UNIVERSIDAD NACIONAL DE MOQUEGUA

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

INFORME DE EXAMEN PROFESIONAL

SEGURIDAD DE LA INFORMACIÓN

PRESENTADO POR:

BACH. MIGUEL SLIP CORNEJO VALCARCEL

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMATICA

MOQUEGUA – PERÚ

2022

UNIVERSIDAD NACIONAL DE MOQUEGUA

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

INFORME DE EXAMEN PROFESIONAL

SEGURIDAD DE LA INFORMACIÓN

PRESENTADO POR:

BACH. MIGUEL SLIP CORNEJO VALCARCEL

PARA OPTAR EL TITULO PROFESIONAL DE:
INGENIERO DE SISTEMAS E INFORMATICA

_____

BACH MIGUEL SLIP CORNEJO VALCARCEL

_____

ASESOR M.Sc. HUGO EULER TITO CHURA

MOQUEGUA - PERÚ

2022

Folio Nº 003

ACTA DE TITULACIÓN

I. Modalidad:
Examen Profesional

II. Documento de aprobación:
Resolución de Comisión Organizadora Nº 636-2022-UNAM

Fecha: 19 agosto 2022

III. Título de Informe de Examen Profesional:
Seguridad de la Información.

Bachiller: Miguel Slip Cornejo Valcarcel

Asesor Principal: MSc. Hugo Euler tito Chura

Co-Asesor: .....

IV. Se dictamina con las siguientes notas:

Examen Escrito: 14.40 Entrevista: 1.87 Promedio: 16

Promedio en letras: Dieciséis por lo que: Sí [X] No [ ]

Opta el Título Profesional de INGENIERO DE SISTEMAS E INFORMÁTICA.

Siendo las 12:50 horas, del 29 de setiembre del año 2022 se procede con la firma en conformidad de lo dictaminado.

M.Sc. Hugo Euler Tito Chura
Presidente del Comité de Grados y Títulos
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

MSc. Victor Yana Mamani
Director
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

M. Sc. Hugo Euler Tito Chura
Asesor
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Bach. Miguel Cornejo Valcárcel

DEDICATORIA

Dedico la elaboración de este informe final, a las pocas personas que han puesto un fragmento de su confianza, los cuales han sido en parte el motivo e inspiración personal, dejándome saber que, en medio de tantas pruebas, dificultades y sacrificios, todo se puede lograr…

Y con mucho amor, a mi querida Madre en vida, y a mi difunto Padre, y espero que de alguna forma este trabajo le sirva como base y ejemplo a otros, de que cuando se quiere, se puede lograr, si ‘la luchamos’ sin pensar tanto en los obstáculos.

AGRADECIMIENTO

Agradezco a las II.EE en las cuales compartí aulas y así empezó mi forjamiento académico formándome como una persona que aporta al desarrollo de esta localidad y/o región.

Agradezco a mi casa superior de estudios, mis estimados y queridos docentes, que me impartieron un poco de sus conocimientos y valores para ser el profesional que llegare a ser y mejor de lo que seré mediante las buenas decisiones.

Agradezco a mi Asesor el cual fue idóneo y comprensivo orientador durante la realización de este informe.

RESUMEN

El informe que a continuación presento, ha sido estructurado de forma tal que se puedan visualizar los logros y avances conseguidos en las diversas investigaciones, desarrollos y esfuerzos aplicados para asumir nuevos desafíos y formas de hacer las cosas.

Se describirán igualmente aspectos esenciales, especiales y técnicos, que fueron de apoyo o factores condicionantes para brindar estos resultados y factibilidades.

Vale la pena comentar que las mejoras se obtuvieron a raíz de una revisión detallada y delicada en factor de las propuestas que buscaron mejorar los procesos internos y centrales, así como la asignación de responsabilidades y la obtención de metas; Concluyendo que no puede existir función estratégica sin el control de la operación.

ABSTRACT

The report that I present below has been structured in such a way that the achievements and progress made in the various investigations, developments and efforts applied to take on new challenges and ways of doing things can be visualized.

Essential, special and technical aspects will also be described, which were support or conditioning factors to provide these results and feasibility.

It is worth mentioning that the improvements were obtained as a result of a detailed and delicate review of the proposals that sought to improve the internal and central processes, as well as the assignment of responsibilities and the achievement of goals; Concluding that there can be no strategic function without control of the operation.

INDICE

Índice 1

Acrónimos y abreviaturas 4

Introducción 8

CAPÍTULO I – ASPECTOS GENERALES 9

1.1 La seguridad en términos generales 9

1.2 El concepto de seguridad Informática 10

1.3 Descripción práctica acerca de la Seg. De la Información 10

1.4 Contemplaciones en la seguridad 10

CAPÍTULO II – DESARROLLO DEL TEMA 12

2.1 Seguridad de la Información respecto a los virus informáticos 12

2.2 Clasificación de los virus informáticos 12

2.2.1 Tipo Virus 13

2.2.2 Alteradores 13

2.2.3 Daño colateral 13

2.3 Autenticación – Concepto 13

2.4 Concepto de encriptación en seguridad informática 14

2.5 Métodos de encriptación 15

2.6 Los 3 Pilares de la ciber seguridad 16

2.7 Categorización en riesgos, amenazas y vulnerabilidades 17

2.8 Pruebas de Vulnerabilidad, OWASP y reporte ZAP 19

CAPÍTULO III – ANTECEDENTES INTERNACIONALES Y NACIONALES 23

3.1 Antecedentes internacionales 23

3.2 Antecedentes nacionales 26

CAPÍTULO IV – CONCLUSIONES Y RECOMENDACIONES 27

4.1 Conclusiones 27

4.2 Recomendaciones 27

BIBLIOGRAFÍA 28

INDICE DE GRÁFICOS

Figura 1	14
Figura 2	15
Figura 3	16
Figura 4	17
Figura 5	18
Figura 6	19
Figura 7	19
Figura 8	20
Figura 9	21
Figura 10	22

ACRONIMOS Y ABREVIATURAS

Confidencialidad: Son las garantías relacionadas a la información, y a la accesibilidad reservada a usuarios permitidos y/o autorizados temporal o permanentemente.

Integridad: Relacionado a todo lo referido a la precisión, exactitud y disponibilidad de la data, así como diversos métodos o técnicas de tratamiento y/o procesamiento.

Disponibilidad: Atributo que permite un acceso controlado, así como a herramientas y demás activos en conjunto, desde cualquier lugar y momento.

Autenticidad: El objetivo es garantizar que toda la data consultada o requerida, sea fehaciente y/o verídica dentro de la organización y/o del origen de la misma data.

Auditabilidad: Atributo que permite y facilita relativamente que la data o información, pueda ser verificada y registrada para controles futuros de comportamiento.

Protección a la duplicación: Se trata de la capacidad de impedir que al momento de cualquier operación, proceso y/o transferencia de data realizada, no provoque duplicidad sobre dicha operación específica.

No repudio: Atributo que le permite a toda información enviada y/o recepcionada entre entidades y/o usuarios, dar negativa de que no fue recepcionado o enviado, dependiendo de la circunstancias.

Legalidad: Tiene que ver con el obedecimiento del marco legal, reglamentos y/o accesibilidades a las que está bajo sus efectos legales.

Confiabilidad de la Información: Cualidad de la informacion para que citada en temas de interés y decisión, pueda ser idónea para justificaciones dentro de lo necesitado.

Información: Conjunto de fragmento de datos, que en grupo conforman ideas contextuales para la utilización en resolución de incógnitas y/o divergencias informáticas.

Sistema de Información: Conjunto de procesos y código, con recursos a su disposición y posesión, que se encuentra ordenada y categorizada, para la recolección, tratamiento, monitorización, seguimiento y publicación de informacion según procesos específicos.

Tecnología de la Información: Básicamente son HW y SF operando en cyber sinergia digital, operados por una IA o por un administrador físico, utilizado para la obtención de datos e informacion necesaria o crucial.

Activo de información: Activo cyber digital de la "WWW", esta puede contener informacion de extremo interés para interesas privados de algunas terceras o gobiernos.

Análisis de Riesgos: Procesos de tratamiento de informacion que se tiene, para poder identificar y reducir posibles, presentes y futuros peligros inmersos en la circunstancia.

Alcance de Auditoria: Rango, estipulaciones y limitaciones para la realización de la auditoria.

Auditor: Individuo cuyo objetivo es el de verificar los requerimientos conforme a los estándares vigentes a niveles: nacional e internacional.

Ciber amenaza o amenaza cibernética: Origen de un evento "CDT" -Cyber Digital Threat- que posee características y comportamientos altamente dañinos hacia la información o datos del objetivo al que se ha apuntado.

Cyber Ataque: Sucede cuando se ejecuta una operación indiscriminada e ilegal, con el único objetivo de perjudicar a los objetivos informáticamente.

Cyber Espacio: Ecosistema binario e informático, donde conviven todo tipo de elementos, usuarios, programas, herramientas, software open source o privados, etc. Su naturaleza es lógica o digital, lo cual indica que no es tangible en la normalidad.

Cyber Defensa: Conjunto de métodos, protocolos y técnicas destinadas a proteger, preservar y restaurar grandes bloques de informacion, en caso de ser efecto de cyber ataques, se deberán tener todos los recursos necesarios para mitigar toda amenaza surgente o reincidente.

Cifrar: Técnica informática para encrestar u ocultar de forma segura y discreta datos, cifras numéricas y minería de datos, etc.

CSIRT: Siglas que en español refieren al grupo de trabajo responsable de reaccionar rápido frente a incidentes posibles.

Contraseña: Dígitos, letras, caracteres, utilizados en un orden especifico, brindando una sensación de seguridad y discreción por encima de otros usuarios, seguridad básica para cuidar datos personales o importantes.

Cortafuegos: Muro lógico invisible al humano, pero detectable a nivel lógico-digital, usado como segundo verificador luego de Win Def. Utilizado para verificar datos de orígenes sospechosos, maliciosos o no identificados, previene la infección del ordenador en el peor de los casos.

Criterios mínimos: Conforma este concepto, los 3 atributos elementales de la informacion, las cuales son: confidencial, integral y disponible.

INTRODUCCIÓN

En el mundo corporativo y empresarial, se enfocaron a conservar los activos ambiguamente ya conocidos, infraestructura, maquinaria, vehículos, etc. No obstante, no se debe dejar pasar la existencia de los bienes intangibles como: un portfolio de clientes potenciales, algunas tarifas que se contemplan, la propiedad intelectual empresarial o individual y el prestigio o reputación.

Actualmente hay empresas dedicadas al rubro de tratar la data o información, similar a los del rubro prensa, marketing (publicidad), medios de difusión como radio y TV, multimedia, etc. Sin concluir que solamente estos rubros han de dedicarse a la protección y seguridad de la información.

Reflexionemos a raíz de las consecuencias que provocarían la pérdida o sustracción de la información de una organización, portafolio de clientes, información confidencial, cuentas bancarias secretas o hasta propiedad intelectual de la organización.

Todo lo antes mencionado ejemplifica mente, forman parte de la realidad en la actualidad de toda organización, lo que convierte a la información, como un activo vital el cual debe preservarse y resguardarse apropiadamente, a esto lo denominamos seguridad de la información.

CAPITULO I

ASPECTOS GENERALES

1.1- LA SEGURIDAD INFORMÁTICA - CONCEPTO GENERAL:

Si señalas todos los tecnicismos que tienen que ver con la seguridad informática, para ello, primero se debe comprender todo lo elemental que ello corresponde, lo cual a su vez forma parte de los cimientos esenciales de esta rama de investigación en constante evolución, proporcionando cada más resguardo y defensa digital. Si tiene q ver con cuestiones empresariales, entonces se puede decir que paralelamente toma el rol de revisar, evaluar y administrar todo tipo de riesgos sea del origen que sea.

La misma siempre ha sido como objetivo, administrar, evaluar y gestionar todo tipo de amenaza que se suscite, ejecutando todos los procedimientos y/o protocolos configurados en su programación, las cuales son:

- ➔ Prevenir
- ➔ Transferir
- ➔ Mitigar
- ➔ Aceptar

Así que cuando se está pensando hacer algo más protegido o seguro, estas acciones básicas son consideradas sin importar el área, aplicable a cualquier intento por mejorar o reinventar la seguridad en la competencia que se necesite o requiera.

1.2 - CONCEPTO DE SEGURIDAD INFORMÁTICA:

Según el concepto descrito aquí, se trata de gestionar la seguridad del ecosistema informático, es la rama de investigación que tienen como objetivo, todos los métodos, eventos, tiempos y sucesiones digitales, que enfocan los esfuerzos del mismo en darle análisis, tratamiento, contención y transmisión de la data.

1.3 – DESCRIPCION PRÁCTICA ACERCA DE LA SEG. DE LA INFORMACIÓN:

Trata no solo del entorno digital de datos, sino que incluye también todo aquello que puede o podría poseer informacion de valor, prácticamente se preocupa por casi todo, por lo que se asumen sus diferencias lo más resaltante son los universos que interpretan cada concepto relacionado al tema.

1.4 - CONTEMPLACIONES EN LA SEGURIDAD:

Los usuarios, son significantes como el eslabón más vulnerable de la data, en los usuarios humanos, es menor probable calcular y manejar el error humano, esto significaría que pueda causar efectos negativos en el sistema de informa indirecta, a la vez podría causar daños invisibles a los sistemas e informacion, se considera que deben cuidarse, incluso hasta de los mismos usuarios.

La información, es el recurso informático valioso por muchas fuentes y bases de datos de proceso y tratamiento de la misma, es considerada como el activo de data crucial para muchas entidades públicas y privadas, gubernamentales y hasta militares, nacionales o internacionales.

La infraestructura, es el medio físico o tangible, con más secciones de control por seguridad, pero aun así, esto no asegura que se experimenten menos amenazas. Siempre se debe tener en cuenta que para resguardar los sistemas de amenazas complejas o perjudiciales, se debe poseer un esquema capaz de soportar tanto ataques digitales o físicos, como procedimientos de corrección y reestructuración de errores de datos vacíos o campos nulos, así como una estructura hardware adecuada.

CAPITULO II

DESARROLLO DEL TEMA.

2.1 – SEGURIDAD DE LA INFORMACIÓN RESPECTO A LOS VIRUS INFORMÁTICOS:

Son programas grandes o pequeños, cuyo propósito es causar daños al sistema o causar daños al funcionamiento del periférico de escritorio o portátil. No siempre suele ser un programa completo, algunas veces pueden ser mini fragmentos en la cadena de ejecución de un programa.

Con la capacidad de acceder a la data sin permiso, puede hacer muchas cosas desde ahí, como eliminar archivos, Ingresos a los ordenadores, extracción o robo de informacion de alto valor general, bloqueo y desactivación de procesos de conexión y acceso a los ordenadores, inhibidor de procesos y funcionalidades del Software, o del mismo periférico o Laptop.

2.2 - CLASIFICACIÓN DE LOS VIRUS INFORMÁTICOS:

2.2.1 - TIPO VIRUS:

Sector de Arranque (BOOT)

Archivos ejecutables sospechosos (.exe)

Macros (VB, EXC)

Lenguajes de Script

2.2.2 - ALTERADORES Y CONTROLADORES DE EJECUCION INMEDIATA:

Malware (daña procesos, llaves de registros, etc.)

Gusano (worm replicador, ocultador o devorador)

Spyware (vigilante silencioso)

Keylogger (capturador de caracteres)

Adware (rompe protección contra anuncios invasivos)

Dialers (intrusión por medio de llamadas invasivas)

Backdoors (proceso maestro que omite la línea de seguridad secreta del sistema)

2.2.3 - TIPO DAÑO COLATERAL O DIRECTO:

Rootkit (intrusión indirecta)

Bacteria (infecta data o corrompe procesos)

Bomba de tiempo (destructor de SW o de HW)

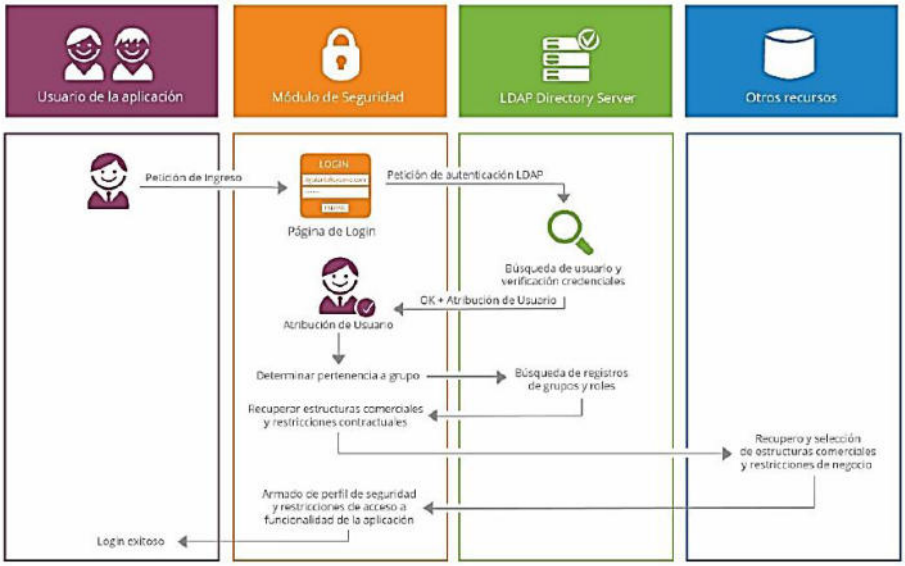
2.3 - AUTENTICACIÓN – CONCEPTO:

Se define como el proceso utilizado para confirmar la veracidad del momento, el objetivo no trata de ubicar a la persona registrada, algunas veces estos no coinciden en cuanto a su interacción entre ellos; No obstante la autenticación es necesaria para saber si un dato es correcto o no, considere que no solo los usuarios requieren de este proceso, al contrario quizás sea o pueda ser utilizado para cualquier sistema, driver o usuario.

En algunos casos muy usuales de autenticación usados en:

- ➔ Redes sociales
- ➔ Credenciales de sistemas privados
- ➔ Credenciales de sistemas públicos
- ➔ Banca y finanzas digitales.
- ➔ Sistemas de identificación internacional
- ➔ Crypto activos
- ➔ Autenticación de usuarios

Figura 1
Diagrama de Autenticidad de los usuarios



Nota. Adaptado de *Diagrama de Autenticidad de los usuarios*, de INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018, Fuente: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

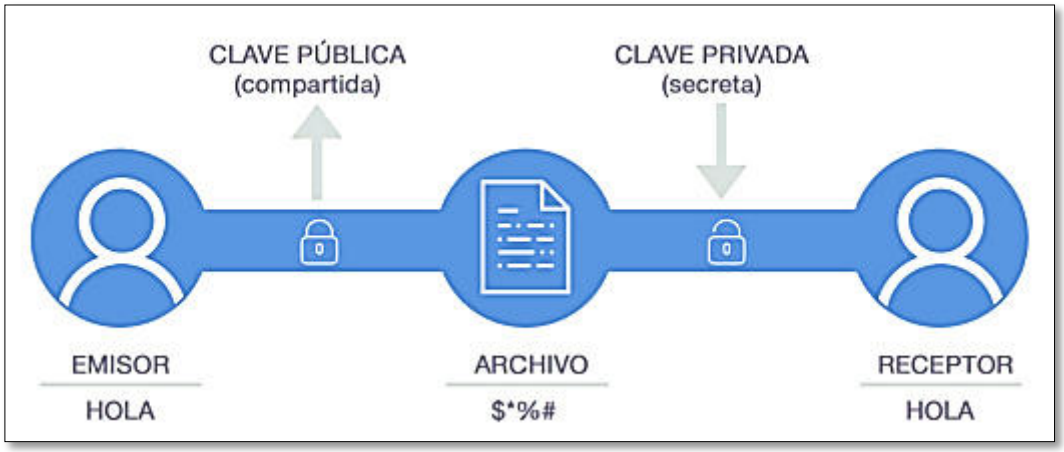
2.4 –ENCRIPTACIÓN EN SEGURIDAD INFORMÁTICA:

Conocido como codificación secreta, es utilizado como proceso cuyo objetivo tiene por enfoque a la data o informacion de esta forma se garantiza que sea irreconocible en lectura o imposible de leer. Una vez ejecutado este método sobre dicha informacion o data, ya deja de tener utilidad frente a otros usuarios de acceso

restringido, y, más allá de que el mensaje resultante sea captado, parte de la situación real, resulta no ser de mucha significancia para el interceptor, ya que no cuenta con los componentes implicados en el cifrado, en conclusión la data o informacion no es de utilidad.

Los atributos matrices en la encriptación y cifrado de información son: Confidencialidad, autenticación e integridad de los datos.

Figura 2
Ejemplificación del método de cifrado.



Nota. Adaptado de *Ejemplificación del método de cifrado, de* INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018, Fuente: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

2.5 – METODOS DE ENCRIPTACIÓN:

Actualmente existen métodos de cifrado disponible conocidos, entre ellos se puede mencionar a:

→ Encriptación simétrica (Sames keys).- Cifrado DES (x56 bits), IDEA (x128 bits)

→ Encriptación asimétrica PK & FK.- Custodia del propietario, conocido por el usuario.

→ Encriptación WPA.- Aplicable a servidores de autentificación.

→ Encriptación WEP.- Aplicable a la red WIFI. (X64, x128, x256 bits)

→ Firma Digital DSA.- Sistema de 2 claves, 1ra. Publica (emisor) y 2da. Privada (receptor)

2.6 – LOS 3 PILARES DE LA CIBER SEGURIDAD:

Los componentes base para la Ciber seguridad en la informacion, basan sus esfuerzos en enfocarse a la ayuda o función necesaria para conseguir o colectar data o informacion, la relevancia, solidez y accesibilidad, con un riesgo disminuido considerablemente, obteniendo resultados óptimos.

Figura 3
Pilares de la Ciber Seguridad



Nota. Adaptado de *Pilares de la Ciber Seguridad, de* INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018, Fuente: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

2.7 – CATEGORIZACIÓN EN RIESGOS, AMENAZAS Y VULNERABILIDADES:

Cuando se centran los esfuerzos en optimizar la seguridad digital de una entidad, siempre se debe considerar, distintas variables, las cuales son mencionadas a continuación:

- ➔ Logística (Recursos digitales)
- ➔ Cyber amenazas digitales
- ➔ Cyber vulnerabilidades o puntos vacíos
- ➔ Potenciales Riesgos o Peligros latentes.

Debe de comprenderse que, la logística envuelta, ya sean activos físicos o no físicos, con los que se dispone para la ejecución de dicha tarea, todos los datos que se poseen, son considerados como un bien o activo digital, que reside en la B D de, distribuidores, logísticos, transportes, guías o manuales, investigaciones, usuarios y derechos intelectuales.

Figura 4
Ejemplo de bienes tangibles e intangibles.



Nota. Adaptado de *Ejemplo de bienes tangibles e intangibles., de* INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018, Fuente: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

Riesgo.- Aparición de un suceso, de origen negativo, suele perjudicar a todo recurso o dato, ya sea tangible o digital, ocasionando varios impedimentos para poder ejecutar la labor corporacional o empresarial.

Amenazas.- Actividad o hecho suscitado, en la cual puede desencadenar daños directos o indirectos hacia los activos de X entidad.

Vulnerabilidades.- Vendrían a ser todos los defectos o fallas, presentes u originados en los diversos sistemas de resguardo o cuidado de datos, e incluso entre los mismos usuarios, aprovechado para ejecutar las actividades, que le permiten al usuario malintencionado, tener éxito en cuanto surge un inconveniente o imprevisto.

Figura 5
Formula para medir el riesgo.



Nota. Adaptado de *Formula para medir el riesgo, de* INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018, Fuente: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

2.8 –PRUEBAS DE VULNERABILIDAD, OWASP Y REPORTE ZAP

Figura 6
Sitio web para vulnerabilidades.



Nota. Adaptado de *Sitio web para vulnerabilidades., por Hostedscan.com, 2022*

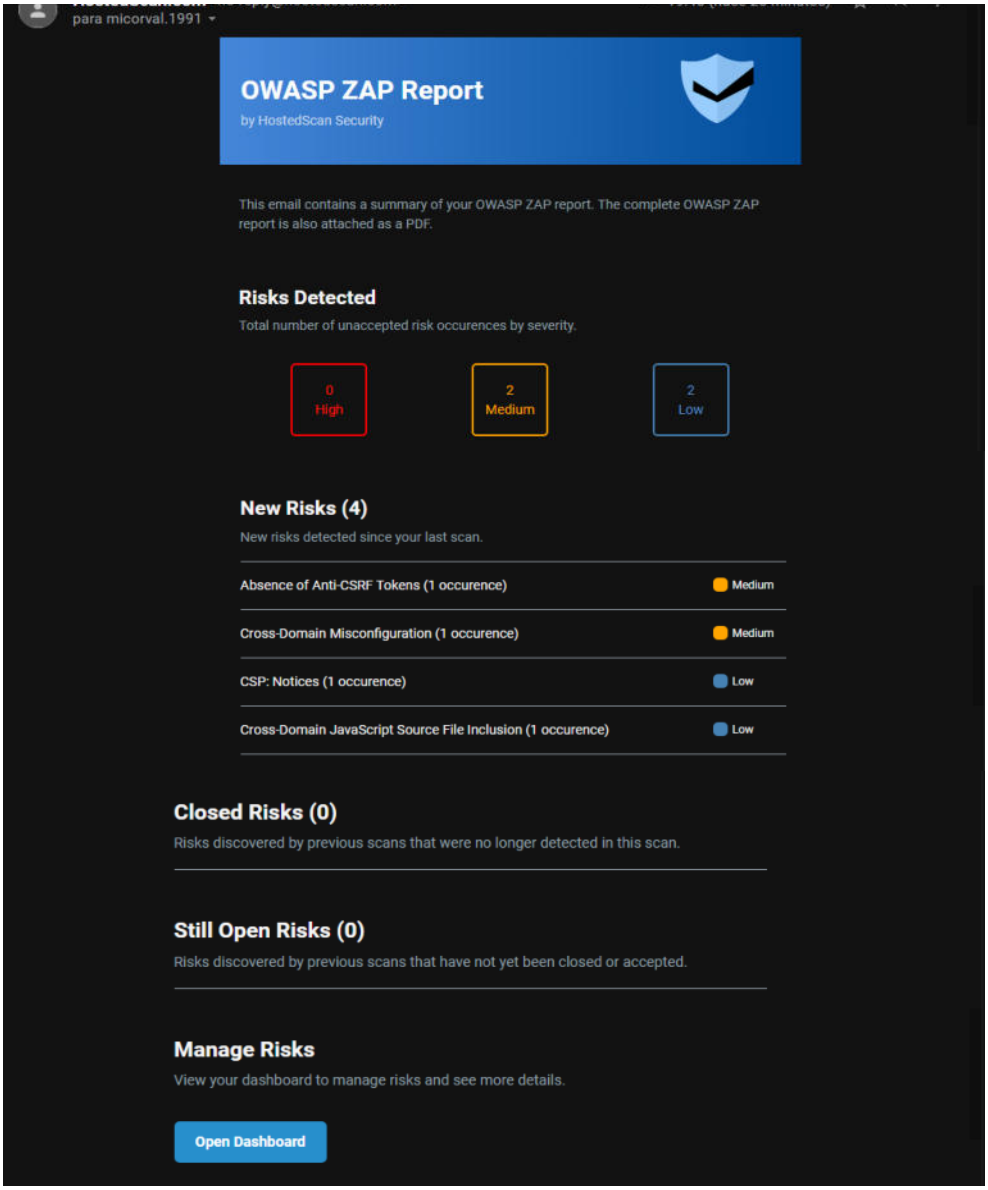
Figura 7
Resultado del escaneo de la IP Pública de Google, vía Email registrado.



Nota. Adaptado de Resultado del escaneo de la IP Pública de Google, vía Email registrado., *por Hostedscan.com, 2022*

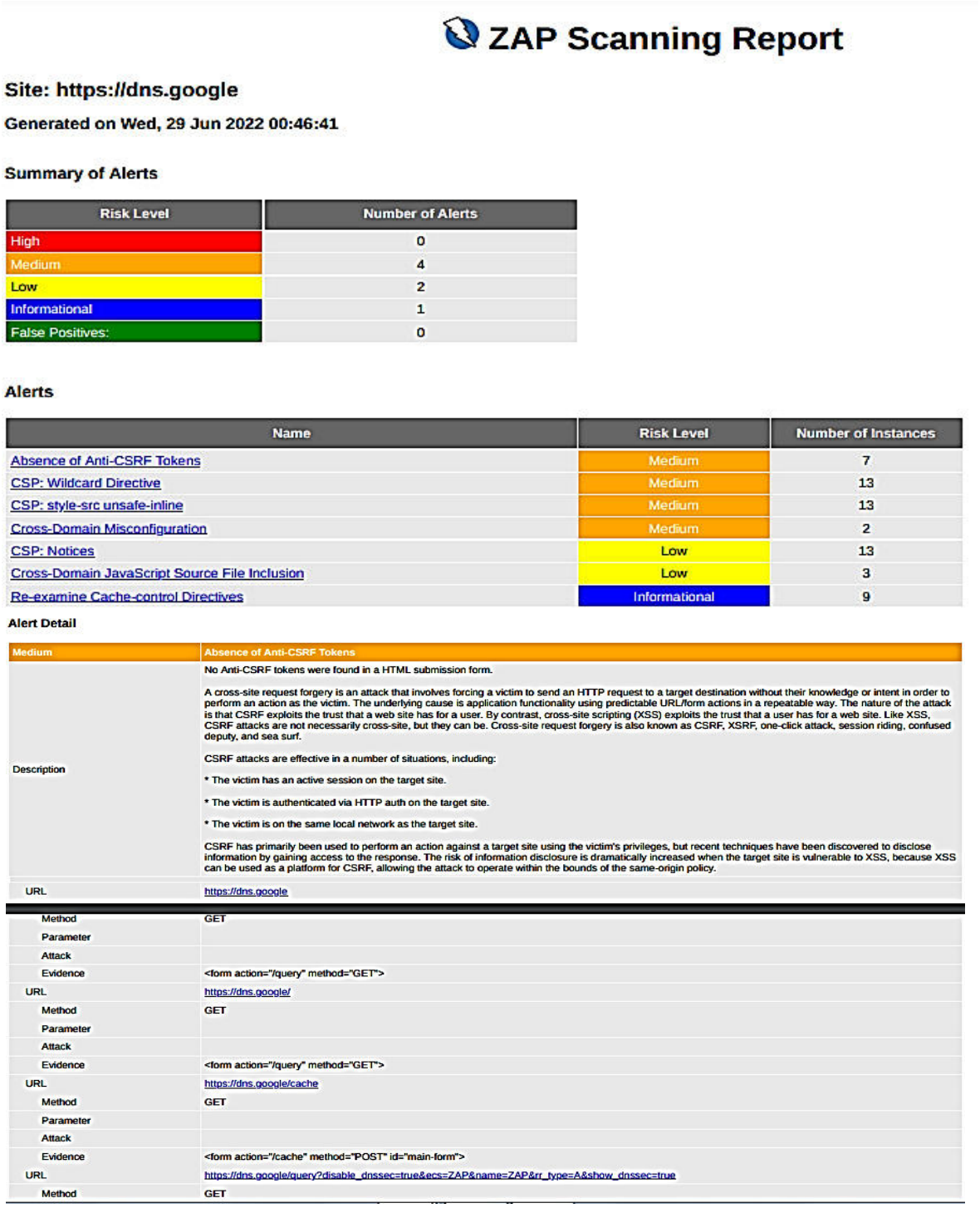
Figura 8

Resumen del escaneo de la IP Pública de Google, vía OWASP ZAP.



Nota. Adaptado de Resumen del escaneo de la IP Pública de Google, vía OWASP ZAP*, por Hostedscan.com, 2022*

Figura 9
ZAP Reporte de Escaneo detallado (DNS Google)



ZAP Scanning Report

Site: https://dns.google

Generated on Wed, 29 Jun 2022 00:46:41

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	2
Informational	1
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	7
CSP: Wildcard Directive	Medium	13
CSP: style-src unsafe-inline	Medium	13
Cross-Domain Misconfiguration	Medium	2
CSP: Notices	Low	13
Cross-Domain JavaScript Source File Inclusion	Low	3
Re-examine Cache-control Directives	Informational	9

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://dns.google
Method	GET
Parameter	
Attack	
Evidence	<form action="/query" method="GET">
URL	https://dns.google/
Method	GET
Parameter	
Attack	
Evidence	<form action="/query" method="GET">
URL	https://dns.google/cache
Method	GET
Parameter	
Attack	
Evidence	<form action="/cache" method="POST" id="main-form">
URL	https://dns.google/query?disable_dnssec=true&ecs=ZAP&name=ZAP&rr_type=A&show_dnssec=true
Method	GET

Nota. Adaptado de *ZAP Reporte de Escaneo detallado, por Hostedscan.com, 2022*

Figura 10

ADA es una plataforma de análisis avanzado de malware.



Nota. Adaptado de *ADA CCN CERT*, por Instituto Criptográfico Nacional en España, 2022, Ccn Cert https://www.ccn-cert.es

Nota: Esta clase de páginas analizan, filtran y buscan informacion vulnerable o expuesta por parte de los fabricantes, recursos y hasta versiones o seriales, etc. Los cuales pueden ser gestionados por ordenadores configurados ante respuestas a incidentes que expongan a la informacion valiosa o relevante. Toda entidad (pública y/o privada) comparte y difunden estos datos, ya que no solo ayuda a la optimización global relacionada al resguardo de la información y otros datos relevantes o críticos, sino que también aumenta su seguridad singular e impulsa a los programadores y manufactureros a eliminar falencias y puntos vacíos en los sistemas que gestionan.

CAPITULO III

ANTECEDENTES INTERNACIONALES Y NACIONALES.

3.1 – ANTECEDENTES INTERNACIONALES:

TITULO DE TESIS O TRABAJO CONSULTADO: Política de Seguridad de la Información

AUTOR O AUTORES DEL TRABAJO: Comité de Seg. Inf.

AÑO EN EL QUE FUE PRESENTADO: 2008

INSTITUCIÓN QUE LO PRESENTA: Universidad Nacional de Córdova (UNC)

TITULO QUE OPTABA AL PRESENTAR EL TRABAJO: No Aplica

RESEÑA DE LAS CARACTERISTICAS DEL TRABAJO: En el cumplimiento de las dictaminaciones legales dispuestas actuales, tienen por objetivo administrar con idoneidad, todos los recursos referidos a la seguridad de información, infraestructura informática e incluso el ecosistema tecnológico adaptado.

APORTE QUE APORTA A MI TRABAJO EN EL CURSO DE LA INVESTIGACION: Términos y definiciones.

TITULO DE TESIS O TRABAJO CONSULTADO: Política de Seguridad de la Información

AUTOR O AUTORES DEL TRABAJO: Pacific Credit Rating

AÑO EN EL QUE FUE PRESENTADO: 2019

INSTITUCIÓN QUE LO PRESENTA: Pacific Credit Rating

TITULO QUE OPTABA AL PRESENTAR EL TRABAJO: No Aplica

RESEÑA DE LAS CARACTERISTICAS DEL TRABAJO: Aplicada para categorizar y asignar una matriz calificada de riesgos, de forma que manejan los datos de diversas fuentes externas e internas, lo que se concluye como una necesidad de poseer políticas de seguridad informacion.

APORTE QUE APORTA A MI TRABAJO EN EL CURSO DE LA INVESTIGACION: Propuestas, lineamientos en materia de resguardo y protección de información.

TITULO DE TESIS O TRABAJO CONSULTADO: Política de Seguridad de la Información Informe de evaluación Seguridad en la Información basada en la norma ISO 27001

AUTOR O AUTORES DEL TRABAJO: UPSG

AÑO EN EL QUE FUE PRESENTADO: 2015

INSTITUCIÓN QUE LO PRESENTA: UPSG

TITULO QUE OPTABA AL PRESENTAR EL TRABAJO: Ingeniero de Sistemas

RESEÑA DE LAS CARACTERISTICAS DEL TRABAJO: Utilizando un enfoque de riesgos del tipo "MAGERIT", la cual brinda implementos requeridos para poder ejecutar la evaluación, reconociendo identificación de activos, amenazas y debilidades, a través de todos los elementos existentes, lo cual facilita identificar específicamente cada riesgo de cada activo.

APORTE QUE APORTA A MI TRABAJO EN EL CURSO DE LA INVESTIGACION: Opción como SGSI, útil para definir políticas que controlan y regulan todo lo relacionado a seguridad de la informacion, en cualquier entidad u organización.

TITULO DE TESIS O TRABAJO CONSULTADO: Informes de incidentes de Seguridad

AUTOR O AUTORES DEL TRABAJO: Grupo de Seguridad RedIRIS, IRIS-CERT

AÑO EN EL QUE FUE PRESENTADO: 2001-2002

INSTITUCIÓN QUE LO PRESENTA: Grupo de Seguridad RedIRIS, IRIS-CERT

TITULO QUE OPTABA AL PRESENTAR EL TRABAJO: No Aplica

RESEÑA DE LAS CARACTERISTICAS DEL TRABAJO: Este informe de incidente de seguridad muestra lo más relevante ocurrido durante la gestión de incidentes de seguridad, a su vez un resumen de las posibles soluciones a los problemas de seguridad más frecuentes.

APORTE QUE APORTA A MI TRABAJO EN EL CURSO DE LA INVESTIGACION: Informacion relacionada con ataques significativos contra servidores IIS, servidores SSH1, servidores FTP, Rootkit Linux, Solaris, Denegación de Servicio.

TITULO DE TESIS O TRABAJO CONSULTADO: Introducción a la Seguridad informática y el análisis de vulnerabilidades

AUTOR O AUTORES DEL TRABAJO: Varios Autores

AÑO EN EL QUE FUE PRESENTADO: 2018

INSTITUCIÓN QUE LO PRESENTA: UESM

TITULO QUE OPTABA AL PRESENTAR EL TRABAJO: No Aplica

RESEÑA DE LAS CARACTERISTICAS DEL TRABAJO: Tiene como objetivo central, reconocer e identificar los diferentes significados de la seguridad informática, se

investigan los procesos mecánicos, tanto en preveer y reducir, corregir e identificar rápidamente para evitar las amenazas que puedan surgir.

APORTE QUE APORTA A MI TRABAJO EN EL CURSO DE LA INVESTIGACION: Generalidades a la Seguridad Informática, Ciberseguridad, Vulnerabilidades y Antecedentes de pruebas de punto vacío.

3.2 – ANTECEDENTES NACIONALES:

TITULO DE TESIS O TRABAJO CONSULTADO: Auditoría a la SG. INF.

AUTOR O AUTORES DEL TRABAJO: Oficina de TI & CCS.

AÑO EN EL QUE FUE PRESENTADO: 2020

INSTITUCIÓN QUE LO PRESENTA: Senamhi

TITULO QUE OPTABA AL PRESENTAR EL TRABAJO: No Aplica

RESEÑA DE LAS CARACTERISTICAS DEL TRABAJO: La presente Política de Seguridad de la Información se basa en gestionar y ejecutar una auditoria de seguridad de la información, para evaluar el seguimiento de los requisitos determinados dentro del estándar nacional e internacional en materia a lo relacionado.

APORTE QUE APORTA A MI TRABAJO EN EL CURSO DE LA INVESTIGACION: Definiciones y siglas, Base Legal en Seguridad de Información, ámbito nacional e internacional, Ley Nº 29733, Ley Nº 30096, RS Nº 004-2016-PCM, NTP ISO/IEC 27001:2014

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 - CONCLUSIONES:

- En la actualidad, en estos tiempos, siguen surgiendo nuevas amenazas y vulnerabilidades a varios tipos de sistemas, la mayoría ocurridos a raíz de la falta de conocimientos sobre los riesgos que estos traen consigo el no preverlas.
- Los ataques ocasionados o producidos contra los diferentes sistemas, nos revela que tuvieron una mayor probabilidad de éxito debido a que afectaron a las zonas más "débiles" dentro de los sistemas atacados.
- Es importante y exigible un estado de alerta permanente y continuo, ya que la seguridad como tal, posee un proceder continuo, el cual obtiene su feedback a raíz de las experiencias propias.
- No debe considerarse la seguridad de la información como un producto ajeno a los demás procesos. Este debe formar parte de las organizaciones públicas o privadas.

4.2 - RECOMENDACIONES:

- No abrir SMS, Emails, sitios web sospechosos y/o maliciosos.
- Navegar por fronteras web seguras o de confianza.
- Elimine todo tipo de Email de supuestas entidades bancarias u otra entidad, que le solicite sus credenciales de acceso, contraseñas.
- Utilice contraseñas seguras, compuestas de una variedad de caracteres y símbolos al ser ingresado, mínimamente de 8 caracteres.

BIBLIOGRAFIA

Fundación ESYS (2014). ***Informe anual de la Seguridad en España***, País España. *https://www.fundacionesys.com/es/system/files/documentos/Informe%20de%20Seguridad%202014.pdf*

Gobierno Regional Metropolitano de Santiago (2016). ***Informe de cumplimiento del Plan de Seguridad de la Información***, Distrito Santiago, Chile. *https://www.gobiernosantiago.cl/wp-content/uploads/2016/01/Informe-de-cumplimiento-del-Plan-de-seguridad-de-la-Informaci%C3%B3n.pdf*

Ingeniería, servicios y comunicaciones S.A. (2019). ***Manual de Seguridad de la Información***, País Chile. *https://www.isc.cl/wp-content/uploads/2020/04/MANUAL-DE-POLI%CC%81TICAS-DE-SEGURIDAD-DE-LA-INFORMACIO%CC%81N-DE-ISC.pdf*

IRIS-CERT (2002). ***Informe de incidentes de seguridad IRIS-CERT <cert@rediris.es> Id: informe. Tex, v1.52002/06/0700: 05: 45paco*Exp**, Distrito País no especificado. *https://www.rediris.es/cert/doc/informes/2002-06/informe.pdf*

Industria y Comercio Superintendencia (2019). ***Informe Final Auditoria de Gestión de Seguridad de la Información,*** Distrito Bogotá, Colombia. *https://www.sic.gov.co/sites/default/files/files/2020/control%20interno/Archivo%2011_%20Informe%20Final%20Auditoria%20de%20Gesti%C3%B3n%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf*

Instituto Nacional de Ciberseguridad (año no mencionado). ***Protección de la Información***, País España.

Ministerios de Tecnologías de Información MINTIC (2016). ***Procedimientos de Seguridad de la Información - Seguridad y Privacidad de la Información***, País Colombia.

https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Pacific Credit Rating (2019). **Política de Seguridad de la *Información***, Distrito País no especificado. *https://www.ratingspcr.com/application/files/6915/8569/3306/PCR-OR-GIR-POL-RE-01_Politica_de_Seguridad_de_la_Informacion.pdf*

Senamhi (2020). ***Auditoria a la seguridad de la información Procedimiento: PR-OTI-005***, País Perú. *https://www.senamhi.gob.pe/load/file/00711SENA-29.pdf*

Superintendencia de Seguridad Social (2019). ***Borrador Circular Seguridad de la Información***, Distrito Santiago, Chile. *https://www.suseso.cl/612/articles-616373_archivo_01.pdf*

Universidad de Córdoba (2008). ***Política de Seguridad de la Información***, Distrito Córdoba, Argentina.

https://www.unc.edu.ar/sites/default/files/PoliticadeSeguridad08.pdf

Universidad Politécnica Salesiana sede Guayaquil. (2015). ***Informe de evaluación de seguridad en la información basada en la norma ISO 27001 en el Departamento de TI de una empresa de lácteos***, Distrito Guayaquil, Ecuador. *https://dspace.ups.edu.ec/bitstream/123456789/10307/1/UPS-GT001204.pdf*

Universidad Estatal del Sur de Manabí (2018). ***Introducción a la seguridad informática y el análisis de vulnerabilidades***, Distrito Manabí, Ecuador. *https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf*

FORMATO DE AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL UNAM

Formulario de autorización para la publicación electrónica en la página web del Repositorio Institucional de la Universidad Nacional de Moquegua, de conformidad con la Ley N° 30035 Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y Resolución de Comisión Organizadora N° 041-2022-UNAM que aprueba el Reglamento que regula el Repositorio Institucional Digital de la UNAM.

1. DATOS DEL AUTOR

Nombres y Apellidos : Miguel Slip, Cornejo Valcarcel
DNI/Carnet de Extranjería/Pasaporte N° : 46911703
Correo electrónico : Micorval.1991@gmail.com
Teléfono/Celular : 930125085

2. GRADO, TITULO O ESPECIALIZACIÓN (Marque con una X)

Bachiller	Título Profesional	Magister	Doctor	Segunda Especialidad
	X			

3. TIPO DE PUBLICACIÓN (Marque con una X)

a) Articulo ( )
b) Tesis de pregrado ( )
c) Tesis de Maestría ( )
d) Tesis de Doctorado ( )
e) Monografía (X)
f) Reporte de caso científico o hallazgos ( )
g) Libro ( )
h) Parte de un libro ( )
i) Revisión ( )
j) Conferencia ( )
k) Presentación ( )
l) Artículo preliminar ( )
m) Articulo antes de ser publicado ( )
n) Artículo de prensa ( )
o) Documentos internos ( )
p) Imagen ( )
q) Documentos técnicos ( )
r) Ponencias presentadas en eventos científicos (Jornada, Congreso, Simposio Conferencias, etc.) ( )
s) Informes de suficiencia profesional ( )
t) Patentes producidas por académicos/as ( )

4. TIPO DE TRABAJO DE INVESTIGACIÓN (Marque con una X)

a) Tesis ( )
b) Trabajo de Investigación ( )
c) Trabajo de suficiencia profesional ( )
d) Trabajo académico (**X**)

5. DATOS DE LA PUBLICACION

a) Título: .....Seguridad de la Información.....
.....
.....
b) Campo del conocimiento OCDE (Indicar el código de clasificación OCDE de la obra: https://catalogos.concytec.gob.pe/vocabulario/ocde_ford.html): .....2.02.04.....
c) Fecha de publicación: .....Año 2022.....

6. DATOS DEL ASESOR:

a) Nombres y Apellidos: .....Hugo Euler Tito Chura.....
b) DNI/Pasaporte/Cédula: .....01315850.....
c) ORCID: .....0000-0001-8269-0655.....

FIRMA : .....

DOCUMENTO DE IDENTIDAD : .....46911703.....
NOMBRES Y APELLIDOS : .....Miguel Slip, Cornejo Valcarcel.....

LICENCIAS

Licencia Estándar

Bajo los siguientes términos, autorizo el depósito de mi trabajo de investigación en el Repositorio Institucional Digital de la UNAM.

Con la autorización de depósito de mi trabajo de investigación, otorgo a la Universidad Nacional de Moquegua, una Licencia No Exclusiva para reproducir. distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi trabajo de investigación (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios provistos por la Universidad, creados o por crearse, tales como el Repositorio Institucional Digital de la UNAM, Colección de Tesis, entre otros, en el Perú y en el extranjero, por el tiempo y veces que considere necesarias, y libre de remuneraciones.

En virtud de dicha Licencia, la UNIVERSIDAD NACIONAL DE MOQUEGUA, podrá reproducir mi trabajo de investigación en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con los propósitos de seguridad, respaldo y preservación.

Declaro que el trabajo de investigación es una creación de mi autoría y exclusiva titularidad, o coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicho trabajo de investigación no infringe derechos de autor de terceras personas.

La UNIVERSIDAD NACIONAL DE MOQUEGUA consignara el nombre del/los autor/es del trabajo de investigación, y no le hará ninguna modificación más de la permitida en la presente licencia.

Autorizo el depósito (marque con una X).

(X) **SI autorizo que se deposite inmediatamente.**

FIRMA : .....

DOCUMENTO DE IDENTIDAD : 46911703

NOMBRES Y APELLIDOS : Miguel Slip, Cornejo Valcarcel

FECHA : 29 de Septiembre de 2022