UNIVERSIDAD NACIONAL DE MOQUEGUA

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

INFORME DE EXAMEN PROFESIONAL

CIBERSEGURIDAD

PRESENTADO POR:

BACH. BOJORQUEZ HUANCA JEYMI SHIRLEY

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERA 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

[CIBERSEGURIDAD]

PRESENTADO POR:

BACH. BOJORQUEZ HUANCA JEYMI SHIRLEY

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERA DE SISTEMAS E INFORMATICA

_____

BACH. BOJORQUEZ HUANCA JEYMI SHIRLEY

_____

MSC. HUGO EULER TITO CHURA

ASESOR

MOQUEGUA – PERÚ

2022

UNAM
UNIVERSIDAD NACIONAL DE MOQUEGUA

UNIVERSIDAD NACIONAL DE MOQUEGUA
SECRETARIO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Folio Nº 024

ACTA DE TITULACIÓN

I. Modalidad:
Examen Profesional

II. Documento de aprobación:
Resolución de Comisión Organizadora N° 636-2022-UNAM
Fecha: 19 de agosto de 2022

III. Título de Informe de Examen Profesional:

" CIBERSEGURIDAD "

Bachiller: Jeymi Shirley Bojorquez Huanca
Asesor Principal: M.Sc. Hugo Euler Tito Chura
Co-Asesor: .....

IV. Se dictamina con las siguientes notas:

Examen Escrito: 14.00 Entrevista: 2.67 Promedio: 17

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

Opta el Título Profesional de INGENIERO DE SISTEMAS E INFORMÁTICA.

Siendo las 15:15 horas, del 24 de octubre 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

M.Sc. 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. Jeymi Bojorquez H.

10

DEDICATORIA

El presente trabajo está dedicado en primer lugar a Dios quien me dio la fortaleza espiritual para continuar en el cumplimiento de mis objetivos profesionales, a mi Familia que con su amor y cariño siempre me apoyaron en los momentos difíciles a lo largo de mi formación académica.

A ellos dedico el presente por confiar siempre en mí.

AGRADECIMIENTO

Mi profundo agradecimiento a mis padres por el amor y la motivación constante, en esta etapa de mi vida profesional y laboral.

De igual manera a mi asesor por el apoyo brindado, su dirección, tiempo y conocimientos profesionales para la revisión del presente informe profesional.

Finalmente quiero expresar mi más grande y sincero agradecimiento a la Universidad Nacional de Moquegua, mi alma Mater, por la formación profesional a través de la escuela Profesional de Ingeniería de Sistemas e Informática y sus docentes universitarios.

RESUMEN

El presente informe de examen profesional tiene como propósito el poder desarrollar la definición, los antecedentes históricos, de ciberseguridad. Además, se extiende información acerca del comportamiento de la ciberseguridad dentro de una empresa y las recomendaciones que se deben de seguir para poder proteger los datos y evitar vulnerabilidades dentro del sistema.

La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos (IBM, 2022)

La ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión en la cual las relaciones sociales pueden efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información. (Hirare, 2017)

ABSTRACT

The purpose of this professional examination report is to develop the definition, the historical background, of cybersecurity. In addition, information is provided about the behavior of cybersecurity within a company and the recommendations that must be followed in order to protect data and avoid vulnerabilities within the system.

Cybersecurity is the set of procedures and tools that are implemented to protect the information that is generated and processed through computers, servers, mobile devices, networks and electronic systems (IBM, 2022)

Cybersecurity is a condition to allow citizens, organizations and institutions to benefit from the use of cyberspace as a dimension in which social relations can be carried out more quickly and economically compared to other known forms of information exchange. (Hiraré, 2017)

ÍNDICE GENERAL

INTRODUCCIÓN **1**

CAPITULO I: ASPECTOS GENERALES **2**

1.1. CIBERSEGURIDAD 2

CAPITULO II: DESARROLLO DEL TEMA **3**

1.1. CIBERSEGURIDAD 3

1.2. HISTORIA DE CIBERSEGURIDAD 3

1.3. DIFERENCIAS CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN 5

1.4. HERRAMIENTAS DE CIBER DELITOS 7

1.4.1. Respaldo de la información 7

1.4.2. Protección contra el virus 8

1.4.3. Acciones Propias 8

1.5. LA WEB PROFUNDA, LA WEB INVISIBLE (DEEP WEB) 9

1.6. SEGURO DE CIBERRIESGOS EN LA EMPRESA 9

1.7. USOS Y APLICACIONES 10

1.8. ESTRATEGIAS, PROTOCOLOS Y NORMAS PARA SEGURIDAD INFORMÁTICA. 11

1.9. VENTAJAS 11

1.10. DESVENTAJAS 12

1.11. CONTEXTO ACTUAL Y DESAFÍOS DE LA CIBERSEGURIDAD 12

1.11.1. Los Bring Your Own Device (BYOD). 14

1.11.2. Cloud computing y big data 15

1.11.3. Internet de las cosas (Internet of Things) 15

1.11.4. Apps Móviles 16

1.11.5. Desafíos legales de la ciberseguridad 16

CAPITULO III: ANTECEDENTES 17

2.1. ANTECEDENTES INTERNACIONALES 17

2.2. ANTECEDENTES NACIONALES 18

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES 20

CONCLUSIONES 20

RECOMENDACIONES 21

BIBLIOGRAFÍA 22

ÍNDICE DE FIGURAS

Figura 1 *La ciberseguridad ligada a seguridad de la información y seguridad informática* 2

Figura 2 *Costo total promedio por ataque millones de $* 6

ÍNDICE DE TABLAS

Tabla 1 *Distribución de la población mundial usuarios con acceso a internet, 2022* 6

Tabla 2 *Incidentes cibernéticos internacionales (2003-2020)* 13

LISTA DE ACRÓNIMOS Y ABREVIATURAS

APT: Amenaza persistente avanzada

CSIRT: Equipo de respuesta a incidentes de seguridad informática

ITCB: Consejo de Tecnologías de la Información y Ciberseguridad

SIC: Sistemas de información y comunicaciones

SRI: Seguridad de las redes y de la información

TIC: Tecnologías de la información y de las comunicaciones

Amenaza persistente avanzada: Ataque de usuario no autorizado accede a un sistema o red con el fin de robar datos sensibles.

Ciberespacio: entorno global el software y los servicios se comunican a través de redes de ordenadores.

Ciberespionaje: la práctica de obtener secretos e información de Internet.

Ciberseguridad: Medidas para proteger las redes e infraestructuras informáticas.

Ingeniería social: Manipulación psicológica para engañar a las personas con el fin de que compartan información confidencial.

Phishing: Envío de mensajes de correo electrónico que simulan proceder de una fuente de confianza para engañar a los destinatarios.

Prueba de penetración: Método para evaluar la seguridad de un sistema informático

INTRODUCCIÓN

Actualmente, la red es parte de nuestra vida diaria que, por medio de los diferentes dispositivos como el celular, y otros dispositivos electrónicos que nos dan acceso a esta plataforma de acceso e información con diferentes posibilidades, se ha convertido en extensiones de nuestros cuerpos y mentes volviéndonos seres dependientes con una necesidad constante de estar en comunicación con la sociedad digital que nos rodea

La ciberseguridad depende de la seguridad de la información, que consiste en preservar la confidencialidad, la integridad y la disponibilidad de la información, implica identificar, prevenir y detectar incidentes cibernéticos, responder a ellos y recuperarse de ellos.

Ya desde hace algunos años en el mundo informático han aumentado los riesgos con respecto a la seguridad de la información que compromete tres aspectos sustanciales sobre la seguridad de la información, la integridad, la confidencialidad y la disponibilidad.

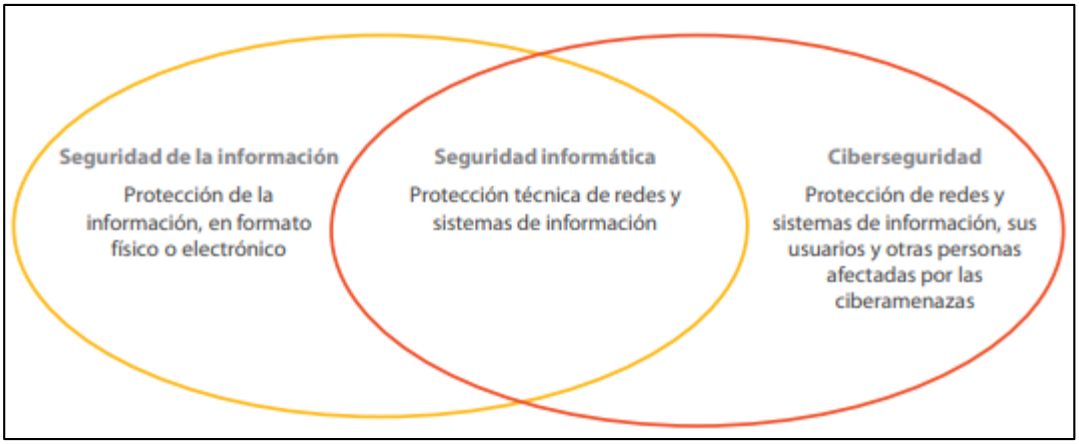
CAPITULO I: ASPECTOS GENERALES

1.1. CIBERSEGURIDAD

Se conoce como ciberseguridad a la práctica basada en proteger los sistemas informáticos, las redes y los programas de ataques digitales. En general, en una organización se trata de una estrategia que implica a las personas, los procesos y las tecnologías para crear múltiples capas de protección ante los ciberataques. (2019, p. 3)

Figura 1

La ciberseguridad ligada a seguridad de la información y seguridad informática



Nota. Tribunal de cuentas europeas

CAPITULO II: DESARROLLO DEL TEMA

1.1. CIBERSEGURIDAD

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. (indeadiversity, 2016)

La ciberseguridad tiene como foco la protección de la información digital que vive en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información. (SGSI, 2017)

1.2. HISTORIA DE CIBERSEGURIDAD

Detalles de algunas de las reseñas históricas relacionadas a los ataques informáticos que impulsaron e impulsan a mejorar las prácticas de la seguridad informática

El primer hacker de la historia fue Nevil Maskelyne que logró interceptar la primera transmisión del telégrafo inalámbrico, que, en 1903, iba a ser inaugurado por Marconi en Inglaterra. Mientras se estaba enviando el mensaje inicial, el mago Maskelyne, a través de una antena logro interceptar el mensaje inaugural, demostrando las vulnerabilidades del telégrafo inalámbrico creado por Marconi.

El primer ciberdelincuente de la historia puede ser un personaje denominado “Capitan Crunch” debido a que utilizó un pequeño silbato que venía en una caja de cereal para engañar a la central telefónica con el sonido de dicho silbato, logrando realizar llamadas telefónicas de larga distancia, consiguiendo engañar a las empresas de telefonía con dicho fraude.

El primer virus se llamaba “Creeper” (enredadera), era un programa que se replicaba a sí mismo y se difundía de un nodo a otro por la red. No era un programa malicioso, y simplemente viajaba por la red replicándose de computador a computador, con el mensaje “soy una enredadera, atrápame si puedes”, a partir de allí la industria de los virus o malware ha evolucionado hasta el día de hoy, logrando dejar ingresos por estos delitos de cerca de 400.000 millones de euros.

El mayor ataque de la historia denominado “Wannacry” afecto más de 200 mil computadores en cerca de 120 países en todo el mundo, dicho ataque fue un “ramsomware”, que es un secuestro de información, a través del cual, el ciberdelincuente encripta la información del computador, es decir que lo pone una clave desconocida para que el dueño de la información no la pueda utilizar y pide un dinero para entregar dicha clave.

1.3. DIFERENCIAS CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

Para tener una idea clara de las diferencias existentes partimos de la información, que puede encontrarse de diferentes formas, por ejemplo, en formato digital, en forma física, así como la manera no representada, como pueden ser las ideas o el conocimiento de las personas. En este sentido, todos los activos de información pueden encontrarse de diferentes formas.

La ciberseguridad se enfoca de forma principal a la información en formato digital y a los sistemas interconectados que la procesan, almacenan o transmiten.

La seguridad de la información se sustenta en las metodologías, en las normas, en las técnicas, en las herramientas, en las estructuras, organizaciones y en la tecnología. Soportan la idea de protección en las diferentes facetas de la información. (SGSI, 2017)

Tabla 1

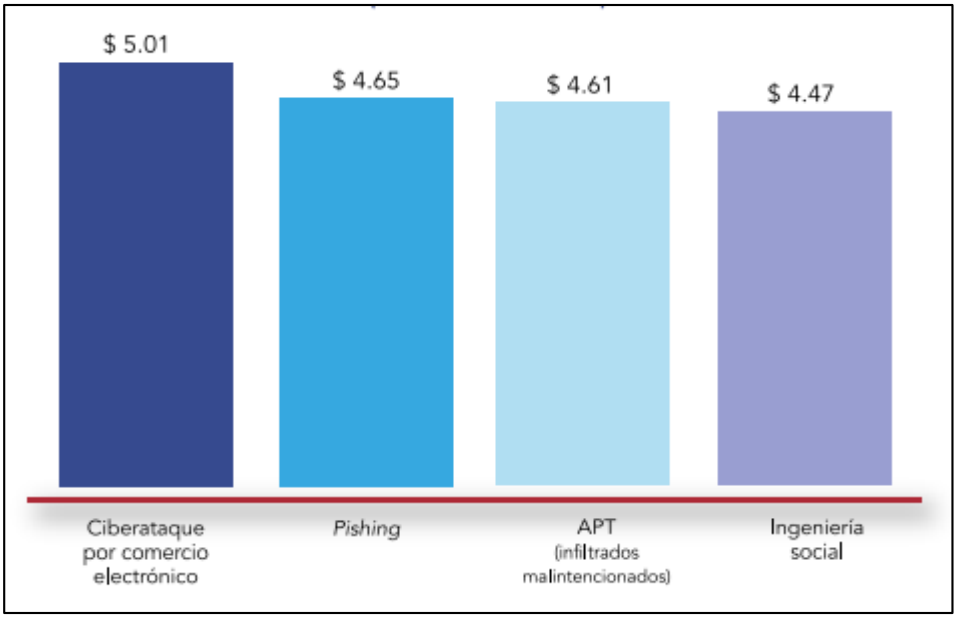
Distribución de la población mundial usuarios con acceso a internet, 2022

REGIÓN	POBLACIÓN ESTIMADA (Q1/2019)	PORCENTAJE POBLACIÓN MUNDIAL (%)	USUARIOS DE INTERNET (Q1/2019)	RATIO DE PENETRACIÓN (%)	PORCENTAJE INTERNET MUNDIAL (%)
África	1.340.598.447	55,1	2.366.213.308	55,1	11,3
Asia	4.294.516.659	55,1	2.366.213.308	55,1	50,9
Europa	834.995.197	10,7	727.848.547	87,2	15,7
Latinoamérica y Caribe	658.345.826	8,5	453.702.292	68,9	10,0
Medio Este	260.991.690	3,3	183.212.099	70,2	3,9
América del Norte	368.869.64	4,7	348.908.868	94,6	7,5
Oceanía y Australia	42.690.838	0,5	28.917.600	67,7	0,6
Total mundial	7.796.949.710	100	4.648.228.067	59,6	100

Nota. Porcentaje de usuarios que acceden a internet sean víctimas de un ciberataque.

Figura 2

Costo total promedio por ataque millones de $



Nota. Información de IBM Segurity 2022.

1.4. HERRAMIENTAS DE CIBER DELITOS

Existen diversas herramientas que se suelen usar para obtener información de los usuarios o incluso dañar esta, entre ellas tenemos:

1.4.1. Respaldo de la información

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups. Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (solo se copian los ficheros creados o modificados desde la última copia de seguridad).

Un buen sistema de respaldo debe contar con ciertas características:

- Continuo: El respaldo de datos debe ser completamente automático y continuo.
- Seguro: Muchos softwares de respaldo incluyen cifrado de datos, lo cual debe ser hecho localmente en el equipo antes del envío de la información.
- Remoto: Los datos deben quedar alojados en dependencias alejadas de la empresa.
- Mantenimiento de versiones anteriores de los datos: Se debe contar con un sistema que permita la recuperación diaria, semanal y mensual de los datos.

1.4.2. Protección contra el virus

Los virus son uno de los medios más tradicionales de ataque a los sistemas y a la información que sostienen.

- Control del software instalado

Tener instalado en la máquina únicamente el software necesario reduce riesgos.

- Control de la red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos como portátiles.

1.4.3. Acciones Propias

- La protección antifraude o pishing:

Estas es una de las más importantes, el sentido común. El engaño, se ha convertido en una de las prácticas más usadas en internet.

- Ser previsivos:

Estas herramientas constan en conseguir por varios medios la supervivencia de la organización o empresa, después de un inconveniente de seguridad, dentro de esta solución se encuentran, copias de seguridad en la nube o en otros dispositivos.

- Protección de comunicaciones:

Estas soluciones se encargan de proteger a la organización de un grupo de amenazas, como los ataques de denegación de servicios, accesos no autorizados o la intercepción de las comunicaciones.

1.5. LA WEB PROFUNDA, LA WEB INVISIBLE (DEEP WEB)

Existe una creciente dificultad para detectar y erradicar las redes de robots (botnets) que se siguen utilizando para la diseminación de spam, para la ejecución de ataques DDoS, spear-phishing, click-fraud, keylogging, así como la difusión de ransomware o la sustracción de dinero digital.

Los datos de 2014 señalaban, por aquel entonces, un descenso en el número de botnets detectadas, aunque no su eficacia y su peligrosidad. De hecho, los atacantes ahora utilizan la red TOR para ocultar botnets y/o servidores de mando y control (C & C), lo que dificulta enormemente su detección y erradicación [CCN-CERT 2015, 14-15]. Recordemos que el CCN-CERT define TOR como:

"TOR (abreviatura de The Onion Router) es un software diseñado para permitir el acceso anónimo a internet.

1.6. SEGURO DE CIBERRIESGOS EN LA EMPRESA

Un informe de Allianz Global sobre ciberseguridad, dado a conocer el 8 de septiembre de 2015, señalaba que las primas mundiales de seguros cibernéticos superarán los 20.000 millones de dólares en la próxima década frente a los 2.000 millones que captan en la actualidad. El aumento de este negocio se producirá por una mayor concienciación sobre estos riesgos y por los cambios normativos que propician la contratación de esta cobertura asegurada por parte de las empresas, señala el citado estudio. «En la actualidad menos del 10 % de las empresas suscriben una póliza para cubrirse de losrie sgos cibernéticos». La «ciberdelincuencia» cuesta

445.000 millones de dólares anuales a la economía mundial y la mitad de este importe recae en las diez principales economías mundiales (Estados Unidos con 108.000 millones lidera la clasificación, seguida de China con 60.000 millones y Alemania con 59.000 millones).

Los expertos recomiendan a las compañías que, además de ser innovadoras en tecnología y atención al cliente, deberían hacer una inversión especial en ciberseguridad, tanto en protección como en la respuesta a los ataques de los hackers, ya que los datos que manejan a diario son un material sensible por contener información personal de sus clientes.

1.7. USOS Y APLICACIONES

Rodríguez (2019), nos explica que las principales amenazas en seguridad son:

- El **malware**, programas maliciosos. La toma de control de nuestro ordenador para realizar tareas que requieren un alto procesamiento.
- El **phishing**, suplantar información de una empresa u organización, para obtener información del usuario.
- El **robo económico**, al acceder a las cuentas bancarias del usuario.
- El **robo lúdico** de fotografías, vídeos o cualquier otro material.
- El **robo de imagen** para dañar a algún usuario por medio de las redes sociales. (p. 7)

1.8. ESTRATEGIAS, PROTOCOLOS Y NORMAS PARA SEGURIDAD INFORMÁTICA.

Según Rodríguez (2019, p. 12), en todos ellos se pueden apreciar las siguientes fases:

- **Prevención:** requiere una formación continua con el objetivo de conocer las nuevas amenazas que acechan en las redes en cada momento y las medidas que realizar para no arriesgar la información y los sistemas corporativos.

- **Detección de un ataque:** puede tener lugar en tiempo real o después de que haya ocurrido. Esta fase del ciclo de la ciberseguridad reposa sobre dos acciones complementarias, la monitorización y la identificación.

- **Respuesta:** cuando finalmente se ha sufrido un ciberataque se inicia esta etapa, que conlleva la recuperación y la aplicación de medidas de seguridad.

- **Inteligencia:** se trata de compartir la información sobre los ataques con otras empresas e instituciones, así como con organismos relacionados con la seguridad, para conocer mejor la operativa de agresión y hacer más efectiva la respuesta al cibercrimen.

1.9. VENTAJAS

La seguridad informática se encarga de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Capacita a la población general sobre las nuevas tecnologías y las amenazas que pueden traer.

La ciberseguridad te ofrece protección, para tus equipos, teléfonos móviles y demás artículos tecnológicos.

1.10. DESVENTAJAS

Una de sus más grandes desventajas son que los elementos tecnológicos a los cuales se aplica la ciberseguridad, son perjudiciales para el Medio Ambiente.

En los equipos más desactualizados un antivirus realmente efectivo puede ser muy pesado, puede hacerlos más lentos, y ocupar mucho espacio en memoria.

Los requisitos para su creación de contraseñas son cada vez más complejos. La mayoría de los sitios web requieren inicios de sesión, y el cambio de contraseñas con frecuencia se ha vuelto obligatorio en muchos lugares de trabajo.

Con el avance de la tecnología, es más fácil robar información y por eso es necesario contratar servicios de Ciberseguridad, muchos de estos servicios tienen costos elevados.

1.11. CONTEXTO ACTUAL Y DESAFÍOS DE LA CIBERSEGURIDAD

La ciberseguridad ha terminado siendo un asunto global pues el ciberespacio no tiene arraigo en ningún país y por ello el ecosistema digital, y su protección frente a las actividades ilícitas, terminó siendo un asunto que atañe a todas las naciones y sin fronteras claras. (Díaz, 2020)

Tabla 2

Incidentes cibernéticos internacionales (2003-2022)

Año	Incidente
2003	Acusación de EEUU a China sobre ataques informáticos (Titan Rain).
2007	Ataques a Estonia que inutilizaron infraestructuras críticas.
2008	Explosión, por ataque cibernético, del oleoducto BTC en Refahiye (Turquía).
2010	El gusano informático *Stuxnet* genera daños en plantas de uranio iraníes y sabotea proyectos estratégicos nacionales.
2012	Borrado de 30.000 discos duros de la empresa petrolera Saudí Aramco.
2016	Presunto ciberataque ruso (servicios de seguridad rusos) en las elecciones presidenciales de EEUU con filtraciones de información de los servidores de correo del Comité Nacional Demócrata y de su candidata Hillary Clinton, publicación de documentos para afectar su imagen y posible manipulación de elecciones en favor de Donald Trump.
2018	Supuestos ciberataques contra estructuras de información de Rusia en la copa mundial de futbol y contra redes de suministro eléctrico en 2019.
2019	Presuntos ataques cibernéticos a la infraestructura eléctrica de Venezuela.

Año	Incidente
2020	Acusaciones entre potencias por presuntos ataques cibernéticos para robo de propiedad intelectual e información sobre vacunas COVID 19.
2022	Intrusión a la plataforma de videoconferencias Zoom para extraer información, infiltrar datos y boicotear reuniones remotas.

Nota. Información de incidentes cibernéticos.

1.11.1. Los Bring Your Own Device (BYOD).

Es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos. Así, en muchas empresas los empleados pueden trabajar con su ordenador portátil, centralizar toda la información empresarial en su smartphone personal para no tener que llevar dos móviles o acceder a la red corporativa desde casa.

Sin embargo, no todo son ventajas: la ausencia de políticas de seguridad adecuadas puede poner en riesgo información confidencial, y hay otros inconvenientes derivados del BYOD. Sigue leyendo y descubre las características de este fenómeno, sus pros y sus contras.

1.11.2. Cloud computing y big data

Uno de los riesgos más importantes a la hora de utilizar el cloud computing es la pérdida de control en el uso de las infraestructuras de la nube. Esto sucede porque el cliente cede necesariamente control al proveedor de la nube en algunos asuntos que pueden afectar a la seguridad.

- Al tratarse de una tecnología nueva, el desconocimiento por parte de las organizaciones que lo aplican puede hacer que sea más vulnerable.
- La autenticación de usuarios y el acceso a los datos desde múltiples ubicaciones pueden no estar suficientemente controlados.
- Se puede ofrecer una oportunidad significativa para la entrada de datos maliciosos o para una inadecuada validación de los datos.

1.11.3. Internet de las cosas (Internet of Things)

El Internet de las cosas supone que millones de dispositivos se encuentren continuamente generando datos y, lo que es más relevante desde el punto de vista de la seguridad, compartiendo esos datos en Internet. Una tendencia que se cree que tendrá un crecimiento exponencial en los próximos años, tal y como se ha mostrado en la introducción de esta sección, ante la que la seguridad es fundamental para lograr que la tendencia se materialice según las previsiones; y es que la falta de seguridad o de privacidad podría suponer una vía de inseguridad que podría ser utilizada por los ciberdelincuentes.

1.11.4. Apps Móviles

La capacidad de las apps de recolectar datos personales y de comportamiento continuamente las convierten en un foco de posibles fugas de información que afecten a la privacidad de las personas. Una de las principales dificultades para evitar esta situación e incluso para analizarla de una forma global reside en las diferencias regulatorias en los distintos países, todo ello en un modelo en el que los servicios tienen un carácter global.

1.11.5. Desafíos legales de la ciberseguridad

El reforzamiento de la ciberseguridad no solo presenta desafíos tecnológicos. Una regulación adecuada y la existencia de mecanismos legales adaptados a los avances tecnológicos son fundamentales en la lucha contra el ciberdelito. De los desafíos analizados en los apartados anteriores, dos son los que más relevancia tienen desde un punto de vista legal, dada su rápida expansión y su relación con la generación, transmisión y custodia de información a través de las redes de comunicación: la prestación de servicios de cloud computing y el desarrollo de soluciones del Internet de las Cosas (IoT.).

CAPITULO III: ANTECEDENTES

2.1. ANTECEDENTES INTERNACIONALES

Según (Díaz, **Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia, 2020**), en su trabajo de investigación hace referencia la ciberseguridad como conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios [disponibilidad, integridad, autenticidad, confidencialidad, etc.]

Según (Pachacama, 2019), en su trabajo de tesis denominado **"Análisis de la ciberseguridad a la infraestructura tecnológica de la universidad técnica de Cotopaxi";** cuyo objetivo principal es: Analizar la ciberseguridad a la infraestructura tecnológica de la universidad técnica de Cotopaxi, a través del sistema operativo Kali Linux, virtualizado en una maquina física para disminuir riesgos existentes a sus sistemas informáticos. Para esta investigación se evalúo una muestra de 217 personas a las que se les aplicó una encuesta; para evaluar esta muestra se aplicó una investigación de tipo bibliográfica, investigación de campo e investigación experimental. Los resultados que se obtuvieron fueron que el nivel de vulnerabilidad que posee su sistema informático, de modo que en los tiempos actuales las nuevas

herramientas tecnologías permiten realizar un análisis más detallado permitiéndonos verificar sus posibles brechas de seguridad y de esa manera dar futuras recomendaciones para evitar ser atacados por los hackers.

2.2. ANTECEDENTES NACIONALES

Según (RUIZ, 2021), en su trabajo de investigación **Estudio de viabilidad técnica económica para instalar una agencia de ciberseguridad en piura, 2021** hace referencia la ciberseguridad como conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios [disponibilidad, integridad, autenticidad, confidencialidad, etc.]

Según (Vilcarromero Zubiate, 2018), en su proyecto de investigación titulado **:"Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones"**; teniendo por objetivo principal: Proveer al área del SOC un marco de ciberseguridad para generar una solución que le permita implantar, operar, monitorear, revisar y mejorar los controles de Ciberseguridad, con el fin de ser un SOC de referencia y llegar a ser competitivo en el mercado.

Se usó una metodología de tipo aplicada con un nivel descriptivo y diseño no experimental. Cuyos resultados fueron que el VPN fue positivo de S/ 392,905.16 y el TIR 11.74% y por lo tanto el autor concluye que este proyecto es rentable.

Según (Ramos, 2018), en su investigación denominada **"Ciberseguridad en la actividad organizacional de la era digital"**, teniendo por objetivo principal la investigación fue determinar en qué medida la ciberseguridad mejora la actividad organizacional en la era digital. Aplicando una metodología de tipo básica con un nivel exploratorio con diseño no experimental. Los resultados obtenidos de la presente investigación fueron que la ciberseguridad mejora la planificación de la actividad organizacional en la era digital, con un 85% de reducción de tiempos de operación, asimismo, con una disponibilidad del 99% de disponibilidad de datos; además que genera un 79% de reducción de los gastos operativos. La Ciberseguridad mejora la aplicación de la actividad organizacional en la era digital. Con 86% de reducción de problemas de infraestructura. En conclusión, el autor consideró que la ciberseguridad tiene un efecto positivo en la mejora la actividad organizacional respecto de la planificación y la aplicación en la era digital.

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Se evidenció claramente en 2020 con el aumento de las interacciones mediadas por internet y otras TIC, derivado del aislamiento preventivo decretado para enfrentar la pandemia (COVID-19) y que generó un aumento significativo en los delitos cibernéticos contra gobiernos, organizaciones y personas.

Debido a los riesgos existentes actualmente para la seguridad de la información y ataques masivos de virus informáticos ocurridos recientemente es importante que las organizaciones estén concientizadas sobre ello, además de tomar acciones preventivas y estar preparadas para posibles ataques.

Finalmente, se debe fomentar la denuncia de delitos cibernéticos para poder determinar la magnitud real del fenómeno y los frentes prioritarios de acción y como apoyo a la gestión de las autoridades encargadas y avanzar rápidamente en términos legislativos para lograr la penalización de los delitos informáticos.

RECOMENDACIONES

En la actualidad se tienen en cuenta las siguientes recomendaciones para evitar posibles ataques: (SGSI, 2018)

Recomendaciones más transcendentales en términos de seguridad en Internet y que sigue siendo molesta para muchos usuarios son las contraseñas seguras, en lo que respecta a la protección más sencilla, resultan muy efectivas, ya sea para impedir que un usuario inicie un ordenador ajeno o para bloquear a un hacker que intenta acceder una cuenta de correo.

Un cortafuego resulta efectivo cuando se combina con un programa antivirus, que no solo ofrece protección contra virus, troyanos y malware, sino que también los elimina en el acto. Por eso son imprescindibles los análisis regulares en el ordenador y deben convertirse en un trabajo rutinario para obtener un nivel de ciberseguridad óptimo.

BIBLIOGRAFÍA

Díaz, M. R. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia.

Díaz, M. R. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia.

Gregorio, F. F. (2015). Elementos de sistemas operativos, de representación de la información y de procesadores hardware y software. *Escuela Técnica Superior de Ingenieros de Telecomunicación*, pág. 366.

Hirare, C. S. (2017). Ciberseguridad.

IBM, K. (2022). *Ciberseguridad concepto, tipos, amenazas y estrategias.*

indeadiversity. (2016). Seguridad informática.

Pachacama, A. L. (2019). *Análisis de la ciberseguridad a la infraestructura tecnológica de la universidad técnica de Cotopaxi.*

Ramos, G. (2018). *Ciberseguridad en la actividad organizacional de la era digital.*

RUIZ, J. A. (2021). *Estudio de viabilidad técnica económica para instalar una agencia de ciberseguridad en piura, 2021* .

SGSI. (2017). Seguridad de la Información.

Vilcarromero Zubiate, V. L. (2018). *Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones.*

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	: Jeymi Shirley Bojorquez Huanca
DNI/Carnet de Extranjería/Pasaporte N°	: 46951754
Correo electrónico	: jeymi.sbh@gmail.com
Teléfono/Celular	: 973581167

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 : Ciberseguridad
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 : 46951754
NOMBRES Y APELLIDOS : Jeymi Shirley Bojorquez Huanca

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 da 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 : 46951754

NOMBRES Y APELLIDOS : Jeymi Shirley Bojorquez Huanca

FECHA : **24 de Octubre del 2022**