Seguridad y Control
en Sistemas Informáticos

UNIVERSIDAD NACIONAL DE TUCUMAN
FACULTAD DE CIENCIAS ECONÓMICAS

Capa 8

UN PROYECTO INNOVADOR PARA CONCIENTIZAR SOBRE CIBERSEGURIDAD A LA COMUNIDAD. APLICABLE A LAS PyMES.

Busto, *María Dina*
Gimena, *Rocío*
Heredia, *Bruno Agustín*
Ledesma, *Guido Augusto*
Quispe, *Nicanor Facundo*

Profesor: Marcelo García

Noviembre 2024

Declaración jurada del origen de los contenidos:

Por medio de la presente, los autores manifiestan conocer y aceptar el "Reglamento para la Presentación de Trabajo Final" vigente de la asignatura "Seguridad y Control en Sistemas Informáticos", haciéndose responsables por la totalidad de los contenidos del presente documento, los cuales son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación nacional e internacional de Propiedad Intelectual.

Busto, María Dina. **FIRMADO.**

Gimena, Rocío. **FIRMADO.**

Heredia, Bruno Agustín. **FIRMADO.**

Ledesma, Guido Augusto. **FIRMADO.**

Quispe, Nicanor Facundo. **FIRMADO.**

ÍNDICE

CAPA8

UN PROYECTO INNOVADOR PARA CONCIENTIZAR SOBRE CIBERSEGURIDAD A LA COMUNIDAD. APLICABLE A LAS PYMES.

Busto, María Dina – Gimena, Rocío – Heredia, Bruno Agustín – Ledesma, Guido Augusto – Quispe, Nicanor Facundo
marrdb96@gmail.com - *gs.rocio93@gmail.com* - *agustinheredia38@gmail.com* – *guido.ledesma@gmail.com* – *quispefacundo62t@gmail.com*

Resumen

En un mundo cada vez más intercomunicado, donde la tecnología tiene un papel cada vez más preponderante en nuestra vida cotidiana, así como en los negocios, la ciberseguridad se ha posicionado como un tema de vital importancia.

Con el objetivo de abordar esta problemática, hemos trabajado en llevar a cabo este proyecto, que busca concientizar sobre Ciberseguridad a la comunidad, de una manera interactiva y accesible para todos, independientemente de sus conocimientos previos, edad, entre otros factores que se podrían considerar como limitantes.

En el presente trabajo se busca exponer el prototipo de la herramienta concientizadora, la cual tiene como objetivo introducir al usuario en el mundo de la seguridad de la información, propiciando que este se convierta, desde el momento de empezar a usarla y para el resto de su vida, en un actor proactivo en la protección de su información personal.

Para el desarrollo de dicha herramienta, fue necesario realizar un relevamiento previo, destinado a investigar acerca del conocimiento de un amplio espectro de usuarios en cuanto a la problemática enunciada.

Finalmente, y como medio de adaptación para el uso organizacional, se propone realizar una evaluación posterior a la experiencia, para dar cuenta de los nuevos conceptos que pudieran, o no, haberse adquirido con el uso de la herramienta.

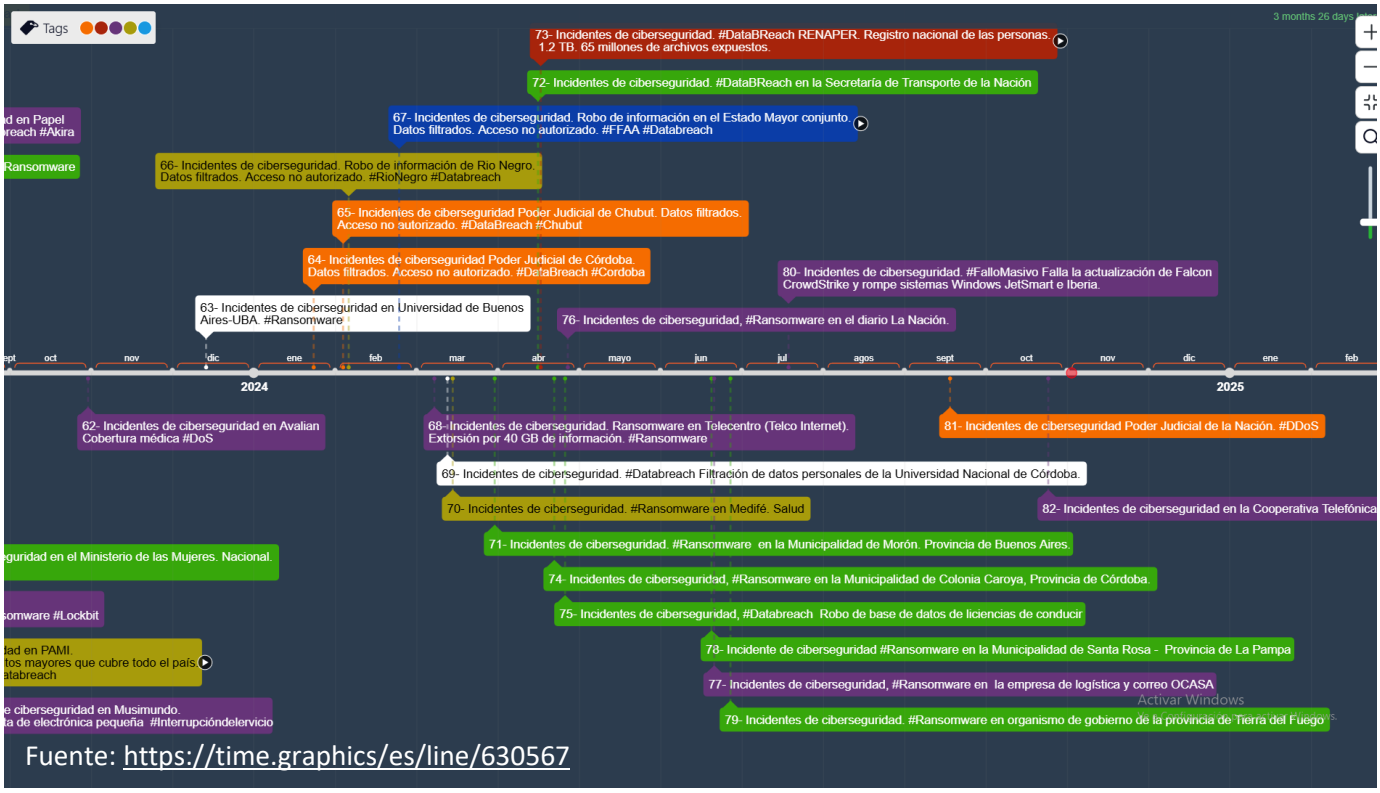
Palabras clave: ciberseguridad, comunidad, concientización.

Introducción

A medida que nos conectamos a redes sociales, realizamos compras en línea y almacenamos información personal en dispositivos, la probabilidad de ser víctimas de una amenaza cibernética se hace cada vez más presente.

Desde el robo de identidad hasta los ataques de *ransomware*, los peligros asociados con la falta de protección en línea pueden tener consecuencias devastadoras, tanto a nivel personal como profesional, ya que estos riesgos no solo afectan a los individuos, sino que también pueden comprometer la integridad de organizaciones enteras, exponiendo datos críticos que perjudiquen su funcionamiento y afectando la confianza de los clientes.

Los ataques cibernéticos se vuelven más sofisticados día a día, y los delincuentes emplean técnicas ingeniosas para vulnerar la seguridad de los sistemas. Los correos electrónicos de *phishing*, por ejemplo, engañan a las personas para que revelen información confidencial, mientras que el *malware* puede infiltrarse en dispositivos y robar datos sin que el usuario lo note. La falta de conciencia sobre estos métodos hace que muchas personas se conviertan en víctimas, lo que subraya la necesidad urgente de educar a la población sobre los peligros que acechan en el ciberespacio.



Fuente: https://time.graphics/es/line/630567

En la imagen precedente se pueden observar, solo por poner ejemplos, ataques sufridos por entes tanto públicos como privados en lo que va de 2024 en Argentina. Es importante recalcar que estos son únicamente los datos que fueron informados y de los que se tiene público conocimiento. Pensar en la cantidad de ataques que no transcienden en los medios en la actualidad, resulta preocupante.

Frente a esta realidad, es esencial adoptar buenas prácticas en ciberseguridad que ayuden a mitigar los riesgos. La creación de contraseñas robustas, el uso de la autenticación de dos factores y la actualización regular de software son solo algunas de las medidas que cada persona puede implementar en su vida diaria. Además, es fundamental ser cauteloso al hacer clic en enlaces desconocidos o al compartir información personal en línea. La adopción de estas prácticas no solo protege a los individuos, sino que también contribuye a un entorno digital más seguro para todos.

A pesar de la creciente conciencia sobre estos riesgos, muchos continúan navegando en el ciberespacio sin la preparación adecuada. Por ello, es crucial fomentar un cambio cultural donde la ciberseguridad se convierta en una prioridad en nuestra vida cotidiana. Esta transformación se puede lograr a través de iniciativas de concientización que involucren a la comunidad, a las empresas y a las instituciones educativas.

La propuesta de este equipo de trabajo para colaborar con esas iniciativas se llama Capa8.

Planificación y Desarrollo

¿Qué es Capa8?

Es un proyecto desarrollado por estudiantes de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán, en el marco de la materia "Seguridad y Control en Sistemas Informáticos". El mismo comprende dos fases: el Análisis de los Conocimientos en Ciberseguridad mediante las respuestas obtenidas de un formulario en línea (Google Forms) y la Concientización en materia de Ciberseguridad a través del empleo de la herramienta propuesta por el equipo, esto es, un relato de tipo secuencial que hemos nombrado "El Incidente"; ambas fases fueron destinadas a la comunidad. Con la posibilidad de agregar una Tercera Fase de Evaluación, hecha de la misma forma que el Análisis realizado en la Primera Fase, con un cuestionario, que en este trabajo se destinó igualmente a la comunidad con el propósito de simular como se desarrollaría esta última fase, si el "Proyecto: Capa8" se aplicara a una organización.

Considerando que en la actualidad existe gran cantidad de información disponible circulando, lo cual hace que las personas, a la hora de querer aprender algo nuevo, se sientan sobrepasadas y pierdan la iniciativa y motivación para hacerlo; además, teniendo presente el

ritmo de vida acelerado del día a día y la necesidad de obtener resultados rápidamente, se plantea el siguiente interrogante:

¿Cómo podemos ayudar a las personas a adquirir conocimientos de forma dinámica?

La respuesta se presentó ante nosotros al recordar la forma en la que el profesor a cargo del dictado de esta materia ayudó a que los conceptos importantes queden en nuestra memoria: a través de propuestas lúdicas en dinámicas grupales.

De acuerdo con esto, decidimos crear una historia interactiva, en forma de relato secuencial, que incorpora situaciones relativas a la ciberseguridad y a las consecuencias que puede haber cuando no se le presta la debida atención dentro de una organización y también en nuestro día a día. Esta historia se titula “El Incidente”.

“El Incidente”

“El Incidente” es una historia de tipo no lineal, presentada mediante una herramienta multimedia, la cual fue desarrollada a través del software Twine, el cual tiene como propósito facilitar la creación de este tipo de narrativa, usualmente con fines de entretenimiento u ocio, y que nosotros decidimos aplicar con el objetivo de concientizar sobre la importancia de la Ciberseguridad. En este trabajo se presenta un prototipo de “El Incidente”.

La misma puede ser experimentada a través de un navegador web ya sea desde una computadora (preferiblemente, por cuestiones gráficas), como desde un Smartphone.

En esta experiencia, el usuario se verá inmerso en una historia donde se le presentarán situaciones relacionadas con el entorno de la Ciberseguridad, desde aspectos de la vida cotidiana hasta del entorno organizacional.

Captura de pantalla de un pasaje de la historia

El propósito fue situar a los participantes en escenarios simulados y analizar cómo se desempeñan en los mismos. Para ello, se puso a su disposición distintas opciones (diálogos, acciones, elementos, etc.) entre las que decidieron para poder avanzar en la trama.

Para adicionar a este objetivo de despertar conciencia, los personajes que encontrarán a lo largo de la historia, están nombrados en referencia a conceptos relacionados a este mundo al cual deseamos introducirlos, de manera que vayan adquiriendo terminologías específicas de forma indirecta.

Apuntamos a que esta combinación de elementos intrigue e induzca a cada usuario a indagar más sobre la Seguridad de la Información y lograr que se fomente una cultura donde la misma sea un pilar fundamental en cuanto a prácticas tanto organizacionales, como personales de cada uno de los que tengan la posibilidad de experimentarlo.

Al final de la historia, de acuerdo con que decisiones hayan escogido, los usuarios recibirán una insignia, como forma de evaluar el camino que decidieron seguir.

Link de descarga de "El Incidente": https://drive.google.com/drive/folders/10mJLbXS-eaHqLddIsfn2FQFphJhtVrr4?usp=drive_link

Relevamiento previo

Como ya se ha mencionado, en paralelo a la creación de la historia, hicimos una investigación sobre los conocimientos en materia de Ciberseguridad, dirigida a un grupo compuesto por aproximadamente 30 personas seleccionadas de manera aleatoria de entre las amistades y familiares de los integrantes del equipo de trabajo. Para este propósito se distribuyó el link de un formulario en línea (Google Forms) a través de aplicaciones de mensajería y de email.

El alcance de esta encuesta estuvo dirigido hacia una muestra representativa de individuos sin que exista un rango de edad y ocupación específicos. La intervención se limitó a analizar el conocimiento y las prácticas actuales de los encuestados, sin la intención de intervenir directamente en el desarrollo de sus habilidades.

Finalmente, la evaluación de los resultados se realizó a través de análisis estadísticos descriptivos. Los datos se presentaron en gráficos que ilustran las principales tendencias y áreas de riesgo detectadas.

Estos resultados, que revelaron una mezcla de curiosidad y confusión en algunos aspectos por parte de los entrevistados, evidenciaron la necesidad de una mayor educación en este ámbito. A su vez, sirvieron para fundamentar parte de la estructura argumental de "El Incidente", tales como inclusión, modificación o supresión de algunas situaciones o personajes, así como diálogos específicos.

Para ver el Informe completo correspondiente a esta serie de encuestas, consultar "Anexo A".

Por otra parte, para poder adaptar la herramienta correctamente, se debe hacer un Relevamiento previo (primera fase) más exhaustivo, que incluya, además de la evaluación de los conocimientos de los miembros, un entendimiento integral de la organización interesada en implementar el proyecto.

Evaluación

De acuerdo con el trabajo realizado estamos convencidos de que este modelo de proyecto (en principio de Dos fases y destinado a la comunidad), puede ser adaptado para su aplicación en un entorno más profesional y formativo, con un mayor grado de complejidad y que brinde una capacitación a la altura de otras herramientas destinadas al mismo fin, lo cual requiere incorporar una Tercera fase, que se enfoque en la Evaluación.

Para modelar esta nueva etapa los integrantes del equipo de trabajo, junto con los profesores, que pasaron a conformar el grupo de testeo "Alfa", probaron la herramienta con el fin de establecer un tiempo mínimo aproximado que se requeriría para finalizar la historia y en busca de fallos o inconsistencias que pudiera tener la misma. Esta prueba arrojó un tiempo aproximado de una hora.

Posteriormente, se estableció un segundo grupo denominado “Beta”, integrado por voluntarios del primer grupo encuestado al principio del presente proyecto (Primera Fase), que se comprometieron a finalizar la historia (las veces que ellos desearan) y brindar comentarios en una nueva encuesta. Además, esta segunda tanda de encuestas tuvo el propósito de poner a prueba los nuevos conocimientos que pudieran o no haber adquirido los participantes.

Finalmente se realizó un segundo informe de resultados correspondiente a esta encuesta. Consultar Anexo B, para ver el informe completo.

Resultados

Mediante el uso de Twine, un software destinado a la creación de historias no lineales, conseguimos plasmar casi en su totalidad las expectativas del grupo, logrando crear una herramienta didáctica diseñada para introducir conceptos clave de ciberseguridad de manera lúdica y atractiva, la cual no solo busca hacer el aprendizaje más ameno, sino también reforzar la retención de la información a través de la práctica y la interacción.

Fruto de la formación recibida en el cursado, junto con cursos e información complementaria, se consiguió crear una historia que tiene sentido y a la vez resulta informativa para que el público pueda experimentarla sin perder la inmersión en la trama que se presenta.

Conclusiones y Avances a Futuro

Conclusiones

Con los conocimientos adquiridos en la materia “Seguridad y Control en Sistemas Informáticos”, percibimos que la falta de educación continua en ciberseguridad, unida a la confianza excesiva en la seguridad de la información personal, puede llevar a:

- **Incremento de Ataques Cibernéticos**: Con el aumento de las amenazas digitales, una comprensión limitada de las mejores prácticas puede dejar a los usuarios vulnerables.
- **Pérdida de Datos Sensibles**: La gestión inadecuada de contraseñas y la falta de herramientas avanzadas pueden resultar en robos de información personal y financiera.
- **Desconfianza en el Entorno Digital**: La percepción de que la información no está segura puede llevar a un comportamiento defensivo que limite el uso de tecnologías útiles y necesarias en el entorno laboral.
- **Erosión de la Privacidad**: Sin la verificación de la identidad de los solicitantes de información, los encuestados corren el riesgo de compartir datos sensibles, lo que puede tener consecuencias negativas tanto a nivel personal como profesional.

Entonces nos propusimos crear un prototipo de una herramienta que intente dar solución a lo que consideramos como la cuestión de fondo de los problemas en Ciberseguridad, esto es la falta de conciencia en lo importante que es seguridad de la información en el día a día y en las organizaciones.

A través de la comparación de los resultados obtenidos en la Primera Fase con los de la Tercera Fase, concluimos que la aplicación de la herramienta concientizadora representa un avance positivo en el objetivo de posicionar a la Ciberseguridad como un tópico relevante en la vida de las personas.

Por otra parte, si bien, somos conscientes de lo complicado que puede ser tomar una muestra de la población y luego inferir los resultados sobre esta última, lo planteamos con esta estructura para que sea aplicable a una organización / PyME: Determinando el conocimiento inicial (Primera Fase), Desarrollando e Implementando una historia interactiva que cumpla con

los requerimientos específicos de la organización (Segunda Fase) y posteriormente Evaluando los resultados obtenidos (Tercera Fase).

Avances a Futuro

De cara al futuro del proyecto, se plantean los siguientes pasos:

- Incorporación de nuevos elementos multimedia para enriquecer la experiencia. Tales como: sonidos a los que reaccionar, videos que el usuario pueda analizar, salto hacia una plataforma de multidimensional (transformación en un videojuego).
- Exploración de medios alternativos a través de los cuales se pueda presentar la herramienta (aplicaciones móviles, para PC, plataforma web propia, etc.), a fin de que llegue al mayor número de usuarios posibles.
- Inclusión de distintos escenarios que se adapten a los requerimientos de la organización interesada, de modo que sea una herramienta más completa y flexible, adaptable a distintas industrias.
- Parametrización de elementos de la herramienta para la producción de métricas relacionadas a conocimientos y conciencia en Ciberseguridad, de tal manera que los resultados producidos sean fácilmente comprensibles.

Bibliografía

Cátedra "Seguridad y Control en Sistemas Informáticos" (2024). *Material Didáctico*. Obtenido de https://campus2.unt.edu.ar/course/view.php?id=167

CISCO. (4 de Octubre de 2024). *Introducción a Ciberseguridad.* Obtenido de https://www.netacad.com/es/courses/introduction-to-cybersecurity?courseLang=es-XL

INCIBE. (27 de Enero de 2016). *Protección de la Información*. Obtenido de https://www.incibe.es/empresas/que-te-interesa/proteccion-informacion

INCIBE. (27 de Enero de 2016). *Buenas Prácticas en el Área de Informática*. Obtenido de https://www.incibe.es/empresas/que-te-interesa/buenas-practicas-area-informatica

ISO/IEC (2022). *"Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos"*. Capital Federal, Argentina: Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (IRAM). Argentina.

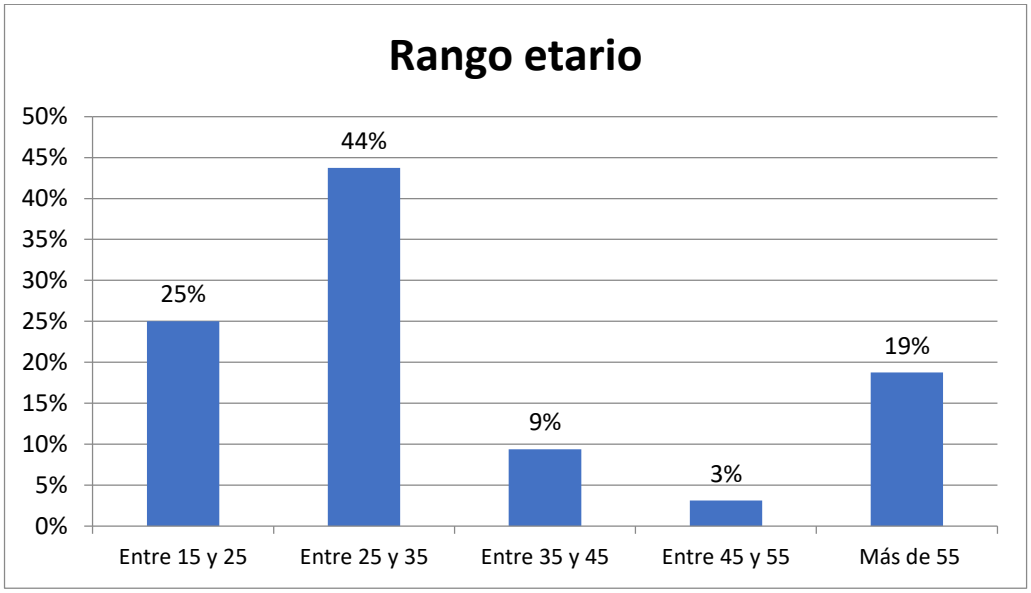
Pallero, M. (1 de Noviembre de 2024). *Ciberincidentes relevantes en Argentina*. Obtenido de https://time.graphics/es/line/630567

ANEXOS

ANEXO A: Informe sobre Resultados de la Encuesta de Primera Fase: Relevamiento Previo

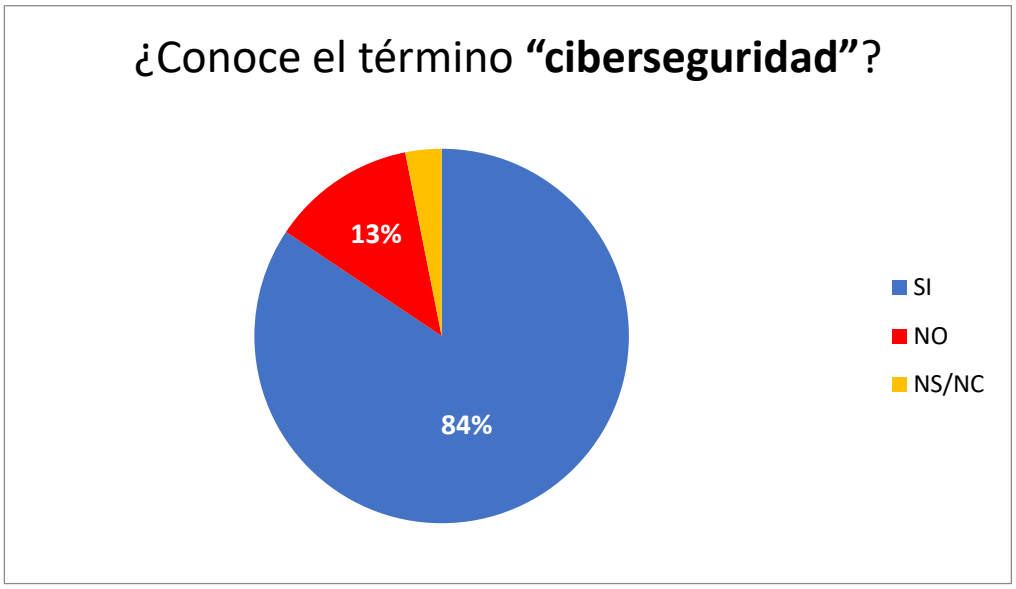
La encuesta realizada buscó explorar el conocimiento y la percepción sobre la **ciberseguridad** entre un grupo diverso de participantes. Los resultados presentaron un panorama interesante que refleja tanto el nivel de conciencia como las prácticas actuales en torno a la seguridad de la información.

En términos demográficos, la mayoría de los encuestados se encuentra en la franja de edad entre 25 y 35 años, un grupo que, al estar en la etapa laboral activa, podría estar más expuesto a riesgos digitales y, por ende, más consciente de la ciberseguridad. En contraste, una porción menor de los encuestados pertenece a edades más avanzadas (más de 55 años), lo que sugiere que la percepción sobre ciberseguridad puede variar significativamente según la generación. Este aspecto plantea preguntas sobre la educación y el acceso a la información sobre tecnologías de la información en diferentes cohortes de edad.



Fuente: Elaboración propia

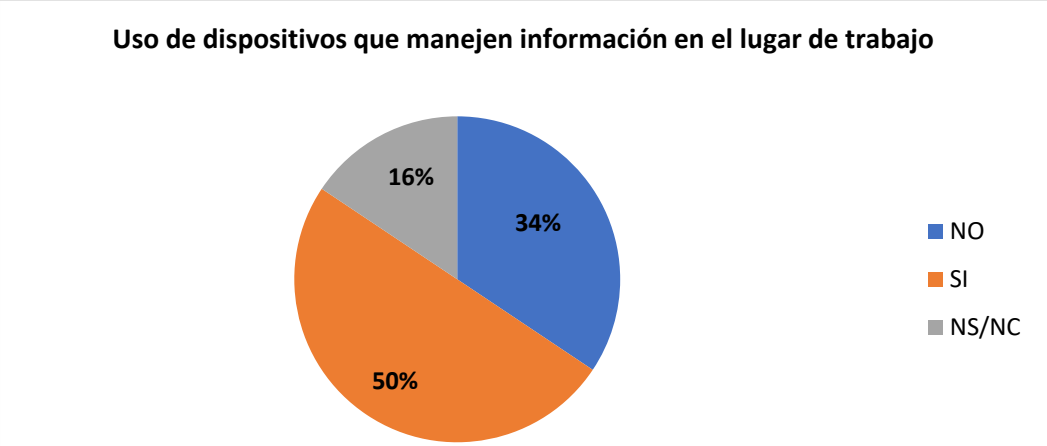
El conocimiento sobre el término “ciberseguridad” se destaca positivamente: 84% de los encuestados lo conocen, lo que representa una gran mayoría. Sin embargo, la presencia de un 13% de personas que no lo conocen puede señalar una brecha en la educación que, aunque pequeña, es significativa en un contexto donde la seguridad digital es cada vez más crucial. Esta percepción elevada de conocimiento no se traduce automáticamente en una confianza plena respecto a la seguridad personal, como lo evidencian un 78% encuestados que sienten que su información está en internet. Este dato reveló una inquietud sobre la exposición de datos personales, sugiriendo que, aunque hay conciencia sobre el tema, también hay un reconocimiento del riesgo que conlleva.



Fuente: Elaboración propia

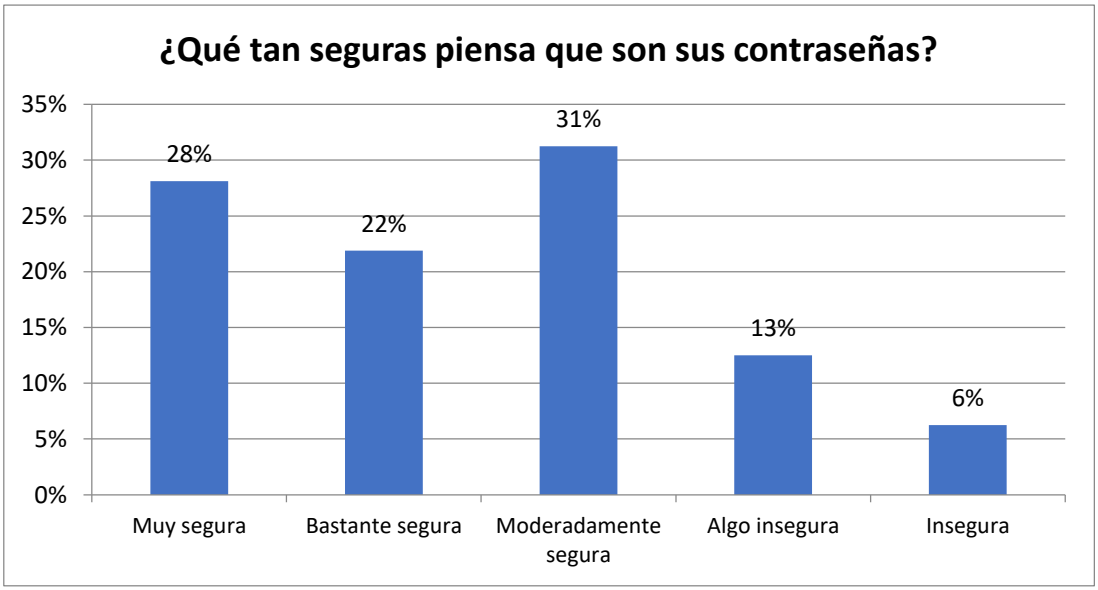
Al abordar la importancia de la información como recurso, un 75% de las personas consideraron que es "muy importante". Este consenso refuerza la idea de que la información es un activo valioso, aunque la presencia de un 9% de los encuestados que la ven como "moderadamente importante" planteó una reflexión sobre la diversidad de opiniones y el posible subestimar de la seguridad en contextos no críticos. En cuanto al uso de dispositivos que

manejan información en el trabajo, un 34% de los participantes declararon no usar tales dispositivos, lo que podría indicar que hay un sector que opera en un entorno menos digitalizado o que, por el contrario, no está consciente de la seguridad necesaria en dispositivos que puedan contener información sensible.



Fuente: Elaboración propia

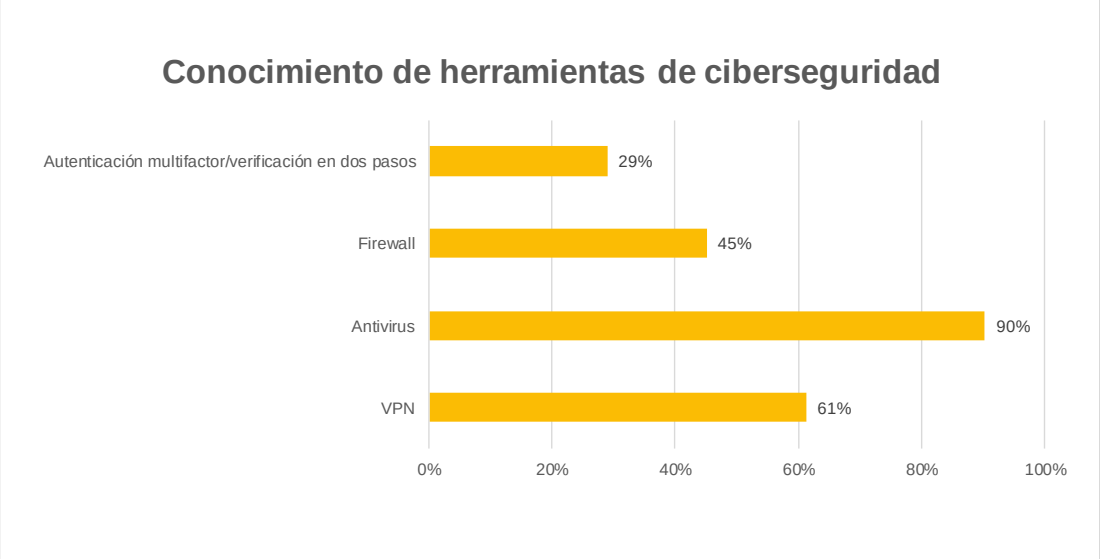
Las percepciones sobre la seguridad de las contraseñas revelaron un panorama mixto. Si bien un 28% de los encuestados consideraron que sus contraseñas son "muy seguras", un 50% (que incluyen a quienes tienen contraseñas moderadamente seguras o inseguras) mostró que hay una percepción de riesgo latente. Esto sugiere que, aunque se adopten buenas prácticas,



Fuente: Elaboración propia

puede haber una falta de educación en la creación de contraseñas robustas y en la necesidad de revisarlas periódicamente.

El conocimiento de herramientas de seguridad, como VPN y antivirus, es relativamente alto, con un número notable de encuestados familiarizados con estas tecnologías. Sin embargo, el número reducido de personas que conocen la autenticación multifactor indica que aún existe una necesidad de mayor educación sobre herramientas que proporcionan capas adicionales de protección.

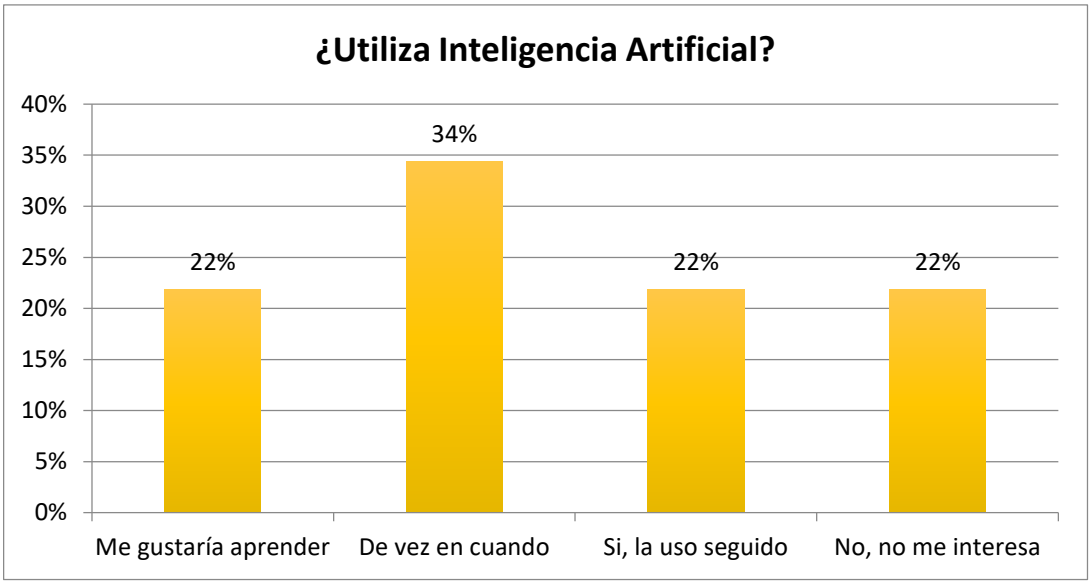


Fuente: Elaboración propia

La disposición a verificar la autenticidad de sitios web y correos electrónicos es notable, ya que 72% de las personas afirmaron realizar estas verificaciones. Este comportamiento proactivo reflejó una buena práctica en ciberseguridad. La alta tasa de escepticismo hacia mensajes no solicitados (94% de los encuestados que manifiestan sospecha) sugiere que existe una cultura de precaución, lo que es alentador en un contexto donde las estafas digitales son comunes.

La atención a actividades sospechosas en cuentas y dispositivos también es alta, con +1% de las personas que están alertas. Sin embargo, el hecho de que el 97% de los encuestados no proporcionen información personal sin verificar la identidad del solicitante mostró que hay una sólida consciencia sobre la protección de datos, lo que es crucial en la lucha contra el fraude y las estafas.

En términos de uso de inteligencia artificial, la distribución de respuestas es variada, lo que refleja un interés creciente pero también una falta de uniformidad en la adopción de esta tecnología. La variedad de respuestas indica que hay un potencial significativo para la educación en este campo.



Fuente: Elaboración propia

Finalmente, la baja incidencia de problemas relacionados con ciberseguridad (un 13% de las personas han tenido experiencias negativas) puede ser interpretada como un signo de la eficacia de las prácticas actuales entre los encuestados. Sin embargo, también podría ser un indicativo de que la percepción de seguridad es engañosa, y resalta la importancia de seguir educando sobre los riesgos potenciales.

Link para consultar preguntas realizadas en la Encuesta de la Primera Fase:

https://drive.google.com/drive/folders/1z6QWkN2IoOdz7KjchcWsFiyiCT-NIUU7?usp=drive_link

ANEXO B: Informe sobre Resultados de la Encuesta de Tercera Fase: Evaluación

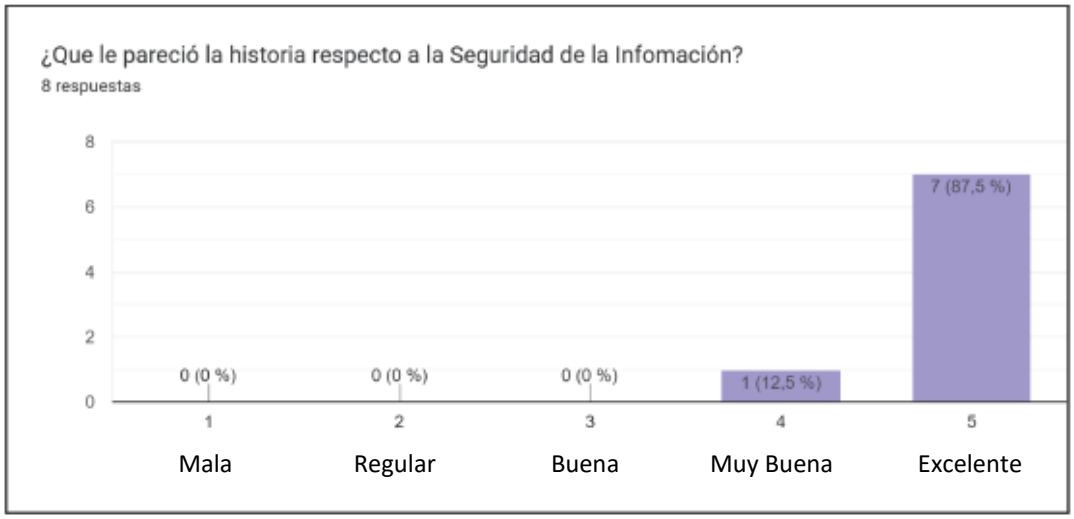
Este segundo ciclo de encuestas buscó determinar qué avances hubo entre los participantes en relación a la Conciencia sobre la importancia de la Ciberseguridad. Razón por la cual se optó por dirigirla al mismo grupo que participó en la primera encuesta.

En esta oportunidad se consiguieron respuestas de 8 personas, lo que representa un 26.66% de la cantidad que completó la primera instancia. Esto puede tener distintas causas, entre las que destacamos:

Mayor grado de compromiso: para esta segunda instancia se les pidió a los participantes que se aseguraran de realizar la encuesta habiendo completado (total o parcialmente) la Historia que se presentó como herramienta concientizadora. Al tener un requisito extra, esto pudo desalentar a las personas de participar de esta etapa.

Mayor extensión de la tarea: como se menciona precedentemente, antes de completar la encuesta de Evaluación, los encuestados tenían que experimentar la Historia. Se pudo apreciar que gran parte de los que pudieron experimentarla la percibieron como muy extensa, debido al tiempo que lleva completarla (entre 30 y 60 minutos), lo cual es comprensible puesto que se buscó abarcar un panorama general de la temática.

Falta de Incentivo: al no ser una actividad de carácter obligatorio para los participantes, ya que sólo se apelaba a su buena voluntad, y/o al no existir una recompensa por completarla, es entendible que los mismos no se sientan tan inclinados a realizarla.



Fuente: Elaboración propia

Fuente: Elaboración propia

Sin embargo, pese al reducido número de usuarios, la implementación de la herramienta de concientización ha demostrado ser efectiva en aumentar la conciencia y el conocimiento sobre la ciberseguridad y cambiar comportamientos hacia prácticas más seguras. Como puede observarse en los dos gráficos precedentes.

Puntualizando, esta instancia reveló que los participantes mostraron un mayor nivel de consideración en lo comprometida que podría estar su información antes de realizar una acción, así como una mejor comprensión de la importancia de la Confidencialidad e Integridad en la seguridad de la información, lo cual puede evidenciarse, por ejemplo, a través del mayor grado

de sospecha y precaución con respecto a mensajes y actividades sospechosas observadas en las respuestas de los participantes.

El análisis de la información obtenida por esta encuesta refleja que se cumplió con el objetivo del proyecto. Entre los aspectos más destacados y en los que se buscó una mejor concientización se encuentran:

Aumento de la Conciencia sobre la Ciberseguridad: Se ha incrementado la importancia de la Ciberseguridad entre los usuarios y su entorno.

Mejora en los Hábitos y prácticas de Seguridad: Los usuarios ahora reconocen la importancia de tener contraseñas seguras y robustas, además de no compartir sus credenciales o información confidencial. También prestan más atención a inicios de sesión inusuales, llamadas de números privados, entre otros.

Impacto en la comunidad y en el entorno organizacional: A través de esta herramienta, no solo benefician individuos a nivel personal, sino que también puede tener un impacto muy positivo en el entorno laboral, promoviendo una cultura de seguridad entre los empleados.

En conclusión, el Proyecto Capa8 ha demostrado que podría ser una inversión valiosa en la educación y preparación de los usuarios frente a las amenazas cibernéticas en un mundo tan globalizado.

Link para consultar preguntas realizadas en la Encuesta de la Tercera Fase:

https://drive.google.com/drive/folders/1z6QWkN2IoOdz7KjchcWsFiyiCT-NIUU7?usp=drive_link