UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN EN SEGURIDAD INFORMÁTICA

Tema:

Videojuego serious game de simulación de eventos de seguridad informática para fomentar una cultura de ciberseguridad en los estudiantes de primer semestre de la carrera de Software de la Universidad Técnica del Norte.

Trabajo de Grado previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR(A):

Ing. Wilson Raúl Yépez Ponce

DIRECTOR(A):

Msc. Carpio Agapito Pineda Manosalvas

Ibarra, 2023

CERTIFICACIÓN DIRECTOR

Ibarra, 20 de noviembre de 2023

Por medio de la presente, yo Carpio Pineda, certifico que el Ing. Wilson Raúl Yépez Ponce con CI Nro. 1004144554 desarrolló el trabajo de grado "**videojuego serious game de simulación de eventos de seguridad informática para fomentar una cultura de ciberseguridad en los estudiantes de primer semestre de la carrera de Software de la Universidad Técnica del Norte**", previo a la obtención del título de Magíster en Computación con Mención en Seguridad Informática, realizándolo en su totalidad con interés profesional y responsabilidad.

Es todo cuanto puedo certificar en honor a la verdad.

CARPIO AGAPITO PINEDA MANOSALVAS

Firmado digitalmente por CARPIO AGAPITO PINEDA MANOSALVAS
Fecha: 2023.11.29 11:49:57 -05'00'

Msc. Carpio Agapito Pineda Manosalvas

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004144554		
APELLIDOS Y NOMBRES:	WILSON RAÚL YÉPEZ PONCE		
DIRECCIÓN:	INES HERNANDEZ #5-31 Y AV. ATAHUALPA		
EMAIL:	pryw95@gmail.com		
TELÉFONO FIJO:	062951565	**TELÉFONO MÓVIL:**	0978833504

DATOS DE LA OBRA	
TÍTULO:	Videojuego serious game de simulación de eventos de seguridad informática para fomentar una cultura de ciberseguridad en los estudiantes de primer semestre de la carrera de Software de la Universidad Técnica del Norte
AUTOR (ES):	WILSON RAÚL YÉPEZ PONCE
FECHA: DD/MM/AAAA	28/11/2023
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☑ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con Mención en Seguridad Informática
ASESOR /DIRECTOR:	Msc. Carpio Agapito Pineda Manosalvas

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 28 días del mes de noviembre de 2023

EL AUTOR:

Firmante digital:WILSON RAUL YEPEZ PONCE
Razón:He leído y acepto estos términos y y condiciones.
Ubicación:Ibarra, Ecuador
Fecha:29/11/2023 11:56:08 -05:00

(Firma)……

Nombre: WILSON RAÚL YÉPZ PONCE

DEDICATORIA

Dedico este trabajo a mi familia, docentes, amigos, colaboradores externos y a todos quienes me han brindado de su apoyo incondicional.

Además, quiero hacer una mención especial a mi novia Lizeth Cueva por su apoyo.

AGRADECIMIENTOS

Mis más sinceros agradecimientos a todos quienes me han dado su apoyo para lograr culminar esta etapa de mi vida académica con éxito.

Wilson Raúl Yépez Ponce

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este proyecto de tesis muestra el proceso que se realizó para evaluar el nivel de impacto generado en la cultura de ciberseguridad en los estudiantes de primer semestre de la Carrera de Software de la Universidad Técnica del Norte, por medio del desarrollo de un videojuego serious game, manteniendo un diseño interactivo y atractivo, usando como base fundamental de enseñanza la integración de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, con el objetivo de analizar la posibilidad de educar sobre las amenazas cibernéticas. Para mantener la seguridad de la información de los jugadores, se hizo un análisis comparativo entre los métodos de encriptación como AES, RSA y MD5, evaluando su adecuación y efectividad para la estructura que tiene el videojuego. Mediante encuestas aplicadas antes y después de la exposición de los estudiantes al videojuego, se analizó su impacto del respecto a la comprensión y actitud de los estudiantes hacia la ciberseguridad. Los resultados revelan un incremento significativo del 41,9% en el conocimiento de los estudiantes sobre Confidencialidad, Integridad y Disponibilidad (CID) de la información, datos que obtienen de la Tabla 16, después de jugar al videojuego la concienciación aumentó en un 80,6% de los estudiantes sobre ciberseguridad, datos reflejados en la Tabla 13, confirmando la efectividad del videojuego como herramienta educativa innovadora. La tesis propone que este enfoque lúdico puede extenderse a otros campos educativos, sugiriendo un cambio paradigmático en la enseñanza de temas complejos mediante el uso de tecnologías interactivas.

ABSTRACT

This thesis project illustrates the process conducted to evaluate the impact level generated in cybersecurity culture among first-semester Software students at Universidad Técnica del Norte, through the development of a serious game with an interactive and engaging design. It is based fundamentally on integrating the Information Systems Risk Analysis and Management Methodology, aiming to explore the possibility of educating about cyber threats. To ensure the players' information security, a comparative analysis was made between encryption methods such as AES, RSA, and MD5, assessing their suitability and effectiveness for the game's structure. Surveys conducted before and after students' exposure to the game analyzed its impact on their understanding and attitude towards cybersecurity. The results reveal a significant 41.9% increase in students' knowledge about Confidentiality, Integrity, and Availability (CID) of information, as obtained from Table 16, after playing the game. Furthermore, awareness increased by 80.6% among students about cybersecurity, as reflected in Table 13, confirming the game's effectiveness as an innovative educational tool. The thesis proposes that this playful approach could be extended to other educational fields, suggesting a paradigm shift in teaching complex subjects through the use of interactive technologies.

CAPÍTULO I. INTRODUCCIÓN DE LA INVESTIGACIÓN

1.1. Antecedentes

En Ecuador, el tema de la educación en ciberseguridad a nivel secundario se encuentra en una etapa incipiente. Si bien se reconoce la importancia de promover la conciencia y el conocimiento en este campo entre los estudiantes, aún existen desafíos y limitaciones en la implementación de programas educativos específicos en ciberseguridad.

Actualmente, en el plan de las mallas curriculares del Ministerio de Educación del Ecuador, la ciberseguridad aún no figura como una asignatura dentro del nivel secundario de educación. Las materias que están relacionadas con las tecnologías de la información y comunicación (TIC) se enfocan en temas generales, sin tener en cuenta temas como: seguridad informática y la protección de datos.

A pesar de esta situación, se han realizado esfuerzos por parte de algunas instituciones y organizaciones para fomentar la educación en ciberseguridad en el ámbito secundario. Por ejemplo, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) ha desarrollado el programa "Conéctate Seguro", el cual busca promover el uso responsable y seguro de las TIC entre los estudiantes de todas las edades, incluyendo aspectos de seguridad informática (ARCOTEL, 2021).

Asimismo, se han llevado a cabo iniciativas y proyectos a nivel local y regional para brindar talleres y capacitaciones en ciberseguridad dirigidos a estudiantes de secundaria. Estos esfuerzos buscan crear conciencia sobre los riesgos y amenazas en línea, así como promover buenas prácticas de seguridad, como el uso de contraseñas seguras y la protección de la información personal (Ministerio de Telecomunicaciones y de la Sociedad de la información, 2023).

1.1.1. Planteamiento del Problema

1.1.2. Problema

Debido a la corriente de digitalización de la información, la seguridad informática se ha convertido en un aspecto fundamental en el desarrollo no solo para los técnicos en el área sino también para los usuarios regulares, al ser este un factor fundamental en la preservación de la seguridad, como expone el Centro Nacional de Criptografía de

España donde detalla que: “El estudio Uso de contraseñas desde la perspectiva del factor humano, realizado por investigadores de la Universidad de Wisconsin-Madison (EEUU) y la de Tecnología de Copenhague (Dinamarca), concluye que el ser humano, por naturaleza, es uno de los componentes más débiles de la seguridad informática.” (Centro de Criptografía Nacional, 2023), por ende, es de suma importancia que los estudiantes adquieran las habilidades y el conocimiento necesario desde las etapas iniciales de su formación académica; sin embargo, actualmente en el Ecuador existe una brecha en la educación y enfoque hacia la ciberseguridad, dado que en los planes de malla curricular de los bachilleratos unificados no cuentan con un área orientada a la seguridad informática, como se puede observar en el EGC Distribución por Año Bachillerato Técnico Informática o en el Currículo de los Niveles de Educación Obligatoria Tomo 1 y 2 (Ministerio de Educación, 2016; Ministerio de Educación, 2017; Ministerio de Educación del Ecuador, 2016), por lo que los estudiantes llegan a la Universidad con una comprensión limitada de los riesgos y medidas de protección necesarias.

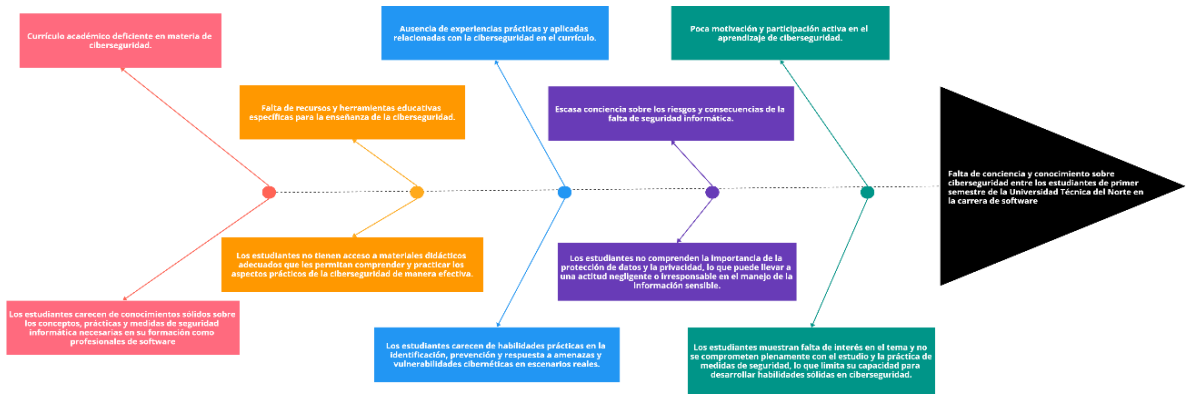


Figura 1 Planteamiento del Problema. Propia

1.1.3. Interrogantes de la Investigación

Para orientar la investigación hacia el cumplimiento del objetivo propuesto relacionado con la medición del impacto de un videojuego serious game respecto a su influencia en la cultura de ciberseguridad en estudiantes de primer nivel de la Universidad Técnica del Norte en la carrera de software, inicialmente se tendrá que hacer un análisis de los elementos más relevantes y críticos de seguridad informática dentro del marco de referencia de MAGERIT v3 y que además sean aplicables para los estudiantes, identificando aquellos eventos de seguridad en los cuales deberían tener noción sobre cómo actuar.

- ¿Cómo se pueden aplicar el catálogo de elementos críticos de seguridad, detallados en MAGERIT v3, para mejorar la cultura de ciberseguridad en los estudiantes de la Universidad Técnica del Norte?
- ¿Qué eventos de seguridad informática son más relevantes y representativos para mejorar la cultura de ciberseguridad de los estudiantes?
- ¿Qué desafíos técnicos y de diseño se deben abordar para garantizar una experiencia de juego envolvente y educativa en el videojuego?
- ¿Qué nivel de impacto genera en los usuarios el uso de un videojuego respecto a la cultura de ciberseguridad?

1.2. Objetivos de la Investigación

1.2.1. Objetivo General

Evaluar el impacto en la cultura de ciberseguridad generado por el videojuego serious game de simulación de eventos de seguridad informática en los estudiantes de primer nivel de la carrera de Software de la Universidad Técnica del Norte.

1.2.2. Objetivos Específicos

- Caracterizar los elementos críticos de seguridad que se puedan aplicar al público objetivo basándose en MAGERIT v3.
- Crear una base de datos de eventos de seguridad informática, basado en los elementos seleccionados.
- Desarrollar un videojuego de simulación de eventos de ciberseguridad en la herramienta Unity, usando un método de encriptación para cifrar los datos de los usuarios y la base de datos.
- Evaluar el videojuego serious game de eventos de seguridad informática, usando el método de análisis comparativo.

1.3. Alcance del Proyecto

La finalidad de la presente investigación es medir la influencia que se puede generar en los estudiantes de los primeros semestres en cuanto a ciberseguridad, por lo que se seleccionará como grupo de estudio a los estudiantes de primer semestre de la carrera de software de la Universidad Técnica del Norte. El recurso seleccionado como medio es un videojuego serious game desarrollado en el motor Unity y se espera

que esta investigación pueda ser usada de base para el desarrollo de una propuesta para el público en general.

El videojuego es un simulador de toma de decisiones, donde se presentarán diferentes eventos a los estudiantes, los cuales estarán basados en el catálogo de amenazas que ofrece Magerit V3, para que los usuarios elijan la opción respecto a la actuación en los diferentes eventos; dichas acciones tendrán repercusión en 5 ítems, que estarán basados en el CID (Integridad, Confidencialidad, Disponibilidad) de la Información, para aumentar la dificultad y lograr que el correcto análisis incremente como ítems de un capital monetario y la satisfacción de las personas, de manera que se asemeje a la vida real, donde a pesar de ser la mejor opción levantar una seguridad no se cuenta con el presupuesto o porque afecta a la usabilidad del producto. El juego terminará cuando alguno de los valores llegue a un nivel crítico, lo cual desencadena la derrota el jugador.

Para el desarrollo de la aplicación se utilizó Unity como entorno de desarrollo por sus excelentes prestaciones para el desarrollo de videojuegos (Andalucía, 2018); para la creación de los eventos de seguridad y sus valores en los ítems se usará el catálogo de elementos proporcionado por la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit v3), que cuenta con un muy fuerte respaldo por parte de la comunidad hispanohablante y es reconocida como una excelente metodología para hacer análisis de gestión de riesgos.

Para la arquitectura del videojuego se utilizó un Unity Asset Store, la tienda oficial de motor de desarrollo para obtener los diferentes recursos visuales, Visual Studio Code para la codificación de los Scripts de acción del Juego, y finalmente Unity como entorno de desarrollo, que generó la aplicación, para el almacenamiento de los eventos y los datos de los usuarios se empleó el servicio de Google Firebase, por la excelente integración que tiene ésta con el motor de desarrollo, además para proteger los datos almacenados en el servicios y se aplicaró un método de encriptación por medio de la librería Easy Crypto – Encryption, para la seguridad y el buen tiempo de respuesta.

1.4. Justificación del Proyecto

La propuesta nace frente a la posibilidad de analizar si un videojuego puede ser una solución efectiva para educar e involucrar a los estudiantes en el aprendizaje de prácticas de ciberseguridad. Ya que, al proporcionar una experiencia atractiva, los estudiantes pueden enfrentar escenarios realistas, tomar decisiones de seguridad

informática y enfrentar las consecuencias de sus acciones, lo que les permite aprender de forma efectiva y fortalecer sus conocimientos en ciberseguridad desde el principio de su carrera académica.

Es importante recalcar que esta investigación también contribuirá en el área educativa, dado que, a través del videojuego, se busca proporcionar una herramienta innovadora y efectiva para mejorar la formación de los estudiantes en ciberseguridad. Lo cual se alinea al objetivo de las ODS en la meta 4 de Educación de Calidad que menciona que “4.7 De aquí a 2030, asegurar que todos los alumnos adquieran los conocimientos teóricos y prácticos necesarios para promover el desarrollo sostenible, entre otras cosas mediante la educación para el desarrollo sostenible y los estilos de vida sostenibles, los derechos humanos, la igualdad de género, la promoción de una cultura de paz y no violencia, la ciudadanía mundial y la valoración de la diversidad cultural y la contribución de la cultura al desarrollo sostenible”(Organización de las Naciones Unidas (ONU), 2022)

Además, la investigación también tiene un impacto regional y local, ya que se enfoca en estudiantes de primer semestre de la Universidad Técnica del Norte, ubicada en la región norte del Ecuador. Al fortalecer la cultura de ciberseguridad en esta población estudiantil, se estará contribuyendo al desarrollo regional en términos de formación de profesionales más preparados y conscientes de los desafíos y riesgos en materia de seguridad informática.

CAPÍTULO II. MARCO REFERENCIAL

2.1. Marco Teórico

2.1.1. Introducción a la Ciberseguridad

La ciberseguridad es un campo crítico en la era digital actual, que se enfoca en prácticas, políticas y tecnologías diseñadas para proteger tanto los equipos, software y la información de posibles amenazas cibernéticas. Las organizaciones en la actualidad están obligadas a proteger la información de sus usuarios y de esta manera no perder reputación o incumplir las normativas (Michael E. Whitman & Herbert J. Mattord, 2018) Para comprender mejor esta disciplina, se ha elaborado un gráfico con los conceptos más relevantes de la ciberseguridad como se presentan en la Figura 2.

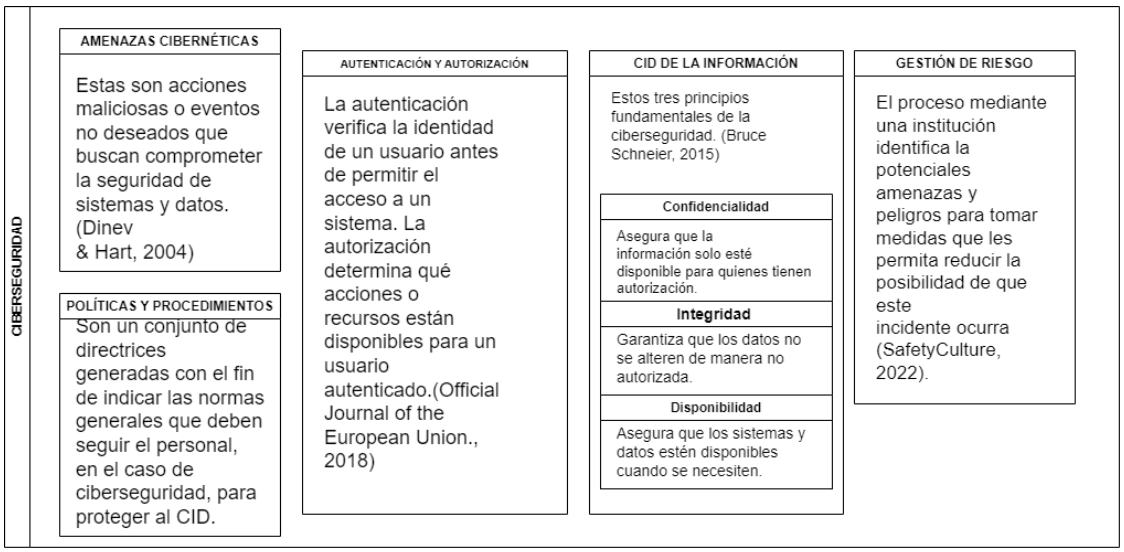


Figura 2 Temas relevantes de Ciberseguridad Fuente:(Dinev & Hart, 2004), (Bruce Schneier, 2015), (Official Journal of the European Union., 2018), (SafetyCulture, 2022).

2.1.2. Importancia de la ciberseguridad en la educación y la sociedad actual

Debido a la constante migración de los servicios al mundo digital, cada día se vuelve más imperativo que la población tenga conocimiento de ciberseguridad, tanto en el ámbito empresarial como en el personal. Algunas estimaciones sugieren que los costos provocados por los ciberdelincuentes a nivel mundial van a tener un incremento de un 15% anual en los próximos años, pasando de los tres billones registrados hasta 2015 a una proyección de 10,5 billones de pérdidas (Equipo Panda Security, 2022).

Según el informe el análisis realizado por Google en “Panorama actual de la ciberseguridad”, alrededor del 98% de las instituciones educativas creen erróneamente que no son un objetivo atractivo para un ciberataque, de estas solo el 35% había comentado que contaba con medidas preventivas para la protección de datos. (ITELCA, 2020)

2.1.3. Metodología de Análisis de Riesgos MAGERIT v3

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información también llamada Magerit es un componente elaborado por el el consejo superior de administración electrónica del gobierno de España, esta metodología de carácter público es principalmente utilizada por las entidades para lograr una gestión de seguridad basada en riesgos y con esto preservar la seguridad de la información, cabe recalcar que Magerit responde a la normativa ISO 31000.(Secretaría General de

Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital), 2012)

Magerit al estar pensada para hacer una herramienta que guíe a las entidades a la gestión de seguridad basada en riesgos, para lo cual está dividida en tres libros, método, catálogo de elementos, guía técnica los cuales se muestran en la Figura 3 un mapa conceptual, que sus contenidos se encuentran basados en los textos escritos por: (Secretaría General de Administración Digital, 2012a, 2012c, 2012b)

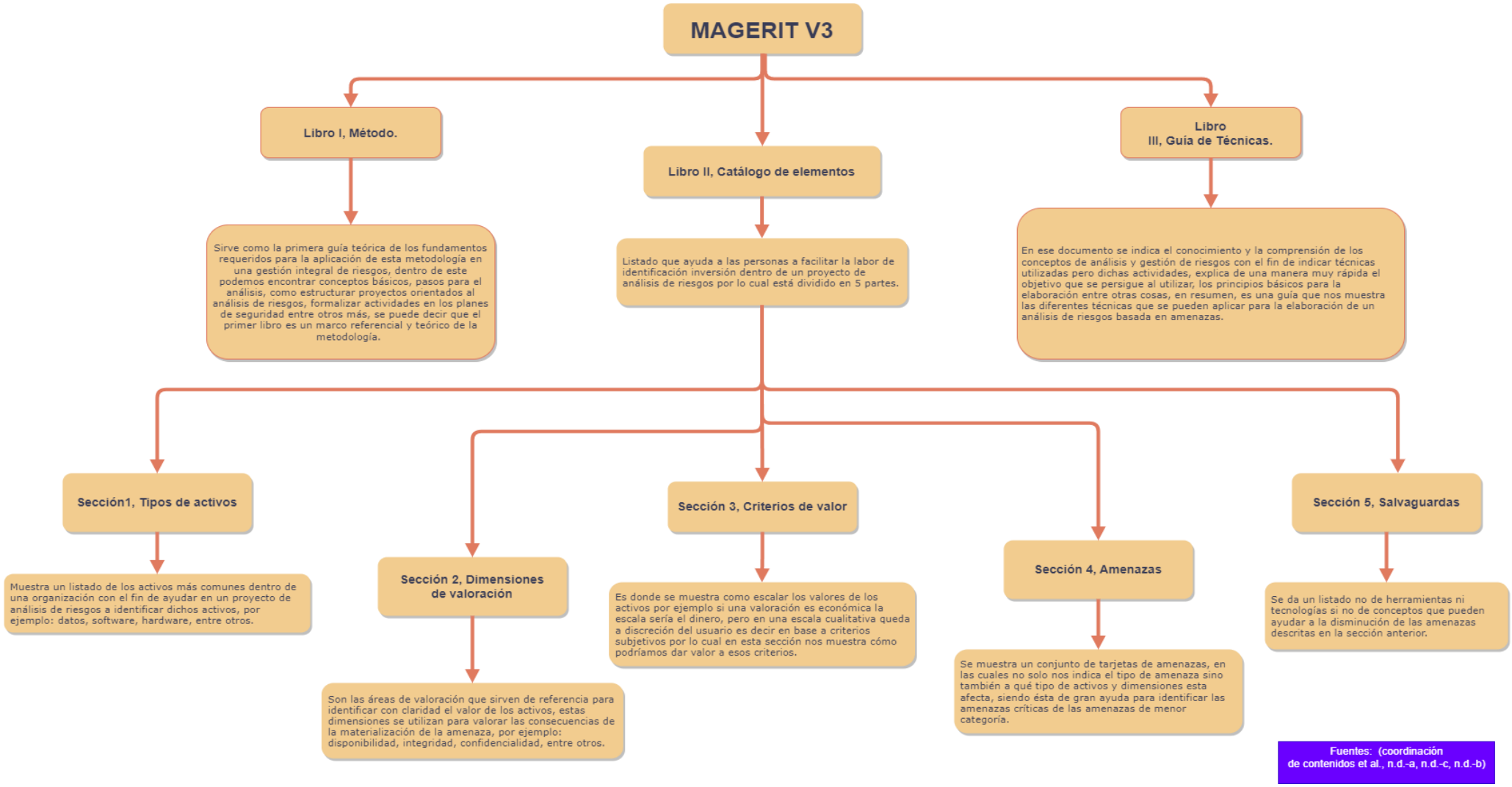


Figura 3 Estructura de los libros que componen Magerit V3 Fuente:(Secretaría General de Administración Digital, 2012a, 2012c, 2012b)

2.1.4. Modelos de Encriptación para la Seguridad de la Información

Antes de poder abordar la descripción y la explicación de los diversos modelos de encriptación, es importante comenzar con una compresión de qué implica el término “encriptación”. Este concepto se refiere a la práctica de la criptografía, que en un proceso que convierte un texto plano de longitud variable en una secuencia de caracteres de longitud fija que resulta legible a través de diversos métodos y algoritmos de encriptación, dependiendo de la clave utilizada. (Kinsta®, 2023)

2.1.5. Tipos de métodos de encriptación y sus aplicaciones.

2.1.5.1. MD5 (Hashing):

El modelo de encriptación Md5 (Message Digest Algorithm 5) es una función hash ampliamente conocida, pero sin embargo es importante destacar que “Md5” no es un modelo de encriptación en el sentido tradicional, sino más bien una función de resumen criptográfico o hash. Su función principal es tomar una entrada (por ejemplo, un mensaje o un archivo) y producir una cadena de caracteres hexadecimales de 32 caracteres que representa de manera única la entrada original.(Avast Security, 2022)

Estas cadenas hash son utilizadas para verificar la integridad de datos y garantizar que no hayan sido modificadas durante la transmisión o el almacenamiento.

2.1.5.2. AES (Estándar de Encriptación Avanzado):

El modelo de encriptación AES (Advanced Encryption Standard) es un estándar de cifrado ampliamente utilizado para proteger datos confidenciales. Fue adoptado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos en 2001 como el sucesor del estándar DES (Data Encryption Standard). AES es un algoritmo de cifrado simétrico, lo que significa que utiliza la misma clave para cifrar y descifrar datos.(Hard Zone, 2023)

Las características clave del algoritmo AES son las siguientes:

- **Tamaño de claves variables:** AES permite el uso de claves de 128 bits, 192 bits o 256 bits, lo que brinda diferentes niveles de seguridad. Cuando mayor sea el tamaño de la clave, mayor será la resistencia a un ataque de fuerza bruta.
- **Bloques datos:** AES opera en bloques de datos de 128 bits. Esto significa que divide los datos que se van a cifrar en bloques de 128 bits antes de aplicar el cifrado.
- **Estructura de rondas:** AES utiliza una estructura de rondas en la que los datos se someten a una serie de transformaciones repetidas, que incluyen sustituciones, permutaciones y mezclas. La cantidad de rondas depende del tamaño de la clave (10 rondas para 128 bits, 12 rondas para 192 bits y 14 rondas para 256 bits).
- **Seguridad Comprobada:** AES ha sido ampliamente utilizado y evaluado por expertos en seguridad. Hasta la fecha de redactado este documento no se ha encontrado vulnerabilidades significativas en AES y es considerado unos de los algoritmos de cifrado más seguros disponibles.

AES se utiliza en una amplia variedad de aplicaciones, desde la protección de comunidades en línea y la seguridad de datos en dispositivos móviles hasta la encriptación de archivos y el almacenamiento seguro de contraseñas. Su versatilidad y robustez lo convierten en una elección popular en el campo de la seguridad de la información.(National Institute of Standards and Technology (NIST), 2001)

2.1.5.3. RSA (Algoritmo Asimétrico)

RSA es uno de los cifrados de clave publica y muy utilizado para el trasporte seguro de datos. Su origen se conoce desde el año 1997 por Ron Rivest, Adi Shamir y Leonard Adleman, y de ahí proviene su nombre (Rivest-Shamir-Adleman).(Shanika Wickramasinghe, 2023)

Metodología de uso del algoritmo RSA:

1. **Claves**: En RSA, cada individuo tiene un par de claves: una pública, que puede ser distribuida, y una privada, que se debe mantener en secreto.
2. **Generación de claves:**
   - Se eligen dos números primos grandes, $p\ y\ q$.
   - Se calcula $n = p\ x\ q\ y\ \emptyset(n) = (p-1)(q-1)$.
   - Se elige el numero e tal que $1 < e < \emptyset(n)\ y\ \gcd(e, \emptyset)(n)) = 1$ este e será la clave pública.
   - Se calcula d de manera que $d\ x\ e \equiv 1\ mod\ \emptyset(n)$ donde d será la clave privada.

1. Cifrado: Una remitente que quiera enviar un mensaje cifrado a una persona utilizará una clave pública de esa manera para poder cifrar el mensaje.

Matemáticamente, el mensaje original M se recuperará como $M \equiv C^d\ mod\ n$

2. Seguridad: La seguridad de RSA se basa en la dificultad de factorizar el producto de 2 números primos grandes. Mientras el tamaño de la clave aumenta, la seguridad también aumenta, con un costo de una menor eficiencia.

Al llegar al resultado final sería una comunicación cifrada de par, en donde se use las 2 claves (pública y privada), para decodificar el mensaje haciendo que este método sea muy usando en la mensajería instantánea actualmente.(Rivest et al., 1978)

2.2. Diseño de juegos educativos.

2.2.1. Experiencia de Juego Serious Game

Los Serious game también llamados juegos serios, tienen como finalidad cumplir un objetivo específico, propuesto por la desarrolladora o desarrollador, por lo cual se los usa comúnmente en el desarrollo de videojuegos educativos, generando una doble experiencia positiva, con una experiencia divertida y educativa. (Gestionet, 2019)

Para esto los serious games dentro del uso en las actividades educativas se tiene dos tipos de metodologías, que pese a ser usadas en conjunto no son lo mismo:

2.2.1.1. Aprendizaje Basado en Juegos (ABJ):

El Aprendizaje Basado en Juegos es una metodología clave en el campo de la pedagogía que incorpora juegos directamente en el proceso educativo para mejorar el logro de objetivos específicos de aprendizaje. Esta estrategia se destaca por combinar elementos pedagógicos con lúdicos, creando un entorno educativo tanto atractivo como positivo (Gee, 2003).

Una de las principales ventajas de adoptar esta metodología es que fomenta activamente la participación estudiantil. Los juegos facilitan la comprensión y asimilación de contenidos de manera efectiva y también permiten una adaptación ágil a diversos niveles y ritmos de aprendizaje individuales, como apuntan (Anderson & Dill, 2000). Esta flexibilidad y capacidad de involucrar a los estudiantes de manera significativa hace del Aprendizaje Basado en Juegos una herramienta valiosa en la educación moderna.

2.2.1.2. Gamificación:

La gamificación, a diferencia del aprendizaje basado en juegos, no se enfoca en fusionar el juego con contenidos lúdicos. En lugar de ello, su objetivo es utilizar los aspectos atractivos de los juegos para captar la atención de los estudiantes, incentivando su compromiso y motivándolos a aprender sobre un tema específico. Esta metodología fomenta habilidades como la toma de decisiones y el trabajo en equipo. Sin embargo, es importante señalar que estas características distintivas, aunque benefician la experiencia del jugador, también pueden limitar la efectividad del juego. Si el juego es demasiado superficial o su dinámica no se alinea adecuadamente con los objetivos educativos, puede no lograr el impacto deseado.(Deterding et al., 2011)

2.2.2. Fundamentos de Juegos de Experiencia Inmersiva

Este tipo de video juegos están diseñado para sumergir al jugador en el entorno y experiencia del juego. Para lograr una inmersión real se puede usar varios elementos que trabajen en conjunto y lograr esa sensación que mantiene al jugador concentrado y participando activamente en el mundo del juego.(Rondón Quiñonez, 2020) Dentro de los aspectos claves para la creación de juegos inmersivos se encontró:

2.2.2.1. Entorno Detallado y Creíble:

En este estilo de juego se presenta un mundo virtual bien construido y detallado, que puede ser realista o fantasioso, pero siempre es coherente. Prestando una atención especial al detalle como: gráficos, la arquitectura del entorno, físicas del juego, en esta

área se puede indicar como ejemplo el juego Cyberpunk 2077 (Figura 4 y 5), donde el juego tiene un entorno con una cantidad muy elevada de nivel de detalle(Albert T. Franch, 2020).

Figura 4 Cyberpunk 2077, Desarrollador CD PROJEKT RED

Figura 5 Cyberpunk 2077, captura en juego, Desarrollador CD PROJEKT RED

2.2.2.2. Narrativa Atractiva:

Otra manera que cautivar al jugador es por medio de la historia de una trama convincente y bien desarrollada, con personajes ricos y una progresión narrativa significativa, impulsa el interés del jugador y la conexión emocional con el juego, en este aspecto Hollow Kigth que aparece en la figura 6 y figura 7, que es un juego de plataforma

sencilla, tiene una historia con trasfondo tan profundo que atrapa a sus jugadores (Albert T. Franch, 2020).

Figura 6 Hollow Knigth, Desarrollador: Team Cherry

Figura 7 Hollow Knigth, captura en juego, Desarrollador: Team Cherry

2.2.2.3. Interactividad Profunda:

Algunos juegos ofrecen un alto nivel de interactividad, permitiendo a los jugadores influir en el mundo del juego y en la historia a través de sus elecciones y acciones, un exponente de este aspecto es la serie de juegos de Life is Strange (Ver Figura 8 y Figura 9), donde el jugador toma las decisiones de una chica adolescente y cada decisión lleva a un resultado diferente (Albert T. Franch, 2020).

Figura 8 Life is Strange, Desarrollador DONTNOD Entertainment

Figura 9 Life is Strange, Decisión si dispara o no, Desarrollador DONTNOD Entertainment

2.2.2.4. Innovación en la Jugabilidad:

Los juegos inmersivos suelen incorporar mecánicas de juego innovadoras o únicas que se integran estrechamente con la narrativa y el entorno del juego, lo que permite una experiencia de juego más rica y variada, como por ejemplo el juego One Hand Clapping (figura 10 y figura 11), donde el personaje avanza dependiendo de que mantengas la nota musical con tu voz.

Figura 10 One Hand Clapping, Desarrollador Bad Dream Games

Figura 11 One Hand Clapping, Captura del Juego, Desarrollador Bad Dream Games

2.2.2.5. Elementos Audiovisuales Envolvedores:

En juego que no tengan tanto trasfondo o una historia atractiva, se puede hacer uso de los elementos gráficos como: la animación y el diseño de sonido, incluyendo música y efectos de sonido, ayuda a crear una atmósfera que absorbe como por ejemplo el juego Ori (Figura 12), un juego de plataforma que, si bien no es muy trabajada la historia, ha ganado premios por su banda musical.

Figura 12 Ori and the Blind Forest, Desarrollador Moon Studios GmbH

2.2.2.6. Interfaz de Usuario Integrada:

Una interfaz de usuario bien diseñada, que se integra de manera fluida con el entorno del juego, asegura que los jugadores permanezcan enfocados en la experiencia sin distracciones innecesarias, en este aspecto un claro ejemplo es Minecraft (Figura 13 y 14) un juego con una interfaz muy acorde con su juego.

Figura 13 Minecraft, Desarrollador Mojang

Figura 14 Minecraft, UI principal del juego, Desarrollador Mojang

2.2.2.7. Realidad Virtual y Aumentada:

Muchos juegos inmersivos aprovechan las tecnologías de realidad virtual (VR) y realidad aumentada (AR) para mejorar la sensación de presencia en el mundo del juego, un gran exponente en este campo es el juego mundialmente famoso Pokemon Go (Figura 15).

Figura 15 Pokemon Go, Desarrollador Niantic

2.2.2.8. Emoción y Empatía:

Los juegos inmersivos a menudo buscan generar una fuerte respuesta emocional, fomentando la empatía y la conexión con los personajes y la historia, un juego que se aprovecha de este aspecto es el juego de móvil My Talking Tom (Figura 16) en el cual generan que tengas un apego emocional por el personaje.

Figura 16 My talking tom, Desarrollador Outfit7

2.2.2.9. Beneficios de la inmersión en el contexto educativo de ciberseguridad

La inmersión de los videojuegos en el ambiente educativo grandes beneficios, dado que puede dar un enfoque revolucionario para la capacitación del aprendizaje. Al sumergir a los estudiantes en escenarios simulados de seguridad informática, lo que

facilita una comprensión más profunda y práctica de las amenazas cibernéticas(Pearson, 2023).

Una de las ventajas de esta metodología es una mejora en la retención de conocimientos teóricos, también desarrolla habilidades críticas de resolución de problemas y toma de decisiones en tiempo real.

2.3. Marco legal

La realización de investigaciones en el campo de la ciberseguridad y educación en ciberseguridad está respaldada por un marco legal y normativo que busca proteger la información, promover buenas prácticas y establecer lineamientos en el ámbito de la seguridad informática. A continuación, se mencionarán algunos instrumentos legales relevantes que enmarcan el tema en estudio y orientan su desarrollo:

Ley de Protección de Datos Personales: Esta ley establece los principios, derechos y obligaciones relacionados con la protección de datos personales en Ecuador. Su objetivo es garantizar la privacidad y seguridad de la información personal, estableciendo medidas de seguridad que deben ser aplicadas en el tratamiento de datos. (Asamblea Nacional, 2021)

Políticas educativas: A nivel nacional, Ecuador cuenta con políticas educativas que buscan promover la educación en tecnologías de la información y la seguridad informática. Estas políticas establecen la importancia de formar a estudiantes en competencias relacionadas con la ciberseguridad y la protección de datos, con el fin de garantizar un uso responsable y seguro de las tecnologías.(Ministerio de Telecomunicaciones, 2021)

CAPÍTULO III. MARCO METODOLÓGICO

3.1. Descripción del grupo de estudio

La investigación se realizó en la Universidad Técnica del Norte, en la carrera de Software y posee un valor práctico sustancial, especialmente considerando la creciente importancia de la ciberseguridad en el mundo digital actual. Al centrarse en estudiantes de primer semestre, cuyos conocimientos iniciales en este campo son limitados, el estudio puede ser un catalizador en la formación de una base sólida en seguridad informática desde el inicio de su carrera académica.

A través de la propuesta de desarrollo de un videojuego educativo, no solo se busca determinar si un videojuego puede incrementar comprensión en los estudiantes

sobre el tema de ciberseguridad; sino también, si a través de este medio es posible lograr un aprendizaje interactivo y atractivo. Esto es particularmente importante en un entorno académico donde los métodos tradicionales de enseñanza podrían no ser suficientes para captar el interés y la participación de los estudiantes en temas técnicos complejos.

Además, al tener un enfoque práctico para enseñar principios de ciberseguridad y si el videojuego cumple con su objetivo se logrará mejorar las habilidades de pensamiento crítico de los estudiantes, preparándolos mejor para los desafíos del mundo real. Esto no solo beneficia a los estudiantes en su formación académica y profesional, sino que también contribuye a formar futuros profesionales más capacitados y conscientes en el ámbito de la ciberseguridad, una necesidad cada vez más crítica en la sociedad actual.

3.2. Enfoque y tipo de investigación

El enfoque cuantitativo ha sido seleccionado en esta investigación con el propósito de alcanzar objetivos claramente cuantificables y para permitir una evaluación precisa del impacto que puede generar un videojuego de simulación en la cultura de ciberseguridad de los estudiantes de primer semestre. Este enfoque es particularmente pertinente y se aplica a toda la cohorte que es de 30 estudiantes, eliminando la necesidad de extrapolar resultados y proporcionando un panorama completo y específico de la influencia del videojuego en su comprensión en temas de seguridad informática.

Al emplear métodos cuantitativos, se asegura una validación rigurosa y alta confiabilidad de los datos obtenidos, gracias al uso de herramientas estandarizadas y procedimientos de análisis estadístico. Este método reduce la posibilidad de sesgos personales y promueve una interpretación objetiva de los resultados, proporcionando una base sólida para obtener conclusiones fiables y acciones fundamentadas. En consecuencia, los hallazgos de este estudio podrán ser utilizados para informar y mejorar las estrategias educativas en ciberseguridad dentro del ámbito académico de la institución.

3.3. Procedimiento de investigación

Para el correcto desarrollo de la investigación se propone lo expuesto en la Tabla 1 que sirve le guía para la investigación.

Tabla 1 Procedimiento de Investigación

	Técnicas de recopilación de datos	**Instrumentos**	**Operacionalización de variables**	**Diseño muestral o grupo de estudio seleccionado**	**Técnicas de análisis de la información**
OBJ. 1	Revisión documental y análisis de la metodología MAGERIT v3.	No aplica	No aplica	No aplica	Análisis de contenido temático y comparativo.
OBJ. 2	Revisión de fuentes bibliográficas y documentos especializados.	No aplica	No aplica	No aplica	Análisis de contenido y síntesis de información relevante.
OBJ. 3	Desarrollo de software utilizando la herramienta Unity.	Software Unity, Librerías de encriptación.	No aplica	No aplica	Evaluación de la funcionalidad y seguridad del videojuego desarrollado.
OBJ. 4	Aplicación de encuestas pre y post-intervención, observación directa	Cuestionarios estructurados, hojas de observación.	Variables relacionadas con el conocimiento de ciberseguridad, actitudes hacia la ciberseguridad	Estudiantes de primer nivel de la carrera de Software de la Universidad Técnica del Norte.	Análisis estadístico descriptivo e inferencial, análisis comparativo de los resultados pre y post-intervención.

Para analizar el impacto que el videojuego logró generar en los estudiantes de primer semestre de la carrea de software, se decidió elaborar una investigación diagnóstica, que se amplía en el acápite 3.3.1.

3.3.1. Herramientas y técnicas de recolección de datos

Para optimizar y agilizar la recolección de datos, se implementaron dos encuestas. La primera (encuesta pre - exposición al videojuego), que tuvo como objetivo determinar el nivel de conocimiento previo en ciberseguridad que poseen los estudiantes. La segunda se administró tras la interacción de los estudiantes con el videojuego (encuesta post - exposición al videojuego), con el fin de evaluar cómo perciben la influencia de éste en su comprensión y manejo de la ciberseguridad. Este enfoque bifásico permite un análisis comparativo antes y después de la experiencia de juego, proporcionando así una visión clara del impacto educativo del videojuego en la conciencia de ciberseguridad de los estudiantes.

CAPÍTULO IV. DISCUSIÓN DE RESULTADOS.

4.1. Presentación de Resultados del videojuego Educativo

4.1.1. Presentación de los Resultados Pre - Exposición al videojuego

Con el objeto de tener un punto de referencia de cuál puede ser el impacto que genera el videojuego creado, se realizó una evaluación antes de exponer a los estudiantes del videojuego y de esta formase dispone de una perspectiva del estado inicial de los estudiantes.

4.1.1.1. Pregunta 1. ¿Estás familiarizado/a con los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?

Análisis Interpretativo: Como se observa en la Tabla 2, la encuesta revela un punto de partida equilibrado en cuanto al conocimiento del CID. Aunque hay estudiantes con menor conocimiento sobre los conceptos de Confidencialidad, Integridad y Disponibilidad.

Tabla 2 Tabla de Frecuencias, Pregunta 1 Pre - Exposición

¿Estás familiarizado/a con los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	16	51,6	51,6	51,6
	No	15	48,4	48,4	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este equilibrio crea una oportunidad para que el videojuego funcione como una herramienta de nivelación, proporcionando un espacio de aprendizaje que pueda reforzar y ampliar el conocimiento de todos los estudiantes, demostrando así la efectividad del videojuego como método de enseñanza en la tesis.

Este resultado inicial destaca la relevancia de introducir herramientas educativas como videojuegos que puedan ayudar a aumentar la comprensión de los conceptos de CID entre aquellos que no están familiarizados con ellos, mientras que también refuerza y amplía el conocimiento de aquellos que ya tienen alguna comprensión de la ciberseguridad.

4.1.1.2. Pregunta 2. ¿Consideras importante la ciberseguridad en tu vida diaria?

Análisis Interpretativo: Analizando los datos obtenidos en la Tabla 3; los estudiantes reconocen la importancia de la ciberseguridad en su vida diaria, lo que indica una valoración alta de la ciberseguridad y su relevancia.

Tabla 3 Tabla de Frecuencias, Pregunta 2 Pre - Exposición

¿Consideras importante la ciberseguridad en tu vida diaria?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	30	96,8	96,8	96,8
	No	1	3,2	3,2	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este reconocimiento de la importancia de la ciberseguridad valida la necesidad y la relevancia del videojuego educativo desarrollado en la tesis, lo que permite interpretar que será bien recibido por los estudiantes.

Este resultado subraya la relevancia de incorporar educación en ciberseguridad, el interés casi unánime en la ciberseguridad proporciona una gran brecha para la adopción de estrategias de aprendizaje que puedan mejorar su conocimiento y habilidades en esta área crítica, como podría ser a través de la interacción con un videojuego educativo que aborde situaciones de ciberseguridad del mundo real.

4.1.1.3. Pregunta 3. ¿Crees que los videojuegos pueden ser una herramienta efectiva para aprender sobre ciberseguridad?

Análisis Interpretativo: Como se observa en al Tabla 4; La mayoría de los estudiantes cree que los videojuegos pueden ser una herramienta educativa efectiva, lo que indica una disposición a aceptar metodologías de aprendizaje innovadoras.

Tabla 4 Tabla de Frecuencias, Pregunta 3 Pre - Exposición

¿Crees que los videojuegos pueden ser una herramienta efectiva para aprender sobre ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	29	93,5	93,5	93,5
	No	2	6,5	6,5	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Esta actitud positiva hacia los videojuegos como herramientas educativas sugiere que el videojuego desarrollado en la tesis tendrá una buena acogida y será una contribución significativa al campo educativo de la ciberseguridad.

La percepción favorable hacia el uso de videojuegos como herramienta educativa sugiere que los estudiantes están abiertos a métodos de aprendizaje interactivos y que podrían estar más motivados y comprometidos con un programa de estudios que incluya elementos de gamificación. Dado que los videojuegos pueden simular escenarios de ciberseguridad y ofrecer práctica en tiempo real de técnicas de protección y respuesta ante incidentes, esta predisposición también destaca el potencial para mejorar el aprendizaje y la retención de conocimientos en ciberseguridad a través de experiencias inmersivas y prácticas.

4.1.1.4. Pregunta 4. ¿Tienes conocimientos sobre cómo protegerte contra ataques al CID de la Información?

En base al análisis de los datos proyectados en la Tabla 5 la encuesta muestra una división equilibrada entre los participantes en cuanto a su conocimiento sobre cómo protegerse contra ataques al CID de la información. Un poco más de la mitad de los encuestados afirmaron tener conocimiento sobre las medidas de protección, lo que indica una conciencia inicial sobre las estrategias de seguridad.

Tabla 5 Tabla de Frecuencias, Pregunta 4 Pre - Exposición

¿Tienes conocimientos sobre cómo protegerte contra ataques al CID de la Información?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	16	51,6	51,6	51,6
	No	15	48,4	48,4	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este resultado implica que hay una oportunidad considerable para educar y reforzar conceptos clave de protección dentro de los principios de CID entre la población estudiantil. El hecho de que una proporción significativa

de estudiantes no esté segura de cómo protegerse destaca la necesidad de intervenciones educativas, como el de este proyecto, que puedan abordar nuevos conocimientos o reforzar los mismos y proporcionar a los estudiantes las habilidades prácticas necesarias para navegar en un entorno digital cada vez más amenazado.

4.1.1.5. Pregunta 5. ¿Conoces Tips de Seguridad para mantener el CID de la información?

Los resultados de la encuesta pre-exposición indican que una leve mayoría de los estudiantes está familiarizada con los tips de seguridad para mantener la Confidencialidad, Integridad y Disponibilidad (CID) de la información, como se observa en la Tabla 5.

Tabla 6 Tabla de Frecuencias, Pregunta 5 Pre - Exposición

¿Conoces Tips de Seguridad para mantener el CID de la información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	17	54,8	54,8	54,8
	No	14	45,2	45,2	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este equilibrio sugiere que, aunque hay una conciencia razonable de las prácticas de seguridad, todavía existe un margen significativo para la mejora y la educación en esta área crítica. El dato refleja una oportunidad para desarrollar y reforzar el entendimiento y la aplicación de medidas de seguridad entre los estudiantes. La implementación de herramientas educativas interactivas, como videojuegos centrados en ciberseguridad, podría ser un medio efectivo para aumentar el conocimiento y las habilidades de los estudiantes, promoviendo una cultura de seguridad informática más sólida.

4.1.1.6. Pregunta 6. ¿Estás al tanto del Catálogo de Elementos de Magerit V3 y su relevancia para la ciberseguridad?

Análisis Interpretativo: Al Analizar la Tabla 7, se puede concluir que una minoría de los estudiantes está al tanto de Magerit y su aplicación en la ciberseguridad, lo que señala una brecha en el conocimiento especializado.

Tabla 7 Tabla de Frecuencias, Pregunta 6 Pre - Exposición

¿Estás al tanto del Catálogo de Elementos de Magerit V3 y su relevancia para la ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	11	35,5	35,5	35,5
	No	20	64,5	64,5	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: La falta de familiaridad con Magerit destaca la contribución potencial del videojuego de la tesis al ofrecer un medio para familiarizar a los estudiantes con este marco y su relevancia en la práctica de la ciberseguridad.

Este hallazgo subraya un área de oportunidad educativa significativa. La familiaridad con Magerit es crucial para los futuros profesionales de la ciberseguridad, ya que proporciona una estructura sistemática para identificar y abordar vulnerabilidades. El videojuego podría desempeñar un papel vital en la introducción y explicación de estos conceptos, convirtiéndose en una herramienta práctica para mejorar la comprensión y la aplicación de las prácticas de gestión de riesgos en ciberseguridad entre los estudiantes.

4.1.1.7. Pregunta 7. ¿Te sientes motivado/a para aprender más sobre ciberseguridad?

Análisis Interpretativo: Casi todos los estudiantes muestran una motivación para aprender más sobre ciberseguridad, lo que refleja una actitud proactiva hacia la adquisición de conocimientos en este campo como se puede observar en la Tabla 8.

Tabla 8 Tabla de Frecuencias, Pregunta 7 Pre - Exposición

¿Te sientes motivado/a para aprender más sobre ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	28	90,3	90,3	90,3
	No	3	9,7	9,7	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: La alta motivación de los estudiantes para aprender sobre ciberseguridad sugiere que el videojuego diseñado en la tesis será un complemento para su educación, mejorando potencialmente la calidad y el impacto del estudio.

La motivación elevada es un indicador prometedor de que compromete a los estudiantes con el contenido del videojuego y es probable que se involucren activamente en el proceso de aprendizaje. Además, esta disposición intrínseca para expandir su conocimiento puede conducir a una mejor retención de la información y la aplicación práctica de lo aprendido, lo que es fundamental en un campo tan dinámico y crítico como la ciberseguridad.

4.1.2. Presentación de los Resultados Post- Exposición al videojuego

Tras la interacción de los estudiantes con el videojuego, se administró de Post - exposición elaborada con el propósito de evaluar el impacto del juego en su comprensión sobre ciberseguridad. Esta encuesta post - exposición fue fundamental para el análisis de datos que permiten establecer correlaciones significativas y medir el progreso en el conocimiento de los estudiantes.

4.1.2.1. Pregunta 1. ¿Comprendes los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?

Análisis Interpretativo: Según los resultados proyectados en la Tabla 9, la encuesta post-exposición revela que, tras interactuar con el videojuego, la mayoría de los estudiantes afirma comprender los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad. Este cambio sugiere que el videojuego ha tenido un efecto educativo positivo, mejorando significativamente el entendimiento de los estudiantes sobre estos principios fundamentales de la ciberseguridad.

Tabla 9 Tabla de Frecuencias, Pregunta 1 Post - Exposición

¿Comprendes los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	28	90,3	90,3	90,3
	No	3	9,7	9,7	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este aumento en la comprensión de los conceptos de CID después de la exposición al videojuego respalda la hipótesis de la tesis de que los videojuegos pueden ser una herramienta efectiva para la educación en ciberseguridad. La mejora en la comprensión del CID sugiere que la tesis logra sus objetivos educativos y demuestra la viabilidad de utilizar videojuegos para fomentar una cultura de seguridad informática más robusta entre los estudiantes. Este resultado es un indicador

positivo del impacto del videojuego en la educación en ciberseguridad y puede motivar futuras investigaciones y desarrollos en este ámbito.

4.1.2.2. Pregunta 2. ¿Pudiste identificar cómo las decisiones tomadas en el juego afectaron la CID de la información?

Análisis Interpretativo: La respuesta de los estudiantes post-exposición indica que casi todos pudieron identificar cómo sus decisiones en el juego afectaron los principios de Confidencialidad, Integridad y Disponibilidad de la información. Esto refleja una comprensión práctica de las consecuencias de las acciones de ciberseguridad, lo que sugiere que el videojuego ha logrado no solo transmitir conocimiento teórico, sino también fomentar una comprensión aplicada de cómo las decisiones pueden impactar la seguridad de la información, estos datos se observan en la Tabla 10.

Tabla 10 Tabla de Frecuencias, Pregunta 2 Post - Exposición

¿Pudiste identificar cómo las decisiones tomadas en el juego afectaron la CID de la información?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	29	93,5	93,5	93,5
	No	2	6,5	6,5	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este alto nivel de reconocimiento de la importancia de las decisiones en ciberseguridad apoya firmemente la tesis de que el videojuego sirve como un medio efectivo para educar a los estudiantes en la aplicación práctica de la ciberseguridad. Este resultado positivo implica que el videojuego puede tener un impacto significativo en el desarrollo de la habilidad de los estudiantes para tomar decisiones informadas en situaciones relacionadas con la seguridad informática, lo cual es esencial en el mundo digital actual. La tesis se beneficia de estos hallazgos, ya que demuestra que la metodología implementada puede mejorar efectivamente la cultura de ciberseguridad en el contexto educativo.

4.1.2.3. Pregunta 3. ¿Ha cambiado tu percepción sobre la importancia de la ciberseguridad en tu vida diaria tras jugar?

Análisis Interpretativo: Analizando la tabulación de la Pregunta 3 en la Tabla 11, se determina que los resultados de los estudiantes post-exposición al videojuego, la gran mayoría ha experimentado un cambio en su percepción sobre la importancia de la ciberseguridad en su vida diaria. Lo que indica que el videojuego ha tenido un impacto en la

valoración personal que los estudiantes le otorgan a la ciberseguridad, potencialmente aumentando su interés y compromiso con el tema.

Tabla 11 Tabla de Frecuencias, Pregunta 3 Post - Exposición

¿Ha cambiado tu percepción sobre la importancia de la ciberseguridad en tu vida diaria tras jugar?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	29	93,5	93,5	93,5
	No	2	6,5	6,5	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: El cambio en la percepción sobre la importancia de la ciberseguridad tras interactuar con el videojuego respalda la premisa de la tesis de que los métodos educativos interactivos pueden influir positivamente en las actitudes de los estudiantes. Este resultado demuestra que el videojuego no solo sirve como una herramienta pedagógica para transmitir conocimiento, sino que también puede fortalecer la conciencia de los estudiantes sobre la relevancia de la ciberseguridad en el mundo real. Esto refuerza la relevancia del trabajo de la tesis, confirmando que el videojuego desarrollado es un medio efectivo para promover una cultura de ciberseguridad más sólida entre la población estudiantil.

4.1.2.4. Pregunta 4. ¿Consideras ahora que los videojuegos son una herramienta efectiva para aprender sobre ciberseguridad?

Análisis Interpretativo: En la Tabla12, la respuesta unánime de los estudiantes post-exposición al videojuego refleja una aceptación total de los videojuegos como una herramienta efectiva para aprender sobre ciberseguridad. Este consenso indica que la experiencia del videojuego ha sido positiva y convincente en cuanto a su valor educativo.

Tabla 12 Tabla de Frecuencias, Pregunta 4 Post - Exposición

¿Consideras ahora que los videojuegos son una herramienta efectiva para aprender sobre ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	31	100,0	100,0	100,0

Inferencia para el Desarrollo de la Tesis: Este resultado es extremadamente favorable para la tesis, ya que refuerza la idea de que el videojuego no solo es aceptado, sino también completamente validado por los estudiantes como un medio para aprender ciberseguridad. Esto confirma que el videojuego diseñado es un aporte al campo educativo y que podría ser un modelo para futuros desarrollos educativos en ciberseguridad. La

aceptación completa por parte de los estudiantes sugiere que la tesis podría tener un impacto significativo en la educación de ciberseguridad, ofreciendo un método innovador que es tanto atractivo como instructivo.

4.1.2.5. Pregunta 5. ¿El juego ha influenciado tu percepción sobre la importancia de la ciberseguridad, tanto a nivel personal como organizacional?

Análisis Interpretativo: La mayoría de los estudiantes, tras interactuar con el videojuego, cambiaron su perspectiva de la ciberseguridad, tanto a nivel personal como organizacional. Esta respuesta indica que el videojuego ha sido eficaz no solo en transmitir la importancia de la ciberseguridad personalmente, sino que también ha logrado expandir la conciencia sobre su relevancia en un entorno organizacional, eso es lo que revela los resultados mostrados en la Tabla 13.

Tabla 13 Tabla de Frecuencias, Pregunta 5 Post - Exposición

¿El juego ha influenciado tu percepción sobre la importancia de la ciberseguridad, tanto a nivel personal como organizacional?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	25	80,6	80,6	80,6
	No	6	19,4	19,4	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este cambio en la percepción de los estudiantes refuerza la tesis de que los videojuegos pueden ser una plataforma poderosa para educar y cambiar actitudes. La capacidad del videojuego para influir en la percepción de la ciberseguridad a un nivel más amplio que el personal sugiere que el enfoque de aprendizaje es altamente efectivo y puede ser aplicado en el mundo real. Para este proyecto el resultado es positivo, ya que muestra que la intervención educativa propuesta puede efectivamente mejorar la cultura de ciberseguridad entre los futuros profesionales. Esto también sugiere que los estudiantes están mejor equipados para aplicar conocimientos de ciberseguridad.

4.1.2.6. Pregunta 6. ¿Consideras útil el contenido basado en Magerit para comprender mejor las amenazas de ciberseguridad?

Análisis Interpretativo: Los estudiantes respondieron de manera positiva que el contenido basado en Magerit fue útil para comprender mejor las amenazas de ciberseguridad. Este indica que la integración del catálogo de Magerit en el videojuego ha sido valiosa y ha mejorado su entendimiento de las amenazas en ciberseguridad.

Tabla 14 Tabla de Frecuencias, Pregunta 6 Post - Exposición

¿Consideras útil el contenido basado en Magerit para comprender mejor las amenazas de ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	28	90,3	90,3	90,3
	No	3	9,7	9,7	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: La percepción positiva sobre la utilidad del contenido de Magerit subraya la efectividad del videojuego como herramienta didáctica y respalda la metodología de la tesis. Este hallazgo implica que la tesis ha logrado su objetivo de proporcionar un recurso educativo que no solo es atractivo sino también profundamente informativo. La integración exitosa de Magerit refuerza la argumentación de la tesis de que el aprendizaje interactivo puede mejorar significativamente la comprensión conceptual y práctica de la ciberseguridad, preparando a los estudiantes para enfrentar y gestionar las amenazas en entornos tanto personales como profesionales.

4.1.2.7. Pregunta 7. ¿Te ha motivado el videojuego a buscar más información y seguir educándote en ciberseguridad?

Análisis Interpretativo: Según la Tabla 15, La gran mayoría de los estudiantes se sintieron motivados por el videojuego a buscar más información y continuar educándose en ciberseguridad. Esto después de jugar indica que el videojuego no solo capturó su atención, sino que también estimuló el deseo de aprendizaje.

Tabla 15 Tabla de Frecuencias, Pregunta 7 Post - Exposición

¿Te ha motivado el videojuego a buscar más información y seguir educándote en ciberseguridad?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	29	93,5	93,5	93,5
	No	2	6,5	6,5	100,0
	Total	31	100,0	100,0	

Inferencia para el Desarrollo de la Tesis: Este resultado es un indicador fuerte de que el videojuego diseñado en la tesis no solo es un contenido educativo, sino también permite el aprendizaje autodirigido. La motivación para buscar más conocimiento es un paso crucial en la educación efectiva y sugiere que la tesis ha logrado más que su objetivo inicial de enseñar; ha inspirado a los estudiantes a ser proactivos en su educación en ciberseguridad.

4.2. Correlación de Resultados sobre la Aceptación del videojuego

4.2.1. Comprensión del CID (Confidencialidad, Integridad y Disponibilidad)

Análisis Interpretativo: La tabla cruzada Tabla 16, muestra la relación entre el conocimiento previo con los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad y la comprensión posterior de estos conceptos después de interactuar con el videojuego. Se observa que la mayoría de los estudiantes que ya estaban familiarizados con el CID en ciberseguridad también comprendieron estos conceptos después de jugar. Es notable que algunos estudiantes que inicialmente no estaban familiarizados con el CID, después de jugar, lograron comprender estos conceptos.

*Tabla 16 Tabla cruzada: Pregunta1. Pre-Exposición * Pregunta1. Post-Exposición*

Tabla cruzada: Pregunta1. Pre-Exposición * Pregunta1. Post-Exposición

			¿Comprendes los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?		Total
			Si	No	
¿Estás familiarizado/a con los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?	Si	Recuento	15	1	16
		% del total	48,4%	3,2%	51,6%
	No	Recuento	13	2	15
		% del total	41,9%	6,5%	48,4%
Total		Recuento	28	3	31
		% del total	90,3%	9,7%	100,0%

Por lo que se puede concluir que el videojuego ha sido efectivo en reforzar y expandir el conocimiento de los estudiantes sobre la ciberseguridad, independientemente de su conocimiento previo. El hecho de que la comprensión del CID es alta entre los estudiantes previamente familiarizados indica que el juego podría servir como una herramienta de refuerzo positivo para los conceptos ya aprendidos. Además, el aumento en la comprensión entre los que no estaban familiarizados previamente con el CID destaca el valor educativo del juego como un medio para introducir y explicar conceptos fundamentales de ciberseguridad.

4.2.2. Percepción de la Importancia de la Ciberseguridad

Análisis Interpretativo: La tabla cruzada Tabla 17, muestra la relación entre la percepción inicial de la importancia de la ciberseguridad en la vida diaria de los estudiantes y si esta percepción cambió después de jugar al videojuego. La mayoría de los estudiantes que ya consideraban importante la ciberseguridad en su vida diaria mantuvieron esa percepción después de la exposición al videojuego. Incluso entre el pequeño grupo que inicialmente no valoraba la ciberseguridad como un aspecto importante de su vida diaria, casi todos cambiaron de opinión después de jugar.

*Tabla 17 Tabla cruzada: Pregunta 2. Pre-Exposición * Pregunta 3. Post-Exposición*

Tabla cruzada: Pregunta 2. Pre-Exposición * Pregunta 3. Post-Exposición

			¿Ha cambiado tu percepción sobre la importancia de la ciberseguridad en tu vida diaria tras jugar?		Total
			Si	No	
¿Consideras importante la ciberseguridad en tu vida diaria?	Si	Recuento	28	2	30
		% del total	90,3%	6,5%	96,8%
	No	Recuento	1	0	1
		% del total	3,2%	0,0%	3,2%
Total		Recuento	29	2	31
		% del total	93,5%	6,5%	100,0%

Este cambio de percepción indica que el videojuego ha sido efectivo en los estudiantes sobre la relevancia de la ciberseguridad en su vida cotidiana.

Se puede concluir que después de jugar el videojuego se ha fortalecido la conciencia sobre los riesgos cibernéticos y la necesidad de protección personal y profesional.

4.2.3. Efectividad Educativa del videojuego

Análisis Interpretativo: La tabla cruzada Tabla 18, indica la percepción de los videojuegos como herramientas efectivas para aprender sobre ciberseguridad antes y después de jugar. La consistencia en la respuesta afirmativa es significativa, lo que indica que el videojuego ha cumplido en cuanto a su utilidad educativa. El hecho de que todos los estudiantes que inicialmente dudaban de la efectividad de los videojuegos como herramientas de aprendizaje hayan cambiado su opinión a una positiva después de la experiencia del juego es un indicador de la potencia de los videojuegos como medio de enseñanza en el campo de la ciberseguridad.

*Tabla 18 Tabla cruzada: Pregunta 3. Pre-Exposición * Pregunta4. Post-Exposición*

Tabla cruzada: Pregunta3. Pre-Exposición * Pregunta4. Post-Exposición

			¿Consideras ahora que los videojuegos son una herramienta efectiva para aprender sobre ciberseguridad?	Total
			Si	
¿Crees que los videojuegos pueden ser una herramienta efectiva para aprender sobre ciberseguridad?	Si	Recuento	29	29
		% del total	93,5%	93,5%
	No	Recuento	2	2
		% del total	6,5%	6,5%
Total		Recuento	31	31
		% del total	100,0%	100,0%

Se concluye con estos resultados que la hipótesis de que el videojuego desarrollado es una herramienta efectiva para la educación en ciberseguridad y podría ser un modelo para seguir para futuras iniciativas educativas en este campo.

4.2.4. Conocimiento Práctico y Aplicación de Mitigaciones

Análisis Interpretativo: La tabla cruzada Tabla 19, indica un cambio en la percepción de la importancia de la ciberseguridad después de jugar al videojuego. Se observa que una proporción notable de estudiantes que no estaban inicialmente informados sobre cómo protegerse contra ataques al CID de la información reconoce ahora la importancia de la ciberseguridad tanto en el ámbito personal como organizacional. Esto indica que el videojuego no solo ha servido como una herramienta educativa para aumentar el conocimiento sino también para fomentar una mayor conciencia sobre la aplicación práctica de la ciberseguridad.

*Tabla 19 Tabla cruzada: Pregunta 4. Pre-Exposición * Pregunta 5. Post-Exposición*

Tabla cruzada: Pregunta 4. Pre-Exposición * Pregunta 5. Post-Exposición

			¿El juego ha influenciado tu percepción sobre la importancia de la ciberseguridad, tanto a nivel personal como organizacional?		Total
			Si	No	
¿Tienes conocimientos sobre cómo protegerte contra ataques al CID de la Información?	Si	Recuento	15	1	16
		% del total	48,4%	3,2%	51,6%
	No	Recuento	10	5	15
		% del total	32,3%	16,1%	48,4%
Total		Recuento	25	6	31
		% del total	80,6%	19,4%	100,0%

4.2.5. Motivación para Aprender más sobre Ciberseguridad

Análisis Interpretativo: La correlación de la Tabla 2, entre la motivación para aprender más sobre ciberseguridad y la influencia del videojuego indica que en su mayoría los estudiantes que se sintieron motivados inicialmente para aprender sobre ciberseguridad también se sintieron inspirados por el videojuego para profundizar sus conocimientos, por lo que puede ser una herramienta poderosa para mantener y potenciar la curiosidad y el deseo de aprendizaje en los estudiantes.

*Tabla 20 Tabla cruzada: Pregunta7. Pre-Exposición * Pregunta 7. Post-Exposición*

Tabla cruzada: Pregunta7. Pre-Exposición * Pregunta 7. Post-Exposición

			¿Te ha motivado el videojuego a buscar más información y seguir educándote en ciberseguridad?		Total
			Si	No	
¿Te sientes motivado/a para aprender más sobre ciberseguridad?	Si	Recuento	26	2	28
		% del total	83,9%	6,5%	90,3%
	No	Recuento	3	0	3
		% del total	9,7%	0,0%	9,7%
Total		Recuento	29	2	31
		% del total	93,5%	6,5%	100,0%

4.3. Contrastación de los resultados obtenidos con las preguntas de investigación.

4.3.1. Adaptación del Catálogo de elementos MAGERIT v3, para el videojuego.

La incorporación del catálogo Magerit en la dinámica del videojuego se ha realizado con notable éxito, logrando una integración exhaustiva y efectiva de las 60 amenazas identificadas dentro del marco del juego. Este logro refleja la cuidadosa planificación y la aplicación metódica de los principios de ciberseguridad en el contexto lúdico, lo que evidencia no solo la viabilidad sino también la eficacia de utilizar videojuegos como una herramienta pedagógica en la enseñanza de conceptos complejos de ciberseguridad.

4.3.2. Método de encriptación es el más conveniente.

Se realizo un análisis comparativo de las diferentes características de los métodos de encriptación que se explican en la Tabla 21, donde se demuestra que debido al diseño del videojuego la mejor alternativa es implementar el método de Encriptación AES.

4.3.3. Garantizar una experiencia de juego envolvente y educativa.

Para garantizar una experiencia de juego envolvente en un videojuego educativo, se planteó la idea de crear un videojuego retro con tonos alegres que capturen la atención de los jugadores, inspirando el estilo en el mismo de los juegos retro, con el fin de generar un ambiente de nostalgia, pero si dejar de lado mecánicas modernas como es la sección de elección de la mitigación con un mecánica moderna, el objetivo es que el jugador pueda sentir un apego emocional pero a la vez una experiencia divertida.

4.3.4. Análisis de los resultados obtenidos y que se puede mejorar.

En base a los resultados obtenidos de las encuestas se puede inferir que en efecto el videojuego puede llegar a ser una herramienta que permita a los jugadores incrementar su conocimiento en ciberseguridad, para una posible mejora puede ser en un futuro incrementar la cantidad de mecánicas y mapas, de tal manera que el jugador nunca pierda el interés y teniendo una partida diferente cada vez.

CAPÍTULO V. DESARROLLO

5.1. Comparativa de métodos de encriptación en términos de seguridad y rendimiento.

Para la decisión crítica sobre la selección del método de encriptación que sea el más conveniente para proteger los datos sensibles tanto del Jugador, con base en la revisión de la literatura en el artículo publicado por Cloudflare donde se indica los algoritmos más comunes usados para el cifrado de datos (Cloudflare, 2020), permitió que se recopile información como para generar la Tabla 21, y determinar el método de encriptación óptimo para el videojuego.

Tabla 21 Comparativa de métodos de Encriptación

Algoritmo	Tipo	Seguridad	Rendimiento	Tamaño Máximo de Cifrado (256 bits)	Aplicación
AES	Simétrico	Alta (varias longitudes de clave, hasta 256 bits)	Muy alto (eficiente en hardware y software)	Ilimitado (limitado solo por el tamaño del almacenamiento y la memoria)	Cifrado de datos
RSA	Asimétrico	Alta (depende de la longitud de la clave, eficaz para intercambio de claves)	Bajo (más lento, especialmente con claves largas)	Limitado (depende del tamaño de la clave, generalmente menor que AES)	Cifrado de datos, intercambio de claves
HASH (General)	Función Hash	Alta para integridad de datos (no reversible, no para cifrado)	Generalmente alto (rápido para verificar integridad)	No aplicable (no para cifrado)	Verificación de integridad, no para cifrado
MD5	Función Hash	Baja (vulnerable a colisiones y ataques rápidos)	Alto (pero comprometido por baja seguridad)	No aplicable (no para cifrado)	Históricamente usado para verificación de integridad

Por el resultado obtenido de la recopilación de características y en base a que el juego está destinado a dispositivos móviles que no tiene la facilidad y escalar como un computador y la capacidad con la que puede incrementarse la información que ser necesario encriptar, el

mejor método que se puede utilizar es AES, por su velocidad de procesamiento y la amplitud de datos que permite encriptar con una clave del mismo tamaño.

5.2. Adaptación del Catálogo de Elementos Magerit V3.

Una vez explicado lo que es Magerit, para la construcción del catálogo de elementos que fue utilizado en el videojuego se decidió mediante una revisión bibliográfica tomar el catálogo de amenazas descrita en la sección cuatro del segundo libro de Magerit, para la creación de los eventos se utilizó como recurso para los eventos presentados en el juego, para cada elemento se analizaron tres propuestas que podrían influenciar en el mantenimiento del CID de la Información, además de analizar el cual sería el impacto en caso de rechazar la mitigación.

Y aunque inicialmente se planteó seleccionar los elementos más relevantes que sean aplicables para los estudiantes, pero después de un análisis en profundidad se notó la importancia de dar a conocer todos los elementos de la categoría de amenazas, dado que el videojuego su objetivo es generar aprendizaje para los jugadores, era necesario instruirles no en un grupo limitado de elementos.

5.2.1. Análisis de los elementos Amenaza en el Catálogo Magerit V3

Por medio de la investigación en la documentación disponible en el Portal de Administración Electrónica del Gobierno de España, en el Libro II de la Metodología de Análisis de Riegos Magerit V3, se listaron las amenazas detalladas en dicha documentación y posteriormente hacer un análisis de la importancia que esta tiene para los estudiantes como se muestra en la Tabla 22.

Tabla 22 Análisis Amenazas y su importancia para los estudiantes.

Elemento	Significado	Importancia para Estudiantes
Amenaza 1: Desastres Naturales	Eventos extremos naturales que pueden impactar las infraestructuras.	Conciencia sobre planes de respaldo de datos y seguridad de equipos.
Amenaza 2: Fuego de Origen Natural	Incendios causados por fenómenos naturales como rayos o sequías.	Importancia de medidas de seguridad y protección contra incendios.
Amenaza 3: Daños por Agua de Origen Natural	Daños a equipos y estructuras debido a inundaciones naturales.	Protección de dispositivos electrónicos frente a daños por agua.

Amenaza 4: Desastres Naturales de Origen Industrial	Desastres naturales exacerbados por la actividad industrial.	Entender el impacto de desastres industriales en la seguridad de la información.
Amenaza 5: Fuego de Origen Industrial	Incendios en instalaciones industriales con riesgos de seguridad.	Conocimiento sobre la seguridad en instalaciones industriales.
Amenaza 6: Daños por Agua de Origen Industrial	Inundaciones o daños por agua en entornos industriales.	Manejo de equipos y datos frente a riesgos de inundaciones industriales.
Amenaza 7: Desastres Industriales	Accidentes graves en la industria que afectan la tecnología.	Comprensión de cómo los accidentes industriales afectan la tecnología.
Amenaza 8: Contaminación Mecánica	Daño en dispositivos por partículas o sustancias mecánicas.	Protección de dispositivos frente a contaminantes mecánicos.
Amenaza 9: Contaminación Electromagnética	Interferencias en equipos electrónicos por campos electromagnéticos.	Conocimiento sobre los efectos de la contaminación electromagnética.
Amenaza 10: Avería de Origen Físico o Lógico	Fallos en sistemas debido a errores físicos o errores en software.	Manejo de fallos y errores en sistemas y equipos.
Amenaza 11: Corte del Suministro Eléctrico	Pérdida de energía eléctrica que afecta a equipos y sistemas.	Conocimiento sobre la importancia de sistemas de respaldo de energía.
Amenaza 12: Condiciones Inadecuadas de Temperatura o Humedad	Ambientes con temperaturas o humedades extremas dañinas para los equipos.	Entender la necesidad de condiciones ambientales adecuadas para equipos.
Amenaza 13: Fallo de Servicios de Comunicaciones	Fallos en servicios de comunicación que impiden la conectividad.	Importancia de tener planes de contingencia para fallos de comunicación.
Amenaza 14: Interrupción de Otros Servicios y Suministros Esenciales	Interrupciones de servicios esenciales como agua, calefacción o aire acondicionado.	Conciencia sobre la dependencia de servicios esenciales y cómo gestionar interrupciones.
Amenaza 15: Degradación de los Soportes de Almacenamiento de la Información	Deterioro de medios como discos duros o unidades flash que contienen datos.	Comprensión de la importancia del mantenimiento adecuado de soportes de almacenamiento.

Amenaza 16: Emanaciones Electromagnéticas	Interferencias causadas por fuentes electromagnéticas externas.	Conocimiento de cómo proteger equipos de interferencias electromagnéticas.
Amenaza 17: Errores y Fallos No Intencionados	Errores o malfuncionamientos en sistemas o equipos no provocados intencionalmente.	Reconocimiento de la importancia de sistemas robustos y fiables.
Amenaza 18: Errores de los Usuarios No Intencionados	Errores cometidos por usuarios debido a falta de conocimiento o atención.	Entender la necesidad de formación y atención al operar sistemas y equipos.
Amenaza 19: Errores del Administrador No Intencionados	Errores cometidos por administradores de sistemas en la gestión de infraestructuras.	Conocimiento sobre la importancia de una gestión adecuada de sistemas por parte del personal técnico.
Amenaza 20: Errores de Monitorización (Log) No Intencionados	Fallos en la supervisión o monitorización de sistemas que llevan a una gestión inadecuada.	Comprensión de la importancia de un monitoreo efectivo para la seguridad de la información.
Amenaza 21: Errores de Configuración No Intencionados	Errores en la configuración de sistemas y aplicaciones.	Conocer la importancia de configurar correctamente para evitar brechas de seguridad.
Amenaza 22: Deficiencias en la Organización No Intencionados	Fallas organizativas que afectan la seguridad de la información.	Entender cómo la estructura organizativa puede impactar la seguridad de la información.
Amenaza 23: Difusión de Software Dañino No Intencionados	Propagación no intencionada de software malicioso.	Conciencia sobre los riesgos de difundir malware y cómo prevenirlo.
Amenaza 24: Errores de Re-Encaminamiento	Desvíos incorrectos en el flujo de datos o comunicaciones.	Comprensión de los riesgos asociados con errores en el enrutamiento de datos.
Amenaza 25: Errores de Secuencia No Intencionados	Errores en la secuencia o el orden de las operaciones.	Conocer la importancia de mantener el orden correcto en procesos técnicos.
Amenaza 26: Escapes de Información No Intencionados	Información confidencial expuesta accidentalmente.	Entender cómo proteger la información personal y académica de exposiciones no deseadas.
Amenaza 27: Alteración Accidental de la Información No Intencionados	Cambios no deseados en los datos causados por errores.	Reconocer la importancia de precisión en el manejo de datos.
Amenaza 28: Destrucción de Información No Intencionados	Pérdida accidental de información valiosa.	Conciencia sobre la necesidad de proteger los datos contra pérdidas accidentales.
Amenaza 29: Fugas de Información No Intencionados	Información sensible que se filtra sin intención.	Comprensión de cómo prevenir fugas de información y sus consecuencias.

Amenaza 30: Vulnerabilidades de los Programas (Software)	Debilidades en el software que pueden ser explotadas.	Conocimiento de las vulnerabilidades comunes en el software y cómo mitigarlas.
Amenaza 31: Errores de Mantenimiento/Actualización de Programas (Software)	Errores durante la actualización o mantenimiento del software.	Conocer la importancia de actualizaciones y mantenimientos adecuados para la seguridad.
Amenaza 32: Errores de Mantenimiento/Actualización de Equipos (Hardware)	Errores al realizar mantenimiento o actualizaciones en el hardware.	Entender cómo el mantenimiento del hardware impacta la seguridad y el rendimiento.
Amenaza 33: Caída del Sistema por Agotamiento de Recursos	Sistemas que fallan por uso excesivo o mal manejo de recursos.	Conciencia sobre la gestión eficiente de recursos en sistemas y equipos.
Amenaza 34: Pérdida de Equipos	Extravío o robo de dispositivos y equipos que contienen datos sensibles.	Reconocer la importancia de la seguridad física y el seguimiento de dispositivos.
Amenaza 35: Indisponibilidad del Personal	Falta de personal disponible para gestionar o mantener sistemas.	Conocimiento sobre la planificación de recursos humanos para la continuidad operativa.
Amenaza 36: Ataques Intencionados	Acciones deliberadas para dañar, alterar o acceder a sistemas y datos.	Comprensión de las amenazas cibernéticas y cómo protegerse de ataques maliciosos.
Amenaza 37: Manipulación de los Registros de Actividad (Log) Intencionados	Alteración maliciosa de registros de actividad para ocultar acciones.	Conciencia de la importancia de registros seguros y cómo detectar manipulaciones.
Amenaza 38: Manipulación de la Configuración Intencionados	Cambios no autorizados en la configuración de sistemas y redes.	Entender los riesgos de configuraciones inseguras y cómo verificar la integridad.
Amenaza 39: Suplantación de la Identidad del Usuario	Suplantación para obtener acceso no autorizado a sistemas.	Conocimiento de las técnicas de suplantación y cómo proteger la identidad digital.
Amenaza 40: Abuso de Privilegios de Acceso	Uso indebido de permisos de acceso para fines no autorizados.	Comprensión de la gestión de privilegios y la importancia de su uso responsable.
Amenaza 41: Uso No Previsto	Uso de sistemas o aplicaciones de formas no intencionadas.	Conocer los riesgos de utilizar tecnología de manera no prevista.
Amenaza 42: Difusión de Software Dañino Intencionado	Propagación deliberada de malware y software malicioso.	Entender cómo identificar y prevenir la difusión de malware.
Amenaza 43: Re-Encaminamiento de Mensajes Intencionado	Redirección maliciosa de comunicaciones.	Reconocer los peligros del re-encaminamiento malicioso de datos.

Amenaza 44: Alteración de Secuencia	Cambios intencionados en el orden de operaciones o procesos.	Conocer cómo la alteración de secuencias puede afectar a los sistemas.
Amenaza 45: Acceso No Autorizado	Ingresos no autorizados a sistemas o datos.	Conciencia sobre la seguridad de acceso y cómo prevenir intrusiones.
Amenaza 46: Análisis de Tráfico	Monitoreo de comunicaciones para recopilar información.	Entender la importancia de la privacidad y cómo proteger las comunicaciones.
Amenaza 47: Repudio Intencionado	Negación de acciones realizadas en sistemas o redes.	Reconocer la importancia de mecanismos para prevenir y detectar el repudio.
Amenaza 48: Interceptación de Información (Escucha)	Escucha o captura clandestina de comunicaciones.	Conocimiento sobre cómo proteger la información durante la transmisión.
Amenaza 49: Modificación Deliberada de la Información	Cambios intencionados y maliciosos en datos.	Entender cómo prevenir y detectar modificaciones no autorizadas en la información.
Amenaza 50: Destrucción de Información Intencionado	Eliminación maliciosa de datos importantes.	Conciencia sobre la importancia de respaldos y recuperación de datos.
Amenaza 51: Divulgación de Información Intencionado	Revelación deliberada de información confidencial.	Conciencia sobre la protección de datos y las consecuencias de su divulgación.
Amenaza 52: Manipulación de Programas Intencionado	Modificación maliciosa de software para alterar su funcionamiento.	Entender los riesgos y cómo protegerse de la manipulación de software.
Amenaza 53: Manipulación de los Equipos Intencionado	Cambios físicos o lógicos malintencionados en el hardware.	Reconocer la importancia de la seguridad física y lógica de los equipos.
Amenaza 54: Denegación de Servicio Intencionado	Ataques que buscan hacer inaccesible un recurso o servicio.	Comprender las tácticas de denegación de servicio y cómo mitigarlas.
Amenaza 55: Robo	Sustracción física de equipos o información.	Conocimiento de cómo prevenir el robo de dispositivos y proteger la información.
Amenaza 56: Ataque Destructivo	Acciones dirigidas a dañar o destruir infraestructura o datos.	Conciencia sobre los daños potenciales de ataques y cómo responder a ellos.
Amenaza 57: Ocupación Enemiga	Control no autorizado de sistemas o instalaciones.	Entender las implicaciones de la toma de control hostil de sistemas.
Amenaza 58: Indisponibilidad del Personal	Ausencia de personal clave para operaciones y seguridad.	Reconocer la importancia de la planificación de recursos humanos y respaldos.
Amenaza 59: Extorsión	Coacción para obtener beneficios mediante amenazas.	Conocimiento sobre cómo manejar situaciones de extorsión en el ámbito digital.

Amenaza 60: Ingeniería Social (Picaresca)	Manipulación psicológica para obtener información o acceso.	Comprensión de las técnicas de ingeniería social y cómo protegerse de ellas.

5.2.2. Adaptación de elementos del Catalogo Magerit para el videojuego

Para una integración eficientemente de los elementos descritos anteriormente en el diseño del videojuego, se implementó una fase de decisión estratégica, la cual permitirá que el jugador tome la decisión sobre si aceptar dicha mitigación o la rechaza y de esta manera ver cómo afecta la decisión en los indicadores propuestos en el diseño. Esta integración se refleja en la Tabla 23 diseñada como un checklist que destaca los elementos específicos de Magerit adaptados para su aplicación dentro del juego.

Tabla 23 Checklist de Mitigaciones Adaptadas

Amenaza Catálogo Magerit V3	Adaptado
Amenaza 1: Desastres Naturales	✓
Amenaza 2: Fuego de Origen Natural	✓
Amenaza 3: Daños por Agua de Origen Natural	✓
Amenaza 4: Desastres Naturales de Origen Industrial	✓
Amenaza 5: Fuego de Origen Industrial	✓
Amenaza 6: Daños por Agua de Origen Industrial	✓
Amenaza 7: Desastres Industriales	✓
Amenaza 8: Contaminación Mecánica	✓
Amenaza 9: Contaminación Electromagnética	✓
Amenaza 10: Avería de Origen Físico o Lógico	✓
Amenaza 11: Corte del Suministro Eléctrico	✓
Amenaza 12: Condiciones Inadecuadas de Temperatura o Humedad	✓
Amenaza 13: Fallo de Servicios de Comunicaciones	✓
Amenaza 14: Interrupción de Otros Servicios y Suministros Esenciales	✓
Amenaza 15: Degradación de los Soportes de Almacenamiento de la Información	✓
Amenaza 16: Emanaciones Electromagnéticas	✓
Amenaza 17: Errores y Fallos No Intencionados	✓
Amenaza 18: Errores de los Usuarios No Intencionados	✓
Amenaza 19: Errores del Administrador No Intencionados	✓
Amenaza 20: Errores de Monitorización (Log) No Intencionados	✓
Amenaza 21: Errores de Configuración No Intencionados	✓

Amenaza 22: Deficiencias en la Organización No Intencionados	✓
Amenaza 23: Difusión de Software Dañino No Intencionados	✓
Amenaza 24: Errores de Re-Encaminamiento	✓
Amenaza 25: Errores de Secuencia No Intencionados	✓
Amenaza 26: Escapes de Información No Intencionados	✓
Amenaza 27: Alteración Accidental de la Información No Intencionados	✓
Amenaza 28: Destrucción de Información No Intencionados	✓
Amenaza 29: Fugas de Información No Intencionados	✓
Amenaza 30: Vulnerabilidades de los Programas (Software)	✓
Amenaza 31: Errores de Mantenimiento/Actualización de Programas (Software)	✓
Amenaza 32: Errores de Mantenimiento/Actualización de Equipos (Hardware)	✓
Amenaza 33: Caída del Sistema por Agotamiento de Recursos	✓
Amenaza 34: Pérdida de Equipos	✓
Amenaza 35: Indisponibilidad del Personal	✓
Amenaza 36: Ataques Intencionados	✓
Amenaza 37: Manipulación de los Registros de Actividad (Log) Intencionados	✓
Amenaza 38: Manipulación de la Configuración Intencionados	✓
Amenaza 39: Suplantación de la Identidad del Usuario	✓
Amenaza 40: Abuso de Privilegios de Acceso	✓
Amenaza 41: Uso No Previsto	✓
Amenaza 42: Difusión de Software Dañino Intencionado	✓
Amenaza 43: Re-Encaminamiento de Mensajes Intencionado	✓
Amenaza 44: Alteración de Secuencia	✓
Amenaza 45: Acceso No Autorizado	✓
Amenaza 46: Análisis de Tráfico	✓
Amenaza 47: Repudio Intencionado	✓
Amenaza 48: Interceptación de Información (Escucha)	✓
Amenaza 49: Modificación Deliberada de la Información	✓
Amenaza 50: Destrucción de Información Intencionado	✓
Amenaza 51: Divulgación de Información Intencionado	✓
Amenaza 52: Manipulación de Programas Intencionado	✓
Amenaza 53: Manipulación de los Equipos Intencionado	✓
Amenaza 54: Denegación de Servicio Intencionado	✓

Amenaza 55: Robo	✓
Amenaza 56: Ataque Destructivo	✓
Amenaza 57: Ocupación Enemiga	✓
Amenaza 58: Indisponibilidad del Personal	✓
Amenaza 59: Extorsión	✓
Amenaza 60: Ingeniería Social (Picaresca)	✓

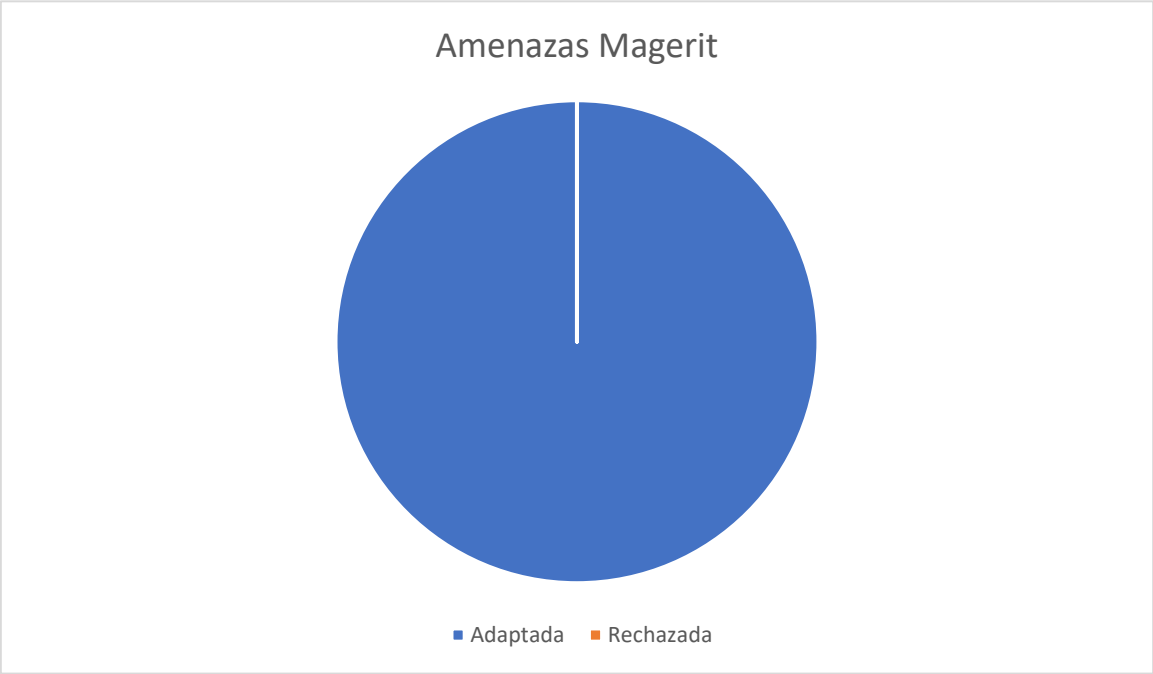


Figura 17 Gráfico del porcentaje de Mitigaciones Adaptadas para el videojuego

Como se puede observar en la Tabla 23 y en la Figura 17, el 100% de los elementos que comprenden el catálogo de amenazas descritas por Magerit, se han adaptado, debido a la importancia que estos tienen.

5.2.3. Análisis de las Mitigación por Amenaza.

Al haber generado las mitigaciones para adaptar las amenazas y usarlas dentro del videojuego, se elaboraron tablas con tres tipos de propuestas útiles para mitigar las amenazas con su respectivo análisis, como se puede observar en el Anexo A4. Tablas de Análisis de Mitigaciones.

5.3. Desarrollo del videojuego serious game

En el desarrollo de la programación e implementación de las mecánicas del juego, se presta atención a la jugabilidad suave y a la respuesta a acciones del jugador. Se incorporan efectos visuales estilo píxel art y sonido para incrementar la experiencia de juego.

5.3.1. Diseño del videojuego

Para el diseño del videojuego se desarrolló un documento de diseño (Figura 18), este documento se utiliza para la socialización del proyecto con los integrantes del grupo inversor, otorgando una idea general del funcionamiento del proyecto, además de dar al equipo de desarrollo una idea general de cómo tendría que ser el resultado del desarrollo.

Diseño del videojuego

Datos Informativos	
Título	What If
Diseñadores	Wilson Yépez
Género	Arcade, Decisión, Educativo
Plataforma	Android Móvil
Versión	V001
Sinopsis de Jugabilidad y contenido	El videojuego consistirá en ir perdiendo sobre ciberseguridad mientras mantienes los índices del CID de la Información en niveles elevados, ya sea capturando los ítems buenos que caen en la Escena Arcade o en la toma de elecciones las cuales están basadas en el catálogo de Amenazas de expuestas en Magerit.
Categoría	El producto resultante del desarrollo será un videojuego de tipo arcade, además de contar con mecánicas de un juego de cartas.
Mecánica	**Recolección de Premios:** Los jugadores deben maniobrar con destreza su personaje para recoger premios, incrementando así su puntaje. **Evitar Hackers:** Se introduce un elemento de estrategia al perder vida al interactuar con hackers, dinamizando el juego. **Drops de restauración:** Los drops especiales permiten a los jugadores restaurar los recursos del jugador y despliega un consejo de seguridad. Propuesta de Mitigación: Al obtener el consejo de seguridad se desplazará a una pantalla donde el jugador podrá tomar decisiones en base a la dificultad presentada, dependiendo de su respuesta al seleccionar la izquierda o a la derecha sus estadísticas se verán alteradas y por ende obtener consecuencias, así cumpliendo un ciclo y volviendo al minijuego para poder volver a recolectar premios y tratar de mejorar las estadísticas. **Niveles Progresivos:** El juego se despliega a través de niveles de dificultad creciente, con incrementos en velocidad y complejidad. Cada etapa presenta desafíos y oportunidades para que los jugadores aprendan jugando.

	Sistema de Puntuación y Competencia: Se implemento un sistema de puntuación para incentivar la competencia y el aprendizaje. **Estética y Ambientación:** Con una estética retro encantadora, "What If" destaca por su ambiente, Se llevaron a cabo pruebas para asegurar un equilibrio óptimo entre desafío y entretenimiento. Las opiniones de los testers fueron clave para pulir el juego.
Tecnología	Para el desarrollo se utilizará: Unity, C#, Firebase, Simple Encrypt Library y programación con el uso de Hilos.
Público	El videojuego está dirigido a estudiantes de primer semestre de la carrea de Software de la Universidad Técnica del Norte.
Visión general del juego	
La visión general de "What If PixelArt" se centra en ofrecer una experiencia de juego única que combina la nostalgia de los gráficos pixelados con la emoción y el desafío de las mecánicas modernas de juego. Este juego está diseñado para cautivar tanto a los aficionados de los videojuegos retro como a una audiencia más joven acostumbrada a experiencias de juego más contemporáneas, además que colaborar en la enseñanza de ciberseguridad.	
Mecánica del juego	
Cámara	Cámara Isométrica
Periféricos	Celular
Controles	Táctiles en la pantalla
Puntaje	El juego consiste en la recolecta de Drops del CID, además de los Drops Premium que otorgan vida y puntaje extra.
Guardar / Cargar	El juego cuenta con un archivo encriptado que contiene las mitigaciones para la sección de cartas, al iniciar se comprueba que este actualizado y en cuanto a los puntajes de jugador siempre se descargan al iniciar sesión, y se actualizan al perder la partida, No cuenta con opción de pausa o guardado de partida.
Estados del juego	
El jugador comienza en una pantalla de inicio de sesión, en la cual también podrá registrarse, si ya esta registrado y a verificado su correo, continuará a una pantalla de carga de contenidos donde se verifica si ya ha descargado los catálogos antes en caso de ya contar con lo archivos encriptados verifica si la versión es correcta, de no ser correcta descargará y actualizará los archivos además obtendrá en memoria los puntajes del jugador, después entran en una pantalla de menú donde podrá elegir entre ver su historial de partidas o iniciar una nueva partid donde iniciará en la escena de donde caerán los drops y posterior mente entraremos a la escena de toma de decisión de la mitigación y el ciclo se repetiría hasta la que algún indicador llegue a 0, lo que envía al jugador a la pantalla de Game Over y posterior mente regresa al menú inicial.	
Detalles de Producción	
Fecha de Inicio	28 de agosto 2023
Fecha de Terminación	3 de noviembre de 2023
Presupuesto	$ 1000

Figura 18 Documento de Diseño videojuego

5.3.2. Personas y roles del proyecto

En la metodología Scrum, existen diferentes roles a cumplir como fundamentales en la implementación de un proyecto de software, los cuales se detallan en la Tabla 25.

Tabla 24 Roles y personas del Proyecto

Rol	Nombre	Descripción del Rol	Funciones Específicas
Scrum Máster / director del Juego	Ing. Wilson Yépez (PRYW)	Facilitador del equipo de desarrollo y director del juego. Asegura que el equipo siga los principios de Scrum, eliminando obstáculos para un desarrollo fluido del juego.	1. Coordina y lidera el equipo de desarrollo. 2. Elimina obstáculos que afectan el desarrollo. 3. Fomenta la comunicación efectiva.
Product Owner / Diseñador de Juegos	Ing. Wilson Yépez (PRYW)	Representa los intereses del cliente y define las características del producto. Define la visión del juego y sus características clave.	1. Define y prioriza las características del juego. 2. Asegura que la visión del juego se refleje en el producto final. 3. Toma decisiones sobre diseño y funcionalidad.
Equipo de Desarrollo / Desarrolladores del Juego	Ing. Wilson Yépez (PRYW)	Compuesto por profesionales que trabajan en la creación del producto, incluyendo programadores, artistas, diseñadores de niveles y otros especialistas.	1. Colabora en la planificación y estimación de tareas. 2. Implementa las características del juego. 3. Participa en reuniones diarias de Scrum.

5.3.3. Artefactos

5.3.3.1. Pila de producto (Product Backlog)

Para el modelo del ProductBacklog se toma como parámetro de definición el número de la historia, su fecha de planificación, la épica a la cual pertenece, nombre de la historia y los puntos válidos para el desarrollo, todos reunidos en la Tabla 26.

Tabla 25 Product BackLog What If

Número	Fecha	Épica	Nombre	Puntos
#16	28/08/2023	Módulo de Juego	Contadores de puntaje	25
#17	28/08/2023	Módulo de Juego	Barras de Vida	44
#18	28/08/2023	Módulo de Juego	Selección de Preguntas	46

#19	28/08/2023	Módulo de Juego	Ciclos	30
#21	11/09/2023	Seguridad y Debugging	Guardado de archivos locales	14
#22	11/09/2023	Seguridad y Debugging	Cifrado de Archivos	40
#23	11/09/2023	Seguridad y Debugging	Acceso Seguro	40
#12	25/09/2023	Módulo Inicio	Comienzo del juego	34
#6	25/09/2023	Módulo Inicio	Inicio de Sesión	18
#7	25/09/2023	Módulo Inicio	Registro de Usuarios	7
#8	25/09/2023	Módulo Inicio	Recuperación de Contraseñas	11
#10	09/10/2023	Módulo Home	Nuevo Juego	18
#11	09/10/2023	Módulo Home	Historial de Juegos	18
#12	09/10/2023	Módulo Home	Pantallas de Carga	12
#13	09/10/2023	Módulo Home	Carga de Contenido	10
#123	20/10/2023	Minijuego Interactivo	Recogiendo Premios Básicos	20
#124	20/10/2023	Minijuego Interactivo	Evitando Hackers	15
#125	20/10/2023	Minijuego Interactivo	Recogiendo Regalos especiales	15
#126	20/10/2023	Minijuego Interactivo	Mejorando Atributos con regalos	15
#127	20/10/2023	Minijuego Interactivo	Niveles de dificultad progresivo	15
#128	20/10/2023	Minijuego Interactivo	Puntuación de los Atributos	20
#129	20/10/2023	Minijuego Interactivo	Elementos gráficos y de sonido	15
Resumen del Product Backlog				
Épicas Totales:			5	
Historias Totales:			22	
Puntos Totales del Desarrollo:			600	

5.3.3.2. Planificación de la pila del sprint (Sprint Backlog)

Para garantizar el flujo de trabajo se consideró dividir el proyecto en 5 Sprint cada uno con sus historias y tareas por cumplir.

Su identificación se considera partiendo de la sigla (DEV) y aumentando dos guiones y un número comenzando desde el número 1 hasta el 5.

5.3.4. Planificación de los Sprints

5.3.4.1. Sprint DEV-001

En el Sprint DEV-001 se completó con éxito, cumpliendo con las actividades detalladas en el mismo, no se produjo ninguna observación, la planificación se la puede observar en la Figura 19

Detalles del Sprint: DEV—001	Fecha de Inicio: 28 de agosto de 2023
	Fecha de Finalización: 07 de septiembre de 2023
Total, de Puntos Asignados: 115	Total, de Puntos Completados: 115

Historia: #16 Contadores de Puntaje		
ID Tarea	Descripción de Tarea	Estado
#41	Asegurar que el puntaje se actualice en tiempo real a medida que el jugador avanza en el juego.	Completado
#40	Desarrollar función para guardar y cargar puntajes máximos, y mostrarlos en pantalla de inicio o tabla de clasificación.	Completado
#36	Diseñar y crear interfaz de usuario para mostrar puntaje del jugador.	Completado
#38	Implementar lógica para disminuir puntaje del jugador por errores o fallos en preguntas.	Completado
#37	Implementar lógica para incrementar puntaje del jugador al responder correctamente preguntas de seguridad.	Completado
#39	Crear animación o efecto visual para realzar cuando puntaje del jugador aumenta.	Completado
Historia: #17 Barras de vida		
ID Tarea	Descripción de Tarea	Estado
#48	Asegurarse de que las barras de vida se actualicen visualmente en tiempo real.	Completado
#47	Añadir la posibilidad de que el jugador pueda ganar vida extra o incrementar la seguridad en el juego a través de ciertos logros o acciones específicas.	Completado
#43	Diseñar y crear las barras de vida que representarán los hitos de la seguridad de la información (CID), Reputación y presupuesto.	Completado
#46	Implementar una función que verifique si las barras de vida llegan a cero, lo que podría significar el fin del juego o la necesidad de reiniciar.	Completado

#45	Implementar lógica para incrementar puntaje del jugador al responder correctamente preguntas de seguridad.	Completado
Historia: #18 Selección de Preguntas		
ID Tarea	Descripción de Tarea	Estado
#31	Diseñar una interfaz para que el jugador seleccione la categoría de preguntas que desea responder.	Completado
#34	Integrar un sistema de retroalimentación para indicar si la respuesta del jugador es correcta o incorrecta.	Completado
#35	Añadir un contador de preguntas respondidas correcta e incorrectamente.	Completado
#30	Crear una base de datos de propuestas de mitigación basadas en los elementos de Magerit.	Completado

Figura 19 Sprint DEV-001

La Figura 9 muestra una visualización de las primeras partes del videojuego.

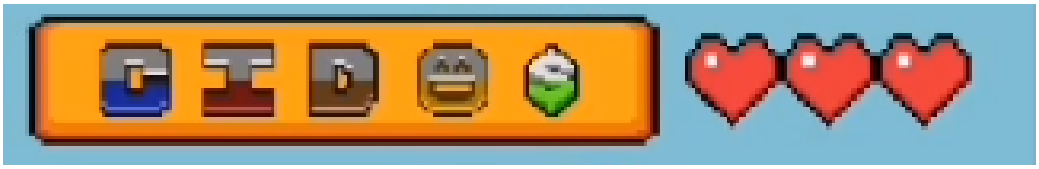


Figura 1 Game UI de indicadores y barras de Vida

5.3.4.2. Sprint DEV-002

En el Sprint DEV-002 se completó con éxito, cumpliendo con las actividades detalladas, no se produjo ninguna observación, la planificación se observa en la Figura 20

Detalles del Sprint: DEV—002	Fecha de Inicio: 11 de septiembre de 2023
	Fecha de Finalización: 21 de septiembre de 2023
Total, de Puntos Asignados: 94	Total, de Puntos Completados: 94
Historia: #21 Guardado de Archivos Locales	
ID Tarea	Descripción de Tarea	Estado
#51	Desarrollar una función de carga para restaurar y descifrar el progreso del juego desde el servidor	Completado
#53	Implementar una función que sobrescriba el catálogo de elementos de Magerit.	Completado
#50	Implementar la función de guardar el progreso del juego, como el puntaje del jugador y el número de rondas que jugo, cifrado en el servidor.	Completado
#49	Diseñar una estructura de directorios para el almacenamiento en el servidor del juego, asegurando que sea organizada y fácil de administrar.	Completado
Historia: #23 Acceso Seguro		
ID Tarea	Descripción de Tarea	Estado
#55	Implementar un sistema de autenticación en el juego, como un inicio de sesión y registro de cuentas de usuario.	Completado
#59	Implementar medidas de seguridad contra ataques comunes, como ataques de fuerza bruta y ataques de inyección de SQL.	Completado

#57	Añadir una capa de seguridad(encriptación) para proteger los datos del usuario.	Completado
#48	Implementar el servicio de Firebase Authentication.	Completado
#118	Añadir una capa de seguridad(encriptación) para proteger el archivo en local que contiene el catálogo de elementos de Magerit	Completado
Historia: #22 Cifrado de Archivos		
ID Tarea	Descripción de Tarea	Estado
#61	Investigar y seleccionar un algoritmo de cifrado adecuado para proteger los archivos del juego.	Completado
#62	Implementar la funcionalidad de cifrado en el juego, de manera que los archivos se cifren al llegar al servidor.	Completado
#63	Desarrollar una función de descifrado para permitir que los archivos cifrados se utilicen en el juego de manera segura.	Completado
#64	Asegurarse de que el cifrado sea lo suficientemente robusto y resistente a ataques de descifrado ilegítimos.	Completado

Figura 20 Sprint DEV-002

La primera visualización de la pantalla de inicio de sesión se presenta en la Figura 21 y los archivos encriptados.

Figura 21 Pantalla de Inicio de Sesión

5.3.4.3. Sprint DEV-003

En el Sprint DEV-003 se completó con éxito, se cumplen las actividades detalladas y no se produjo ninguna observación. La planificación se observa en la Figura 22.

Detalles del Sprint: DEV—003	Fecha de Inicio: 25 de septiembre de 2023
	Fecha de Finalización: 05 de octubre de 2023
Total, de Puntos Asignados: 100	Total, de Puntos Completados: 100

Historia: #12 Comienzo del Juego		
ID Tarea	Descripción de Tarea	Estado
#68	Crear una animación de introducción o una secuencia de inicio para dar la bienvenida a los jugadores.	Completado
#72	Asegurarse de que la pantalla de inicio sea fácil de navegar y esté optimizada para diferentes resoluciones de pantalla.	Completado
#67	Diseñar una pantalla de inicio atractiva que incluya elementos como el nombre del juego, opciones de inicio de sesión, registro de usuarios y un botón para comenzar a jugar.	Completado
Historia: #19 Ciclos		
ID Tarea	Descripción de Tarea	Estado
#68	Establecer condiciones de juego y definir cómo se manejarán.	Completado
#72	Implementar la lógica para avanzar entre las diferentes fases del ciclo de juego.	Completado
Historia: #6 Inicio de Sesión		
ID Tarea	Descripción de Tarea	Estado
#86	Registrar la sesión del usuario y mantenerlo conectado mientras juega.	Completado
#119	Crear funcionalidades para ejecutar y manejar el resultado del inicio de sesión en firebase authentication.	Completado
#83	Implementar la validación de credenciales para garantizar que el inicio de sesión sea seguro.	Completado
#85	Proporcionar mensajes de error claros en caso de credenciales incorrectas o problemas de inicio de sesión.	Completado
#82	Diseñar una interfaz de inicio de sesión que solicite al jugador su dirección de correo electrónico y contraseña.	Completado
Historia: #7 Registro de Usuario		
ID Tarea	Descripción de Tarea	Estado
#92	Proporcionar retroalimentación clara al usuario sobre el éxito del registro y cómo proceder.	Completado
#89	Implementar la validación de datos durante el registro para garantizar la integridad de la información.	Completado
#91	Enviar una confirmación de correo electrónico al usuario registrado para verificar la dirección de correo electrónico (si es necesario).	Completado
#88	Diseñar una interfaz de registro de usuarios que solicite la información necesaria, como nombre, dirección de correo electrónico y contraseña.	Completado

#90	Crear funcionalidades para ejecutar y manejar el resultado del registro de usuario en firebase authentication.	Completado
Historia: #8 Recuperación de Contraseña		
ID Tarea	Descripción de Tarea	Estado
#93	Crear una función de recuperación de contraseñas que permita a los usuarios restablecer sus contraseñas en caso de olvido.	Completado
#95	Enviar un correo electrónico al usuario con un enlace seguro para restablecer su contraseña.	Completado

Figura 22 Sprint DEV-003

La Figura 23 y la Figura 24 presenta una visualización de la pantalla de registro de nuevo usuario con los controles de validación.

Figura 23 Pantalla de Registro de Usuario


Verifica el correo electrónico para whatifwilsonyepez

De noreply@whatifwilsonyepez.firebaseapp.com
a WILSON RAUL YEPEZ PONCE

Hola, PRYW:

Visita este vínculo para verificar tu dirección de correo electrónico.

https://whatifwilsonyepez.firebaseapp.com/__/auth/action?mode=verifyEmail&oobCode=qg1Zpve5CpRElscbAPpY3gl2OZvlD5GLoJpO-pecKX0AAA(
9jQ&apiKey=AIzaSyDwgcCcsPRFVjjmEskm6loCvEJKxBS5qPY&lang=es-419

Si no solicitaste la verificación de esta dirección, ignora este correo electrónico.

Gracias.

El equipo de whatifwilsonyepez

Figura 24 Correo de Verificación de Correo

5.3.4.4. Sprint DEV-004

En el Sprint DEV-004 se completó con éxito, cumpliendo con las actividades detalladas en el mismo, no se produjo ninguna observación, la planificación se la puede observar en la Figura 25.

Detalles del Sprint: DEV—004	Fecha de Inicio: 09 de octubre de 2023 Fecha de Finalización: 20 de octubre de 2023
Total, de Puntos Asignados: 58	Total, de Puntos Completados: 58

Historia: #10 Nuevo Juego		
ID Tarea	Descripción de Tarea	Estado
#102	Proporcionar retroalimentación al jugador sobre el inicio exitoso del nuevo juego.	Completado
#98	Diseñar una opción en la pantalla de inicio para que los jugadores creen un nuevo juego.	Completado
#100	Iniciar un nuevo ciclo de juego con un puntaje y configuración predeterminados.	Completado
Historia: #11 Historial de Juegos		
ID Tarea	Descripción de Tarea	Estado
#107	Diseñar una interfaz que nuestre la tabla del histórico de puntajes del jugador.	Completado
#103	Diseñar una sección en el menú principal que muestre el historial de juegos del jugador.	Completado
#104	Almacenar información relevante de cada partida, que contendrá el hito de derrota, el puntaje y la cantidad de rondas superadas.	Completado
#105	Desarrollar un algoritmo que permita a los jugadores ver detalles de partidas anteriores, como resultados y estadísticas.	Completado
Historia: #13 Pantallas de Carga		
ID Tarea	Descripción de Tarea	Estado
#108	Diseñar pantallas de carga atractivas con elementos visuales, como barras de progreso o animaciones, para mantener a los jugadores comprometidos mientras se carga el juego.	Completado
#110	Desarrollar pantallas de carga intermedias que se muestren al cargar niveles o recursos adicionales en el juego.	Completado
#112	Optimizar los tiempos de carga tanto como sea posible para brindar una experiencia de juego fluida.	Completado
#111	Asegurarse de que las pantallas de carga sean informativas y proporcionen consejos o información relevante mientras se espera.	Completado
Historia: #14 Cargar el Contenido		
ID Tarea	Descripción de Tarea	Estado
#116	Asegurarse de que el guardado de archivos sea compatible con el sistema.	Completado
#120	Implementar la funcionalidad para cargar los resultados de la partida al servidor.	Completado

#121	Encriptar los datos al finalizar la partida con contraseña única.	Completado

Figura 25 Sprint DEV-004

La Figura 26, muestra la generación de una de las pantallas de carga y la del nuevo juego de Dorps.

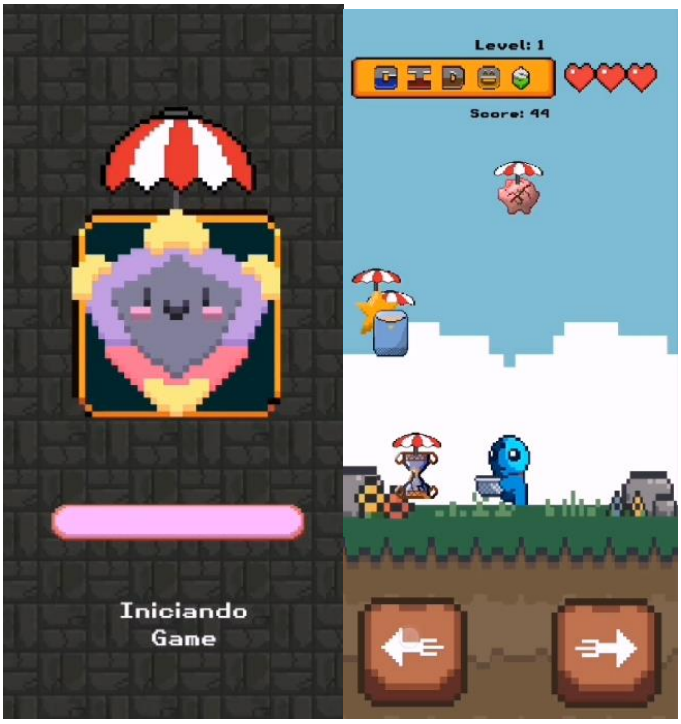


Figura 26 Pantallas de Carga de contenidos y Juego Drops

5.3.4.5. Sprint DEV-005

El último Sprint DEV-005 se completó con éxito, cumpliendo con las actividades detalladas en el mismo, no se produjo ninguna observación, la planificación se observa en la Figura 27.

Detalles del Sprint: DEV—005	Fecha de Inicio: 20 de octubre de 2023
	Fecha de Finalización: 03 de noviembre de 2023
Total, de Puntos Asignados: 110	Total, de Puntos Completados: 110

Historia: #129 Elementos gráficos y sonido		
ID Tarea	Descripción de Tarea	Estado
#146	Además, deseo que la música y los efectos de sonido se ajusten al tono del juego, contribuyendo a una experiencia envolvente.	Completado
#145	Quiero disfrutar de gráficos coloridos y atractivos que hagan que la experiencia de juego sea visualmente agradable.	Completado
Historia: #128 Puntuación de atributos		
ID Tarea	Descripción de Tarea	Estado

#144	Esperar ver iconos que me muestren mi estado actual.	Completado
#143	Como jugador, se quiere que mi puntuación se registre.	Completado
Historia: #127 Niveles de dificultad progresiva		
ID Tarea	Descripción de Tarea	Estado
#142	Los hackers podrían volverse más rápidos o numerosos, mientras que los premios podrían ser más difíciles de alcanzar, manteniendo el desafío a medida que progreso.	Completado
#141	Deseo experimentar un aumento gradual en la dificultad a medida que avanzo en el juego.	Completado
Historia: #126 Mejora de Atributos con regalos		
ID Tarea	Descripción de Tarea	Estado
#135	Puedo utilizar los regalos y acumular beneficios.	Completado
#134	Como jugador, quiero poder usar los regalos recolectados para mejorar las habilidades y atributos de mi personaje.	Completado
Historia: #125 Recogiendo regalos especiales		
ID Tarea	Descripción de Tarea	Estado
#140	Estos regalos podrían incluir mejoras para las estadísticas base.	Completado
#139	Quiero encontrar regalos especiales dispersos en el juego que brinden beneficios mi personaje.	Completado
Historia: #124 Evitando hackers		
ID Tarea	Descripción de Tarea	Estado
#138	Al perder vida, espero ver una animación o efecto que indiqué claramente que cometí un error y que debo evitar a los hackers.	Completado
#137	Como jugador, quiero que mi personaje pierda vida si recolecta un hacker en lugar de un premio.	Completado
Historia: #123 Recogiendo Premios Básicos		
ID Tarea	Descripción de Tarea	Estado
#138	Como jugador, quiero poder controlar a mi personaje pequeño para que pueda recolectar premios básicos en el juego.	Completado
#137	Cada premio recolectado aumentará mi puntaje total, brindándome una sensación de logro.	Completado

Figura 27 Sprint DEV-005

Generando ya la versión completa del videojuego (Figura 28), listo para las pruebas con los estudiantes.

Figura 28 Capturas del videojuego Terminado

5.3.5. Implementación de la Arquitectura de la solución

Para la Arquitectura del videojuego se plantea le uso de las varias herramientas como se detalló en el documento de diseño anteriormente, además para mejorar la compresión de la arquitectura se ha elaborado una imagen para mostrar la arquitectura en la que se basa el videojuego What If como se muestra en la Figura 29.

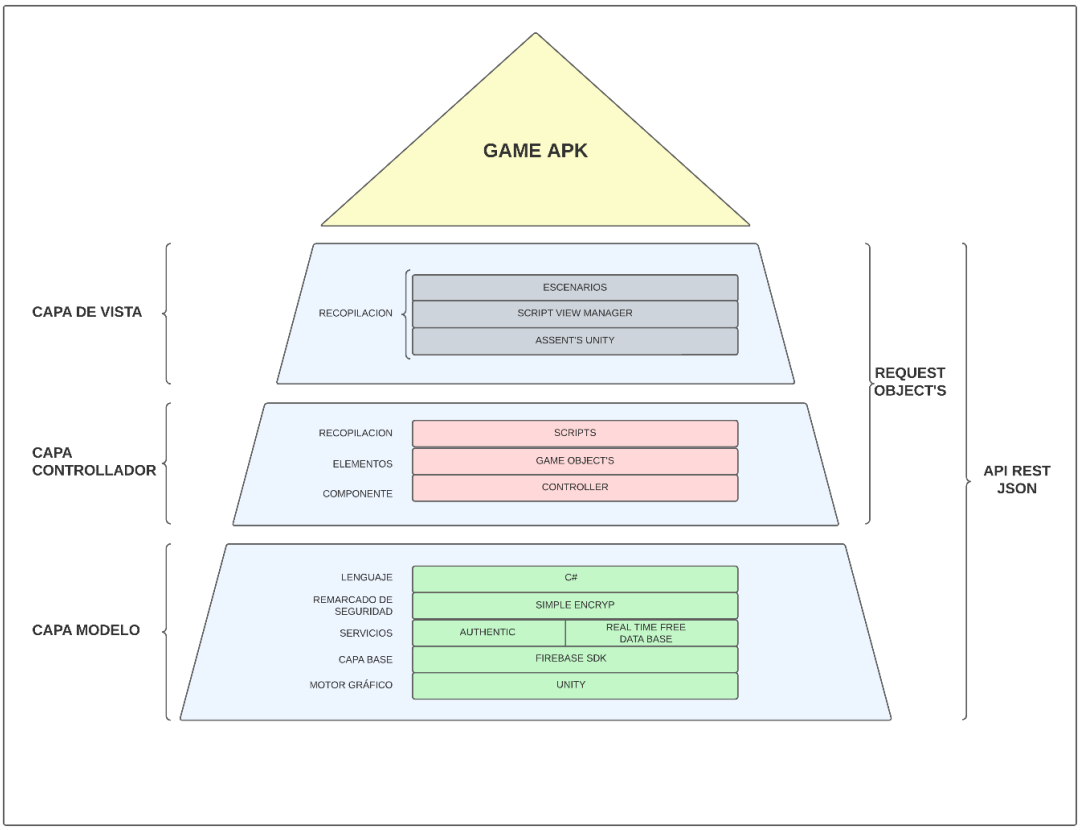


Figura 29 Imagen de Arquitectura de la aplicación What If, Autor Propia

Como se puedo observar en el anterior grafico la aplicación se compone en un modelo MVC, en el capa modelo se tiene toda la parte de lógica de juego y recursos como las bases de datos los servicios de autenticación, entre otros, después se cuenta con la capa de controlador, en esta se encuentran los componente que servirán para comunicar la información de la capa modelo con la capa de vista y finalmente se tiene la capa de vista donde se tendrá todos los elementos con los que nuestro público objetivo podrá interactuar.

5.3.6. Implementación de Diseño de Datos

Para el diseño de como estarán distribuidos los datos y al utilizar el servicio de Firebase RealTime DataBase base de datos almacenada por nodos, se planteó dividir la base en dos áreas para poder manejar los controles de seguridad con mayor efectividad, separando la base de datos en dos nodos principales.

5.3.6.1. Private Data

Nodo destinado para el almacenamiento de información esencial para la aplicación con la base de datos de las mitigaciones que se mostrarán en el juego y los catálogos de TIP de ciberseguridad para la enseñanza dentro del juego, este nodo tendrá protecciones contra escritura de cualquier usuario, pero sí de lectura solo para los usuarios que se han autenticado satisfactoriamente.

5.3.6.2. Public Data

En este nodo está destinado para almacenar los datos de los jugadores, pese a que los datos de los jugadores se encuentran encriptados, se ha creado las reglas para que solo usuarios autenticados puedan leer y escribir.

Dando como resultado la siguiente expresión para las reglas que se mostrara a continuación en la Figura 30.

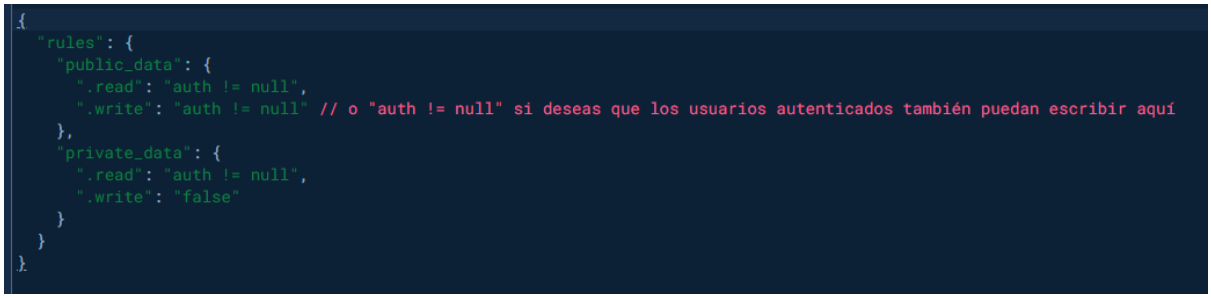


Figura 30 Reglas de Seguridad Firebase RealTimeDataBase

5.3.7. Reporte Postmortem

5.3.7.1. Descripción del Producto

Con el propósito de fortalecer la cultura en ciberseguridad de los estudiantes de la carrear de software de la Universidad, se ha desarrollado un videojuego con una estética retro de 8 bits que fusiona con mecánicas modernas llamado “What IF”, se espera que a través de este juego poder capturar la atención de los estudiantes, el flujo de la aplicación se explica al detalle más adelante.

Aquí se muestra cuál va a ser el fujo que tendrá el jugador dentro de la aplicación desde la descarga de la aplicación, que dado el alcance del proyecto solo es para Android. Posteriormente el registro de la cuenta en los servicios de la nube y el correspondiente inicio de sesión; después el jugador entra a una pantalla de carga que verifica si los datos almacenados en local están actualizados y en caso de no estarlos son descargados y posteriormente actualizados. A continuación ingresa en un menú de inicio donde es posible elegir entre iniciar una nueva partida, ver historial de partidas, leer cómo jugar o mirar los créditos; si selecciona nueva partida, se carga una pantalla donde el avatar del jugador debe esquivar los ítems “malos” y tomar los buenos, hasta que obtenga un Ítem Premium el cual le muestra un Tip del área que pertenece y cambia a la escena de la elección de la mitigación donde el jugador mediante el deslizamiento del dedo puede elegir entre aceptarla o rechazarla, en cualquiera de los casos si no ha perdido antes regresa a la pantalla de la “Lluvia de Drops”, pero en caso de perder se dirige a la pantalla de game over y retorna a la pantalla del menú de inicio.

5.3.7.2. Restricciones

Con el fin de preservar el flujo adecuado de los jugadores dentro de la aplicación, el juego mantiene algunas restricciones como:

- Necesidad obligatoria de verificar el correo electrónico por seguridad de las cuentas de los jugadores.
- Mantener las reglas de seguridad en el Servicio de Realtime Database, para evitar modificaciones mal intencionadas.
- Restringir la creación de cuentas a solo una cuenta por correo, para evitar saturación del servicio.
- Conexión a Internet obligatoria, para mantener los datos catálogos actualizados, datos sensibles y descargar el historial del jugador.
- Permisos de Escritura a la aplicación para guardar una copia de los datos (encriptados).

CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- El catálogo Magerit se puede integrar efectivamente mediante el uso de las mitigaciones como propuestas dentro del escenario del videojuego, evitando que el juego se convierta en una clase de trivia, pero sin interferir en que los estudiantes comprendan de manera visual las consecuencias de las diferentes amenazas.
- Para una enseñanza de calidad es necesario abordar la mayor cantidad de elementos en este caso el 100% de los elementos como se expresa en la Figura 17, de tal manera que la enseñanza no se enfoque solo en elementos comunes, sino que los estudiantes puedan desarrollar una compresión muy amplia de los riesgos que existen en el mundo.
- Pese a la cantidad de aspectos para la creación de videojuegos envolvente, es una tarea realmente compleja, dado que se requiere ejecutar de manera precisa y efectiva, logrando cautivar al espectador.
- Los videojuegos pueden lograr un impacto en la cultura de los estudiantes, como se ve demostrado en la Tabla 19 donde un 93,5% de los estudiantes han comentado que el videojuego ha cambiado su percepción de la importancia de la ciberseguridad.

6.2. Recomendaciones

- Para futuros desarrollo se podría plantear la integración de otras metodologías o alguna herramienta de tal manera que el juego se adapte a un rango de captación mayor.
- Incrementar la cantidad de mitigaciones de los elementos (contenido nuevo) dependiendo de los avances tecnológicos futuros, para evitar que se interrumpa el atractivo del videojuego y entre a etapa de abandono.
- Implementar nuevas mecánicas o minijuegos para variar el tipo de partida que los jugadores se podría encontrar o la integración de nuevos personajes, aumentado el guion argumental del videojuego.
- Los videojuegos pueden lograr un impacto en la cultura de los estudiantes, como se ve demostrado en la Tabla 19 donde un 93,5% de los estudiantes han comentado que el videojuego ha cambiado su percepción de la importancia de la ciberseguridad.

Bibliografía

Albert T. Franch. (2020). *Introducción al Diseño de Videojuegos*.

Andalucía, D. (2018). *7 plataformas con las que crear juegos para móviles*. https://www.blog.andaluciaesdigital.es/crear-juegos-para-moviles/

Anderson, C. A., & Dill, K. E. (2000). Video Games and Aggressive Thoughts, Feelings, and Behavior in the Laboratory and in Life. *Journal of Personality and Social Psychology*, *78*(4), 772–790. https://doi.org/10.1037//O022-3514.78.4.772

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Avast Security. (2022). *¿Qué es el algoritmo hash MD5 y cómo funciona?* | *Avast*. https://www.avast.com/es-es/c-md5-hashing-algorithm

Bruce Schneier. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Cloudflare. (2020). *¿Qué es la encriptación?* | *Cloudflare*. https://www.cloudflare.com/es-es/learning/ssl/what-is-encryption/

Secretaría General de Administración Digital. (2012a). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. http://administracionelectronica.gob.es/

Secretaría General de Administración Digital. (2012b). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de elementos*. http://administracionelectronica.gob.es/

Secretaría General de Administración Digital. (2012c). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas*. http://administracionelectronica.gob.es/

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification." *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek 2011*, 9–15. https://doi.org/10.1145/2181037.2181040

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *APA PsycInfo*, 413–422.

Equipo Panda Security. (2022, October). *¿Por qué la ciberseguridad sigue siendo importante?* https://www.pandasecurity.com/es/mediacenter/ciberseguridad-importante/

Gee, J. P. (2003). What video games have to teach us about learning and literacy. *Computers in Entertainment*, *1*(1), 20–20. https://doi.org/10.1145/950566.950595

Gestionet. (2019). *SERIOUS GAMES: qué son, ejemplos y tipos - GESTIONET*. https://gestionet.net/serious-games-blog/

Hard Zone. (2023). *Cifrado AES-256 bits, cómo funciona y ¿es realmente seguro?* https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/

ITELCA. (2020). *La importancia de la ciberseguridad en las Instituciones Educativas – Itelca*. https://www.itelca.com.co/la-importancia-de-la-ciberseguridad-en-las-instituciones-educativas/

Kinsta®. (2023). *¿Qué es la Encriptación de Datos? Definición, Tipos y Buenas Prácticas.* https://kinsta.com/es/base-de-conocimiento/que-es-la-encriptacion/

Michael E. Whitman, & Herbert J. Mattord. (2018). *Principles of Information Security* (1st ed., Vol. 1).

Ministerio de Telecomunicaciones. (2021). *ACUERDO MINISTERIAL 006-2021*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

National Institute of Standards and Technology (NIST). (2001). ADVANCED ENCRYPTION STANDARD (AES). *National Institute of Standards and Technology (NIST)*.

Official Journal of the European Union. (2018). EU General Data Protection Regulation (GDPR). *Official Journal of the European Union.*

Pearson. (2023). *Aprendizaje inmersivo: destrezas y valores en los videojuegos educativos*. https://blog.pearsonlatam.com/en-el-aula/destrezas-valores-con-los-juegos-educativos

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 120–126.

Rondón Quiñonez, C. A. (2020). *El videojuego como experiencia inmersiva*. https://repository.upb.edu.co/handle/20.500.11912/9453

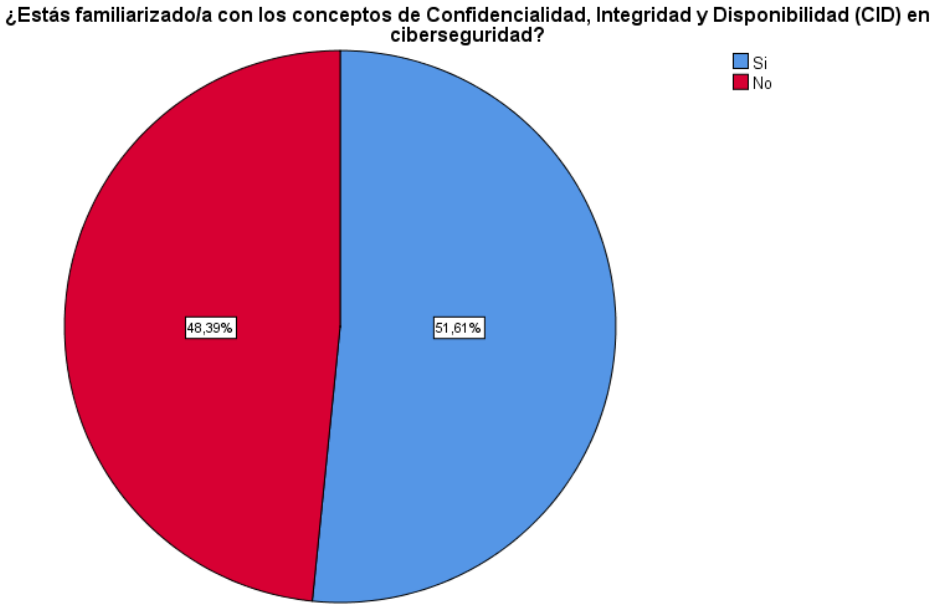
SafetyCulture. (2022). *Gestión de riesgos: Qué es y por qué es importante | SafetyCulture*. https://safetyculture.com/es/temas/gestion-de-riesgos/

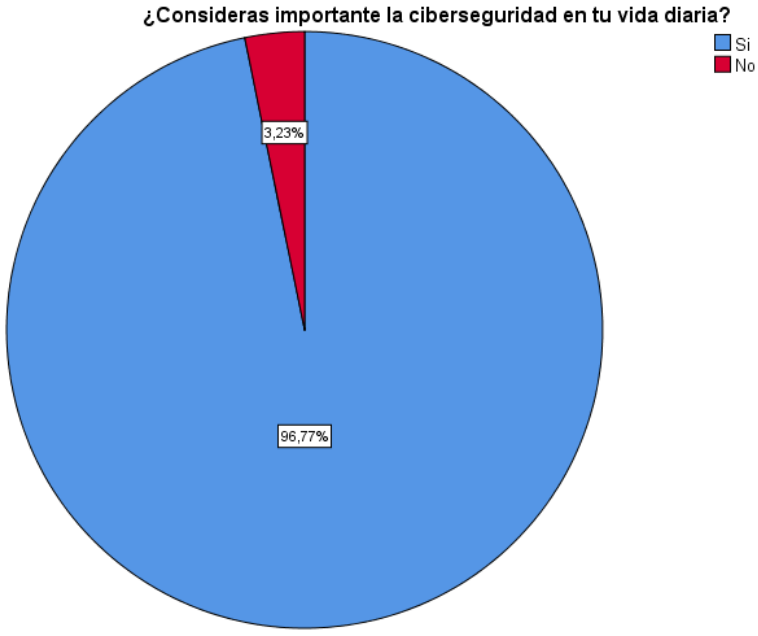
Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital). (2012). *PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Shanika Wickramasinghe. (2023). *RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained | Splunk*. https://www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html

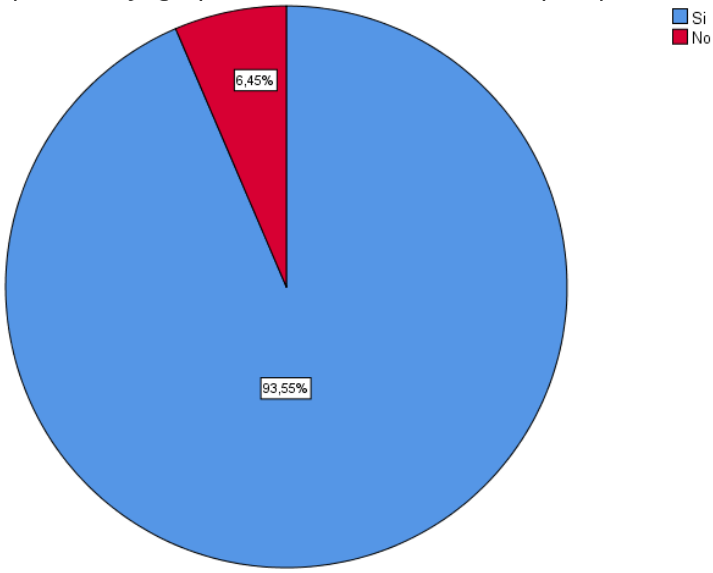
Anexos

A1. Tabulación Evaluación Pre-Exposición al videojuego

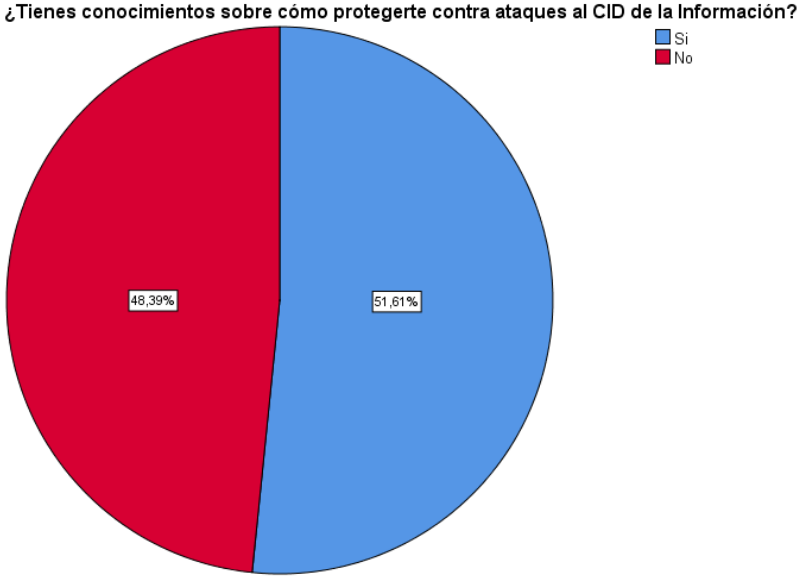


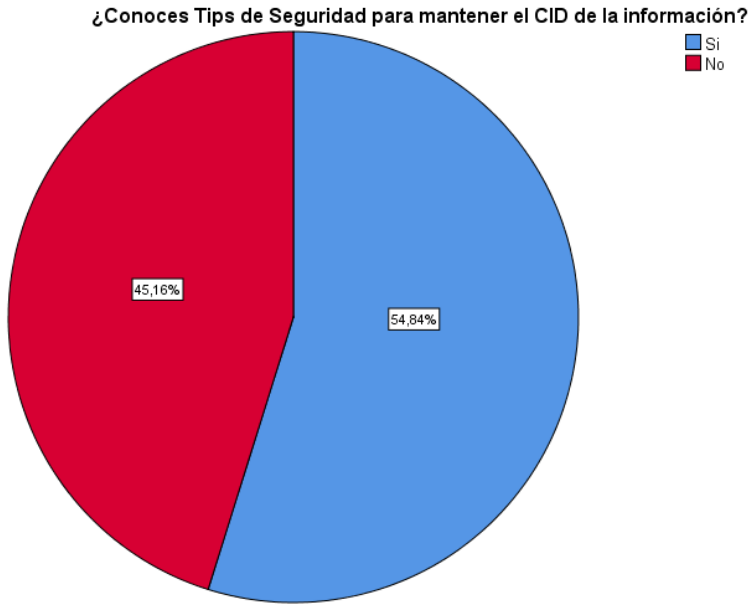


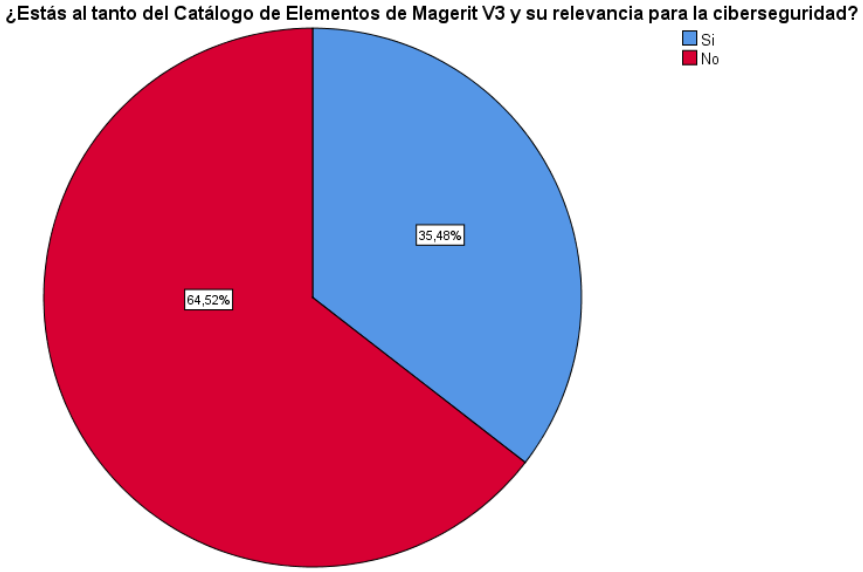
¿Crees que los videojuegos pueden ser una herramienta efectiva para aprender sobre ciberseguridad?

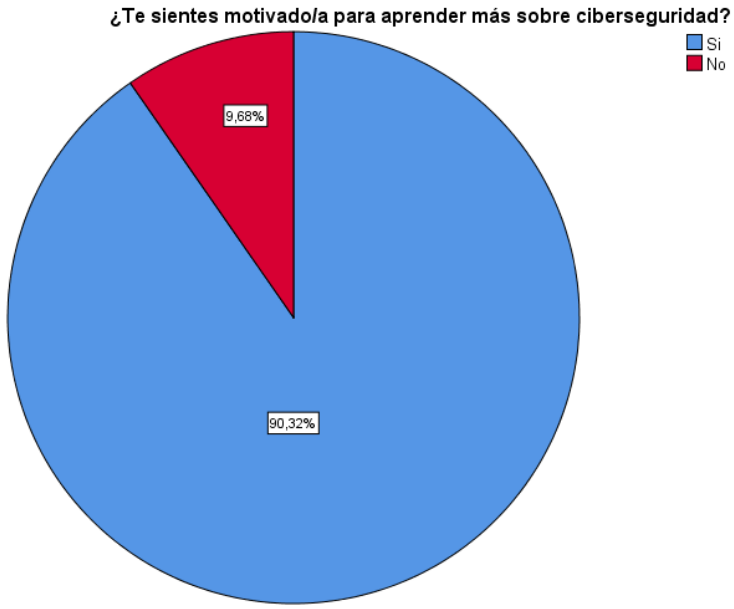


¿Tienes conocimientos sobre cómo protegerte contra ataques al CID de la Información?

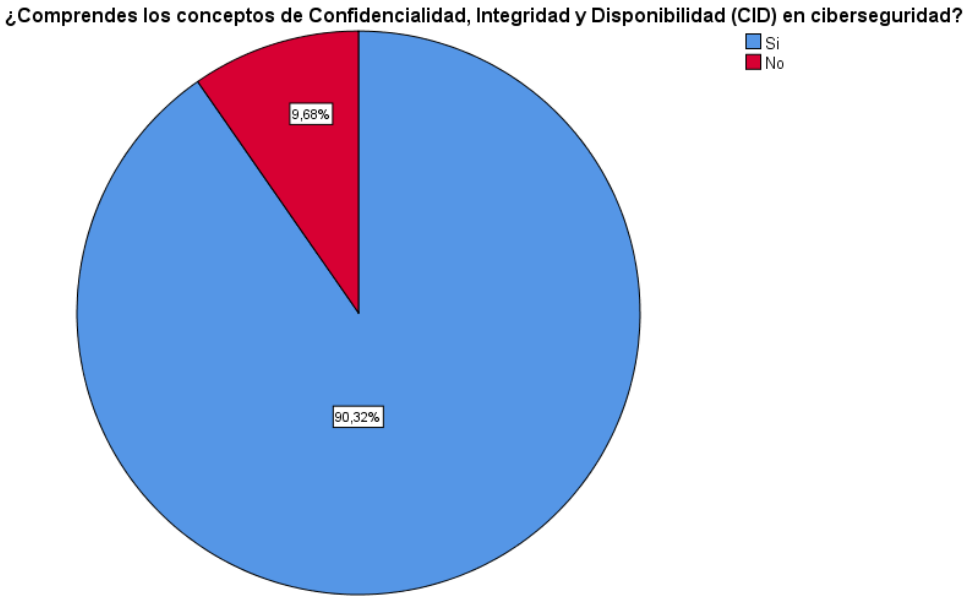



¿Conoces Tips de Seguridad para mantener el CID de la información?
Si
No
45,16%
54,84%

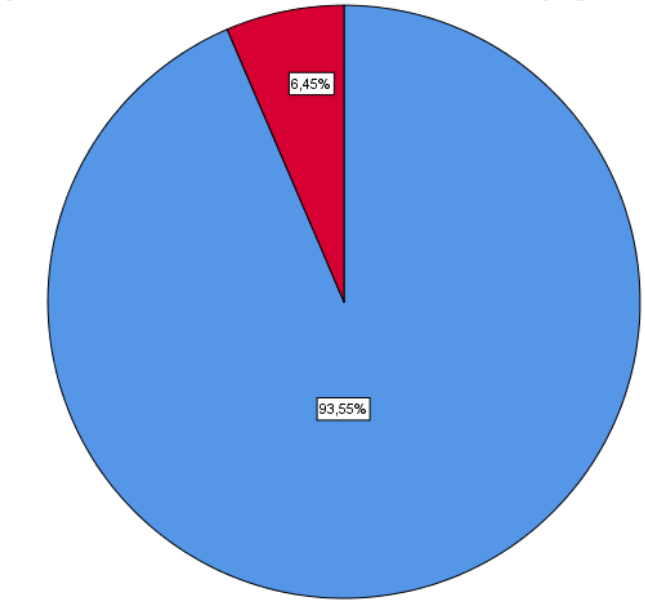

¿Estás al tanto del Catálogo de Elementos de Magerit V3 y su relevancia para la ciberseguridad?
Si
No
35,48%
64,52%



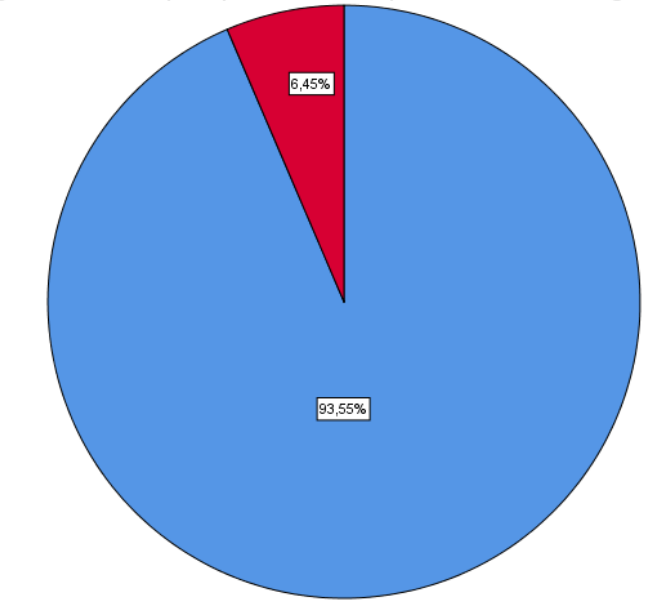
A2. Tabulación Evaluación Post-Exposición al videojuego



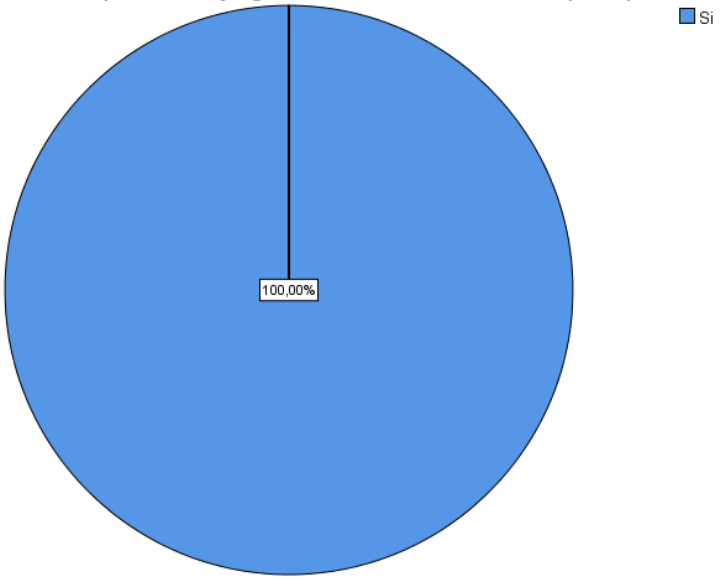
¿Pudiste identificar cómo las decisiones tomadas en el juego afectaron la CID de la información?



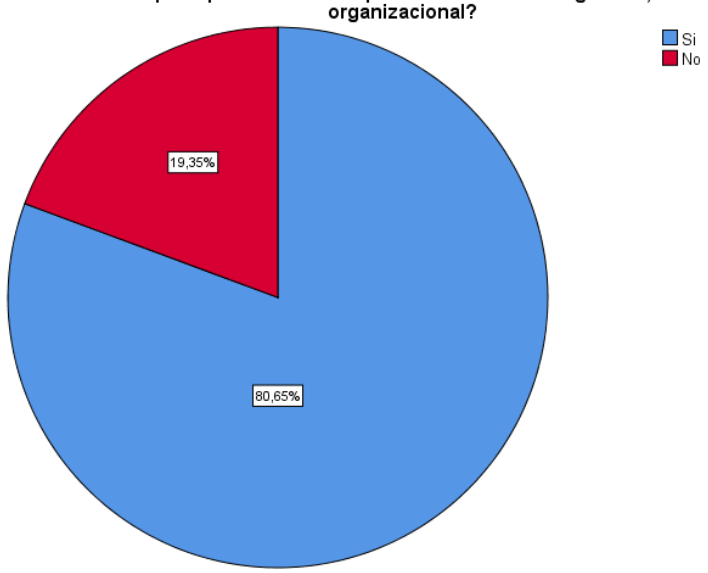
¿Ha cambiado tu percepción sobre la importancia de la ciberseguridad en tu vida diaria tras jugar?



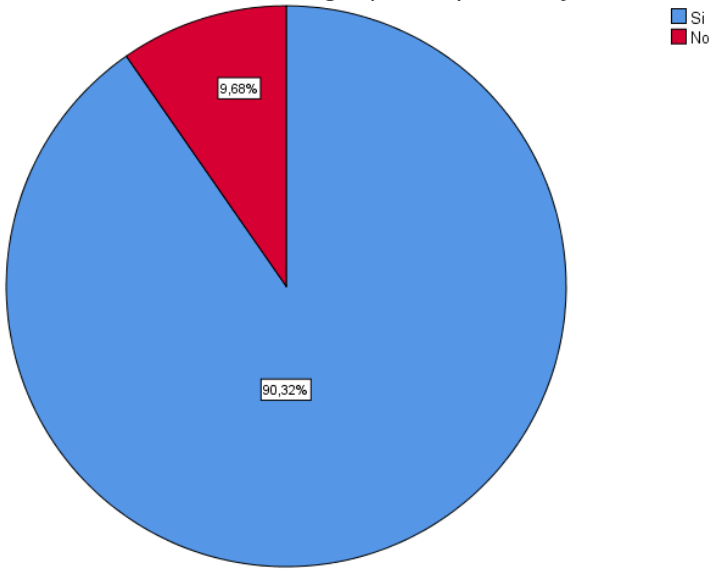
¿Consideras ahora que los videojuegos son una herramienta efectiva para aprender sobre ciberseguridad?



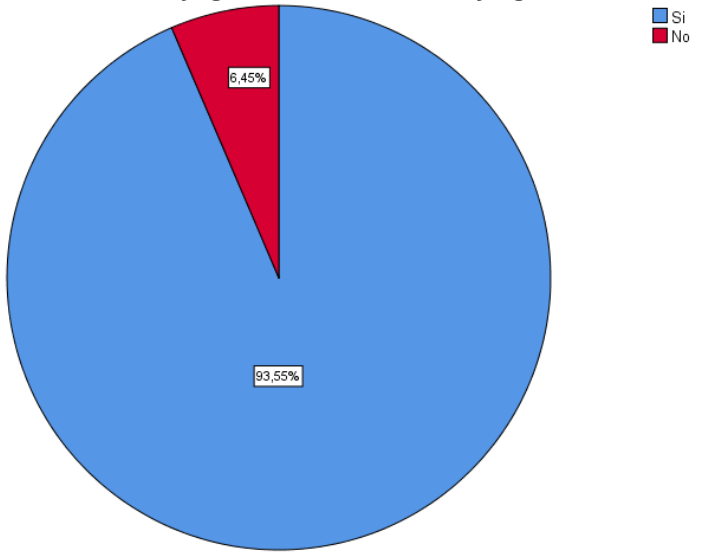
¿El juego ha influenciado tu percepción sobre la importancia de la ciberseguridad, tanto a nivel personal como organizacional?

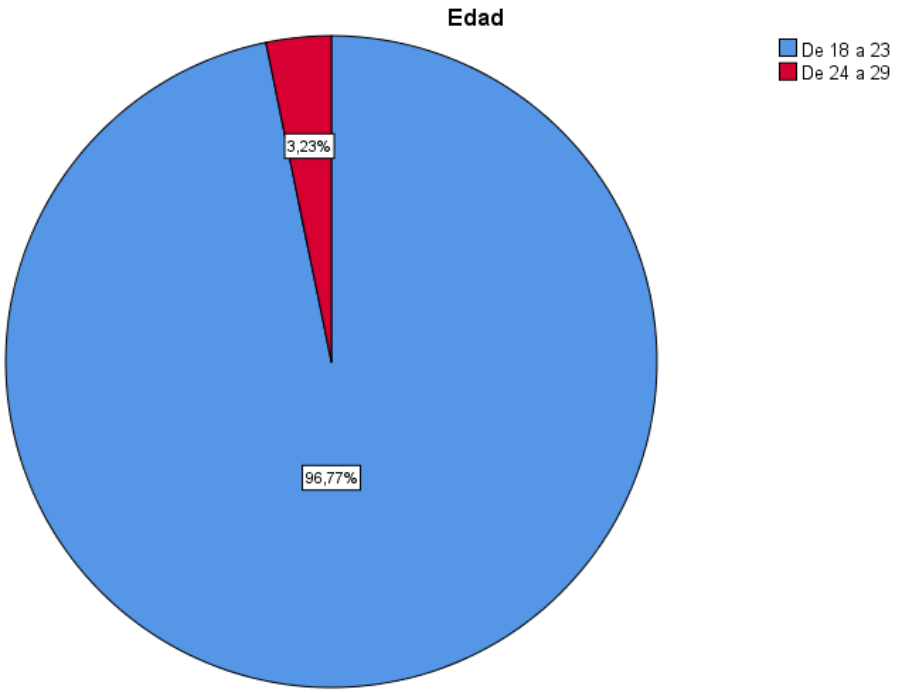


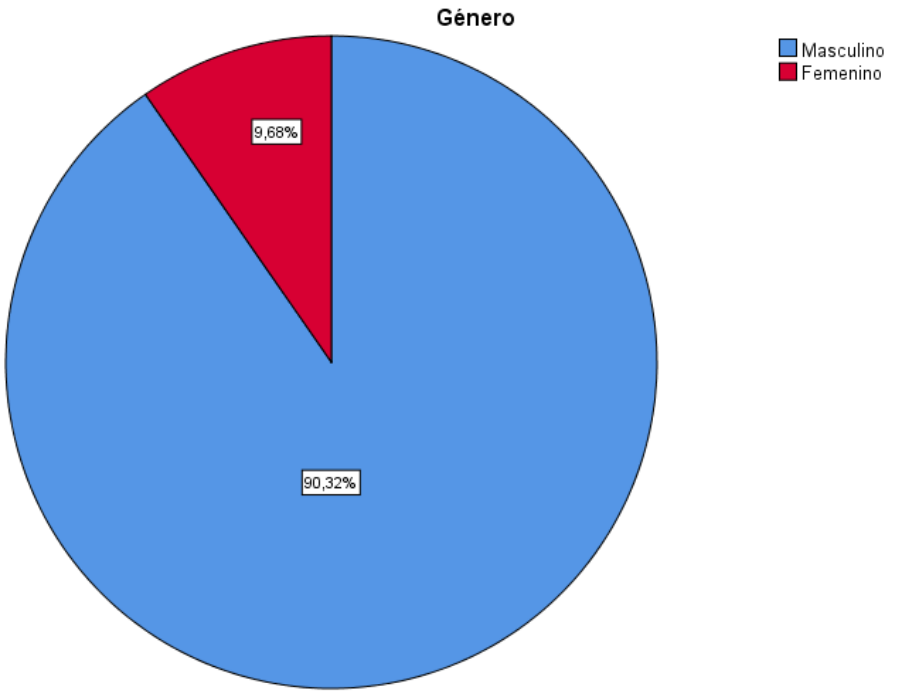
¿Consideras útil el contenido basado en Magerit para comprender mejor las amenazas de ciberseguridad?



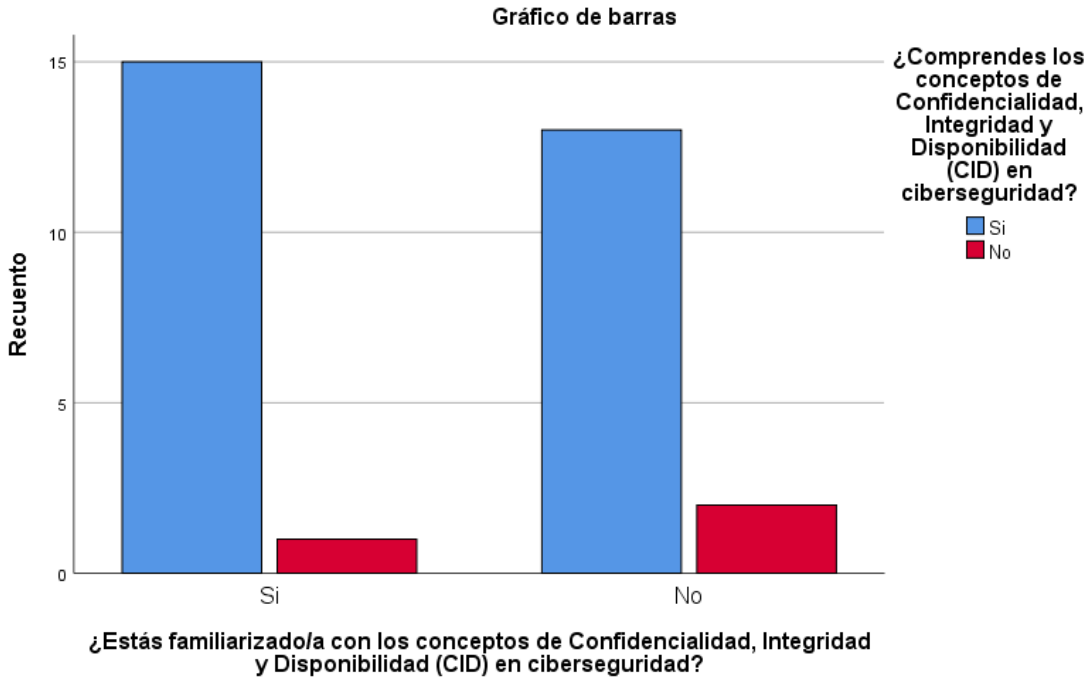
¿Te ha motivado el videojuego a buscar más información y seguir educándote en ciberseguridad?

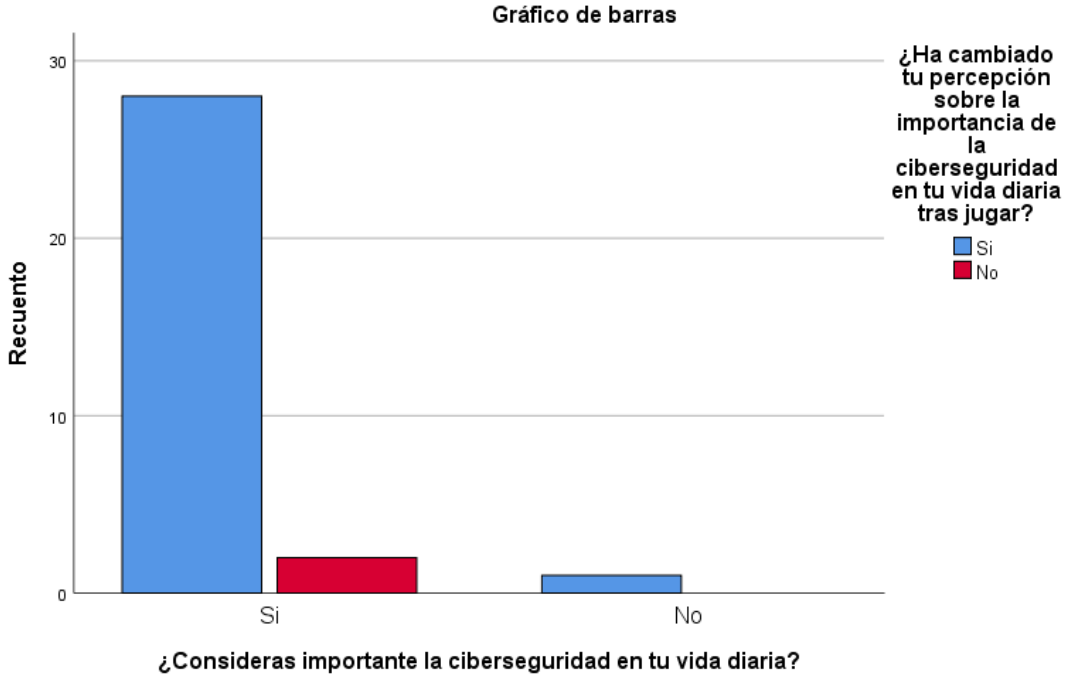



Edad
De 18 a 23
De 24 a 29
3,23%
96,77%


Género
Masculino
Femenino
9,68%
90,32%

A3. Graficas Correlaciones





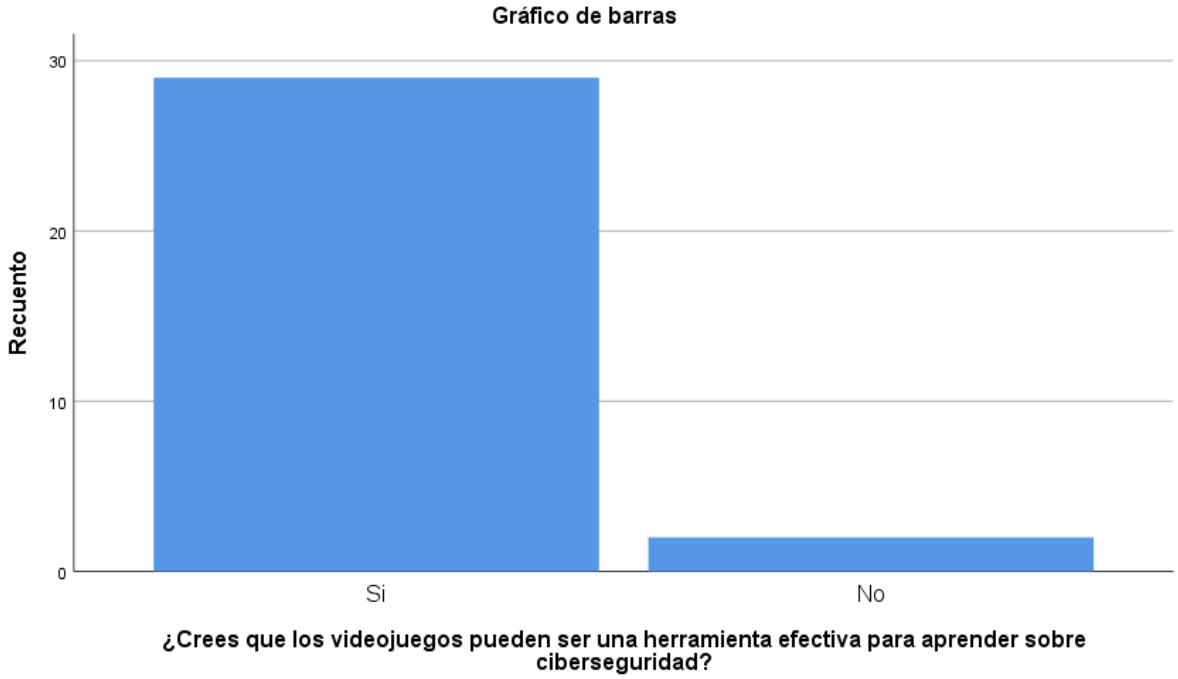


Gráfico de barras
Recuento
30
20
10
0
Si
No
¿Crees que los videojuegos pueden ser una herramienta efectiva para aprender sobre ciberseguridad?

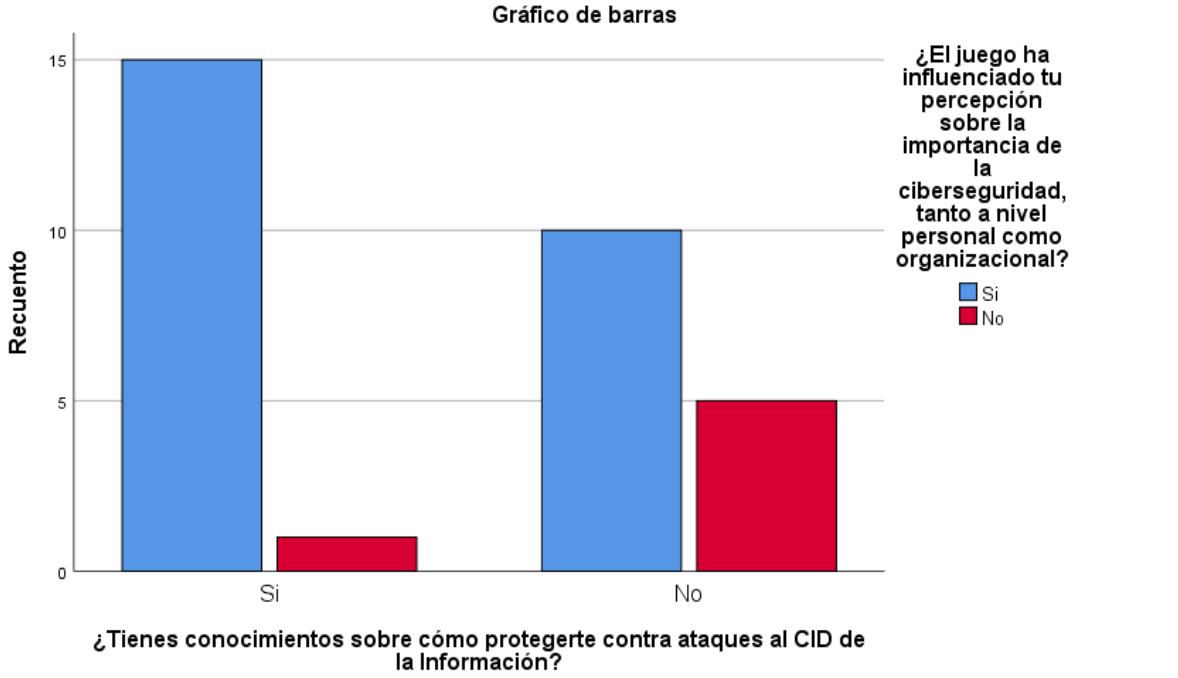
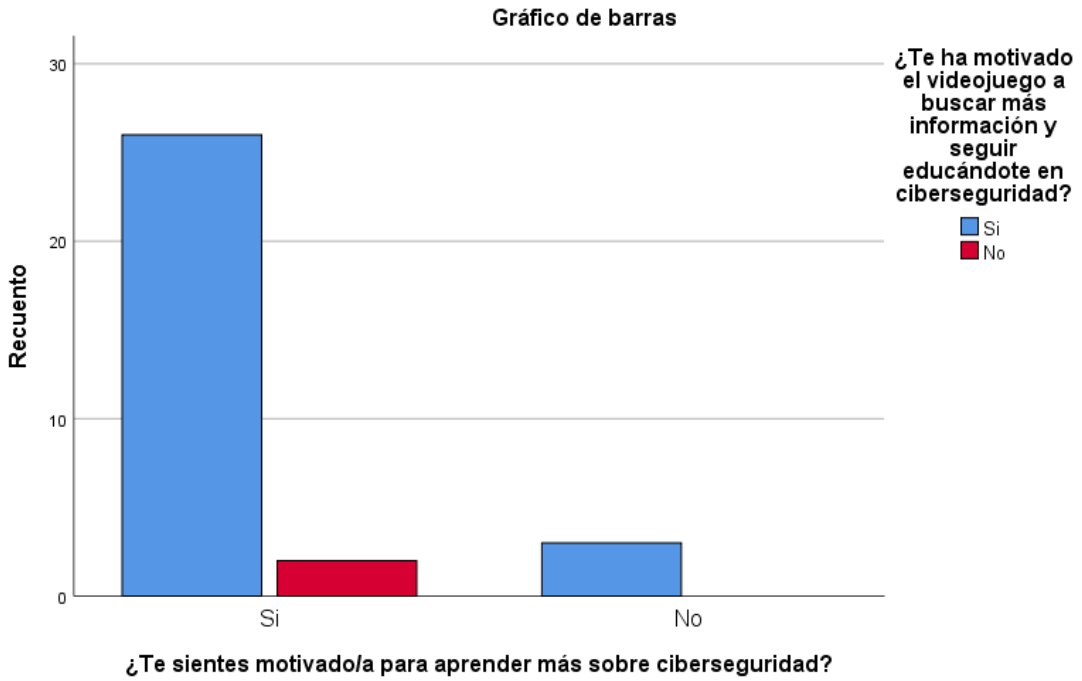


Gráfico de barras
Recuento
15
10
5
0
Si
No
¿El juego ha influenciado tu percepción sobre la importancia de la ciberseguridad, tanto a nivel personal como organizacional?
Si
No
¿Tienes conocimientos sobre cómo protegerte contra ataques al CID de la Información?



A4. Tablas de Análisis de Mitigaciones.

Bloque 1: Desastres Naturales

Tabla 26 Análisis Mitigaciones: Desastres Naturales

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Invertir en infraestructuras más resistentes y sistemas de alerta temprana	Aumentará la disponibilidad (+20) y la integridad (+5) de los servicios, pero requerirá una inversión significativa (-30). La aprobación de las personas aumentará (+5), al sentirse más seguros.	Se mantendrá el riesgo de interrupciones (-20) y se ahorrará dinero a corto plazo (+20), pero los empleados y ciudadanos se sentirán menos seguros (-10).
Implementar un plan de evacuación y respuesta de emergencia más efectivo	Mejorará la disponibilidad (+15) y la integridad (+5), y aumentará la confianza de las personas (+10), pero requerirá inversión (-20).	Aumentará el riesgo de tiempo de inactividad (-15) y ahorrará dinero a corto plazo (+10), pero disminuirá la confianza y seguridad percibida (-10).
Programas de educación pública sobre preparación para desastres	Aumentará la disponibilidad (+10), la integridad (+5) y significativamente la aprobación de las personas (+15), aunque requerirá inversión (-20).	Disminuirá la preparación y resiliencia de la comunidad (-10), pero ahorrará dinero a corto plazo (+15), aunque podría disminuir ligeramente la confianza y seguridad percibida (-5).

Bloque 2: Fuego de Origen Natural

Tabla 27 Análisis Fuego de Origen Natural

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Mejorar la vigilancia y el control de áreas propensas a incendios	Mejorará significativamente la disponibilidad (+20) y la integridad (+10) de las instalaciones y los servicios, pero implicará un costo adicional (-30). La aprobación de las personas aumentará (+10) al sentirse más seguros.	Mantener la situación actual podría llevar a daños graves en caso de incendio (-30), aunque se ahorraría dinero a corto plazo (+20), pero los empleados y clientes podrían sentirse menos seguros (-10).
Invertir en tecnologías y equipos de extinción de incendios más avanzados	Aumentará la disponibilidad (+15) y la integridad (+15) de las instalaciones y los servicios, aunque requerirá una inversión considerable (-30). Los empleados y clientes se sentirán más seguros, aumentando la aprobación (+10).	No hacer esta inversión podría resultar en una respuesta ineficiente en caso de incendio (-25), se ahorraría dinero a corto plazo (+15), pero podría disminuir la confianza y seguridad percibida (-10).
Establecer barreras naturales o artificiales para prevenir la propagación de incendios	Mejorará la disponibilidad (+20) y la integridad (+10), protegiendo las instalaciones y servicios, pero requerirá inversión y planificación (-25). Aumentará la confianza y seguridad percibida (+15).	No hacerlo podría resultar en una mayor vulnerabilidad a los incendios forestales (-20), se ahorraría dinero a corto plazo (+20), pero podría disminuir la confianza y seguridad percibida (-10).

Bloque 3: Daños por Agua de Origen Natural

Tabla 28 Análisis Daños por Agua de Origen Natural

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Construir o mejorar infraestructuras de control de inundaciones	Aumentará la disponibilidad (+20) y la integridad (+10) de las instalaciones y servicios, reduciendo el riesgo de daños por inundaciones. Sin embargo, requerirá una inversión considerable (-30). La aprobación de las personas aumentará (+5), ya que se sentirán más seguras.	No realizar estas mejoras podría resultar en daños graves por inundaciones (-30) y pérdida de datos, pero se ahorraría dinero a corto plazo (+20). Los empleados y clientes podrían sentirse menos seguros (-10).
Revisar y actualizar los planes de respuesta a inundaciones	Contribuirá a la integridad (+10) y permitirá una respuesta más eficiente en caso de inundaciones. Requerirá inversión en revisión y	La falta de revisión podría resultar en una respuesta ineficiente en caso de inundaciones (-15), aunque ahorraría dinero a corto plazo

	actualización (-20). La aprobación de las personas aumentará (+5) al sentirse más seguras.	(+10). Los empleados y clientes podrían sentirse menos seguros (-10).
Desarrollar programas de concienciación sobre riesgos de inundación y medidas de seguridad	Aumentará la concienciación y preparación de las personas (+15), lo que puede mejorar la respuesta a inundaciones. Requerirá inversión en programas (+10) y tiempo para educar al personal y al público (-10).	No desarrollar programas de concienciación podría resultar en una menor preparación y una respuesta más lenta (-10), aunque ahorraría dinero a corto plazo (+10). La concienciación y seguridad percibida aumentarán ligeramente (+5).

Bloque 4: Desastres Naturales de Origen Industrial

Tabla 29 Análisis Desastres Naturales de Origen Industrial

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Implementar protocolos de seguridad industrial más estrictos	Aumentará la integridad (+15) y la seguridad de las operaciones. Requerirá inversión en formación y actualización de protocolos (-20). La aprobación de las personas aumentará (+10) al sentirse más seguros.	No implementar protocolos más estrictos podría resultar en futuros desastres (-20), afectando negativamente la integridad y seguridad. Ahorraría dinero a corto plazo (+15), pero la aprobación de las personas disminuiría (-10).
Invertir en tecnologías y equipos para prevenir y mitigar desastres	Mejorará la disponibilidad (+15) y la capacidad de respuesta ante desastres, aumentando también la integridad (+10). Requerirá una inversión significativa (-25). La aprobación de las personas aumentará (+10) al saber que se toman medidas preventivas.	No invertir en tecnologías y equipos podría resultar en daños mayores en caso de desastre (-30), afectando la disponibilidad y la integridad. Se ahorraría dinero a corto plazo (+20), pero la aprobación de las personas disminuiría (-10).
Establecer planes de respuesta y recuperación ante desastres industriales	Mejorará la capacidad de respuesta (+20) y reducirá el tiempo de inactividad en caso de desastre. Requerirá inversión en planificación y formación (-20). La aprobación de las personas aumentará (+10) al sentirse más seguros.	No tener planes de respuesta y recuperación podría resultar en tiempos de inactividad prolongados (-20) y pérdida de integridad. Se ahorraría dinero a corto plazo (+10), pero la aprobación de las personas disminuiría (-10).

Bloque 5: Fuego de Origen Industrial

Tabla 30 Análisis Fuego de Origen Industrial

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Revisar y mejorar los sistemas de prevención y	Mejorará la disponibilidad (+15) y la seguridad. Requerirá inversión en actualizaciones y	Ignorarlo podría resultar en daños mayores en caso de incendio (-30), afectando la disponibilidad y

respuesta a incendios	mantenimiento (-20). Aumentará la confianza y aprobación de los empleados (+10).	seguridad. Ahorraría dinero a corto plazo (+20), pero disminuiría la aprobación de los empleados (-10).
Mejorar la capacitación del personal en prevención y respuesta a incendios	Aumentará la confianza y la habilidad del personal para responder (+20), y mejorará la aprobación de los empleados (+10). Requerirá inversión en formación y recursos (-20).	No mejorar la capacitación podría resultar en una respuesta ineficaz en caso de incendio (-20), afectando la disponibilidad y la seguridad. Ahorraría dinero a corto plazo (+10), pero disminuiría la aprobación de los empleados (-10).
Invertir en sistemas de detección de incendios más avanzados	Mejorará la detección temprana y la seguridad (+20), y aumentará la confianza de los empleados (+10). Requerirá una inversión significativa (-30).	No invertir podría resultar en una detección tardía de incendios (-20), afectando la disponibilidad y la seguridad. Ahorraría dinero a corto plazo (+15), pero disminuiría la confianza de los empleados (-10).

Bloque 6: Daños por Agua de Origen Industrial

Tabla 31 Análisis Daños por Agua de Origen Industrial

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Mejorar sistemas de contención y drenaje	Mejorará la disponibilidad (+15) y la seguridad. Requerirá inversión en infraestructura (-20). Aumentará la aprobación de los empleados (+10).	Ignorarlo podría resultar en daños mayores en caso de inundación (-30), afectando la disponibilidad y seguridad. Ahorraría dinero a corto plazo (+20), pero disminuiría la aprobación de los empleados (-10).
Implementar protocolo de respuesta rápida para derrames	Aumentará la capacidad de respuesta (+20) y mejorará la aprobación de los empleados (+10). Requerirá inversión en formación y recursos (-20).	No tener un protocolo podría resultar en una respuesta ineficaz en caso de derrame (-20), afectando la disponibilidad y la seguridad. Ahorraría dinero a corto plazo (+10), pero disminuiría la aprobación de los empleados (-10).
Realizar inspecciones y mantenimientos más frecuentes	Mejorará la integridad de los sistemas de almacenamiento (+20) y aumentará la confianza de los empleados (+10). Requerirá inversión en personal y recursos (-20).	No hacer inspecciones podría resultar en fallos de los sistemas (-20), afectando la disponibilidad y la integridad. Ahorraría dinero a corto plazo (+10), pero disminuiría la confianza de los empleados (-10).

Bloque 7: Desastres Industriales

Tabla 32 Análisis Desastres Industriales

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Revisar y reforzar medidas y protocolos de seguridad	Mejorará la seguridad (+20) y la integridad de las operaciones. Requerirá inversión en auditorías y actualizaciones (-20). Aumentará la confianza de los empleados (+10).	Ignorarlo podría resultar en accidentes (-30), afectando la seguridad y la integridad. Ahorraría dinero a corto plazo (+20), pero disminuiría la confianza de los empleados (-10).
Invertir en sistemas de detección y prevención	Mejorará la detección temprana de condiciones peligrosas (+20) y la seguridad. Requerirá una inversión significativa (-30). Aumentará la confianza de los empleados (+10).	No invertir podría resultar en una detección tardía de peligros (-20), afectando la seguridad. Ahorraría dinero a corto plazo (+15), pero disminuiría la confianza de los empleados (-10).
Implementar programa de formación continua	Mejorará la capacitación y la habilidad de respuesta del personal (+20), y la confianza de los empleados (+10). Requerirá inversión en recursos y tiempo (-20).	No implementar el programa podría resultar en una falta de preparación (-20), afectando la seguridad y la respuesta. Ahorraría dinero a corto plazo (+10), pero disminuiría la confianza de los empleados (-10).

Bloque 8: Contaminación Mecánica

Tabla 33 Análisis Contaminación Mecánica

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de filtrado y limpieza	Mejorará la integridad de las operaciones (+15) y la seguridad. Requerirá inversión en tecnología y mantenimiento (-20). Aumentará la aprobación de los empleados (+10).	Ignorarlo podría resultar en daños a las máquinas (-20), afectando la integridad y la disponibilidad. Ahorraría dinero a corto plazo (+20), pero disminuiría la aprobación de los empleados (-10).
Mejorar procedimientos de manejo y disposición de residuos	Mejorará la integridad ambiental (+20) y la seguridad. Requerirá revisión y actualización de protocolos (-20). Aumentará la aprobación de los empleados (+10).	No hacerlo podría resultar en contaminación (-20), afectando la integridad ambiental y la seguridad. Ahorraría dinero a corto plazo (+20), pero disminuiría la aprobación de los empleados (-10).
Realizar capacitaciones sobre manejo seguro de materiales contaminantes	Mejorará la seguridad (+20) y la habilidad de respuesta del personal. Requerirá inversión en formación y tiempo (-20). Aumentará la aprobación de los empleados (+10).	Ignorarlo podría resultar en accidentes (-20), afectando la seguridad. Ahorraría dinero a corto plazo (+15), pero disminuiría la aprobación de los empleados (-10).

Bloque 9: Contaminación Electromagnética

Tabla 34 Análisis Contaminación Electromagnética

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Invertir en tecnología y materiales de blindaje electromagnético	Mejorará la disponibilidad (+10) y la integridad (+15) de los dispositivos, protegiendo los datos críticos. También se incrementará la confidencialidad (+15) y la moral del personal (+5), aunque con una inversión significativa (-30).	Aumentará el riesgo de errores y corrupción de datos (-10), se ahorrará dinero (+20), pero se reducirá la confidencialidad y la integridad de los datos (-15 cada uno) y disminuirá la moral del personal (-5).
Revisar y optimizar la disposición y diseño de los espacios de trabajo y equipos	Mejorará la disponibilidad (+10) y la integridad (+10) de los dispositivos, así como la confidencialidad (+10) y la moral del personal (+5), aunque requerirá una inversión moderada (-10).	Aumentará el riesgo de errores y corrupción de datos (-10), se ahorrará dinero (+10), pero se reducirá la confidencialidad y la integridad de los datos (-10 cada uno) y disminuirá la moral del personal (-5).
Implementar un protocolo para monitorear y gestionar los niveles de contaminación electromagnética	Mejorará la disponibilidad (+15) y la confidencialidad (+15), y mejorará ligeramente la moral del personal (+5), aunque requerirá una inversión significativa (-20).	Aumentará el riesgo de errores y corrupción de datos (-15), se ahorrará dinero (+20), pero se reducirá la confidencialidad (-15) y disminuirá la moral del personal (-5).

Bloque 10: Avería de Origen Físico o Lógico

Tabla 35 Análisis Avería de Origen Físico o Lógico

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Actualizar y mejorar los sistemas de mantenimiento preventivo de hardware y software	Mejorará la integridad (+10) y la disponibilidad (+15) de los sistemas, reduciendo la probabilidad de averías. También aumentará la confidencialidad (+5), aunque requerirá una inversión significativa (-25).	Se mantendrá el riesgo de averías no planificadas (-10), y se ahorrará dinero a corto plazo (+20). Sin embargo, la confidencialidad y la integridad de los datos pueden verse comprometidas (-5 cada una).
Implementar herramientas de monitoreo y diagnóstico para detectar y abordar problemas de forma proactiva	Aumentará la integridad (+10) y la disponibilidad (+15), permitiendo una respuesta más rápida a problemas potenciales. También aumentará la confidencialidad (+5), aunque requerirá una inversión moderada (-20).	Se mantendrá el riesgo de averías no planificadas (-10), y se ahorrará dinero a corto plazo (+15). Sin embargo, la confidencialidad y la integridad de los datos pueden verse comprometidas (-5 cada una).

Desarrollar un protocolo de respuesta y recuperación de sistemas más efectivo y eficiente	Aumentará la disponibilidad (+10) y la confidencialidad (+5) de los sistemas, y permitirá una recuperación más rápida. También mejorará la moral del personal (+5), aunque requerirá una inversión moderada (-20).	Se mantendrá el riesgo de averías no planificadas (-10), y se ahorrará dinero a corto plazo (+15). Sin embargo, la integridad de los datos podría verse comprometida (-10).

Bloque 11: Corte del Suministro Eléctrico

Tabla 36 Análisis Corte del Suministro Eléctrico

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Invertir en sistemas de respaldo de energía más robustos y fiables	Esto mejorará la disponibilidad (+20) de los sistemas críticos, asegurando operaciones continuas durante cortes de energía. Aunque requerirá una inversión significativa (-30), también aumentará la confianza y seguridad percibida por los empleados y clientes (+10).	No hacer esta inversión mantendrá el riesgo de interrupciones significativas (-20) y ahorrará dinero a corto plazo (+20), pero disminuirá la confianza y seguridad percibida por los empleados y clientes (-10).
Revisar y optimizar los protocolos de respuesta a cortes de suministro eléctrico	Mejorará la disponibilidad (+15) y permitirá una respuesta más rápida y eficiente durante un corte de energía, aumentando la confianza y seguridad percibida (+5). Requerirá una inversión moderada (-20).	No hacerlo mantendrá el riesgo de respuestas ineficientes (-15), ahorrará dinero a corto plazo (+15), pero disminuirá la confianza y seguridad percibida (-5).
Considerar fuentes de energía alternativas y renovables para casos de emergencia	Aumentará la disponibilidad (+10) y la sostenibilidad de las operaciones. Aunque requerirá una inversión significativa (-25), también mejorará la imagen de la empresa (+10) y contribuirá a la sostenibilidad ambiental.	No hacerlo mantendrá el riesgo de dependencia de la red eléctrica (-10) y ahorrará dinero a corto plazo (+25), pero podría tener un impacto negativo en la imagen de la empresa y en la sostenibilidad ambiental (-10).

Bloque 12: Condiciones Inadecuadas de Temperatura o Humedad

Tabla 37 Análisis Condiciones Inadecuadas de Temperatura o Humedad

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Invertir en sistemas de control climático más avanzados y precisos	Desde el punto de vista de ciberseguridad, esta inversión es crucial. Mejorará la integridad (+10) y disponibilidad (+10) de los sistemas, previniendo fallos por condiciones inadecuadas. Aunque supone una inversión inicial (-15), los beneficios a largo plazo son	Ignorar esta medida podría llevar a fallos en los sistemas, comprometiendo la integridad (-10) y disponibilidad (-10). Se ahorraría dinero a corto plazo (+5), pero los riesgos a largo plazo son elevados. La resistencia al cambio puede

	significativos. Puede haber resistencia al cambio por parte del personal, pero la formación y concienciación pueden mitigar este aspecto.	ser menor, pero a costa de la seguridad.
Realizar mantenimientos regulares y monitoreo del ambiente de trabajo	Es esencial para asegurar el buen funcionamiento de los sistemas, mejorando la integridad (+10) y disponibilidad (+10). Requiere una inversión constante (-10), pero ayuda a prevenir fallos graves. Puede haber resistencia al cambio y a la inversión requerida, pero la formación y la demostración de los beneficios pueden ayudar.	Evitar esta medida podría resultar en fallos no detectados y condiciones de trabajo subóptimas, afectando la integridad (-10) y disponibilidad (-10) de los sistemas. Se ahorra dinero a corto plazo (+5), pero los riesgos son significativos.
Implementar protocolos para responder a condiciones climáticas adversas en el interior	Aumenta la preparación y resiliencia, mejorando la integridad (+10) y disponibilidad (+10) de los sistemas. Requiere inversión (-10), pero mejora significativamente la seguridad. Puede haber resistencia al cambio, pero la formación y simulacros pueden ayudar a superarla.	No implementar protocolos específicos aumenta el riesgo de respuesta inadecuada, afectando la integridad (-10) y disponibilidad (-10) de los sistemas. Se ahorra dinero a corto plazo (+5), pero se compromete la seguridad.

Bloque 13: Fallo de Servicios de Comunicaciones

Tabla 38 Análisis Fallo de Servicios de Comunicaciones

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Invertir en sistemas de comunicación redundantes y de respaldo	Esto mejorará significativamente la disponibilidad (+20) y la resiliencia de los sistemas de comunicación, aunque requerirá una inversión importante (-20). A largo plazo, esto podría mejorar la confidencialidad (+5) al asegurar que los canales de comunicación estén siempre disponibles para transmitir información crítica de forma segura. Puede haber resistencia al cambio debido a la inversión necesaria, pero destacar la importancia de la comunicación constante puede mitigar esto.	Evitar esta inversión podría resultar en una menor disponibilidad (-20) y resiliencia en los sistemas de comunicación, poniendo en riesgo la confidencialidad (-5) al no poder comunicarse de manera segura durante un incidente. Se ahorra dinero a corto plazo (+10), pero se pone en riesgo la operatividad y seguridad de la empresa.
Revisar y mejorar los protocolos de recuperación y respuesta a fallas de comunicación	Esto mejorará la integridad (+10) y disponibilidad (+15) de los sistemas de comunicación, y aunque requiere inversión y esfuerzo para la revisión y la implementación (-10), los	Ignorar esta medida podría llevar a una respuesta ineficiente ante fallos de comunicación, afectando la integridad (-10) y disponibilidad (-15) de los sistemas. Se ahorra

	beneficios a largo plazo son significativos. La resistencia al cambio puede ser un factor, pero la capacitación y la concienciación pueden ayudar.	dinero a corto plazo (+5), pero se pone en riesgo la eficiencia operativa y la seguridad.
Entrenar al personal en procedimientos de emergencia de comunicación	Mejorará la preparación del personal y la resiliencia organizativa, aumentando la integridad (+10) y disponibilidad (+10) de los sistemas de comunicación en situaciones de emergencia. Requiere inversión en formación (-10), pero los beneficios en términos de respuesta eficiente y seguridad son claros. La resistencia al cambio y a la inversión en formación pueden ser desafíos, pero destacar la importancia de la preparación puede ayudar.	No proporcionar esta formación podría resultar en una respuesta ineficiente y caótica en situaciones de emergencia, afectando la integridad (-10) y disponibilidad (-10) de los sistemas de comunicación. Se ahorra en formación (+5), pero se compromete la seguridad y eficiencia.

Bloque 14: Interrupción de Otros Servicios y Suministros Esenciales

Tabla 39 Análisis Interrupción de Otros Servicios y Suministros Esenciales

PROPUESTA DE MITIGACIÓN	Análisis de Aceptación	Análisis de Rechazo
Desarrollar planes de contingencia para la interrupción de servicios esenciales	Esto mejorará significativamente la disponibilidad (+20) y la resiliencia de la empresa, aunque requerirá tiempo y recursos para desarrollar e implementar los planes (-15). La integridad de los datos y sistemas se mantendrá (+10), y los empleados se sentirán más seguros y preparados (+5). Puede haber resistencia debido al tiempo y recursos necesarios, pero la importancia de estar preparados puede ayudar a superar esto.	No tener un plan de contingencia puede resultar en una baja disponibilidad (-20) y pérdida de integridad (-10) en caso de una interrupción. Se ahorra tiempo y recursos a corto plazo (+10), pero se pone en riesgo la continuidad del negocio y la integridad de los datos.
Obtener contratos con proveedores alternativos o de respaldo	Mejorará la disponibilidad (+15) y reducirá el riesgo de interrupción de los servicios esenciales. Aunque esto podría aumentar los costos (-10), la resiliencia añadida y la menor dependencia de un solo proveedor justifican la inversión. Puede haber resistencia debido a los costos adicionales, pero la seguridad de tener alternativas puede ser un fuerte argumento.	No tener proveedores alternativos puede resultar en una baja disponibilidad (-15) y un mayor riesgo en caso de falla de un proveedor. Se ahorra dinero a corto plazo (+5), pero se aumenta el riesgo y la dependencia de un solo proveedor.
Realizar simulacros regulares de	Esto mejorará la preparación del personal y la capacidad de respuesta de la empresa,	No realizar simulacros puede resultar en una baja preparación y capacidad de

interrupción de servicios y poner a prueba los protocolos de respuesta	aumentando la integridad (+10) y la disponibilidad (+10). Requiere inversión en tiempo y recursos (-10), pero los beneficios en términos de preparación y respuesta a emergencias son significativos. Puede haber resistencia debido al tiempo y esfuerzo requeridos, pero la importancia de estar preparados y la mejora en la seguridad pueden ayudar a superar esta resistencia.	respuesta, afectando la integridad (-10) y la disponibilidad (-10). Se ahorra tiempo y recursos a corto plazo (+5), pero se compromete la seguridad y la capacidad de respuesta en situaciones de emergencia.

Bloque 15: Degradación de los Soportes de Almacenamiento de la Información

Tabla 40 Análisis Degradación de los Soportes de Almacenamiento de la Información

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Actualizar y reemplazar regularmente los sistemas de almacenamiento de datos	Mejora significativa de la integridad (+20) y la disponibilidad (+20), asegurando que los datos estén siempre accesibles y sean confiables. La inversión requerida es alta (-20), pero necesaria para prevenir pérdidas de datos. Puede haber resistencia al cambio y a la inversión necesaria, pero los beneficios a largo plazo y la protección contra pérdidas de datos son argumentos fuertes a favor.	Se ahorran costos a corto plazo (+20), pero se pone en riesgo la integridad (-30) y la disponibilidad (-30) de los datos, lo que podría resultar en pérdidas significativas a largo plazo. La resistencia al cambio puede ser menor, pero se corre un riesgo considerable.
Implementar soluciones de respaldo y recuperación de datos más efectivas	Aumento de la disponibilidad (+20) y la integridad (+15), asegurando que los datos se puedan recuperar en caso de pérdida. Requiere inversión (-15), pero proporciona una red de seguridad crucial. Puede haber resistencia debido a la complejidad y al costo, pero la importancia de proteger los datos es un argumento convincente.	Ahorro de costos a corto plazo (+15), pero riesgo significativo de pérdida de integridad (-20) y disponibilidad (-20) de los datos. La resistencia al cambio puede ser menor, pero se juega con la continuidad del negocio.
Realizar auditorías y monitoreos continuos del estado de los dispositivos de almacenamiento	Mejora de la integridad (+10) y la disponibilidad (+10) mediante la detección temprana de posibles problemas. Requiere inversión (-10) y esfuerzo constante, pero previene problemas mayores. Puede haber resistencia debido al trabajo adicional y al costo, pero asegura la salud a largo plazo de los sistemas de almacenamiento.	Se ahorran costos a corto plazo (+5), pero se pone en riesgo la integridad (-15) y la disponibilidad (-15) de los datos. La resistencia al cambio puede ser menor, pero se ignoran los beneficios preventivos.

Bloque 16: Emanaciones Electromagnéticas

Tabla 41 Análisis Emanaciones Electromagnéticas

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Investigar e implementar tecnologías de blindaje y filtrado electromagnético	Mejora significativa de la integridad (+15) y disponibilidad (+10) de los dispositivos afectados. Requiere inversión (-15) y tiempo para la investigación e implementación. Puede haber resistencia debido al costo, pero la mejora en la estabilidad del sistema es un fuerte argumento a favor.	Se ahorran costos a corto plazo (+10), pero se pone en riesgo la integridad (-20) y disponibilidad (-15) de los dispositivos. La resistencia al cambio puede ser menor, pero los riesgos operativos aumentan.
Realizar evaluaciones periódicas del ambiente electromagnético	Aumento de la integridad (+10) y la disponibilidad (+10) mediante la identificación y mitigación temprana de problemas. Requiere inversión (-10) y esfuerzo constante, pero previene problemas mayores. Puede haber resistencia debido al trabajo adicional, pero asegura un ambiente operativo más estable.	Se ahorran costos a corto plazo (+5), pero se pone en riesgo la integridad (-15) y disponibilidad (-15) de los dispositivos. La resistencia al cambio puede ser menor, pero se ignoran los beneficios preventivos.
Establecer protocolos de manejo y mitigación de interferencias electromagnéticas	Mejora de la integridad (+15) y la disponibilidad (+15) mediante la respuesta rápida y efectiva a las interferencias. Requiere inversión (-10) y tiempo para el desarrollo de los protocolos. Puede haber resistencia debido al cambio en los procedimientos, pero la mejora en la capacidad de respuesta es un beneficio claro.	Ahorro de costos a corto plazo (+10), pero riesgo significativo de pérdida de integridad (-20) y disponibilidad (-20). La resistencia al cambio puede ser menor, pero se pone en juego la estabilidad operativa.

Bloque 17: Errores y Fallos No Intencionados

Tabla 42 Errores y Fallos No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de monitoreo y alerta temprana	Mejora significativa de la disponibilidad (+15) y la integridad (+10) mediante la detección y respuesta temprana a errores. Requiere inversión (-10) y esfuerzo constante, pero previene pérdidas mayores. Puede haber resistencia debido al costo y al cambio en los procedimientos, pero los beneficios en la estabilidad y confiabilidad del sistema son claros.	Se ahorran costos a corto plazo (+10), pero se pone en riesgo la integridad (-15) y disponibilidad (-20). La resistencia al cambio puede ser menor, pero se ignoran los beneficios preventivos.
Mejorar los protocolos de	Aumento de la disponibilidad (+20) y la integridad (+10) mediante la respuesta	Ahorro de costos a corto plazo (+5), pero riesgo

respuesta y recuperación de fallos	rápida y efectiva a fallos. Requiere inversión (-10) y tiempo para el desarrollo de los protocolos. Puede haber resistencia debido al cambio en los procedimientos, pero la mejora en la capacidad de respuesta y recuperación es un beneficio claro.	significativo de pérdida de integridad (-10) y disponibilidad (-15). La resistencia al cambio puede ser menor, pero se pone en juego la estabilidad operativa.
Capacitar al personal en prevención y manejo de errores y fallos	Mejora de la integridad (+10) y la disponibilidad (+10) mediante la habilidad del personal para prevenir y responder a errores. Requiere inversión en capacitación (-5), pero empodera al equipo para mantener la operatividad. Puede haber resistencia debido al tiempo dedicado a la capacitación, pero la mejora en la competencia del personal es un fuerte argumento a favor.	Se ahorran costos y tiempo de capacitación (+5), pero se pone en riesgo la integridad (-10) y disponibilidad (-10). La resistencia al cambio puede ser menor, pero se pone en juego la capacidad del equipo para responder eficazmente.

Bloque 18: Errores de los Usuarios No Intencionados

Tabla 43 Errores de los Usuarios No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Desarrollar programas de educación y capacitación para usuarios	Mejora la integridad (+10) y la confidencialidad (+5) al reducir los errores humanos. Requiere inversión (-5) pero aumenta la conciencia de ciberseguridad. Puede haber resistencia debido al tiempo requerido, pero se fortalece la cultura de seguridad.	Se ahorra en costos de capacitación (+5), pero aumenta el riesgo de errores humanos que afectan la integridad (-10) y confidencialidad (-5). Ignora el valor de la educación en ciberseguridad.
Implementar sistemas de validación y confirmación de acciones críticas	Fortalece la integridad (+15) y la disponibilidad (+5) al prevenir errores graves. Requiere inversión (-10) y puede ralentizar procesos, pero mejora significativamente la seguridad.	Ahorro de costos (+10), pero aumenta el riesgo de errores graves que afectan la integridad (-15) y disponibilidad (-10). Ignora la necesidad de salvaguardas adicionales en acciones críticas.
Mejorar interfaces y experiencias de usuario	Mejora la integridad (+10) y reduce los errores humanos. Requiere inversión en diseño y desarrollo (-10), pero facilita el uso seguro de los sistemas. Puede haber resistencia al cambio, pero mejora la interacción segura.	Ahorro en costos de desarrollo (+10), pero aumenta el riesgo de errores humanos que afectan la integridad (-10). Ignora la importancia de una interfaz intuitiva en la prevención de errores.

Bloque 19: Errores del Administrador No Intencionados

Tabla 44 Errores del Administrador No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Proporcionar formación adicional y soporte a los administradores	Aumenta la integridad (+10) y la confidencialidad (+10) al reducir los errores humanos. Requiere inversión (-5) pero fortalece la competencia del equipo administrativo.	Ahorro en costos de capacitación (+5), pero incremento en riesgo de errores que afectan la integridad (-10) y confidencialidad (-10). Ignora la importancia de mantener actualizadas las habilidades del equipo administrativo.
Implementar sistemas de revisión y auditoría de las acciones administrativas	Mejora la integridad (+15) y la confidencialidad (+10) al detectar errores y actividades sospechosas. Requiere inversión (-10) y puede ralentizar procesos, pero mejora significativamente la seguridad y la rendición de cuentas.	Ahorro de costos a corto plazo (+10), pero aumento del riesgo de errores y actividades maliciosas no detectadas que afectan la integridad (-15) y confidencialidad (-10). Ignora la necesidad de salvaguardas y transparencia en acciones administrativas.
Establecer protocolos de recuperación y respaldo para acciones administrativas	Mejora la disponibilidad (+10) y la integridad (+10) al permitir la restauración rápida en caso de errores. Requiere inversión (-5) y mantenimiento, pero proporciona una red de seguridad crucial.	Ahorro de costos a corto plazo (+5), pero aumento del riesgo de pérdida de disponibilidad (-10) e integridad (-10) en caso de errores. Ignora la importancia de la resiliencia en operaciones críticas.

Bloque 20: Errores de Monitorización (Log) No Intencionados

Tabla 45 Errores de Monitorización (Log) No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Mejorar y refinar los sistemas y procesos de registro y monitoreo de datos	Mejora la integridad (+15) y la disponibilidad (+10) de los datos de registro, haciendo más confiable la monitorización. Requiere inversión (-10) pero es crucial para un diagnóstico preciso y oportuno de problemas.	Ahorro de costos a corto plazo (+10), pero disminución en la confiabilidad de los registros, afectando la integridad (-15) y disponibilidad (-10) de los datos para análisis y respuesta.
Capacitar al personal responsable en la gestión y revisión eficiente de los registros	Aumenta la integridad (+10) y la confidencialidad (+10) al mejorar la competencia del personal en la interpretación de registros. Requiere inversión en capacitación (-5), pero empodera al equipo para un manejo más efectivo de los datos.	Ahorro en costos y tiempo de capacitación (+5), pero aumenta el riesgo de interpretaciones erróneas y pérdida de confidencialidad e integridad, cada una en (-10).
Implementar herramientas de	Mejora la integridad (+15) y la disponibilidad (+10) de los datos	Ahorro de costos a corto plazo (+10), pero los datos

análisis de registros más avanzadas y precisas	analizados, proporcionando información más precisa. Requiere inversión (-10) pero optimiza la respuesta y resolución de problemas.	analizados pueden ser menos confiables, afectando la integridad (-15) y la disponibilidad (-10) de la información crítica.

Bloque 21: Errores de Configuración No Intencionados

Tabla 46 Errores de Configuración No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Desarrollar protocolos de revisión y validación antes de implementar cambios de configuración	Mejora la integridad (+15) y la disponibilidad (+10) asegurando que los cambios son revisados antes de ser aplicados. Requiere inversión en desarrollo de protocolos (-10) y tiempo para revisiones (-5).	Ahorro en tiempo y costos a corto plazo (+10), pero aumenta el riesgo de errores en la configuración, afectando la integridad (-15) y disponibilidad (-10).
Capacitar al personal sobre procedimientos de configuración seguros y efectivos	Aumenta la confidencialidad (+10) y la integridad (+10) al tener personal más informado y capaz. Requiere inversión en capacitación (-5), pero mejora la seguridad y efectividad a largo plazo.	Ahorro en costos y tiempo de capacitación (+5), pero aumenta el riesgo de errores y problemas de seguridad, afectando la confidencialidad (-10) y la integridad (-10).
Implementar herramientas automáticas de gestión y restauración de configuraciones	Mejora la disponibilidad (+15) y la integridad (+10) al tener herramientas que pueden revertir rápidamente los errores. Requiere inversión (-10), pero mejora la resiliencia y la capacidad de recuperación del sistema.	Ahorro de costos a corto plazo (+10), pero aumenta el riesgo de tiempo de inactividad y errores persistentes, afectando la disponibilidad (-15) y la integridad (-10).

Bloque 22: Deficiencias en la Organización No Intencionados

Tabla 47 Deficiencias en la Organización No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Realizar una revisión y optimización de los procesos y estructuras organizativas	Mejora la integridad (+10) y la disponibilidad (+10) al tener procesos más claros y eficientes. Requiere inversión en tiempo (-5) y recursos (-10).	Se evitan costos a corto plazo (+10), pero persisten los problemas organizativos, afectando la integridad (-10) y la disponibilidad (-10).
Implementar herramientas de gestión y comunicación interna más eficientes	Mejora la integridad (+10) y la disponibilidad (+15) al mejorar la comunicación y la gestión de tareas. Requiere inversión en herramientas (-10).	Se evita la inversión en nuevas herramientas (+10), pero se mantiene la ineficiencia y la falta de comunicación, afectando la integridad (-10) y la disponibilidad (-15).

Desarrollar programas de capacitación y concienciación para el personal sobre mejores prácticas organizativas	Mejora la confidencialidad (+10), la integridad (+10) y la disponibilidad (+5) al tener personal más informado. Requiere inversión en capacitación (-5).	Se ahorra en capacitación (+5), pero el personal sigue sin estar adecuadamente informado, afectando la confidencialidad (-10), la integridad (-10) y la disponibilidad (-5).

Bloque 23: Difusión de Software Dañino No Intencionados

Tabla 48 Difusión de Software Dañino No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en soluciones de seguridad de software más avanzadas y confiables	Mejora la integridad (+15) y la confidencialidad (+15) al proteger mejor los sistemas. Requiere inversión en software de seguridad (-10).	Se ahorra en costos de inversión (+10), pero se mantiene en riesgo la integridad (-15) y la confidencialidad (-15) de los datos.
Realizar actualizaciones y revisiones de seguridad regularmente	Mejora la integridad (+10), la confidencialidad (+10) y la disponibilidad (+5) al mantener los sistemas actualizados y seguros. Requiere tiempo y esfuerzo constante (-5).	Se ahorra tiempo y esfuerzo a corto plazo (+5), pero se pone en riesgo la integridad (-10), la confidencialidad (-10) y la disponibilidad (-5) de los sistemas.
Implementar protocolos de revisión y validación para instalaciones y actualizaciones de software	Mejora la integridad (+10) y la confidencialidad (+10) al asegurar que solo software seguro sea instalado. Requiere tiempo y recursos para establecer los protocolos (-5).	Se ahorra en recursos a corto plazo (+5), pero se incrementa el riesgo de instalar software dañino, afectando la integridad (-10) y la confidencialidad (-10).

Bloque 24: Errores de Re-Encaminamiento

Tabla 49 Errores de Re-Encaminamiento

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar herramientas de monitoreo y corrección de rutas de datos en tiempo real	Mejora la disponibilidad (+15) al detectar y corregir errores de enrutamiento rápidamente. Requiere inversión en herramientas (-10).	Se ahorra en costos de inversión (+10), pero se mantiene el riesgo de interrupciones en la disponibilidad (-15) debido a errores de enrutamiento.
Revisar y optimizar los protocolos de enrutamiento y transmisión de datos	Mejora la integridad (+10) y la disponibilidad (+10) al optimizar los caminos de los datos. Requiere tiempo y esfuerzo para la revisión (-5).	Se ahorra tiempo y esfuerzo a corto plazo (+5), pero se incrementa el riesgo de errores en la integridad (-10) y en la disponibilidad (-10) de los datos.
Capacitar al personal en la identificación y	Mejora la integridad (+5) y la disponibilidad (+5) al capacitar al personal para	Se ahorra en costos de formación (+5), pero se mantiene el riesgo de errores en

corrección de errores de enrutamiento	manejar errores de enrutamiento. Requiere inversión en formación (-5).	la integridad (-5) y en la disponibilidad (-5) debido a la falta de conocimiento del personal.

Bloque 25: Errores de Secuencia No Intencionados

Tabla 50 Errores de Secuencia No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de sincronización y ordenación de datos más robustos y automáticos	Mejora la integridad (+20) al asegurar que los datos estén en la secuencia correcta. Requiere inversión en tecnología y desarrollo (-10).	Se ahorra en costos de inversión (+10), pero se mantiene el riesgo de errores en la integridad (-20) debido a problemas de secuencia.
Revisar y corregir regularmente los protocolos de transmisión y procesamiento de datos	Mejora la integridad (+15) y la disponibilidad (+10) al asegurar que los procesos estén optimizados. Requiere tiempo y recursos para revisiones constantes (-5).	Se ahorra tiempo y recursos (+5), pero se incrementa el riesgo de errores en la integridad (-15) y en la disponibilidad (-10).
Desarrollar herramientas de monitoreo y alerta para desviaciones y errores en la secuencia de datos	Mejora la integridad (+10) y ayuda a detectar rápidamente problemas, manteniendo la disponibilidad (+10). Requiere inversión en desarrollo de herramientas (-5).	Se ahorra en costos de desarrollo (+5), pero se mantiene el riesgo de no detectar errores a tiempo, afectando la integridad (-10) y la disponibilidad (-10).

Bloque 26: Escapes de Información No Intencionados

Tabla 51 Escapes de Información No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Reforzar las políticas y herramientas de control de acceso y seguridad de datos	Mejora significativa de la confidencialidad (+20) y la integridad (+10) al controlar y restringir el acceso a los datos. Requiere inversión en tecnología y capacitación (-10).	Ahorro de costos a corto plazo (+10), pero se mantiene el riesgo de incumplimiento de la confidencialidad (-20) y la integridad (-10).
Implementar sistemas de encriptación y protección de datos más avanzados	Aumento de la confidencialidad (+15) mediante la encriptación de datos, protegiéndolos de accesos no autorizados. Requiere inversión en tecnología (-10).	Se ahorra en costos (+10), pero persiste un riesgo de falta de confidencialidad (-15).
Realizar auditorías y capacitaciones de seguridad de datos periódicas	Aumento de la confidencialidad (+10) y mejora de la integridad (+5) al educar al personal y verificar el cumplimiento. Requiere inversión en capacitación y auditorías (-5).	Ahorro de costos (+5), pero persiste un riesgo de falta de confidencialidad (-10) y la integridad (-5).

Bloque 27: Alteración Accidental de la Información No Intencionados

Tabla 52 Alteración Accidental de la Información No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de respaldo y recuperación de datos más robustos	Mejora la integridad (+20) y la disponibilidad (+10) al asegurar la restauración rápida de datos auténticos. Requiere inversión en tecnología y capacitación (-10).	Ahorro de costos a corto plazo (+10), pero se incrementa el riesgo de pérdida de integridad (-20) y disponibilidad (-10).
Realizar revisiones y validaciones periódicas de la integridad de los datos	Aumento de la integridad (+15) al detectar y corregir errores a tiempo. Requiere recursos para revisiones regulares (-5).	Ahorro de recursos (+5), pero se mantiene el riesgo de pérdida de integridad (-15).
Capacitar al personal en la gestión y protección efectiva de los datos	Mejora la integridad (+10) y potencialmente la confidencialidad (+5) al educar al personal sobre prácticas seguras. Requiere inversión en capacitación (-5).	Ahorro de costos (+5), pero se mantiene el riesgo de pérdida de integridad (-10) y potencialmente confidencialidad (-5).

Bloque 28: Destrucción de Información No Intencionados

Tabla 53 Destrucción de Información No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de protección y respaldo de datos más efectivos	Mejora la integridad (+20) y la disponibilidad (+20) asegurando una recuperación rápida y fiel de los datos. Requiere inversión en tecnología y capacitación (-10).	Ahorro de costos a corto plazo (+10), pero riesgo elevado de pérdida de integridad (-20) y disponibilidad (-20).
Invertir en tecnología de almacenamiento más confiable y segura	Aumenta la integridad (+15) y la disponibilidad (+15) mediante la reducción del riesgo de pérdida de datos. Requiere una inversión significativa (-15).	Ahorro a corto plazo (+15), pero mantiene alto riesgo de pérdida de integridad (-15) y disponibilidad (-15).
Realizar auditorías regulares y mantenimiento de los sistemas de almacenamiento de datos	Mejora la integridad (+10) y la disponibilidad (+10) al identificar y corregir problemas antes de que causen daño. Requiere recursos para auditorías regulares (-5).	Ahorro de recursos (+5), pero riesgo elevado de pérdida de integridad (-10) y disponibilidad (-10).

Bloque 29: Fugas de Información No Intencionados

Tabla 54 Fugas de Información No Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y fortalecer las políticas de	Mejora la confidencialidad (+20) y la integridad (+10) al crear un	Ahorro de recursos a corto plazo (+10), pero riesgo

seguridad y privacidad de datos	entorno más seguro para los datos. Requiere tiempo y recursos para la revisión y actualización de políticas (-10).	elevado de pérdida de confidencialidad (-20) y de integridad (-10).
Implementar soluciones de monitoreo y alerta de actividad sospechosa	Mejora la confidencialidad (+15) y ayuda a prevenir incidentes antes de que ocurran. Requiere inversión en tecnología y capacitación (-15).	Ahorro a corto plazo (+15), pero mantiene alto riesgo de pérdida de confidencialidad (-15) y no se detectan incidentes a tiempo.
Capacitación continua del personal en mejores prácticas de manejo de datos	Mejora la confidencialidad (+10) y la integridad (+10) al crear una cultura de seguridad y conciencia. Requiere inversión en programas de capacitación (-10).	Ahorro a corto plazo (+10), pero riesgo elevado de pérdida de confidencialidad (-10) e integridad (-10) debido a errores humanos.

Bloque 30: Vulnerabilidades de los Programas (Software)

Tabla 55 Vulnerabilidades de los Programas (Software)

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Realizar evaluaciones de seguridad de software y actualizaciones regulares	Mejora la integridad (+15) y la seguridad general del software. Requiere inversión en tiempo y recursos (-15).	Ahorro a corto plazo (+15), pero mantiene alto riesgo de vulnerabilidades no detectadas y potencial pérdida de integridad (-15).
Implementar herramientas de protección y monitoreo de seguridad en tiempo real	Mejora la integridad (+20) y la capacidad de respuesta frente a amenazas. Requiere inversión en tecnología y capacitación (-20).	Ahorro a corto plazo (+20), pero mantiene alto riesgo de ataques exitosos y pérdida de integridad (-20).
Adoptar prácticas de desarrollo de software seguro y capacitación relacionada	Mejora la integridad (+10) y la calidad del software desde su creación. Requiere inversión en formación y cambios en la cultura de desarrollo (-10).	Ahorro a corto plazo (+10), pero riesgo elevado de desarrollar software con vulnerabilidades y pérdida de integridad (-10).

Bloque 31: Errores de Mantenimiento/Actualización de Programas (Software)

Tabla 56 Errores de Mantenimiento/Actualización de Programas (Software)

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar protocolos de revisión y validación más estrictos antes de aplicar actualizaciones	Mejora la integridad (+15) y la disponibilidad (+10) al garantizar que las actualizaciones no causen problemas. Requiere inversión en tiempo y recursos (-10).	Ahorro a corto plazo (+10), pero riesgo elevado de problemas no detectados y pérdida de integridad (-15).
Desarrollar procedimientos de respaldo y recuperación previos a la actualización	Aumenta la disponibilidad (+15) al garantizar que los sistemas puedan restaurarse en caso de problemas. Requiere inversión en tiempo y recursos (-10).	Ahorro a corto plazo (+10), pero riesgo de pérdida de integridad y disponibilidad (-15).

Realizar pruebas exhaustivas de cada actualización en un entorno controlado	Aumenta la integridad (+15) al identificar problemas antes de la implementación. Requiere inversión en tiempo y recursos (-10).	Ahorro a corto plazo (+10), pero se mantiene el riesgo de problemas no detectados en un entorno de producción y pérdida de integridad (-15).

Bloque 32: Errores de Mantenimiento/Actualización de Equipos (Hardware)

Tabla 57 Errores de Mantenimiento/Actualización de Equipos (Hardware)

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Proporcionar formación adicional a los técnicos de mantenimiento	Mejora la calidad del mantenimiento (+15) y reduce la probabilidad de errores (-15). Requiere inversión en formación (-10).	Ahorro a corto plazo (+10), pero aumento del riesgo de errores de mantenimiento y problemas de hardware (-15).
Establecer procedimientos de verificación post-mantenimiento más rigurosos	Aumenta la detección de errores (+15) y mejora la integridad del hardware (+10). Requiere tiempo adicional y recursos (-10).	Ahorro de tiempo (+10), pero riesgo elevado de no detectar errores de mantenimiento y pérdida de integridad del hardware (-15).
Revisar y mejorar las herramientas y métodos de mantenimiento y actualización	Mejora la eficacia del mantenimiento (+15) y reduce el riesgo de errores (-15). Requiere inversión en nuevas herramientas y formación (-10).	Ahorro a corto plazo (+10), pero mantenimiento ineficaz y riesgo elevado de errores y problemas de hardware (-15).

Bloque 33: Caída del Sistema por Agotamiento de Recursos

Tabla 58 Caída del Sistema por Agotamiento de Recursos

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en mejoras de capacidad y eficiencia de los sistemas	Aumenta la capacidad del sistema (+15) y mejora la eficiencia (+10). Requiere inversión significativa (-15).	Ahorro a corto plazo (+10), pero riesgo elevado de colapso del sistema y pérdida de disponibilidad (-20).
Desarrollar e implementar soluciones de monitoreo de rendimiento y gestión de recursos en tiempo real	Mejora la detección de problemas y la gestión de recursos (+15). Requiere inversión en herramientas y formación (-10).	Ahorro a corto plazo (+10), pero falta de visibilidad y gestión de los recursos del sistema (-15).
Establecer protocolos de respuesta rápida para picos de demanda inesperados	Mejora la capacidad de respuesta del sistema (+15) y reduce el tiempo de inactividad (-10). Requiere planificación y recursos adicionales (-10).	Ahorro de recursos (+10), pero riesgo elevado de tiempos de inactividad prolongados y pérdida de servicio (-15).

Bloque 34: Pérdida de Equipos

Tabla 59 Pérdida de Equipos

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de rastreo y seguridad para los equipos	Aumenta la seguridad (+10) y reduce el riesgo de pérdida de equipos (-15). Requiere inversión en tecnología de rastreo (-10).	Ahorro a corto plazo (+10), pero riesgo elevado de pérdida de equipos y datos (-20).
Revisar y fortalecer las políticas y protocolos de manejo y almacenamiento de equipos	Mejora la gestión de equipos (+15) y aumenta la conciencia de seguridad (+10). Requiere tiempo y recursos para desarrollo e implementación (-10).	Ahorro de tiempo y recursos (+10), pero mantenimiento del estatus quo con riesgos existentes (-15).
Proporcionar formación adicional al personal sobre la importancia de la gestión responsable de los equipos	Aumenta la conciencia y responsabilidad del personal (+15). Requiere inversión en formación y tiempo (-10).	Ahorro a corto plazo (+10), pero persisten los riesgos asociados con la gestión irresponsable de los equipos (-15).

Bloque 35: Indisponibilidad del Personal

Tabla 60 Indisponibilidad del Personal

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Desarrollar e implementar un sistema de programación y respaldo de personal más robusto	Mejora la planificación de recursos (+15) y asegura la continuidad del trabajo (+10). Requiere inversión en sistemas y planificación (-10).	Ahorro a corto plazo (+10), pero riesgo elevado de discontinuidad y pérdida de productividad (-20).
Proporcionar formación y soporte para garantizar la disponibilidad y compromiso del personal	Aumenta la motivación y el compromiso del personal (+15). Requiere inversión en formación y programas de soporte (-10).	Ahorro de recursos a corto plazo (+10), pero riesgo de baja moral y compromiso del personal (-15).
Contratar personal adicional o de respaldo para cubrir las necesidades críticas	Aumenta la resiliencia y la capacidad de respuesta (+20). Requiere inversión en reclutamiento y salarios (-15).	Ahorro en costos de personal (+10), pero vulnerabilidad a la indisponibilidad del personal y posibles interrupciones (-20).

Bloque 36: Ataques Intencionados

Tabla 61 Ataques Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en soluciones de ciberseguridad más avanzadas y robustas	Mejora la defensa contra ataques cibernéticos (+20), protege la integridad de los datos (+15).	Ahorro a corto plazo (+10), pero riesgo extremadamente alto de

	Requiere inversión significativa en tecnología y recursos (-15).	violaciones de seguridad y pérdida de datos (-30).
Realizar auditorías de seguridad periódicas y pruebas de penetración	Identifica y mitiga vulnerabilidades (+20), mejora la postura de seguridad (+15). Requiere inversión en servicios de auditoría y tiempo para pruebas (-10).	Ahorro en costos de auditoría (+10), pero exposición continua a vulnerabilidades y riesgos de seguridad (-25).
Capacitar al personal en concienciación y prevención de seguridad	Mejora la cultura de seguridad en la empresa (+15), reduce el riesgo de errores humanos en seguridad (+10). Requiere inversión en formación y tiempo del personal (-10).	Ahorro en costos de capacitación (+10), pero mayor riesgo de errores humanos y brechas de seguridad (-20).

Bloque 37: Manipulación de los Registros de Actividad (Log) Intencionados

Tabla 62 Manipulación de los Registros de Actividad (Log) Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de monitoreo y alerta de integridad para los registros de actividad	Mejora la detección de manipulaciones (+20), reduce el tiempo de respuesta a incidentes (+15). Requiere inversión en tecnología y configuración (-10).	Ahorro a corto plazo (+5), pero alta probabilidad de no detectar manipulaciones y brechas de seguridad (-25).
Establecer protocolos de revisión y validación regular de los registros	Asegura la precisión y confiabilidad de los registros (+15), facilita la investigación de incidentes (+10). Requiere tiempo y recursos para revisiones regulares (-10).	Menor carga de trabajo a corto plazo (+5), pero riesgo de no detectar manipulaciones y tomar decisiones basadas en información falsa (-20).
Capacitar al personal en la identificación y respuesta a manipulaciones de registros	Mejora la capacidad de respuesta del personal (+10), fortalece la postura de seguridad general (+10). Requiere inversión en formación y tiempo del personal (-10).	Ahorro en costos de capacitación (+5), pero mayor vulnerabilidad a manipulaciones y respuestas inadecuadas a incidentes (-15).

Bloque 38: Manipulación de la Configuración Intencionados

Tabla 63 Manipulación de la Configuración Intencionados

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar controles y validaciones de cambios de configuración más estrictos	Mejora la seguridad y la estabilidad del sistema (+20), reduce la incidencia de errores y manipulaciones (+15). Requiere inversión en herramientas y tiempo para la configuración (-10).	Menor inversión inicial (+5), pero alta vulnerabilidad a manipulaciones y errores de configuración (-20).

Desarrollar protocolos de recuperación y respaldo rápidos y efectivos	Facilita la restauración rápida del sistema en caso de cambios maliciosos o errores (+15), mejora la resiliencia del sistema (+10). Requiere inversión en soluciones de respaldo y tiempo para pruebas (-10).	Ahorro a corto plazo (+5), pero riesgo de tiempos de inactividad prolongados y pérdida de datos en caso de problemas de configuración (-15).
Capacitar y concienciar al personal respecto a la seguridad de la configuración	Mejora la cultura de seguridad y reduce el riesgo de errores internos (+10), fortalece la postura general de seguridad (+10). Requiere inversión en formación y tiempo del personal (-10).	Ahorro en costos de capacitación (+5), pero mayor riesgo de errores humanos y vulnerabilidad a ataques internos (-15).

Bloque 39: Suplantación de la Identidad del Usuario

Tabla 64 Suplantación de la Identidad del Usuario

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de autenticación multifactor más robustos	Mejora significativa en la seguridad de las cuentas de usuario (+20), reduce el riesgo de accesos no autorizados (+20). Requiere inversión en tecnología y capacitación (-10).	Menos costos iniciales (+5), pero vulnerabilidad significativa a suplantaciones y accesos no autorizados (-20).
Revisar y fortalecer las políticas de seguridad y acceso	Mejora la postura de seguridad general de la organización (+15), establece límites claros y protocolos de acceso (+15). Requiere tiempo y recursos para la revisión y la implementación (-10).	Menos esfuerzo a corto plazo (+5), pero mayor riesgo de brechas de seguridad y accesos no autorizados (-15).
Proporcionar capacitación sobre concienciación y prevención de suplantación de identidad	Mejora la concienciación de los empleados y reduce el riesgo de errores humanos (+15), fortalece la cultura de seguridad (+10). Requiere inversión en programas de formación y tiempo del personal (-10).	Ahorro en costos de capacitación (+5), pero mayor vulnerabilidad a errores humanos y ataques de ingeniería social (-20).

Bloque 40: Abuso de Privilegios de Acceso

Tabla 65 Abuso de Privilegios de Acceso

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y redefinir los niveles de privilegios y accesos de los usuarios	Mejora la seguridad y minimiza el riesgo de abuso de privilegios (+20), requiere tiempo y recursos para implementar (-10).	Menos esfuerzo a corto plazo (+5), pero mayor riesgo de abuso de privilegios y brechas de seguridad (-20).
Implementar sistemas de monitoreo y alerta de	Mejora la detección de actividades sospechosas y abuso de privilegios (+20),	Ahorro en costos de implementación (+5), pero

actividad de usuarios con privilegios	requiere inversión en tecnología y capacitación (-10).	vulnerabilidad significativa a abusos no detectados (-20).
Proporcionar capacitación y concienciación sobre el uso responsable de privilegios de acceso	Mejora la concienciación de los usuarios y reduce el riesgo de abusos (+15), requiere inversión en programas de formación y tiempo del personal (-10).	Ahorro en costos de capacitación (+5), pero mayor riesgo de abusos por desconocimiento o negligencia (-15).

Bloque 41: Uso No Previsto

Tabla 66 Uso No Previsto

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y actualizar las políticas de uso aceptable y las medidas de control	Ayuda a aclarar las expectativas y reglas de uso (+15), puede requerir tiempo y recursos para desarrollar y comunicar los cambios (-10).	Mantenimiento del estatus quo, sin costo adicional (+5), pero riesgo de continuar con usos no previstos y posibles daños (-20).
Proporcionar capacitación y concienciación continua a los usuarios sobre las políticas de uso	Fomenta la comprensión y el cumplimiento de las políticas (+20), requiere inversión en formación y tiempo del usuario (-10).	Ahorro en tiempo y recursos de formación (+5), pero posible ignorancia o malentendido de las políticas por parte de los usuarios (-15).
Implementar sistemas de monitoreo de actividad de usuarios para detectar usos no conformes	Permite la detección proactiva de usos no conformes y la respuesta rápida (+20), requiere inversión en tecnología y posible resistencia de los usuarios a ser monitoreados (-15).	Ahorro en costos de implementación de tecnología (+5), pero riesgo de no detectar usos no conformes hasta que sea demasiado tarde (-20).

Bloque 42: Difusión de Software Dañino Intencionado

Tabla 67 Difusión de Software Dañino Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en soluciones antivirus y antimalware más robustas y actualizadas	Protege contra una amplia gama de amenazas y minimiza el riesgo de infección (+20), requiere inversión en software y recursos para mantenimiento (-10).	Ahorro en costos de software y mantenimiento (+5), pero riesgo significativo de infección y daño potencial a los sistemas y datos (-20).
Realizar análisis y limpiezas de seguridad regulares en los sistemas	Ayuda a detectar y remediar rápidamente cualquier infección (+20), requiere tiempo y recursos para realizar análisis regulares (-10).	Ahorro en tiempo y recursos (+5), pero riesgo de no detectar infecciones a tiempo, lo que podría resultar en daños más graves (-20).
Proporcionar capacitación al	Aumenta la conciencia y la capacidad de respuesta del	Ahorro en tiempo y recursos de formación (+5), pero riesgo de

personal sobre prevención y respuesta ante programa maligno	personal, reduciendo el riesgo de infección (+20), requiere inversión en formación y tiempo del personal (-10).	que el personal no esté preparado para prevenir o responder a infecciones de programa maligno (-20).

Bloque 43: [Re-Encaminamiento] de Mensajes Intencionado

Tabla 68 [Re-Encaminamiento] de Mensajes Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y fortalecer los protocolos y sistemas de seguridad de transmisión de mensajes	Mejora la seguridad en la transmisión de mensajes y reduce el riesgo de re-encaminamiento indebido (+20), requiere inversión en tecnología y tiempo para la revisión (-10).	Ahorro en inversiones y tiempo (+5), pero alto riesgo de exposición de mensajes y compromiso de la integridad (-20).
Implementar soluciones de cifrado y autenticación para la comunicación	Protege la confidencialidad e integridad de los mensajes transmitidos, haciéndolos incomprensibles para los actores maliciosos (+20), requiere inversión en tecnología de cifrado y autenticación (-10).	Ahorro en costos de implementación (+5), pero alto riesgo de intercepción y manipulación de mensajes (-20).
Realizar auditorías y monitorización continua del tráfico de mensajes	Permite la detección temprana y la respuesta a cualquier actividad sospechosa o no autorizada (+20), requiere inversión en herramientas de monitoreo y recursos para la auditoría (-10).	Ahorro en costos de herramientas y recursos (+5), pero riesgo de no detectar re-encaminamientos indebidos, lo que podría resultar en fugas de información y compromiso de la seguridad (-20).

Bloque 44: Alteración de Secuencia

Tabla 69 Alteración de Secuencia

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de verificación y control de secuencia más robustos	Asegura que los datos se reciban y procesen en el orden correcto, manteniendo la integridad y evitando errores (+20), requiere inversión en tecnología y tiempo para la implementación (-10).	Ahorro en inversiones y tiempo de implementación (+5), pero alto riesgo de errores y pérdida de integridad en los datos (-20).
Revisar y mejorar los protocolos y herramientas de transmisión y procesamiento de datos	Mejora la eficiencia y confiabilidad en el manejo de los datos (+20), requiere tiempo y recursos para la revisión y actualización (-10).	Ahorro en tiempo y recursos (+5), pero riesgo de mantener sistemas obsoletos y propensos a errores (-20).

Proporcionar capacitación sobre la importancia de la integridad de la secuencia de datos	Aumenta la concienciación y responsabilidad del personal en mantener la integridad de los datos (+15), requiere inversión en programas de formación (-5).	Ahorro en costos de capacitación (+5), pero falta de conciencia y posibles errores por parte del personal (-15).

Bloque 45: Acceso No Autorizado

Tabla 70 Acceso No Autorizado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y fortalecer las medidas y sistemas de control de acceso	Aumenta la seguridad y reduce el riesgo de accesos no autorizados (+20), requiere inversión en tecnología y tiempo para la implementación (-10).	Ahorro en inversiones y tiempo de implementación (+5), pero alto riesgo de intrusiones y violaciones de seguridad (-20).
Realizar auditorías de seguridad y pruebas de penetración regularmente	Identifica vulnerabilidades y mejora la seguridad de los sistemas (+15), requiere tiempo y recursos para realizar las auditorías y pruebas (-10).	Ahorro en tiempo y recursos (+5), pero mayor exposición a vulnerabilidades no detectadas (-15).
Proporcionar capacitación continua sobre concienciación y prevención de seguridad a los usuarios	Aumenta la concienciación y responsabilidad del personal en la seguridad (+15), requiere inversión en programas de formación (-5).	Ahorro en costos de capacitación (+5), pero falta de conciencia y posibles errores de seguridad por parte del personal (-15).

Bloque 46: Análisis de Tráfico

Tabla 71 Análisis de Tráfico

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar encriptación avanzada para proteger el tráfico de red	Mejora significativa en la confidencialidad y seguridad de la transmisión de datos (+20), requiere inversión en tecnología y posible impacto en el rendimiento (-10).	Ahorro en inversiones y recursos (+5), pero alta exposición a riesgos de espionaje y violación de datos (-20).
Instalar sistemas de detección de intrusiones más efectivos	Aumenta la capacidad para detectar y responder a actividades sospechosas (+15), requiere inversión en herramientas y capacitación (-10).	Ahorro en costos de implementación y capacitación (+5), pero mayor vulnerabilidad a actividades no detectadas y potenciales brechas de seguridad (-15).
Realizar auditorías regulares de seguridad de red	Contribuye a identificar vulnerabilidades y mejorar la postura de seguridad general (+15), requiere tiempo y recursos para llevar a cabo las auditorías (-5).	Ahorro en recursos y tiempo (+5), pero posibilidad de no detectar problemas de seguridad a tiempo (-15).

Bloque 47: Repudio Intencionado

Tabla 72 Repudio Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar un sistema de control de integridad y no repudio más robusto	Asegura la confiabilidad de los registros y la capacidad para atribuir acciones a usuarios específicos (+20), requiere inversión en tecnología y puede ser complejo de implementar (-10).	Ahorro en inversiones y recursos (+5), pero riesgo significativo de no poder probar la autoría de las acciones (-20).
Realizar auditorías regulares y monitoreo continuo de actividades sospechosas	Mejora la detección de actividades sospechosas y la capacidad de respuesta (+15), requiere recursos para monitoreo y auditorías (-10).	Ahorro en recursos y tiempo (+5), pero mayor riesgo de no detectar actividades fraudulentas a tiempo (-15).
Proporcionar capacitación sobre la importancia y las implicaciones legales del repudio	Aumenta la conciencia y la responsabilidad entre los usuarios (+10), requiere tiempo y recursos para la capacitación (-5).	Ahorro en tiempo y recursos (+5), pero menor conciencia y potencial aumento de intentos de repudio (-10).

Bloque 48: Interceptación de Información (Escucha)

Tabla 73 Interceptación de Información (Escucha)

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de cifrado de comunicaciones más avanzados	Fortalece la confidencialidad y seguridad de las comunicaciones (+20), puede requerir inversión significativa en tecnología y capacitación (-10).	Ahorro en costos y recursos (+5), pero riesgo continuo y potencialmente creciente de interceptación de comunicaciones (-20).
Adoptar redes privadas virtuales (VPN) para proteger la transmisión de datos	Mejora la seguridad y privacidad de las comunicaciones, especialmente en entornos remotos o públicos (+15), puede incurrir en costos adicionales y requerir configuración compleja (-10).	Ahorro en costos (+5), pero exposición a riesgos de seguridad en la transmisión de datos, especialmente en redes no seguras (-15).
Realizar revisión y mejora continua de los protocolos de seguridad de comunicación	Asegura que las prácticas de seguridad estén actualizadas y sean eficaces (+10), requiere tiempo y recursos para revisión y actualización constantes (-5).	Menos recursos dedicados a revisión y actualización (+5), pero potencial para que los protocolos de seguridad queden obsoletos y sean menos eficaces (-10).

Bloque 49: Modificación Deliberada de la Información

Tabla 74 Modificación Deliberada de la Información

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de control de integridad de datos más efectivos	Refuerza la confiabilidad y exactitud de los datos (+20), puede requerir una inversión significativa y tiempo para implementarse (-10).	Ahorro en costos y recursos (+5), pero permanece el riesgo de manipulación de datos y la posible pérdida de integridad (-20).
Realizar auditorías de datos y monitorización en tiempo real	Permite la detección rápida y la respuesta a manipulaciones no autorizadas (+15), requiere recursos y herramientas adicionales para monitoreo constante (-10).	Menos inversión en recursos y herramientas de monitoreo (+5), pero mayor riesgo de no detectar manipulaciones a tiempo (-15).
Proporcionar capacitación y concienciación sobre la seguridad e integridad de los datos	Fomenta una cultura de seguridad y prevención entre los empleados (+10), puede requerir tiempo y recursos para el desarrollo de programas de formación (-5).	Ahorro en tiempo y recursos destinados a formación (+5), pero los empleados pueden no estar plenamente concienciados o preparados para prevenir manipulaciones (-10).

Bloque 50: Destrucción de Información Intencionado

Tabla 75 Destrucción de Información Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en soluciones de respaldo y recuperación de datos más robustas y automáticas	Asegura la integridad y disponibilidad de los datos (+20), puede requerir inversión significativa y recursos (-10).	Ahorro en costos y recursos (+5), pero se mantiene el riesgo de pérdida permanente de datos críticos (-20).
Revisar y reforzar las políticas y herramientas de seguridad y protección de datos	Mejora la seguridad general de los datos y reduce la vulnerabilidad a ataques (+15), puede requerir tiempo y recursos para implementación y formación (-10).	Menos inversión en tiempo y recursos (+5), pero permanece la exposición a amenazas y posibles brechas de seguridad (-15).
Realizar pruebas regulares de recuperación de desastres y planes de continuidad de negocio	Asegura la preparación y resiliencia frente a incidentes (+10), puede implicar interrupciones temporales y uso de recursos para pruebas (-5).	Menos interrupciones y ahorro de recursos (+5), pero la organización puede no estar preparada para responder efectivamente a un incidente grave (-10).

Bloque 51: Divulgación de Información Intencionado

Tabla 76 Divulgación de Información Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Reforzar las políticas y prácticas de manejo y clasificación de información confidencial	Aumenta la protección de la información confidencial y mejora la conciencia sobre su manejo adecuado (+15), puede requerir tiempo y recursos para la implementación y capacitación (-5).	Ahorro en tiempo y recursos (+5), pero se mantiene el riesgo de divulgación no autorizada de información (-15).
Invertir en tecnologías avanzadas de cifrado y control de acceso	Refuerza la seguridad y protección de los datos confidenciales (+20), implica costos de inversión y posiblemente tiempo de implementación (-10).	Ahorro financiero y de tiempo (+5), pero permanece la vulnerabilidad de los datos a accesos no autorizados (-20).
Realizar campañas regulares de concienciación sobre seguridad de la información entre el personal	Mejora la comprensión y responsabilidad del personal en la protección de la información (+10), requiere inversión en formación y recursos (-5).	Menor inversión en capacitación y recursos (+5), pero se mantiene un nivel bajo de concienciación y responsabilidad del personal (-10).

Bloque 52: Manipulación de Programas Intencionado

Tabla 77 Manipulación de Programas Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y fortalecer los protocolos de revisión y validación de código	Mejora la calidad y seguridad del código (+15), requiere tiempo y recursos adicionales para implementar los nuevos procesos (-5).	Ahorro en tiempo y recursos (+5), pero persiste el riesgo de manipulación de código y vulnerabilidades (-15).
Implementar sistemas de detección de manipulación de software	Refuerza la seguridad del software y detecta manipulaciones rápidamente (+20), implica costos de inversión y mantenimiento (-10).	Ahorro financiero y de recursos (+5), pero se mantiene expuesto a manipulaciones de software y posibles brechas de seguridad (-20).
Proporcionar capacitación al personal en prácticas seguras de programación y revisión de código	Aumenta la competencia y la conciencia de seguridad del equipo de desarrollo (+10), requiere inversión en formación y tiempo (-5).	Menor inversión en capacitación (+5), pero persiste la falta de concienciación y habilidades en seguridad del software (-10).

Bloque 53: Manipulación de los Equipos Intencionado

Tabla 78 Manipulación de los Equipos Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Revisar y mejorar las medidas de seguridad física y de acceso a los equipos	Refuerza la seguridad del entorno físico (+15), requiere inversión financiera y tiempo (-10).	Ahorro en gastos y recursos (+5), pero persiste la vulnerabilidad en la seguridad física y acceso a los equipos (-15).
Establecer protocolos más estrictos de monitoreo y control de cambios en los equipos	Mejora la trazabilidad y control de las operaciones en los equipos (+20), puede requerir inversión en nuevas tecnologías y capacitación (-10).	Ahorro en inversión tecnológica y capacitación (+5), pero aumenta el riesgo de no detectar manipulaciones a tiempo (-20).
Proporcionar capacitación en seguridad y manejo de equipos a los empleados	Aumenta la concienciación y las habilidades de los empleados para prevenir y detectar manipulaciones (+10), requiere inversión en formación y tiempo (-5).	Menor inversión en capacitación (+5), pero los empleados pueden no estar preparados para prevenir o responder a manipulaciones (-10).

Bloque 54: Denegación de Servicio Intencionado

Tabla 79 Denegación de Servicio Intencionado

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en infraestructura y herramientas para mitigar ataques de denegación de servicio	Mejora la resistencia contra los ataques DDoS, protegiendo la disponibilidad del servicio (+20), requiere una inversión significativa en tecnología y mantenimiento (-15).	Ahorro económico a corto plazo (+5), pero aumenta el riesgo de futuros ataques DDoS y daño a la reputación de la empresa (-20).
Implementar sistemas de monitoreo y respuesta rápida ante caídas de servicio	Mejora la capacidad para detectar y responder rápidamente a los incidentes (+15), puede requerir inversión en tecnología y personal (-10).	Ahorro en inversión tecnológica y de personal (+5), pero aumenta el tiempo de inactividad y el impacto en los usuarios durante un ataque (-15).
Desarrollar y practicar planes de contingencia y recuperación ante incidentes de seguridad	Asegura una respuesta eficaz y una rápida recuperación en caso de incidentes (+15), requiere tiempo y recursos para el desarrollo y práctica de los planes (-10).	Ahorro de recursos y tiempo (+5), pero la empresa queda expuesta y posiblemente mal preparada para responder a incidentes de seguridad (-20).

Bloque 55: Robo

Tabla 80 Robo

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Mejorar las medidas de seguridad física y digital para prevenir robos	Fortalece la protección contra robos y accesos no autorizados (+20), requiere una inversión significativa en tecnología y personal (-15).	Ahorro a corto plazo (+5), pero se mantiene vulnerable a robos y accesos no autorizados, poniendo en riesgo los datos y activos de la empresa (-20).
Implementar sistemas de rastreo y recuperación de datos y equipos robados	Facilita la recuperación de activos y la identificación de los responsables (+15), puede ser costoso implementar y mantener estos sistemas (-10).	Ahorro económico (+5), pero se aumenta el riesgo de pérdida permanente de activos y datos valiosos (-15).
Capacitar al personal sobre procedimientos de prevención y respuesta ante robos	Aumenta la conciencia y preparación del personal frente a posibles robos (+10), requiere tiempo y recursos para la capacitación (-5).	Ahorro de tiempo y recursos (+5), pero el personal podría no estar preparado para prevenir o responder adecuadamente ante un robo (-10).

Bloque 56: Ataque Destructivo

Tabla 81 Ataque Destructivo

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Invertir en soluciones de seguridad cibernética avanzadas y proactivas	Aumenta la resiliencia frente a ataques destructivos (+20), requiere inversión económica significativa (-15).	Ahorro a corto plazo (+5), pero se mantiene vulnerable a ataques destructivos, poniendo en riesgo la integridad de los datos y la continuidad operativa (-20).
Desarrollar y practicar planes de recuperación de desastres y continuidad del negocio	Mejora la capacidad de respuesta y recuperación frente a ataques destructivos (+15), requiere inversión en tiempo y recursos para desarrollo y entrenamiento (-10).	Ahorro de tiempo y recursos (+5), pero la falta de preparación puede resultar en tiempos de inactividad prolongados y pérdida de datos críticos (-15).
Capacitar al personal en la identificación y prevención de ataques destructivos	Aumenta la conciencia y preparación del personal frente a ataques destructivos (+10), requiere tiempo y recursos para la capacitación (-5).	Ahorro de tiempo y recursos (+5), pero el personal podría no estar preparado para identificar o prevenir ataques destructivos, aumentando el riesgo de daño (-10).

Bloque 57: Ocupación Enemiga

Tabla 82 Ocupación Enemiga

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar sistemas de detección y respuesta a intrusiones más efectivos	Aumenta la capacidad de identificar y responder a amenazas rápidamente (+20), requiere inversión económica y de tiempo para implementación y mantenimiento (-10).	Ahorro a corto plazo (+5), pero se mantiene una alta vulnerabilidad ante ocupaciones enemigas, poniendo en riesgo la integridad y disponibilidad de los sistemas (-20).
Revisar y fortalecer las políticas y sistemas de seguridad	Mejora la robustez del entorno de seguridad y reduce el riesgo de intrusiones exitosas (+15), requiere inversión en tiempo y recursos para análisis y mejora (-10).	Ahorro de tiempo y recursos (+5), pero se mantiene un nivel de seguridad posiblemente insuficiente, incrementando el riesgo de ocupaciones enemigas (-15).
Realizar ejercicios regulares de respuesta a incidentes de seguridad	Mejora la preparación y tiempo de respuesta del equipo de seguridad ante incidentes (+10), requiere inversión en tiempo y recursos para planificación y ejecución (-5).	Ahorro de tiempo y recursos (+5), pero puede resultar en una respuesta tardía o ineficiente ante una ocupación enemiga real, aumentando el daño potencial (-10).

Bloque 58: Indisponibilidad del Personal

Tabla 83 Indisponibilidad del Personal

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Desarrollar e implementar planes de sucesión y respaldo de personal	Mejora la resiliencia organizacional frente a la pérdida de personal crítico (+15), requiere inversión en tiempo y recursos para desarrollo e implementación (-5).	Ahorro a corto plazo (+5), pero incrementa la vulnerabilidad ante la indisponibilidad de personal clave, poniendo en riesgo la continuidad de las operaciones (-15).
Invertir en la capacitación y desarrollo de más miembros del equipo en habilidades de seguridad	Aumenta la capacidad interna y reduce la dependencia de individuos específicos (+10), requiere inversión económica y de tiempo para capacitación (-10).	Ahorro económico a corto plazo (+5), pero mantiene una baja redundancia de habilidades críticas, aumentando el riesgo ante la indisponibilidad de personal (-10).
Contratar servicios externos de seguridad cibernética como respaldo	Provee un soporte inmediato y experto en caso de necesidad (+10), implica costos adicionales y posibles cuestiones de confidencialidad (-10).	Ahorro económico (+5), pero aumenta la vulnerabilidad ante situaciones de crisis, careciendo de un respaldo experto inmediato (-10).

Bloque 59: Extorsión

Tabla 84 Extorsión

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Implementar soluciones de seguridad avanzadas para prevenir ransomware	Fortalece la infraestructura de seguridad cibernética, reduciendo la probabilidad de futuros ataques (+15), requiere inversión económica significativa (-10).	Ahorro económico a corto plazo (+5), pero mantiene una alta vulnerabilidad a ataques de ransomware, poniendo en riesgo la integridad y disponibilidad de los datos (-15).
Establecer protocolos de respuesta y recuperación ante ataques de ransomware	Mejora la capacidad de respuesta y minimiza el impacto en caso de ataque (+10), requiere inversión en tiempo y recursos para su desarrollo e implementación (-5).	Ahorro en recursos a corto plazo (+5), pero aumenta el tiempo y costo de recuperación en caso de ataque, y puede resultar en pérdida de datos críticos (-10).
Realizar campañas de concienciación sobre riesgos y prevención de ransomware entre el personal	Aumenta la conciencia y preparación del personal, reduciendo el riesgo de infecciones por programa maligno (+10), requiere inversión en tiempo y recursos para su desarrollo e implementación (-5).	Ahorro en recursos a corto plazo (+5), pero mantiene una baja conciencia y preparación del personal, aumentando el riesgo de ataques exitosos de ransomware (-10).

Bloque 60: Ingeniería Social (Picaresca)

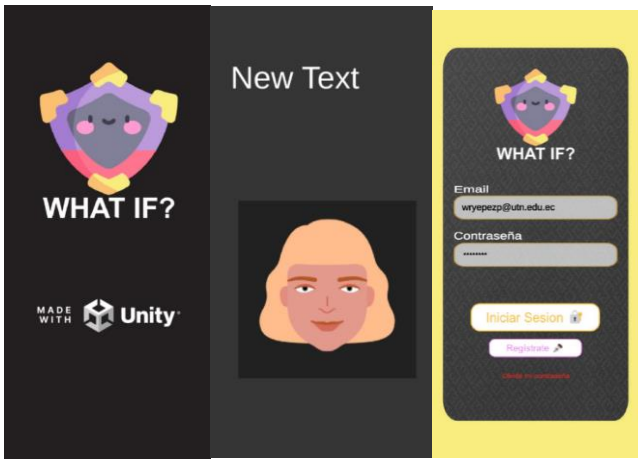
Tabla 85 Ingeniería Social (Picaresca)

Propuesta de Mitigación	Análisis de Aceptación	Análisis de Rechazo
Proporcionar capacitación y concienciación sobre ingeniería social a todos los empleados	Aumenta la conciencia y preparación del personal para detectar y evitar ataques de ingeniería social (+10), requiere inversión en tiempo y recursos para el desarrollo e implementación (-5).	Ahorro en recursos a corto plazo (+5), pero mantiene una baja conciencia y preparación del personal, aumentando el riesgo de ataques exitosos de ingeniería social (-10).
Implementar sistemas de verificación de identidad más estrictos	Fortalece la autenticación y verifica la identidad de las personas que acceden a recursos sensibles (+10), requiere inversión económica en tecnología y capacitación (-5).	Ahorro económico a corto plazo (+5), pero permite una mayor vulnerabilidad a ataques de ingeniería social debido a la autenticación débil (-10).

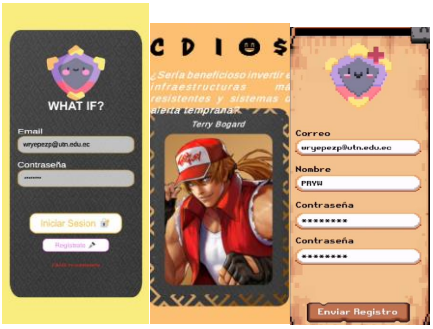
Revisar y reforzar las políticas de seguridad y respuesta ante incidentes de ingeniería social	Mejora las políticas y procedimientos para prevenir, detectar y responder a ataques de ingeniería social (+10), requiere tiempo y recursos para su revisión y actualización (-5).	Ahorro en tiempo y recursos a corto plazo (+5), pero mantiene políticas y procedimientos obsoletos y vulnerables a ataques de ingeniería social (-10).

A5. Evolución de los prototipos del videojuego.

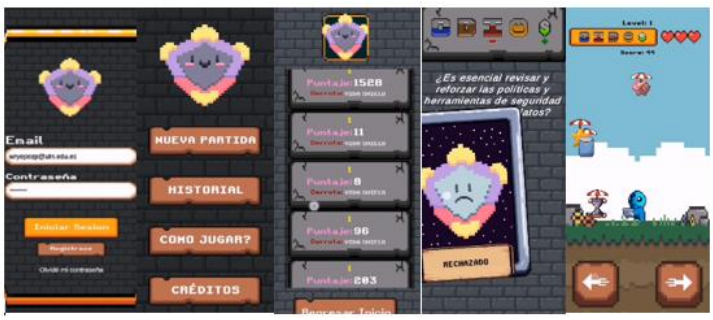
Versión 1



Versión 2



Versión 4



A5. Encuesta

Encuesta de Impacto Videojuego Ciberseguridad

Hola y gracias por participar,

En esta importante fase de nuestra investigación sobre ciberseguridad. Como parte de nuestro estudio para evaluar el impacto de un videojuego educativo en el conocimiento y las actitudes hacia la ciberseguridad, te pedimos que completes dos encuestas breves.

La primera encuesta, que realizarás antes de interactuar con el videojuego, busca comprender tu nivel actual de conocimientos y percepciones sobre la ciberseguridad.

La segunda, que se administrará después de jugar, tiene como objetivo evaluar cualquier cambio o mejora en tu comprensión y actitudes hacia este tema crucial.

Tus respuestas son valiosas y nos ayudarán a medir la eficacia del videojuego como herramienta educativa. Aseguramos la confidencialidad de tus respuestas, que solo se utilizarán con fines de investigación.

¡Agradecemos tu tiempo y tus aportes sinceros!

* Indicates required question

1. Edad

Mark only one oval.

- ◯ 18 a 23
- ◯ 24 a 29
- ◯ 30 a 35
- ◯ 35 o más

2. Género

Mark only one oval.

- ◯ Masculino
- ◯ Femenino

Encuesta Pre-Exposición del Videojuego

Objetivo: Evaluar el nivel de conocimiento hacia la ciberseguridad antes de la experiencia con el videojuego.

Instrucciones: *Por favor, responde las siguientes preguntas basándote en lo que has aprendido de ciberseguridad.*

3. **¿Estás familiarizado/a con los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?** *

**CID: Confidencialidad, Integridad y Disponibilidad de la información*

Mark only one oval.

- ◯ Sí
- ◯ No

4. **¿Consideras importante la ciberseguridad en tu vida diaria?** *

Mark only one oval.

- ◯ Sí
- ◯ No

5. **¿Crees que los videojuegos pueden ser una herramienta efectiva para aprender sobre ciberseguridad?** *

Mark only one oval.

- Sí
- No

6. **¿Tienes conocimientos sobre cómo protegerte contra ataques al CID de la Información?** *

Mark only one oval.

- Si
- No

7. **¿Conoces Tips de Seguridad para mantener el CID de la información?** *

Mark only one oval.

- Sí
- No

8. **¿Estás al tanto del Catálogo de Elementos de Magerit V3 y su relevancia para la ciberseguridad?** *

Mark only one oval.

- Sí
- No

9. **¿Te sientes motivado/a para aprender más sobre ciberseguridad?** *

Mark only one oval.

- Sí
- No

¡Vamos a jugar!

Por favor, descarga el juego e instálalo en tu celular o pídele a al encuestador que te facilite un dispositivo con la aplicación, las credenciales ya están cargadas en el juego, inicia sesión con esa cuenta.

(👉ﾟヮﾟ)👉 *Videojuego de Seguridad*

Encuesta Post-Exposición del Videojuego

Objetivo: Evaluar el impacto del videojuego en la comprensión hacia la ciberseguridad después de la experiencia de juego.

Instrucciones: *Por favor, responde las siguientes preguntas basándote en lo que has aprendido y experimentado después de jugar el videojuego de ciberseguridad.*

10. **¿Comprendes los conceptos de Confidencialidad, Integridad y Disponibilidad (CID) en ciberseguridad?** *

Mark only one oval.

- ◯ Sí
- ◯ No

11. **¿Pudiste identificar cómo las decisiones tomadas en el juego afectaron la CID de la información?** *

Mark only one oval.

- ◯ Sí
- ◯ No

12. **¿Ha cambiado tu percepción sobre la importancia de la ciberseguridad en tu vida diaria tras jugar?** *

Mark only one oval.

- ◯ Sí
- ◯ No

13. **¿Consideras ahora que los videojuegos son una herramienta efectiva para aprender sobre ciberseguridad?** *

Mark only one oval.

- Sí
- No

14. **¿El juego ha influenciado tu percepción sobre la importancia de la ciberseguridad, tanto a nivel personal como organizacional?** *

Mark only one oval.

- Sí
- No

15. **¿Consideras útil el contenido basado en Magerit para comprender mejor las amenazas de ciberseguridad?** *

Mark only one oval.

- Sí
- No

16. **¿Te ha motivado el videojuego a buscar más información y seguir educándote en ciberseguridad?** *

Mark only one oval.

- Sí
- No