

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE UN PROGRAMA DE CIBERSEGURIDAD PARA LA PREVENCIÓN DE CIBERATAQUES EN EL ÁREA DE CENTRO DE OPERACIONES DE SEGURIDAD EN LA EMPRESA VMWARESIS S.A.C.”

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero en Sistema Computacionales

Autor:

Victor Alejandro Mantari Pacheco

Asesor:

Ing. Mg. Ulises Piscoya Silva

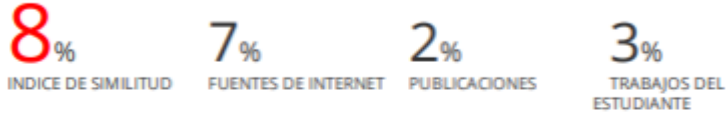
<https://orcid.org/0000-0003-4805-2611>

Lima - Perú

INFORME DE SIMILITUD

Victor Mantari_200423_v1-25042023

INFORME DE ORIGINALIDAD



ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

< 1%

★ repositorio.uns.edu.pe

Fuente de Internet

Excluir citas Apagado Excluir coincidencias Apagado
Excluir bibliografía Apagado

Tabla de contenidos

INFORME DE SIMILITUD.....	2
DEDICATORIA	3
AGRADECIMIENTO.....	4
ÍNDICE DE TABLAS	6
ÍNDICE DE FIGURAS	7
RESUMEN EJECUTIVO	9
CAPÍTULO I. INTRODUCCIÓN	10
1.1. Información General	10
1.2. Misión	13
1.3. Visión.....	13
1.4. Organigrama	13
CAPÍTULO II. MARCO TEÓRICO	15
2.1. Antecedentes	15
2.1.1. Nacionales	15
2.1.2. Internacionales	21
2.2. Fundamente Teórico	29
2.2.1. Ciberseguridad	29
2.2.2. Marco de referencia	30
2.2.3. NIST	30
2.2.4. ISO/IEC 27032.....	31
CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA	38
3.1. Experiencia	38
3.2. Identificación del problema:.....	40
3.3. Planificación	40
3.4. Metodología.....	42
3.5. Implementación.....	43
CAPÍTULO IV. RESULTADOS	62
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES	69
REFERENCIAS	71
Gumucio, J. (2021). Guía de implementación de un programa de gestión de riesgos de ciberseguridad en entidades de intermediación financiera. Universidad de Chile. Chile.	72
ANEXOS	74

ÍNDICE DE TABLAS

Tabla 1. <i>Reuniones establecidas</i>	41
Tabla 2. <i>Plan de inversión</i>	42
Tabla 3. <i>Modelo de negocio Canvas</i>	45
Tabla 4. <i>Procesos críticos de la empresa VMwaresis S.A.C.</i>	46
Tabla 5. <i>Orientación del programa</i>	46
Tabla 6. <i>Nivel 1: Parcial</i>	47
Tabla 7. <i>NIST 2018</i>	48
Tabla 8. <i>Probabilidad</i>	53
Tabla 9. <i>Impacto de riesgo</i>	53
Tabla 10. <i>Zonas de riesgo</i>	54
Tabla 11. <i>Matriz de riesgo</i>	54
Tabla 12. <i>Resultados del Análisis de Riesgo</i>	54
Tabla 13. <i>Principales riesgos identificado por la empresa</i>	56
Tabla 14. <i>Objetivo de capacidades</i>	56
Tabla 15. <i>Nivel 2 de riesgo informado</i>	58
Tabla 16. <i>Determinar, analizar y priorizar GAPS</i>	59
Tabla 17. <i>Implementación de Plan de Acción</i>	60
Tabla 18. <i>Características primarias y secundarias de los modelos de la referencia</i>	62
Tabla 19. <i>Características primarias del marco de referencia</i>	62
Tabla 20. <i>Comparación del Perfil Actual y Perfil Objetivo</i>	63

ÍNDICE DE FIGURAS

Figura 1. Equipo VMwareSis S.A.C.....	10
Figura 2. Unidades de Negocio.....	11
Figura 3. Clientes representativos.....	11
Figura 4. Partners.....	12
Figura 5. Equipamiento - SOC.....	12
Figura 6. Organigrama.....	14
Figura 7. Ciberseguridad.....	30
Figura 8. NIST.....	31
Figura 9. ISO/IEC 27032.....	31
Figura 10. Grupos de higiene cibernética.....	32
Figura 11. Secuencia para el Ciberataque.....	33
Figura 12. Relación asociadas al Riesgo.....	35
Figura 13. Términos clave de ciberseguridad.....	35
Figura 14. Áreas de Servicio.....	36
Figura 15. Pasos del programa de ciberseguridad.....	43
Figura 16. Diagrama de análisis de controles NIST.....	47
Figura 17. Ineficiente distribución de la infraestructura.....	49
Figura 18. Falta de control de seguridad en los accesos.....	49
Figura 19. Falta de certificación en el cableado estructurado.....	50
Figura 20. Falta de control de acceso a la red por autenticación.....	50
Figura 21. Falta de certificación en el cableado estructurado.....	50
Figura 22. Falta de redundancia en UPS con banco de baterías.....	51
Figura 23: Falta de un firewall de NGFW.....	51
Figura 24. Topología – Perfil Identificado – Sin Redundancia.....	52

Figura 25. Diagrama de perfil objetivo.....	57
Figura 26. Infraestructura.....	64
Figura 27. Sistema de control de acceso con un software de gestión.....	65
Figura 28. Recableado.....	65
Figura 29. Sistema de RADIUS.....	66
Figura 30. Banco de baterías.....	66
Figura 31. Sistema de automatización.....	67
Figura 32. NGFW.....	67
Figura 33. Topología – Perfil Objetivo.....	68

RESUMEN EJECUTIVO

En la actualidad a nivel mundial la seguridad nacional y económica dependen básicamente del funcionamiento confiable de su infraestructura. Las amenazas de ciberseguridad vuelven vulnerables los sistemas de información poniendo en riesgo y afectando directamente la economía de las empresas, paralizando la continuidad del servicio en sus operaciones y finalmente perjudicando al usuario final.

De esta manera el activo más importante para las empresas es la información y el aseguramiento de esta como punto primordial, con el fin de obtener ventajas competitivas y generar valor, manteniendo a buen resguardo la confidencialidad, disponibilidad e Integridad de la información.

VMwareSis S.A.C. no es ajeno a los riesgos y amenazas del ciberespacio y con mayor exposición al no contar con un programa de ciberseguridad para la prevención de ciberataques en el área del SOC, en esta oportunidad se logró implementar el programa apalancados con el marco de referencia NIST. El resultado fue el esperado obteniendo un nivel 2 de Riesgo Informado y en su plan de acción se implementó diferentes controles que permitirán mitigar y convivir con un riesgo residual.

Como toda guía de buenas prácticas siempre es importante establecer mejora continua. VMwareSis S.A.C. podrá repetir los procedimientos según sea necesario para alcanzar el nuevo nivel deseado.

NOTA

El contenido de la investigación no se encuentra disponible en **acceso abierto**, por determinación de los propios autores amparados en el Texto Integrado del Reglamento RENATI, artículo 12.

REFERENCIAS

- Acayo, R., Jaccoud, L., Lattion, L. y Mikhaylova, Y. (2018). Global Cybersecurity Index.
https://www.gouv.bj/download/12/draft-18-00706_global-cybersecurity-index-ev5_print_2.pdf
- National Cyber Security Index (2021a). NCSI Fulfilment Percentage.
<https://ncsi.ega.ee/compare/>
- Banco Interamericano de Desarrollo. (2020a). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe
<https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe>
- INCEBE-CERT (2018a). Alerta Temprana: 2.4 millones de usuarios más afectados por el ataque a Equifax. <https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/24-millones-usuarios-mas-afectados-el-ataque-equifax>
- CertiProf (2019a). Lead CyberSecurity Professional Certificate – LCSPC.
<https://certiprof.com/pages/lead-cybersecurity-professional-certificate-lcspc>
- NIST, (2018a). Cybersecurity Framework V1.1: Framework Documents.
<https://www.nist.gov/cyberframework/framework>
- Center For Internet Security (2021a). CIS Critical Security Controls Version 8. [CIS Critical Security Controls Version 8 \(cisecurity.org\)](https://www.cisecurity.org/cis-critical-security-controls-version-8)
- Cabezas, I. (2020). Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima. Universidad San Martín de Porres. [Tesis].
https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/7059/cabezas_jic.pdf?sequence=1&isAllowed=y
- Vilcarromero, L. y Vilchez, E. (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. Universidad Peruana de Ciencias Aplicadas. [Tesis].
https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624832/VilcarromeroZ_L.pdf?sequence=11&isAllowed=y

- Romero, K. (2018). Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera. Universidad San Ignacio de Loyola. [Tesis]. <https://repositorio.usil.edu.pe/server/api/core/bitstreams/c10453a7-ef96-490a-b0f4-a6f27efac39e/content>
- Mendoza, L. y Vega, G. (2019). Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC. Universidad del Pacífico. [Tesis]. https://repositorio.up.edu.pe/bitstream/handle/11354/2250/Luis_Tesis_Maestria_2019.pdf?sequence=1
- Jancachagua, J. (2021). Mejoramiento de la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera. Universidad Tecnológica del Perú. [Tesis]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4401/Jou_Jancachagua_Trabajo_de_investigacion_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y
- Rivera, A. (2019). Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016. Universidad Nacional Alcides Carrión. [Tesis]. http://repositorio.undac.edu.pe/bitstream/undac/1372/1/T026_04066691_M.pdf
- Cañar, J. y Patiño L. (2021). Modelo informático aplicado a la ciberseguridad de dispositivos IOT. Universidad EAN. Colombia [Tesis]. <https://repository.universidadean.edu.co/bitstream/handle/10882/10773/PatinoLucas2021.pdf?sequence=1&isAllowed=y>
- Gumucio, J. (2021). Guía de implementación de un programa de gestión de riesgos de ciberseguridad en entidades de intermediación financiera. Universidad de Chile. Chile. [Tesis]. <https://repositorio.uchile.cl/bitstream/handle/2250/180169/Guia-de-implementacion-de-un-programa-de-gestion-de-riesgos-de-ciberseguridad-en-entidades-de-intermediacion-financiera.pdf?sequence=1&isAllowed=y>
- Chulde, L. (2021). Diseño de un Modelo de Ciberseguridad basado en la Norma ISO/IEC 27002:2017 para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac. Universidad Internacional Sek. Ecuador. [Tesis]. <https://repositorio.uisek.edu.ec/bitstream/123456789/4192/1/Lorena%20Elizabeth%20Chulde%20Obando.pdf>

Mora, D., Agredo, N., Meneses R. (2020). FROGCY - Sistema para la gestión y prevención de riesgos de ciberseguridad en la ciudad de Popayan. Universidad Cooperativa de Colombia. [Tesis].

<https://repository.ucc.edu.co/server/api/core/bitstreams/4a25020e-d4f0-4f28-9a8e-1dcf01316f43/content>

Cando, M. y Medina, R. (2021). Prevención en ciberseguridad: Enfocada a los procesos de infraestructura tecnológica. Vol. 10, N°. 1, 2021, págs. 17-41.
<https://dialnet.unirioja.es/servlet/articulo?codigo=7888164>