la planificación operativa anual.

Falta de herramientas tecnológicas que permitan llevar un mejor control de las actividades y documentación generada por cada uno de los procesos.

Recomendaciones

Es de vital importancia que la estructura organizacional de la Gerencia de Ciberseguridad.

Se debe dar un estricto control y seguimiento a la ejecución del Plan Operativo Anual ya que en este documento se plasma las actividades macros que se deben cumplir en el transcurso del año esto con la convicción del cumplimiento normativo y evitar sanciones.

Referencias

Borrero, P. C. (2019). *Repositorio Institucional UNAD.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/35641/pcborreroo.pdf?sequence=3&isAllowed=y

incibe. (2020). *Incibe*. Obtenido de https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente#:~:text=El%20Concepto&text=El%20ciberdelincuente%20es%20la%20persona,ingenier%C3%ADa%20social%20o%20el%20malware.

SuperIntendencia de Bancos. (2018). Codificación de las Normas de la SB / LIBRO UNO – Sistema Financiero. En *LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO.* Obtenido de https://www.superbancos.gob.ec/bancos/codificacion-de-normas-de-la-sb-libro-uno-sistema-financiero/

Anexo 1

Evidencias de Aprendizaje

https://www.notion.so/Evidencia-de-Aprendizaje-3e8eb5d6d06f428bb7b4d8e11d39b8a0?pvs=4

Anexo 2

Propuesta de Implementación

https://lime-ketch-fbe.notion.site/Propuesta-de-Implementaci-n-0f646056910e4e819c8e55636eb3b261?pvs=4