UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

E.P. Ingeniería De Sistemas

Educación y Concientización en Ciberseguridad: La Base de una Sociedad Digital Segura

PRESENTADO POR:

FLORES LLANQUE Mery Elizabeth

GUTIERREZ ANCO Yesenia Alejandra

HUAHUACCAPA CCAMA Jaqueline

DOCENTE:

HUMPIRI FLORES Milton Edward

CICLO: 4 — GRUPO: 1

2023

Educación y Concientización en Ciberseguridad: La Base de una Sociedad Digital Segura

Introducción:

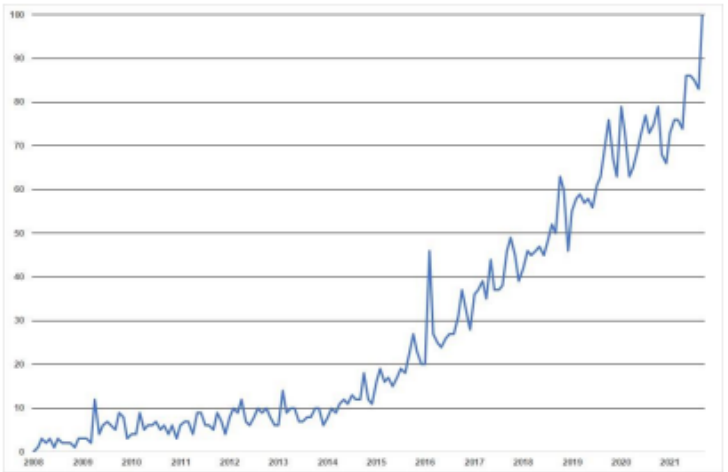
En la sociedad actual, la tecnología digital está estrechamente entrelazada con todos los aspectos de nuestras vidas, ofreciendo comodidad y eficiencia, pero también desafiando la seguridad de nuestros datos y sistemas. En este escenario, la educación y la concientización sobre seguridad ciberseguridad son bases importantes para construir una sociedad digital segura. Desde comprender los riesgos hasta implementar prácticas de seguridad proactivas, la educación y la concientización están surgiendo como elementos críticos para empoderar a las personas y las comunidades a defenderse contra los ciberataques(García, A. M., & Fernández, R. S. (2023)

Sin embargo, esta prosperidad también tiene sus debilidades. Los avances en tecnología no han ido acompañados de avances similares en ciberseguridad. En una sociedad que declara que el recurso más valioso ya no es el petróleo sino los datos (The Economist, 2017), los datos están cada vez más amenazados (Haqaf y Koyuncu, 2018).El primer ciberataque global ocurrió en mayo de 2017. Más de 230.000 ordenadores en todo el mundo han sido atacados por el ransomware WannaCry. Menos de un mes después apareció un nuevo ataque, esta vez una variante de Petya, más sofisticada y dañina (Lozano, 2017). (Mendivil et al., 2022)

En un sentido más técnico, se puede decir que, consiste en la unificación de sensores y dispositivos inteligentes en objetos habituales conectados a Internet a través de redes fijas e inalámbricas, diseñados con el objetivo de aprovechar un mundo conectado de manera digital y para gestionar nuevos crecimientos y oportunidades de negocio para la empresa y la industria.(Vloz, Allaica)

Figura 1.

Evolución del número de búsquedas del término "ciberseguridad"



Métodos:

Métodos de Educación y Concientización en Ciberseguridad:

Según la pedagogía de Freire, implica desarrollar la capacidad de mantener una actitud crítica constante. Esta actitud crítica permite a las personas percibir la situación de opresión en la que se encuentran y entenderla como algo limitante pero transformable.

Freire menciona que tiene que haber relación de la teoría y la práctica; no debe ser únicamente la teoría, sino llevarla a la vida real, a la sociedad en la que el individuo se va a desenvolver y desarrollar, ambos están unidos y no pueden ser separados. Freire a esto le llama en uno de sus principales principios "Práctica-teoría-práctica".(Conde, 2020)

Fase mágica: El individuo se encuentra en situación de impotencia ante fuerzas abrumadoras. No hace nada para resolver los problemas y se resigna a su suerte, esperando un cambio sin acción.

Fase ingenua: El oprimido reconoce los problemas, pero solo en términos individuales. Su comprensión de las causas es parcial, y no entiende completamente las acciones del opresor ni del sistema opresivo. Al pasar a la acción, adopta comportamientos similares al opresor, dirigiendo su agresión hacia sus iguales, su familia o incluso hacia sí mismo.

Fase crítica: En esta fase, el individuo alcanza un entendimiento más completo de la estructura opresiva. Puede ver claramente los problemas en función de su comunidad y comprende cómo la colaboración entre opresor y oprimido contribuye al funcionamiento del sistema opresivo.

Variable	Nivel de Conocimiento en Ciberseguridad (NCC)
Ecuación	NCC = (SR*0.30) + (SS*0.10) + (ES*0.30) + (CF*0.20) + (EBP*0.10)
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de las dimensiones de la variable. Sus umbrales son de: $0<NCC \leq 100$
Meta	Obtener el nivel de conocimiento en ciberseguridad que posee el egresado. Para lograrlo se han establecido diferentes "pesos" a las distintas dimensiones, de acuerdo a su relevancia.
Dimensiones que intervienen	Seguridad de Red (SR) Seguridad de Software (SS) Evaluación de la Seguridad (ES) Cómputo Forense (CF) Estándares y Buenas Prácticas (EBP)

1. **Programas de Formación en Instituciones Educativas:**

   Método: Integración de módulos de ciberseguridad en el currículo escolar.

2. **Simulacros de Ataques Cibernéticos:**

   Método: Realizar ejercicios simulados para enseñar a las personas a reconocer y responder a amenazas.

3. **Campañas de Concientización en Medios de Comunicación:**

   Método: Crear campañas educativas en plataformas mediáticas para llegar a un público más amplio.

4. **Plataformas de Aprendizaje en Línea:**

   Método: Utilización de cursos en línea para ofrecer formación accesible.

5. **Participación en Comunidades en Línea:**

   Método: Incentivar la participación en foros y comunidades en línea para compartir experiencias y conocimientos.

6. **Colaboración con la Industria:**

   Método: Establecer asociaciones con empresas para proporcionar programas de formación basados en casos del mundo real.

7. **Ejercicios Prácticos y Laboratorios:**

   Método: Proporcionar entornos prácticos para que las personas apliquen sus conocimientos.

8. **Juegos Educativos en Ciberseguridad:**

   Método: Desarrollar juegos que enseñen principios de ciberseguridad de manera interactiva.

9. **Seminarios y Conferencias:**

   Método: Participación en eventos que aborden las últimas tendencias y mejores prácticas.

10. **Desarrollo de Material Didáctico Interactivo:**

Método: Crear materiales interactivos, como infografías y videos, para explicar conceptos clave.

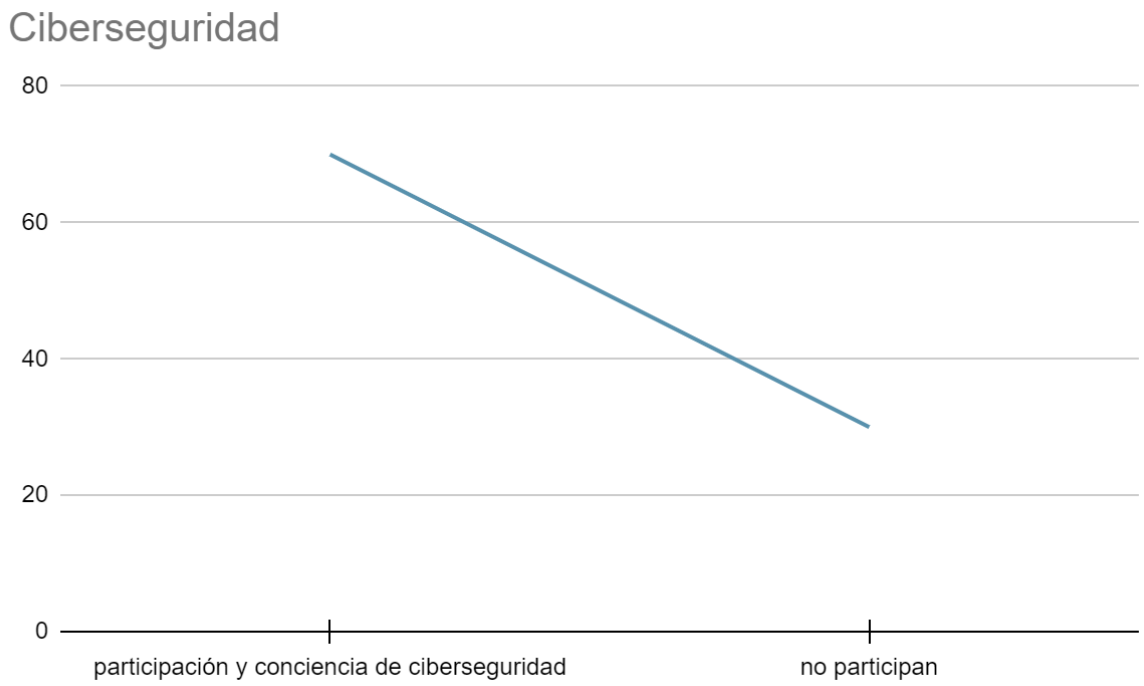
VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
INDEPENDIENTE Nivel de Conocimiento en Ciberseguridad	Profundidad del conocimiento con respecto a los aspectos que comprenden la ciberseguridad con el que cuenta el egresado, o que la empresa espera que tengan sus empleados y/o aspirantes.	Seguridad de Red	Principales Ataques y Cómo Funcionan
			Protocolos Seguros de Comunicación
			Red Privada Virtual
			Control de Acceso a la Red
		Seguridad de Software	Validación de Entrada
			Control de Roles y Privilegios
			Análisis de Vulnerabilidades
			Implementación de Parches
		Evaluación de la Seguridad	Análisis de Riesgos
			Pentesting
			Hacking Ético
			Gestión de Incidentes
		Cómputo forense	Cómo Ejecutar un Análisis Forense
			Software para Cómputo Forense
		Estándares, Buenas Prácticas	Estándares Relacionados a la Seguridad de la Información

Resultados:

- Programas de Formación en Instituciones Educativas

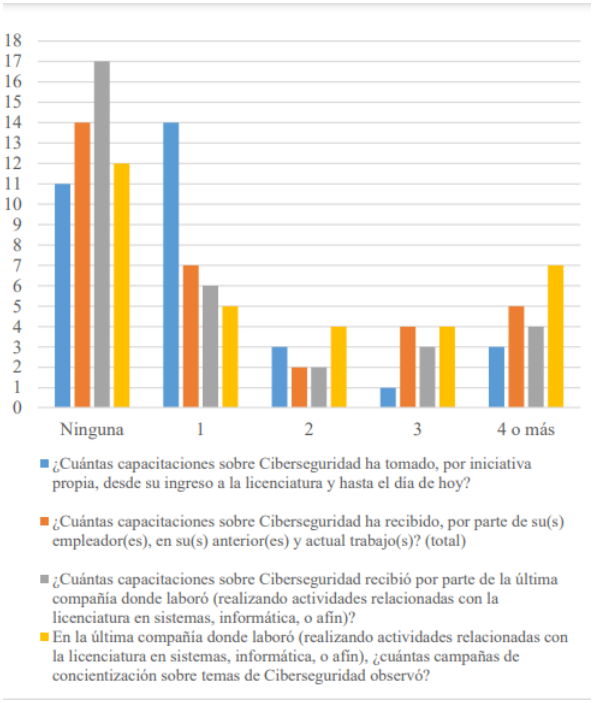
NIVELES DE EFICACIA DE PROGRAMAS DE FORMACIÓN EN INSTITUCIONES EDUCATIVAS
Nivel 1: Baja Integración de Ciberseguridad - Ausencia de programas formales de ciberseguridad en instituciones educativas - Poca conciencia entre profesores y estudiantes sobre riesgos cibernéticos
Nivel 2: Inicio de Integración - Inicio de programas de formación, pero con limitada participación - Conciencia básica sobre ciberseguridad, pero falta de profundidad en el temario
Nivel 3: Integración Satisfactoria - Programas de formación bien establecidos con participación activa - Conciencia sólida sobre ciberseguridad y conocimiento de buenas prácticas
Nivel 4: Excelencia en Ciberseguridad Educativa - Programas avanzados que incorporan prácticas y escenarios del mundo real - Participación activa y entusiasmo entre profesores y estudiantes
Resultado Específico: - Implementación exitosa de un programa de formación en instituciones educativas - Incremento del 70% en la participación y conciencia de ciberseguridad

Implicaciones: La educación en ciberseguridad en instituciones educativas ha demostrado ser efectiva, destacando la importancia de la integración curricular



Para contrarrestar esta percepción de falta de preparación en ciberseguridad, los graduados podrían participar en capacitaciones sobre estos temas, o las empresas para las que trabajan podrían ayudar a los graduados a aprender sobre ciberseguridad; para ello, el cuestionario incluye el problema de la cantidad de formación de los sujetos estudiados. La información relevante se muestra en la Figura 1.

Figura 1. Cantidad de Capacitaciones en Ciberseguridad a las que han Asistido los Encuestados



En la Figura 1 se muestra: a) 14 (43,75%) encuestados han tomado la iniciativa de participar en 1 capacitación sobre temas de seguridad de redes, mientras que el 34,37% (11) encuestados no han participado en ninguna capacitación sobre estos temas. Capacitación ; b) el 14% o el 43,75% de los encuestados no recibieron formación de su anterior empleador; c) el 53,12% (es decir, 17 encuestados) indicaron que no habían recibido ninguna formación en ciberseguridad en su trabajo actual Educación; d) El 37,5% (es decir, 12 encuestados) indicó que no había presenciado campañas de sensibilización sobre cuestiones de ciberseguridad en el lugar de trabajo. Ocupación.

Iniciando con la figura 2 que contiene el resultado de analizar la dimensión Seguridad de Red

Figura 2. Prueba t-student Para Comprobación de Hipótesis en Dimensión Seguridad de Red

Estadísticas de grupo

	Group	N	Media	Desviación Estándar	Err.Est.Media
Escala	EGSR	32	3.03	1.12	.20
	EMSR	15	3.73	.96	.25

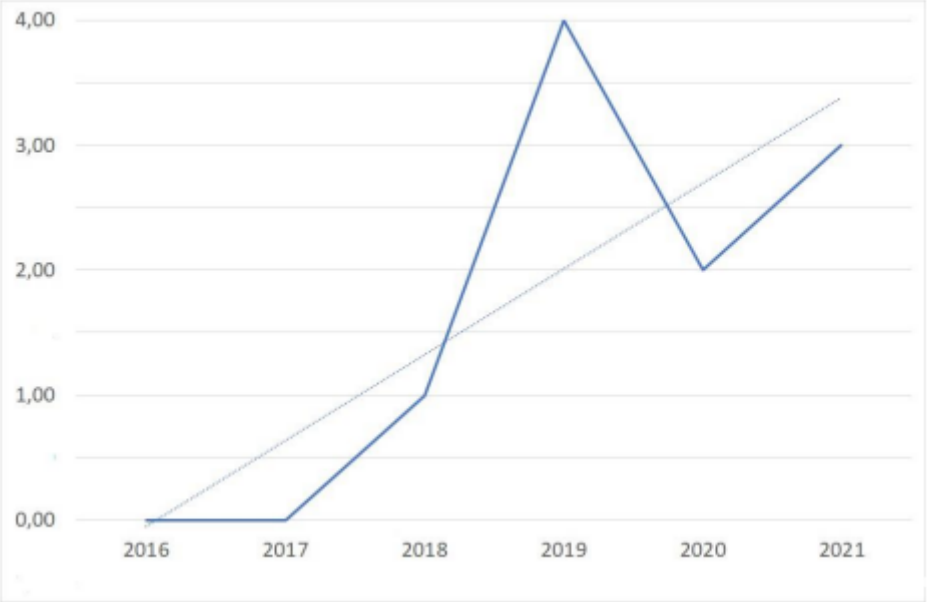
Prueba para muestras independientes

		Prueba de Levene para la igualdad de varianzas		T-Test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sign.	t	df	Sign. (2-colas)	Diferencia Media	Err.Est. de la Diferencia	Inferior	Superior
Escala	Se asume igualdad de varianzas	.27	.607	-2.09	45.00	.042	-.70	.34	-1.38	-.03
	Igualdad de varianzas no asumida			-2.21	31.73	.034	-.70	.32	-1.35	-.05

Como se ve en la Figura 2, el supuesto es que si el valor absoluto de t es mayor que el valor crítico, se rechaza la hipótesis nula; Se puede concluir que la dimensión de seguridad de redes necesita adoptar una hipótesis de investigación que menciona los conocimientos de seguridad de redes requeridos por la empresa y que existe una amplia variación entre los conocimientos que poseen los candidatos en una carrera de alta relevancia en ciberseguridad, lo que solo limita el conocimiento de la ciberseguridad en este contexto específico.

Iniciando con la figura 3 que contiene la Distribución de las metodologías empleadas

Figura 3. Distribución de las metodologías empleadas



Si bien se señala la importancia y la necesidad de capacitar y sensibilizar al personal ajeno a las TIC sobre la ciberseguridad utilizando modelos basados en competencias, quizás el aspecto más notable y la contribución más significativa de este estudio sea identificar la importancia de abordar cuestiones ajenas a las TIC. Empleados en empresas y organizaciones Faltan artículos que abordan el uso de marcos de competencias en la formación y el conocimiento del personal de TI. A pesar del limitado número de publicaciones y estudios que cumplen los criterios de selección, la evolución de su número muestra una clara tendencia ascendente, como se puede observar en la Figura 3, lo que permite indicar el creciente interés.

Resultado 3

El CSAM se implementó y validó utilizando tres escenarios diferentes en la institución de educación superior canadiense. Para implementar y validar el CSAM, también diseñamos el CATRAM que se implementó simultáneamente junto con el CSAM. Nuestras preguntas de investigación se abordaron adecuadamente mediante la creación y validación de dos modelos de ciberseguridad en las áreas de auditoría y concientización. La organización objetivo consideró los tres escenarios como realistas para su evaluación, capacitación de

sensibilización, aseguramiento y auditoría de ciberseguridad. Se concluye que los dos modelos de ciberseguridad son funcionales y útiles según se observa en los resultados de la validación (Tabla 1).(Sabillon, Cano, 2019)

En consecuencia, los modelos de ciberseguridad son adaptables y pueden ser implementados y probados en diversas organizaciones. Blokdyk (2018) emplea un enfoque similar al presentar los resultados del cuadro de mando de ciberseguridad. Este método de autoevaluación se representa gráficamente en un cuadro de mando de radar, resaltando un sistema de puntuación basado en siete criterios: reconocimiento, definición, medición, análisis, mejora, control y mantenimiento. El énfasis recae en la gestión de riesgos en relación con los temas de ciberseguridad.

No.	Ciberdominios	Resultados
2	Gobernanza y Estrategia	35%
3	Marco Legal y Conformidad	90%
4	Activos Cibernéticos	30%
5	Riesgos Cibernéticos	60%
6	Marcos y Regulaciones	30%
7	Arquitectura y Redes	67%
8	Información, Sistemas y Aplicaciones	55%
9	Identificacion de Vulnerabilidades	30%
10	Inteligencia de Amenazas	60%
11	Gestión de Incidentes	10%
12	Análisis Forense Digital	30%
13	Educación de Concientización	60%
14	Ciberseguros	90%
15	Defensa Cibernética Activa	5%
16	Tecnologias Evolutivas	100%
17	Recuperacion ante Desastres	30%
18	Gestión de Recursos Humanos	77%
Nivel de Madurez en Ciberseguridad		**51%**

Tabla 1 – Nivel de Madurez basado en múltiples ciberdominios

Conclusión:

La educación y la sensibilización en materia de ciberseguridad son fundamentales para construir una sociedad digital segura. Utilizando una variedad de métodos y enfoques, desde la integración de módulos en entornos educativos hasta la simulación de ataques cibernéticos, nos esforzamos por educar a las personas y las comunidades sobre las amenazas digitales y las mejores prácticas de seguridad. La conciencia crítica y la comprensión de las amenazas son esenciales para ayudar a las personas a identificar y responder de manera proactiva a posibles ataques. Las campañas de concientización en los medios, la participación de la comunidad en línea y las asociaciones industriales brindan una variedad de canales para difundir conocimientos y desarrollar una cultura de ciberseguridad. El uso de plataformas de aprendizaje en línea, actividades prácticas y juegos educativos no sólo hace que el aprendizaje sea accesible, sino que también brinda experiencias prácticas que refuerzan la aplicación de lo que se aprende. Además, asistir a seminarios, conferencias y desarrollar materiales de capacitación interactivos son factores importantes para mantenerse actualizado con las últimas tendencias y mejores prácticas de ciberseguridad. En última instancia, construir una sociedad digital segura implica no sólo implementar tecnologías de seguridad avanzadas sino también crear una población informada y preparada. La educación y la concientización sobre ciberseguridad son procesos colaborativos continuos que desempeñan un papel importante en el fortalecimiento de la resiliencia digital de la sociedad.

Referencias:

Mendivil, J., Sanz, B., & Gutierrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. ***PIXEL-BIT Revista de Medios y Educación*****, *63*, 197–225. https://revistapixelbit.com**

García, A. M., & Fernández, R. S. (2023)La interconexión digital de objetos habituales con Internet y sus aplicaciones para la empresa y la Industria

Mendoza, J. P. C. (2020). Concientización en Ciberseguridad a través de Ataques de Ingeniería Social. ***INF-FCPN-PGI Revista PGI*****, 62-64.**

National Institute of Standards and Technology (NIST). (2017). NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

SANS Institute. (2021). SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling.

Saltzer & Schroeder, (1975)Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura

National Cyber Security Alliance. (2023). StaySafeOnline Campaign.

Cybrary. (https://www.cybrary.it/)

Coursera. (https://www.coursera.org/)

Stack Exchange. (https://security.stackexchange.com/)

Cybersecurity Training Alliance. (https://www.cybertrainingalliance.com/)

OWASP WebGoat Project. (https://owasp.org/www-project-webgoat/)

OWASP Roots Asylum Project. (https://owasp.org/www-project-roots-asylum/)

RSA Conference. (https://www.rsaconference.com/)

Black Hat. (https://www.blackhat.com/)

Department of Homeland Security. (https://www.stopthinkconnect.org/)

Sabillón, R., & Cano, J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. ***Revista Ibérica de Sistemas e Tecnologias de Informação, 2019,(32)*****.**