UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
**SEGURIDAD DE LA INFORMACIÓN**

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

# PROPUESTA DE ENSEÑANZA DE CIBERSEGURIDAD PARA EJECUTIVOS CON LA FINALIDAD QUE TRANSFORMEN, LIDEREN Y APLIQUEN EN SUS EMPRESAS.

AUTORES:

ROLANDO JAVIER REYES ALTAMIRANO
ROBERTO JOSUÉ RODRÍGUEZ POVEDA

DIRECTOR:

JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR
2024

**Autores:**

**Rolando Javier Reyes Altamirano**
Ingeniero Sistemas mención Telemática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
rreyes@est.ups.edu.ec

**Roberto Josué Rodríguez Poveda**
Ingeniero Sistemas mención Gestión de la Información.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
rrodriguezpo@est.ups.edu.ec

**Dirigido por:**

**José Luis Aguayo Morales**
Ingeniero en Electrónica y Telecomunicaciones.
Magister en Ciberseguridad.
Magister en Redes y Comunicaciones.
Magister en Sistemas Informáticos Educativos.
jaguayo@ups.edu.ec


Propuesta de enseñanza de ciberseguridad para ejecutivos con la finalidad que transformen, lideren y apliquen en sus empresas.

***DEDICATORIA***

A mi querida y amada familia, a mis padres, por su apoyo y amor incondicional en todo este proceso, gracias por enseñarme los valores como el esfuerzo, responsabilidad, dedicación, respeto, honestidad, dedicación, y por ser mi inspiración en cada paso de este camino, sin su confianza en mí y sus consejos este logro más no sería posible. A mis hermanas, por ser mis compañeras de vida y brindarme siempre su aliento y motivación. A mi hijo, desde el momento en que llegaste a mi vida, has sido mi mayor fuente de inspiración y motivación, cada sonrisa y cada gesto me inspiran para salir adelante, esta tesis es un reflejo del amor que siento por ti, y espero que un día comprendas que todo lo que hago es por ti y para ti. Mi amada esposa, gracias por ser mi compañera de vida, mi mejor amiga, y por estar siempre a mi lado, compartiendo sueños, risas, desafíos y las infaltables peleas, no podría haber alcanzado este logro sin tu paciencia y amor inquebrantable.

**Rolando Reyes**

Este trabajo de tesis está dedicado a mis pilares fundamentales de vida, a mi amada esposa, Gabriela Alvear Richards, por su amor incondicional, apoyo constante y por ser mi mayor fuente de inspiración. Sin tu comprensión y paciencia, este proyecto no habría sido posible. A mi madre, Teresa Poveda, por su amor eterno y por ser mi guía y pilar en cada paso de este camino. Tu fortaleza y dedicación me han enseñado el verdadero significado de la perseverancia. Y a mi querido padre, Xavier Bustamante, cuya memoria sigue siendo una fuente de fortaleza y sabiduría. Aunque ya no estás físicamente con nosotros, tu legado y enseñanzas continúan iluminando mi camino.

Con todo mi cariño y gratitud,

**Roberto Rodríguez Poveda**

***AGRADECIMIENTO***

Mi profundo agradecimiento a mis padres por su apoyo, su amor, gracias por enseñarme el valor del esfuerzo, dedicación, honradez, responsabilidad, puntualidad, humildad y perseverancia, por estar siempre a mi lado apoyándome en todas mis decisiones.

A mis hermanas gracias por su apoyo incondicional, por sus consejos, por siempre estar cuando las necesito.

A mi hijo por ser mi inspiración, la fuerza para seguir adelante y por recordarme que el amor es el motor más poderoso. Espero que siempre persigas tus sueños con pasión y determinación.

A mi esposa por su amor, su paciencia durante todo este tiempo, tu apoyo ha sido fundamental para conseguir este logro.

A mis queridos y apreciados maestros, gracias por su guía y por compartir conmigo su conocimiento y experiencia. Su apoyo ha sido fundamental en este proceso.

**Rolando Reyes**

Quisiera expresar mi más sincero agradecimiento a todas las personas que han sido parte de este proceso. A mis profesores, colegas y amigos por sus valiosos consejos y apoyo. Agradezco también a todas las personas que han compartido su tiempo, conocimientos y paciencia conmigo, haciendo posible la culminación de esta tesis. Su contribución ha sido invaluable y profundamente apreciada.

**Roberto Rodríguez Poveda**

# Tabla de Contenido

# Tabla de Figuras

# Propuesta de enseñanza de ciberseguridad para ejecutivos con la finalidad que transformen, lideren y apliquen en sus empresas.


Autor(es):

Rolando Javier Reyes Altamirano
Roberto Josue Rodriguez Poveda

# Resumen

En la actualidad, todas las empresas enfrentan una constante amenaza de ciberataques, sin importar su tamaño o sector. Los líderes empresariales, como ejecutivos, deben comprender plenamente la importancia de la ciberseguridad y estar listos para abordar estos desafíos. Estos ejecutivos tienen la responsabilidad de tomar decisiones estratégicas y operativas que involucran información confidencial de la empresa. Por lo tanto, es esencial que estén capacitados y así proteger los datos y garantizar la privacidad de empleados y clientes. Además, el aumento de las regulaciones de protección de datos hace que la ciberseguridad sea un requisito ineludible para las empresas.

Los ejecutivos deben comprender y asegurarse de que sus organizaciones cumplan con estas regulaciones para evitar sanciones legales y daños a la reputación de la empresa. La capacidad de responder rápidamente y prevenir ciber incidentes es crucial para evitar perjuicios a la imagen empresarial así se mantiene la confianza de sus partes interesadas. Para que los ejecutivos valoren la importancia de la ciberseguridad en términos estratégicos y financieros, es fundamental proporcionarles conciencia sobre este tema. Al capacitar a los ejecutivos, se puede iniciar una instrucción de seguridad en toda la empresa, difundiendo buenas prácticas en todos los niveles. Esto, a su vez, puede brindar una mejoría a nivel competitivo en el cliente, las empresas con sólidas estrategias de ciberseguridad y ejecutivos capacitados suelen ser más atractivas para clientes y socios comerciales.

En última instancia, el programa de formación permitirá que los ejecutivos estén preparados para abordar adecuadamente posibles ciberataques o incidentes de seguridad, tomando decisiones fundamentadas y coordinando respuestas efectivas para minimizar los impactos y recuperarse con éxito. Con ejecutivos capacitados en ciberseguridad, las empresas estarán protegidas y listas para liderar en un entorno digital, protegiendo activos, resguardando la privacidad de los datos y manteniendo la seguridad de todos sus socios comerciales y clientes.

**Palabras clave:**

Ciberseguridad, ejecutivos, empresas, privacidad.

# Abstract

Today, all companies face a constant threat of cyberattacks, regardless of their size or sector. Business leaders, as executives, must fully understand the importance of cybersecurity and be ready to address these challenges. These executives are responsible for making strategic and operational decisions that involve confidential company information. Therefore, it is essential that they are trained to protect data and ensure the privacy of employees and customers. Furthermore, the increase in data protection regulations makes cybersecurity an unavoidable requirement for companies.

Executives must understand and ensure their organizations comply with these regulations to avoid legal penalties and damage to the company's reputation. The ability to respond quickly and prevent cyber incidents is crucial to avoid damage to the business image and maintain the trust of its stakeholders. For executives to value the importance of cybersecurity in strategic and financial terms, it is essential to provide them with awareness on this topic. By training executives, you can initiate company-wide security training, spreading good practices at all levels. This, in turn, can provide an improvement in the client's competitive level; companies with solid cybersecurity strategies and trained executives tend to be more attractive to clients and business partners.

Ultimately, the training program will enable executives to be prepared to appropriately address potential cyberattacks or security incidents, making informed decisions and coordinating effective responses to minimize impacts and recover successfully. With executives trained in cybersecurity, companies will be protected and ready to lead in a digital environment, protecting assets, safeguarding data privacy, and maintaining the security of all their business partners and customers.

**Palabras clave:**
Cybersecurity, executives, companies, privacy.

# 1. Introducción

La ciberseguridad es un tema crítico hoy en día, principalmente para las empresas que manejan información sensible y datos confidenciales de clientes. A medida que los ciberataques continúan evolucionando y volviéndose más sofisticados, los altos ejecutivos deben recibir capacitación en ciberseguridad para liderar e implementar defensas en sus empresas.

Algunos factores que respaldan la propuesta de enseñanza de ciberseguridad a los ejecutivos incluyen:

a) Aumento de ataques cibernéticos empresariales: En los últimos años, ha habido un aumento en los ataques cibernéticos dirigidos a empresas, lo que ha causado importantes pérdidas económicas y daños a la reputación de las empresas afectadas.
b) Falta de conciencia en ciberseguridad: Muchas empresas carecen de una sólida cultura de ciberseguridad, lo que las hace vulnerables a ataques cibernéticos.
c) Regulaciones y requerimientos legales: En Ecuador, existe actualmente la ley de protección de datos personales, es crucial que empresas y ejecutivos estén al tanto de estas regulaciones y se aseguren de cumplirlas.
d) Mejora de la imagen empresarial: Implementar medidas efectivas de ciberseguridad, como la adopción de normas ISO y SGSI, puede mejorar significativamente la imagen de una empresa ante sus clientes y aumentar la confianza en sus servicios y productos.

La información como el activo valioso que debe protegerse debido a su impacto en ámbitos políticos, sociales, económicos y personales. Tanto los ejecutivos como los trabajadores en general deben adquirir conocimientos básicos sobre seguridad de la información para desempeñar sus funciones profesionales de manera responsable y cumplir con los estándares reconocidos para salvaguardar la

información. Para prevenir problemas comunes de ciberseguridad, es esencial integrar la educación tecnológica con prácticas seguras de uso.

El proyecto se enfoca en educar y concientizar sobre la ciberseguridad a todo nivel tanto ejecutivos y trabajadores para mitigar posibles ataques que puedan afectar la información y la salud financiera de las empresas.

# 2. METODOLOGÍA

Para cumplir los objetivos mencionados y planteados anteriormente, se implementa la siguiente metodología:

Análisis de necesidades: Lo primero será plasmar un análisis donde consten las necesidades para determinar las áreas de conocimiento en ciberseguridad que requieren los ejecutivos empresariales. Este análisis incluye una evaluación de riesgos cibernéticos a los que las empresas se exponen y las mejores prácticas de seguridad informática que se deben adoptar, además de analizar de una manera amplia estadísticas, recursos para mitigar ataques cibernéticos y así reducir la afectación de la información, recursos económicos y humanos.

Diseño de ambiente virtual de enseñanza: Una vez que se ha realizado el análisis de necesidades, se debe diseñar un ambiente virtual de enseñanza en la plataforma Moodle. Esto incluye la construcción de una serie de módulos, definición de los metas de aprendizaje, selección de herramientas para la enseñanza que se utilizarán, como videos, infografías, cuestionarios, debates, evaluaciones, etc.

Desarrollo de contenido educativo: Se debe generar el contenido educativo para la enseñanza de las mejores prácticas y conceptos fundamentales de ciberseguridad. El contenido debe ser fácil y breve de comprender para los ejecutivos empresariales y personal de todas las áreas. Además, se debe asegurar que el contenido sea actualizado y relevante a las necesidades de la empresa.

Creación de materiales de concientización para ejecutivos: Desarrollar material específico dirigido a los ejecutivos empresariales, empleados que destaque los riesgos cibernéticos y la importancia de la ciberseguridad para la empresa. Utilizar lenguaje claro y ejemplos relevantes para su comprensión.

Implementación de la metodología: Una vez que se ha desarrollado el contenido educativo, se debe implementar la metodología en la plataforma Moodle. Esto incluye la publicación de los módulos o curso, la creación de grupos de trabajo para los ejecutivos empresariales, empleados y la definición de un cronograma de trabajo.

Evaluación y retroalimentación: Es importante evaluar el aprendizaje de los ejecutivos empresariales, empleados y proporcionar retroalimentación para mejorar el proceso de enseñanza. Esto se puede lograr a través de pruebas y evaluaciones.

La ciberseguridad es un campo en constante cambio, por lo que es esencial mantener el curso actualizado con las últimas tendencias y amenazas en el mundo digital. Revisar y actualizar el contenido periódicamente para garantizar la relevancia y la efectividad del curso, que se verá reflejado en las decisiones empresariales y mitigación de ataques a la empresa.

La metodología que se tomó como referencia para el desarrollo es Magerit (Metodología Análisis y Gestión de Riesgos de Sistemas de Información) como un cuadro de trabajo producido que tiene como objetivo dar a conocer a las empresas, directivos a reconocer, evaluar y tratar los peligros asociados al uso de tecnologías de información.

Magerit, al ser una metodología específica que ayuda a la gestión de riesgos en sistemas de información, proporciona un marco claro para entender cómo las amenazas y vulnerabilidades afectan los activos en una empresa. A través de la identificación de estos riesgos desde el principio, los ejecutivos pueden comprender mejor la importancia de la ciberseguridad y el impacto en una empresa.

Su principal objetico es identificar y evaluar los activos críticos, lo cual es esencial para priorizar la protección en una organización. La metodología proporciona

herramientas y técnicas para realizar evaluaciones de riesgos detalladas, alineadas con los objetivos del curso. Además, incluye procesos para el análisis de vulnerabilidades, lo que permite a los ejecutivos entender las debilidades específicas de sus sistemas y cómo mitigarlas.

Entre uno de los principales objetivos de la metodóloga Magerit es ayudar a estructurar e implementar políticas de seguridad efectivas basadas en los riesgos identificados. Esto es crucial para que los ejecutivos desarrollen estrategias de protección sólidas. La metodología también enfatiza en lo importante del orden para la utilización de tecnologías adecuadas para prevenir incidentes.

Magerit incluye la planificación para la continuidad y respuesta a incidentes de un negocio. Esto facilita a los ejecutivos la creación de procedimientos de respuesta eficaces y la planificación de la recuperación, asegurando que la organización pueda reducir los posibles impactos de incidentes a nivel de seguridad. Magerit fomenta una comunicación estructurada durante las crisis, lo que es vital para la gestión eficaz de incidentes.

La metodología está diseñada para alinearse con normativas y marcos regulatorios, lo que ayuda a los ejecutivos a asegurarse de que sus estrategias de ciberseguridad cumplan con las leyes y estándares aplicables. También facilita la implementación de políticas de cumplimiento y la preparación para auditorías, asegurando una gestión continua y efectiva del riesgo. Es flexible y permite la adaptación a nuevas amenazas y tecnologías emergentes. A través de su enfoque iterativo y de actualización constante, los ejecutivos pueden aplicar estrategias de evolución continua, asegurando que sus empresas estén preparadas para enfrentar los desafíos futuros en ciberseguridad.

# 3. Determinación del Problema

En el mundo actual, las empresas enfrentan constantes amenazas de ciberataques, sin importar su tamaño o sector. Es esencial que los ejecutivos, en su papel como líderes de estas organizaciones, tengan un profundo conocimiento de la importancia de la ciberseguridad y estén preparados para abordar las amenazas. También es fundamental que los ejecutivos asuman el compromiso de ser garantes para el cumplimiento de regulaciones en sus organizaciones, evitando posibles sanciones legales y protegiendo la reputación de la empresa. Además, una reacción efectiva y rápida ante cualquier tipo de incidentes es esencial para preservar la percepción de la empresa y conservar la seguridad de usuarios y asociados.

El Índice Global de Ciberseguridad (GCI) tiene como objetivo evaluar el compromiso con la ciberseguridad de los 194 miembros de la Unión Internacional de Telecomunicaciones. El puesto 97 en ocupado por Ecuador en el ranking global, con una calificación de 0,36 sobre un total de 1 punto. Este informe considera diversos factores, como el marco legal, la existencia de reguladores, la cooperación entre entidades y los programas de investigación y desarrollo ((ENISA), 2021).

Este proyecto se enfocará en analizar los principios de la ciberseguridad, con el propósito de proporcionar una educación más efectiva a los ejecutivos. Esto permitirá que comprendan plenamente el impacto real de los ataques cibernéticos, incluyendo las amenazas a la seguridad de la información de una empresa y el daño financiero que pueden causar. También se proporcionarán conceptos clave y consejos de seguridad que pueden compartirse con sus equipos, asegurando que todos cumplan con los principios de seguridad al identificar claramente las amenazas, vulnerabilidades y controles preventivos.

En los últimos 10 años, el aumento de ataques de virus, malware y otros incidentes tecnológicos ha sido significativo. Según diversos estudios y reportes, hay una relación clara entre la falta de capacitación en temas tecnológicos de los empleados y la prevalencia de estos ataques.

## 3.1 Números claves sobre ciberataques:

- Aumento global de ciberataques: Según el 2023 Data Breach Investigations Report de Verizon, el 74% de las brechas de seguridad en empresas fueron causadas por errores humanos o la participación involuntaria de empleados mal capacitados. Además, el número de ciberataques se ha triplicado desde 2013.

- Ataques de ransomware: El ransomware, que bloquea los diferentes tipos de acceso hasta cuando se cancele el rescate solicitado, ha aumentado de manera alarmante. Según un informe de “Cybersecurity Ventures”, el costo del ransomware fue de 8.5 mil millones de dólares en 2021, y se espera un incremento que alcance 20 mil millones de dólares para 2025. En muchos de estos ataques, los empleados abren correos electrónicos con enlaces maliciosos por falta de capacitación.

- Errores humanos en la ciberseguridad: Según el informe de IBM "Cost of a Data Breach 2023", el 82% de las brechas de seguridad fueron resultado de errores humanos o negligencia interna. La falta de concienciación sobre ciberseguridad es un factor importante que contribuye a estos errores.

- Phishing: Los ciberataques de tipo phishing continúan siendo una de las maneras más usuales de ataque. En 2023, el 80% de los incidentes de seguridad relacionados con phishing involucraron a empleados que fueron engañados para proporcionar credenciales de acceso, lo que refleja una clara falta de formación en el reconocimiento de correos electrónicos sospechosos o sitios falsos.

- Costos asociados a la capacitación inadecuada: Según un informe de Ponemon Institute, el precio intermedio de una brecha de datos debido a la falta de capacitación en ciberseguridad es de 4.24 millones de dólares. En muchos casos, la inversión en capacitación es insuficiente, lo que permite

que los empleados se conviertan en un eslabón débil en la cadena de seguridad.

## 3.2 Relación con la falta de capacitación:

- Falta de formación en ciberseguridad: Muchas empresas no brindan formación suficiente o continua en temas de ciberseguridad a sus empleados, lo que contribuye a la vulnerabilidad. De acuerdo con Gartner, solo el 20% de las organizaciones brindan capacitaciones mensuales o más frecuentes, a pesar de que los ciberataques están en aumento.

- Click en enlaces maliciosos: Según Proofpoint, el 75% de las organizaciones reportaron haber sido víctimas de ataques de phishing, la mayoría debido a que los empleados hicieron clic en enlaces maliciosos. Esto demuestra que, si bien la tecnología es importante, la capacitación es crucial para minimizar el riesgo.

- Actualización insuficiente sobre nuevas amenazas: Las amenazas evolucionan constantemente. El hecho de que los empleados no estén al día con las nuevas formas de ataques, como el deepfake phishing o el spear phishing dirigido, hace que sean más propensos a caer en estos esquemas, comprometiendo los sistemas empresariales.

# 4. Marco teórico referencial

En la actualidad, la ciberseguridad es un tema importante. debido a la creciente cantidad de ciberataques que ocurren en todo el mundo. Los ejecutivos de empresas son especialmente vulnerables a estos ataques, ya que tienen acceso a información confidencial y de alto valor que puede ser manipulada por los ciberdelincuentes y así adquirir beneficios económicos inclusive políticos. Esta sección presenta una revisión exhaustiva de la literatura sobre ciberseguridad en el ámbito empresarial, así como teorías y conceptos relevantes.

## 4.1 Concepto de ciberseguridad:

La ciberseguridad protege los sistemas informáticos, las redes y los dispositivos electrónicos contra el acceso no autorizado, la manipulación de datos y el robo de información. Se trata de un conjunto de métodos y herramientas que se utilizan para garantizar que los datos y sistemas informáticos sean seguros, integrados y accesibles (Gleason, 2022).

## 4.2 Importancia de la ciberseguridad para las empresas:

La ciberseguridad es fundamental para las empresas debido a que la mayoría de los negocios se basan en tecnología y en la información que se maneja por medio de ella. Un ciberataque puede poner en riesgo la continuidad del negocio, la seguridad de los usuarios y la popularidad de la empresa. Además, en muchos casos las empresas pueden ser responsables legalmente por la pérdida o robo de información confidencial.

## 4.3 Enseñanza de ciberseguridad para ejecutivos:

La responsabilidad de tomar decisiones estratégicas y guiar a sus equipos hacia el éxito recae en los ejecutivos de empresas. En este sentido, es esencial que los ejecutivos estén capacitados en ciberseguridad para poder tomar decisiones informadas y para liderar a sus equipos en la ejecución de las medidas de seguridad adecuadas. Además, debido a que los ejecutivos son uno de los primordiales objetivos de los ataques cibernéticos, es crucial que estén preparados para detectar y responder a estos ataques.

## 4.4 Características de una enseñanza de ciberseguridad para ejecutivos:

Las necesidades únicas de cada empresa y ejecutivo requieren una enseñanza de ciberseguridad para ejecutivos. Debe incluir información sobre los peligros y amenazas cibernéticas, las mejores prácticas de seguridad, la implementación de medidas de seguridad y la detección y respuesta a los ciberataques. Además, debe ser realista para la empresa y fomentar una cultura de la seguridad informatica en todos los niveles.

## 4.5 Conciencia y responsabilidad:

Los ejecutivos deben ser responsables de la seguridad de la información y reconocer su papel en la toma de decisiones estratégicas para salvaguardar los datos que son relacionadas con la ciberseguridad.

## 4.6 Gestión de riesgos:

Los líderes deben comprender cómo evaluar y gestionar los riesgos cibernéticos y tomar decisiones informadas para mitigarlos (Gleason, 2022).

## 4.7 Transformación digital:

Se aborda la necesidad de que las empresas adopten tecnologías digitales y cómo esto influye en su exposición a riesgos cibernéticos (Gleason, 2022).

## 4.8 Resiliencia empresarial:

En la era de la información, se entiende como resilencia la capacidad de una empresa para recuperarse en el menor tiempo posible de incidentes o ataques de ciberseguridad. (Gleason, 2022).

## 4.9 Innovación y adaptación:

La ciberseguridad no debe verse como un obstáculo, sino como un facilitador de la innovación y así adaptarse a un entorno empresarial cambiante.

## 4.10 Integración de la ciberseguridad:

Cómo los ejecutivos pueden incorporar la ciberseguridad en la estrategia empresarial, incluyendo la inversión en tecnología y la formación del personal.

## 4.11 Gestión de incidentes:

Contar con planes de respuesta a incidentes y comunicación efectiva en caso de una violación de seguridad es crucial para la seguridad de una empresa ya que esto permitirá salvaguardar la información.

## 4.12 Educación y formación:

La capacitación continua y la concienciación son importantes para garantizar que todos los empleados, incluidos los ejecutivos, estén preparados para abordar los desafíos de la ciberseguridad.

# 5. CIBERSEGURIDAD EN TI

Sin un enfoque monetario la ciberseguridad, se enfoca en el desarrollo de competencias clave como la valoración de riesgos, la ejecución de medidas de protección y la gestión de crisis. El objetivo principal es fomentar un conocimiento de seguridad dentro de las instituciones, ayudando a los ejecutivos a tomar decisiones informadas y proteger los activos críticos de sus empresas, contribuyendo al bienestar general de la organización en lugar de generar ingresos.

Las organizaciones han logrado pocos avances a la hora de abordar el riesgo cibernético, en gran parte porque han visto el problema con un enfoque excesivamente limitado como simplemente una cuestión técnica/operativa, para competir en la economía moderna, las empresas deben emprender la transformación digital, la transformación digital puede generar un aumento sustancial del crecimiento y la rentabilidad, pero también puede aumentar enormemente el riesgo en ciberseguridad, las normas de seguridad fundamentales son necesarias, pero por sí solas no son suficientes para hacer frente a las amenazas cibernéticas. La ciberseguridad debe ser una preocupación central en la gestión de riesgos de toda la empresa., las organizaciones no pueden protegerse completamente, pero pueden gestionar su riesgo cibernético con una comprensión, estructura, inversión y métodos de gestión de riesgos adecuados.

La comunidad de atacantes está ganando la batalla del ciberespacio, que es uno de los hechos más irreversibles si no se toman medidas inmediatas en el campo de la ciberseguridad, y ganando por un margen amplio y creciente. En febrero de 2020, el director ejecutivo del Centro de Ciberseguridad del Foro Económico Mundial, Troels Oerting, se dirigió al Grupo de Trabajo de Economía Digital del G20 en Riad, Arabia Saudita, e informó que el año anterior el cibercrimen le había costado a la economía mundial 2 billones de dólares. El Foro Económico Mundial estimó que las pérdidas aumentarán a 6 billones de dólares en una proyección en tres años. El G20

es un grupo de las economías más grandes del mundo. Aunque la nación del cibercrimen no tiene un Producto Interno Bruto, los daños causados por el cibercrimen en su conjunto son equivalentes al PIB de los 10 principales países del G20, justo por delante del Reino Unido (Gleason, 2022).

Hay varias razones por las que el cibercrimen es un problema tan enorme y creciente, pero ningún es más fundamental que el hecho de que el tema de la ciberseguridad se malinterpreta enormemente. La mayoría de los gobiernos, empresas e individuos consideran la ciberseguridad un problema técnico o de TI. El cual es un nombre inapropiado. La ciberseguridad es un tema importante para la gestión de incidentes de toda la empresa. Obviamente, la tecnología es una parte importante.

Según el Manual de supervisión del riesgo cibernético publicado por la Asociación Nacional de directores Corporativos (NACD): Históricamente, muchas empresas y organizaciones categorizaron la ciberseguridad como una cuestión técnica y operativa donde debía manejarse por el área tecnológica de cada organización. Este malentendido se vio alimentado por estructuras operativas aisladas que dejaron que, en la mayoría de las organizaciones, las funciones y unidades de negocios se sienten desconectadas de la responsabilidad de proteger sus propios datos; en cambio, esta responsabilidad crítica recae en TI, un departamento que en la mayoría de las organizaciones tiene pocos recursos y autoridad presupuestaria. Además, transferir la responsabilidad a TI inhibió el análisis crítico y la comunicación sobre cuestiones de seguridad y obstaculizó la adopción de estrategias de seguridad efectivas en toda la organización (Gleason, 2022).

En consecuencia, la gran mayoría de las iniciativas diseñadas para abordar los problemas de ciberseguridad son técnicas y operativas, y las personas seleccionadas para gestionar el problema son casi siempre especialistas en TI.

El 77% de las organizaciones todavía operan con ciberseguridad y resiliencia limitadas contra las ciberamenazas, mientras que el 87% de las organizaciones advierten que aún no tienen suficiente presupuesto para brindar los niveles de

ciberseguridad y resiliencia que desean. La realidad es que la ciberseguridad no es sólo una cuestión de TI. Debe entenderse como un riesgo empresarial estratégico, no sólo como un riesgo de TI. Existen múltiples tipos diferentes de riesgos que una baja ciberseguridad puede generar: pérdida de datos, corrupción de datos, chantaje, daño a la reputación de la organización, así como riesgos legales y de cumplimiento. La responsabilidad de gestionar estos riesgos cibernéticos se extiende a toda la organización, lamentablemente, las relaciones entre la función de ciberseguridad y otros elementos críticos del negocio suelen estar plagadas de malentendidos y desconfianza. Una encuesta realizada en 2020 encontró que, en la mayoría de las organizaciones, había una falla sistémica en la comunicación entre la función de ciberseguridad y las unidades de negocio. Por ejemplo, descubrió que en el 74% de las organizaciones la relación entre la función de ciberseguridad y el departamento de marketing se caracterizaba como, en el mejor de los casos, de neutral a desconfiada o inexistente. En definitiva, la ciberseguridad es responsabilidad de todos. Si una organización considera que la ciberseguridad es esencialmente una cuestión técnica y confiere la gestión del riesgo cibernético únicamente a los departamentos de TI, obtendrá principalmente soluciones de TI que probablemente no serán suficientes para abordar todos sus riesgos cibernéticos. Para garantizar mejor que una organización esté haciendo las preguntas correctas sobre ciberseguridad, los líderes de la organización deben comprender que la ciberseguridad no estará a cargo de las personas de TI. La ciberseguridad debe entenderse y gestionarse de manera integral como un elemento integral del negocio y la misión de la organización. ESI ThoughtLab líderes en investigación y liderazgo completó un estudio de más de mil empresas a principios de 2020 y concluyó que, para reducir las probabilidades de riesgo, las autoridades como directores de seguridad de la información (CISO) deben ir mucho más allá del cumplimiento de los marcos técnicos. Los líderes en ciberseguridad deben integrar estos marcos técnicos en sus negocios. Objetivos, estrategias y perfiles de riesgo individuales. La transformación digital convierte la ciberseguridad en una cuestión empresarial. Las corporaciones han adoptado e incorporado tecnologías en ciberseguridad para infraestructuras y entornos de red y han logrado un crecimiento comercial y económico fenomenal a través de servicios mejorados,

mayor productividad y costos reducidos. Sin embargo, esta transformación digital respaldada por comunicaciones asequibles y dispositivos baratos ha introducido nuevos riesgos, cabe indicar que, en los últimos 25 años, la naturaleza del valor de los activos corporativos ha cambiado significativamente, alejándose de lo físico hacia lo virtual. Esta rápida digitalización de los activos corporativos ha resultado en una correspondiente transformación de estrategias y modelos de negocio, así como la digitalización del riesgo corporativo. Las organizaciones están aprovechando formas completamente nuevas de conectarse con clientes y proveedores, interactuar con los empleados y mejorar la eficacia y la productividad de los procesos internos (Gleason, 2022).

Desde hace varios años está de moda hablar de tecnologías disruptivas que generan modelos de negocio innovador y productivo. Las empresas se han apresurado a incorporar los beneficios de la era digital en sus planes de negocios, como expandir mercados a nivel mundial, reducir costos operativos, establecer nuevas asociaciones estratégicas o mejorar la experiencia de los trabajadores al permitir negocios a través de ubicaciones móviles y remotas. Según un estudio se encontró que el 83% de los directivos dijeron que apoyarían a la gerencia que emprendiera proyectos de innovación potencialmente disruptivos si tuvieran el potencial de aumentar el valor a largo plazo, incluso si crean riesgos adicionales. Un ejemplo regional de esto es América Latina, donde ha habido una adopción generalizada de plataformas de comunicaciones móviles (particularmente en servicios financieros), en un esfuerzo por impulsar el desarrollo económico que se necesita con urgencia. Sin embargo, esta rápida adopción ha llevado al sector a experimentar brechas importantes, ya que gran parte de la tecnología que se está implementando no cuenta con los controles de seguridad adecuados.

## 5.1 La Inteligencia Artificial y Ciberataques

Uno de los facilitadores de negocios más prometedores que se están implementando actualmente es la inserción de Inteligencia Artificial (IA) en los

procesos de negocios. Prácticamente todos los sectores industriales están buscando e implementando estas tecnologías mejoradas para crear nuevas tecnologías y promover ganancias y crecimiento. Sin embargo, al mismo tiempo, los ataques basados en IA tienen el potencial de aumentar enormemente el riesgo cibernético. Con su capacidad de aprender y adaptarse, la IA transformará el ciberdelito al permitir que los agresores ejecuten ataques más personalizados e insidiosos. Este entorno cibernético que cambia rápidamente está creando un panorama de amenazas cada vez más dinámico que exige un enfoque empresarial multidimensional y completo de la ciberseguridad. Los ataques de IA son únicos porque cuando penetran en un sistema, obtienen información sobre el sistema de defensa y evolucionan para contraatacar en consecuencia. Estos intentos no siempre funcionan en el primer intento, pero debido al conocimiento que adquieren, a menudo resultan fructíferos en intentos posteriores. Aunque existe una tendencia a una mayor conciencia de los riesgos de la IA entre los ejecutivos corporativos, pocos líderes han tenido suficiente conocimiento práctico para asociar los riesgos de la IA con el alcance completo de los riesgos sociales, económicos y organizacionales que plantean. Como resultado, los ejecutivos a menudo confían en las capacidades de mitigación de riesgos de la empresa y designan especialistas en TI para hacerlo. Es probable que esta visión unidimensional de la IA resulte contraproducente dados los amplios impactos que estas nuevas tecnologías tendrán en una organización en general. Esto significa que las cuestiones clave relativas a la transformación digital ya no se limitan a cómo la innovación tecnológica puede habilitar los procesos de negocio, sino más bien a cómo equilibrar las grandes transformaciones digitales con una gestión eficaz del riesgo cibernético inherente que puede comprometer los intereses estratégicos a largo plazo de la empresa. La gestión adecuada de este equilibrio difícil y a menudo friccional comienza con la comprensión de que el riesgo cibernético no se limita a dominios técnicos limitados, sino que se extiende por toda la empresa e impacta directamente en los resultados comerciales claves. Los equipos de gestión deben reconocer la tensión entre la necesidad de innovación estratégica (cada vez impulsada por la transformación digital) y los imperativos de preservar la seguridad y la confianza. Este elemento estratégico más amplio claramente necesita

involucrar a los expertos en TI, pero casi con certeza supera su experiencia en áreas que deben considerarse para desarrollar un modelo de negocio coherente y sostenible en la era digital, Con una gestión sofisticada y recursos adecuados, es posible que las organizaciones se defiendan sin dejar de ser competitivas y mantener la rentabilidad. Sin embargo, una ciberseguridad exitosa no puede incorporarse simplemente al final de los procesos comerciales. Debe unirse en las técnicas, procesos y cultura en una institución u organización desde el inicio hasta el final y, esto ayudara a crear una superioridad competitiva.

La ciberseguridad no puede considerarse aislada. Las instituciones pueden obtener la igualdad adecuada entre preservar la seguridad de una institución y atenuar las pérdidas a la vez se continúa garantizando el crecimiento en un medio competitivo. Las empresas líderes ven los riesgos cibernéticos de la misma manera que ven nuevos riesgos de nivel alto: en procesos de una prestación entre riesgo y recompensa. Sin embargo, este enfoque es desafiante por dos razones. En primer lugar, la complejidad de las amenazas cibernéticas ha aumentado drásticamente y continúa evolucionando. Las corporaciones afrontan amenazas más sofisticadas las cuales superan las defensas tradicionales, y los actores para las amenazas se han vuelto más diversos; incluidos no sólo los ciberdelincuentes sino también los hacktivistas. Al mismo tiempo, la necesidad competitiva de implementar tecnologías nuevas y emergentes para reducir gastos optimiza la asistencia al cliente e impulsar la innovación. Como hemos ilustrado, la adopción de estas innovaciones y capacidades tecnológicas puede ofrecer fuertes beneficios, pero también puede aumentar el riesgo cibernético. Si se implementaran adecuadamente, podrían aumentar la seguridad, pero sólo a un costo. La gerencia debe encontrar métodos para determinar cuál es el costo apropiado en relación con los apetitos de riesgo de la organización determinados por el plan de negocios. Las discusiones sobre ciberseguridad ya no pueden tratarse como apéndices, que pueden agregarse al final de una reunión de la junta directiva como una extensión del informe de TI. En la era digital, prácticamente no existe decisión empresarial sustancial que no tenga un componente de ciberseguridad. Si la empresa está considerando una fusión o adquisición, estarán combinando dos o más sistemas de

información altamente complejos. Las posibilidades de que se abran nuevas vulnerabilidades masivas que expongan la propiedad intelectual o los datos de los consumidores son sustanciales.

## 5.2 Ciberseguridad y Riesgo

La pandemia mundial de COVID19 que comenzó a finales de 2019 creó la transformación más grande y rápida en la forma de trabajar en la historia. También complicó aún más la situación del riesgo cibernético. Antes de la pandemia, aproximadamente el 20% de la fuerza laboral estadounidense trabajaba ocasionalmente desde casa, y prácticamente de la noche a la mañana el 80% cambió a plataformas en línea como un paso inevitable para conservar la viabilidad de trabajo. El creciente uso tecnológico, otro subproducto de la COVID19, también pasó factura. Un estudio de CrowdStrike reveló que el 56% de las personas ahora trabajaba desde casa debido al virus del covid19, y el 60% usaba sus dispositivos personales para trabajar. Las intrusiones cibernéticas ya aumentaron en el primer trimestre de 2020 (con el doble de ataques en el 2019), y el informe anticipaba que los ataques aumentarían significativamente a lo largo de 2020. El FBI informó que los ataques cibernéticos (muchos de ellos utilizando el COVID19 como señuelo) aumentaron casi un 200 % a las pocas semanas de que el virus llegara a los EE. UU, Para ser justos, calcular el impacto económico preciso del delito cibernético es extremadamente difícil porque probablemente no nos damos cuenta de la mayoría de los ataques cibernéticos hasta mucho después de que ocurren. Es extremadamente difícil calcular el impacto económico real de la propiedad intelectual robada (normalmente copiada digitalmente), e incluso cuando las empresas descubren ataques, a menudo no se denuncian públicamente. Calcular el impacto financiero de los ciberataques exitosos es sólo un aspecto de los costos de la ciberseguridad. Los ataques cibernéticos han generado todo tipo de costos que, si bien son sustanciales, no pueden calcularse fácilmente en dólares y centavos. Por ejemplo, las 17 agencias de inteligencia estadounidenses han confirmado que los rusos intentaron con éxito utilizar medios cibernéticos para comprometer las elecciones presidenciales estadounidenses de 2016. El costo de estos ataques

(incluso descontando el posible impacto en el resultado electoral) en términos de socavar la democracia estadounidense y la fe en el proceso democrático es literalmente incalculable. En 2015, la Agencia de Gestión de Personal en EE.UU fue atacada con éxito, lo que potencialmente comprometió información de alto valor y colocó en peligro la existencia de los oficiales de inteligencia estadounidenses, Alemania y otros países han informado de incursiones similares. Se dice que el gobierno chino ha intentado piratear en base a datos médicos en un intento de corromper la propiedad intelectual asociada con la investigación que crea una cura para COVID-19 (Gleason, 2022).

## 5.3 Vulnerabilidades

Dado el enorme daño potencial de los ataques cibernéticos, el crecimiento constante del problema durante varios años y con billones de dólares gastados para abordar el problema, sorprende que no haya habido más avances en la lucha contra el delito cibernético. Una posible razón de esta falta de progreso puede ser que la cuestión en general se ha considerado a través de una lente excesivamente estrecho y limitado, esencialmente como una cuestión operativa técnica. La historia de la ciberseguridad hasta el momento se define por su abrumadora atención a las vulnerabilidades de la tecnología operativa. Obviamente, las vulnerabilidades técnicas en el sistema son un elemento importante del problema de la ciberseguridad, pero no son el único elemento del problema. El principal asesor de ciberseguridad del presidente Obama, Michael Daniel, solía comentar que en su puesto tuvo la oportunidad de conocer a algunas de las personas que realmente escribieron los protocolos centrales en los que se basa el Internet. Una de las cosas que el Sr. Daniel informó, es haber aprendido en dichas conversaciones fue que los creadores tenían intenciones bastante modestas al crear Internet. Simplemente intentaban crear un sistema que permitiera a los científicos transmitir algunos datos de investigación de un lado a otro. No estaban tratando de diseñar un sistema que pudiera funcionar en todo el mundo, pero eso es lo que hemos hecho ahora. En el siglo XXI, prácticamente todo está basado en lo digital. Internet no sólo es vulnerable en su esencia, sino que a medida que el sistema continúa evolucionando,

lo hacemos cada vez más vulnerable técnicamente. Prácticamente nadie escribe código completamente desde cero. La técnica común es aprovechar los protocolos (vulnerables) que ya existen. A medida que los sistemas evolucionan, tanto la superficie de ataque como las vulnerabilidades continúan creciendo. Por ejemplo, un único proveedor de tecnología informó al Wall Street Journal en 2020 que en un año necesitaba aplicar 150 millones de parches a solo uno de sus sistemas más nuevos. Eso es solo un sistema y una empresa. Microsoft institucionalizó el modelo de parches en 2003 con el establecimiento de Patch Tuesday, cuando la compañía informa periódicamente sobre los nuevos parches que está lanzando para abordar las vulnerabilidades de sus productos, a veces docenas de parches, a veces cientos. Otros proveedores también lanzan parches, aunque con menos regularidad o transparencia. Algunos expertos han señalado que al martes de parches le sigue inevitablemente el "miércoles vulnerable", cuando los actores maliciosos, recién conscientes de las debilidades, atacan los sistemas en este estado. En 2020, un ISP informó que recibía un promedio de 80 mil millones de análisis maliciosos cada día. La Encuesta de ciberseguridad de EY de 2019 informó sobre un solo ataque que expuso 773 millones de registros, Microsoft ha informado que descubre 77.000 instancias de código malicioso cada mes, en 2019, los ataques de ransomware aumentaron un 41% en comparación con el cuarto trimestre de 2018. Se estima que una empresa será víctima de un ataque de ransomware cada 14 segundos. Una de las razones del aumento es la aparición del ransomware como servicio, el equilibrio económico entre atacantes y defensores en el ciberespacio favorece a los atacantes. Tienen bajos costos y altos márgenes de beneficio. También tienen un gran modelo de negocio porque pueden utilizar los mismos métodos repetidamente en un conjunto mundial de objetivos. Sus reservas de capital son sobresalientes ya que, además de sus enormes márgenes de ganancias, muchos ciberatacantes son estados nacionales reales o están afiliados a estados. Las organizaciones no pueden resolver sus problemas de ciberseguridad, el objetivo de una organización debe ser gestionar su riesgo cibernético a un nivel aceptable y coherente con su plan de negocio exclusivo. Llegar a la conclusión de que el problema de la ciberseguridad es un problema que afecta a toda la empresa y que no se debe simplemente a factores técnicos/operativos, sino que es el resultado de

incentivos económicos sincronizados, es el primer paso hacia la construcción de un sistema resiliente (Gleason, 2022).

## 5.4 Principios de ciberseguridad para juntas directivas

Es función de una junta directiva proporcionar la visión de la empresa, establecer la cultura de la organización, trabajar con la administración para definir en qué situación de riesgo esta una organización y supervisar la administración para garantizar que se esté cumpliendo con su gestión del riesgo cibernético, las juntas tienen ciertas responsabilidades de ciberseguridad que deben ejecutar dentro del contexto de la propia junta. Sin embargo, para tener un programa de riesgo cibernético en toda la empresa en pleno funcionamiento, los directivos y la gerencia deben comunicarse, cooperar entre sí, comprender sus funciones y responsabilidades (tanto para la empresa como entre sí) y garantizar que se cumplan efectivamente, los profesionales cibernéticos y los formuladores de políticas han pedido una mayor participación de las juntas corporativas para abordar las amenazas cibernéticas. En general, esa petición se tradujo en que los profesionales deben enseñar a los órganos directivos sobre conceptos de TI, con la esperanza de que si entendían completamente la tecnología apreciarían mejor la amenaza cibernética y se concentrarían en ella. Un tema importante en ciberseguridad desde la perspectiva de un director, en contraposición a la perspectiva estrictamente de un profesional de TI. La visión es crear un programa en el que la ciberseguridad fluyera de arriba hacia abajo, empezando por la junta directiva, a diferencia del paradigma en el que se esperaba que la ciberseguridad surgiera de los departamentos de TI, entonces, en lugar de explicar los estándares ISO, los marcos NIST y el crecimiento de la vulnerabilidad, el nuevo enfoque se centra en cuestiones comerciales que preocupan a los directores, como la innovación, el crecimiento, la rentabilidad y los índices, en lugar de describir dónde estaban las vulnerabilidades en el nuevo software, las juntas directivas tienen el desafío de preguntar: ¿qué problemas de ciberseguridad surgen al lanzar un nuevo producto? ¿Qué posibles problemas de ciberseguridad se producen al realizar una

fusión o adquisición?. El nuevo enfoque plantea lo cibernético como una cuestión principalmente de TI y lo conceptualizó para las juntas directivas como una cuestión de negocios, y llegaron a un acuerdo amplio, casi unánime sobre cinco principios clave, lo que debería guiar el proceso de la junta directiva en materia de ciberseguridad. Aunque hubo ligeras modificaciones en parte de la terminología utilizada en los distintos manuales, cinco principios básicos de consenso son la base de todos los manuales. Sin embargo, hubo algunas divergencias sustanciales en los diversos conjuntos de herramientas incluidos en las ediciones internacionales basadas en gran medida en las diferencias culturales de las distintas regiones. Los principios básicos del consenso se pueden resumir como:

Principio uno: La ciberseguridad no es una cuestión de "TI". Es un inconveniente de gestión de riesgos que aqueja a toda una organización.

Principio dos: Los directores deben estar al tanto de las implicaciones legales particulares de los riesgos cibernéticos para las circunstancias particulares de su empresa.

Principio tres: Las juntas directivas deben tener acceso suficiente a la experiencia en ciberseguridad, y las conversaciones sobre la gestión del riesgo cibernético deben llevarse a cabo con regularidad y en el tiempo adecuado.

Principio cuatro: Los directores deben esperar que la gerencia implemente un plan de gestión del riesgo cibernético en toda la empresa con personal y fondos adecuados.

Principio Cinco: Las diferencias de la junta en cuanto al riesgo cibernético deben añadir la identificación y cuantificación en la exposición financiera de los riesgos cibernéticos y qué riesgos admitir, mitigar o trasladar.

A medida que la transformación digital continúa acelerándose y los ciberatacantes continúan innovando, las organizaciones deben considerar adaptar sus estructuras para abordar mejor el nuevo panorama empresarial. Actualmente, la tecnología es más integral para la estrategia empresarial. La dirección ha asumido el papel de

implementar, gestionar y proteger nuevas capacidades tecnológicas en toda la organización. La tecnología integra a las instituciones, ya sea que los empleados estén en la misma infraestructura o en cualquier parte del mundo, las estructuras de presentación de informes y los procesos de toma de decisiones que utilizan muchas empresas provienen de un modelo operativo aislado, donde cada departamento y unidad de negocio toma decisiones y gestiona riesgos de forma relativamente independiente, sin tener plenamente en cuenta la interdependencia digital que es un hecho de los negocios modernos, si bien la práctica predeterminada en muchas organizaciones es aislar la ciberseguridad en una categoría separada aparte de la consideración de los activos más valiosos de una entidad, las organizaciones líderes están avanzando hacia una categoría más integrada, un modelo de riesgo integrado debería considerar el riesgo cibernético no como único o separado de otros riesgos comerciales sino como parte de un plan de gestión de riesgos integral. Tener un enfoque integrado del riesgo permite a las empresas abordar de manera más efectiva el riesgo de ciberseguridad en toda la empresa. A medida que las organizaciones adquieren conciencia cada vez más que la ciberseguridad es más que solo una función de TI, se han desarrollado modelos organizacionales que amplían la cantidad y los tipos de experiencia que deberían estar involucradas en la gestión de la función de ciberseguridad.

## 5.5 Riesgo en Ciberseguridad

Una cuestión fundamental a la hora de desarrollar una evaluación útil del riesgo cibernético es definir claramente a qué nos referimos cuando utilizamos el término riesgo cibernético. Los riesgos que podrían amenazar materialmente una empresa, aprovechado por una variedad de atacantes que resultan en pérdidas financieras significativas y tangibles, algunas de las cuales ascienden a miles de millones de dólares, términos como ransomware, filtración de datos y malware se están volviendo comunes tanto en los círculos técnicos como en las salas de juntas, como tal, discutir y evaluar el riesgo cibernético es ahora fundamental para, en última instancia, gestionar el riesgo cibernético de una organización, el riesgo cibernético es la exposición potencial a pérdidas o daños derivados de TI, la tecnología

informática de una organización, la exposición potencial se relaciona directamente con la probabilidad y gravedad del incidente, mientras que las pérdidas y los daños están asociados con daños financieros que surgen del robo o pérdida de propiedad, multas regulatorias, pérdida de clientes, bajas humanas y muchos otros elementos. El riesgo cibernético no es una categoría, es una cantidad que indica cuánto daño proviene de una exposición cibernética entendida en el contexto de la misión empresarial. El riesgo cibernético no se expresa de manera útil como un color, una calificación con letras, una puntuación o cualquier otro valor arbitrario que indique una pérdida real por exposición. El riesgo cibernético se representa de manera más útil en términos financieros dentro del contexto del negocio. El riesgo cibernético debe entenderse como parte de un ecosistema más amplio o en contexto con todos los demás riesgos de la organización, al representar el riesgo cibernético en términos financieros, una organización tiene una manera de compararlo y contrastarlo con todos los demás riesgos en la organización en general, los directores ejecutivos y corporativos no comprenderán valores vagos o confusos esperan comprender el riesgo cibernético de una manera que impulse la toma de decisiones informadas sobre la gestión de riesgos, que mejoren la salud de la institución, mejoren el valor para los accionistas y articulen la debida diligencia y el debido cuidado. Por ejemplo, si un miembro de la junta pregunta a un alto directivo: "¿cuál es nuestro riesgo cibernético en relación con una fusión, el lanzamiento de una nueva asociación estratégica o el despliegue de una nueva tecnología?", entonces querrán saber si esa decisión comprometerá ingresos, aumentar gastos o causar cualquier otro daño a la organización que no pueda resistirse. Cada organización debe establecer su nivel de tolerancia al riesgo. La tolerancia al riesgo es la medida en la que una organización puede distinguir entre el riesgo que no puede soportar y el riesgo que puede soportar fácilmente. Si el riesgo cibernético está por encima de esta tolerancia definida, entonces los directores ejecutivos y corporativos pueden decidir remediar, transferir o evitar ese riesgo, El riesgo cibernético, en el contexto empresarial, es más útil entenderlo no como una categoría sino como una cantidad. Los líderes empresariales no se basan en la intuición ni en valores arbitrarios para gestionar el riesgo cibernético, en cambio,

los líderes empresariales utilizar un método actualizado para evaluar el riesgo cibernético. Un método actual para evaluar el peligro cibernético permitirá:

- Simplificar la contemplación del riesgo cibernético.
- Traducir las métricas tradicionales de ciberseguridad en detalles financieros.
- Proporcionar un medio para una evaluación estándar y repetible del riesgo cibernético.
- Pronosticar la exposición financiera debido al riesgo cibernético.
- Proporcionar un conjunto de orientaciones prioritarias sobre remediación y transferencia.
- Combinar el riesgo cibernético con los reportes de gestión de riesgos de la organización.

Los líderes empresariales no son expertos en ciberseguridad y la mayoría no comprende la importancia de la ciberseguridad, los líderes empresariales necesitan un método que produzca resultados en un lenguaje que comprendan, una evaluación de riesgos moderna traduce las métricas tradicionales de ciberseguridad en detalles financieros. Las métricas técnicas son importantes. Proporcionan una comprensión de la implementación de amenazas, vulnerabilidades y controles, pueden informar los planes tácticos y mostrar pruebas de mejora, sin embargo, no está claro cómo se relacionan directamente con la salud financiera de la empresa, las métricas técnicas son las más utilizadas por los CISO y los oficiales de seguridad de la información (CIO), para comprender mejor la infraestructura de TI. La mayoría de las métricas técnicas son producto de soluciones o herramientas técnicas, algunas de esas herramientas y soluciones incluyen:

- Herramientas de escaneo de vulnerabilidades.
- Herramientas de gestión del cumplimiento.
- Plataformas de monitoreo de eventos de seguridad.
- Plataformas de gestión de incidencias.

Los líderes empresariales generalmente revisan las métricas financieras cada 90 días (o trimestralmente), los líderes empresariales utilizan esta cadencia para

comprender los cambios financieros en el negocio y modificar la estrategia, así como existen prácticas contables estándar, deberían existir prácticas estándar de riesgo cibernético que produzcan evaluaciones repetibles, los líderes empresariales deben estar al tanto de cómo cambia la exposición financiera al riesgo cibernético cada tres meses. Una evaluación de riesgos contemporánea debe basarse en un conjunto estándar de prácticas tales como:

- Estructura.
- Recopilación de datos.
- Modelado.
- Integridad.
- Informes.

## 5.6 Amenazas Internas en Ciberseguridad

Una amenaza interna se define como una amenaza organizacional que se origina en un punto de entrada interno. En el escenario típico, un actor de amenazas emplea o manipula a personas con credenciales de acceso legítimas u obtiene de manera fraudulenta credenciales de acceso válidas para eludir las medidas de seguridad, luego logra ingresar a las instalaciones o sistemas de información de una organización y causa daño a una organización. El daño suele adoptar la forma de fraude, robo de activos, datos o propiedad intelectual o sabotaje, las amenazas internas pueden ser difíciles de reconocer porque no implican una violación obvia de seguridad perimetral, sino que dependen de privilegios de acceso aparentemente legítimos y de conocimientos relacionados con la ubicación de activos digitales valiosos, como tal los indicadores forenses de compromiso suelen ser más difíciles de detectar o más lentos de manifestar que en el caso de una infracción externa donde existe un punto de entrada claro externo a la red, hay tres tipos generales de información privilegiada: maliciosa, negligente e infiltrado. La ingeniería social se encuentra entre otros métodos comunes mediante los cuales los actores externos maliciosos comprometen a los internos negligentes, más del 90% de los ataques comienzan con un correo electrónico de phishing, la mala

administración de datos únicos por parte de personas internas puede resultar en un compromiso, a modo de ejemplo, en 2006, un analista de datos que trabajaba en el Departamento de Asuntos de Veteranos descargó identificaciones personales de 26,5 millones de militares de Estados Unidos (incluida la información de agentes estadounidenses encubiertos que aún se encontraban en posiciones encubiertas), en otro ejemplo, en 2019, Facebook perdió información personal y financieros de decenas de empleados cuando un empleado dejó una computadora portátil corporativa en un automóvil y se la robaron, los infiltrados son en realidad actores maliciosos externos, que de manera fraudulenta obtienen credenciales aparentemente válidas, se hacen pasar por titulares de credenciales válidas y utilizan las credenciales fraudulentas para causar daño a una organización, la amenaza interna más costosa por incidente es el robo de credenciales y la apropiación maliciosa de cuentas, estos incidentes han aumentado significativamente en frecuencia y costo, de hecho, la frecuencia de incidentes por empresa se ha triplicado desde 2016, de un promedio de 1 a 3,2 y el costo promedio ha aumentado de $493 093 a $871 686 en 2019, anualmente las organizaciones gastan más para hacer frente a la negligencia interna, pero el porcentaje del coste del incidente es mucho menor. Para contrarrestar las amenazas internas, las organizaciones deben incorporar profesionales como parte de equipos multidisciplinarios de gestión de amenazas para detectar, disuadir y mitigar eficazmente las amenazas internas. La información que reposa en RR.HH de una institución actúa como un depósito central de información del personal, los profesionales de RR.HH están en la mejor posición para identificar patrones, comportamientos y tendencias que ayudarán a mitigar daños potenciales a una organización y sus empleados, CISA alienta a los departamentos de recursos humanos a participar activamente en los esfuerzos de mitigación de amenazas internas mediante el establecimiento de un marco de evaluación que incluya indicadores de amenazas, perfiles de datos y señales de comportamiento, una comprensión integral de los flujos de datos y la visibilidad de actividades potencialmente anómalas, respetando al mismo tiempo la privacidad y la seguridad. Muchos ciberataques importantes de los últimos años recuerdan cómo las identidades mal administradas y comprometidas presentan un riesgo enorme y

brindan a los atacantes acceso a activos valiosos, tener un programa sólido de gestión de accesos es un elemento crítico para abordar estos riesgos, un plan de respuesta integrado también debe tener en cuenta los riesgos y amenazas internos, si bien el primer paso es desarrollar las capacidades, lo que potencialmente es aún más desafiante a largo plazo es garantizar la sostenibilidad y escalabilidad de estos esfuerzos, probar, ajustar y mejorar rutinariamente los procesos y tecnologías ayudará a abordar y reducir la superficie de riesgo (Gleason, 2022).

## 5.7 Requisitos de Auditoria para Ciberseguridad

La protección de datos de la empresa y la privacidad de los datos de los clientes y empleados está respaldada por una amplia gama de leyes, regulaciones y estándares de ciberseguridad, dada la importancia cada vez mayor de la ciberseguridad dentro de la empresa, es necesario abordar a fondo el papel del cumplimiento y la auditoría, una función de cumplimiento bien diseñada abordará las tres áreas clave, incluidas las políticas (y su documentación), el comportamiento y la tecnología, muchas empresas se apresuran a canalizar sus recursos y tiempo limitados para cumplir con la regulación en lugar de centrarse de manera más integral en desarrollar controles sólidos o pautas de seguridad, históricamente, debido a la naturaleza prescriptiva de las regulaciones de ciberseguridad que busca abordar, gran parte del papel del cumplimiento se ha centrado en iniciativas puntuales que pueden esforzarse por lograr solo el mínimo necesario para cumplir con las reglas prescritas por los reguladores específicos. La seguridad es el resultado de las acciones tomadas para proteger la información de una empresa, el cumplimiento es la documentación de esas acciones, si bien pueden existir controles que sirvan para proteger los sistemas, las redes y el software, una empresa no puede demostrar que los controles son adecuados para su propósito sin documentación. Aunque las funciones de cumplimiento y auditoría dentro de una organización están separadas de la gestión de seguridad/riesgos, cuanto más estrechamente puedan trabajar juntas estas disciplinas, más valor se podrá proporcionar, en pocas palabras, el equipo de seguridad es responsable de

implementar los controles sistemáticos necesarios para resguardar los activos de información, el equipo de cumplimiento valida que todos los controles estén funcionando según lo planeado. Los 2 equipos, trabajando en alianza, garantizarán que los controles de seguridad estén diseñados a escala y que toda la documentación y los informes requeridos sean accesibles para la auditoría. Contar con procesos claros, recursos de ciberseguridad capacitados y competentes y un marco de gobernanza es crucial para abordar las amenazas actuales y emergentes. Si bien aquellos que están siendo auditados bien pueden considerar que reunir evidencia y participar plenamente en la auditoría es una interrupción del negocio, aprender de los que no están a cargo del diseño y operación de los controles y procesos es fundamental para garantizar que el programa está cumpliendo con el objetivo de negocios. El proceso de auditoría, si se realiza correctamente, debería generar una rendición de cuentas adicional y servir para fortalecer el entorno de control interno de una empresa, la función de la auditoría interna en las áreas de ciberseguridad de una organización ha ido evolucionando rápidamente, ligado a la mayor participación del directorio, que realiza su propia supervisión sobre esta área, a medida que las juntas directivas desean obtener más información sobre la ciberseguridad, los auditores deben comprender y mantenerse al día con la evolución de los riesgos de ciberseguridad y brindar información sobre la suficiencia de las contramedidas para proteger mejor a las empresas, los auditores están bien posicionados para informar a toda la junta directiva en cuanto a la eficacia de los programas de ciberseguridad y los procedimientos de reducción de riesgos para mejorar la ciberseguridad general dentro de las organizaciones, además, el Gerente General de la empresa, también ayudará a brindarle a la junta información y asesoramiento sobre los cambios en los requisitos regulatorios, el papel de la auditoría se está ampliando para comprender el riesgo de muchas áreas dentro de la organización con el fin de abordar adecuadamente la seguridad de la información a un nivel organizacional, la adopción de la transformación y la implementación de tecnología, la gestión del talento humano, a medida que la auditoría sale de sus áreas funcionales tradicionales y trabaja con varias contrapartes dentro del negocio, puede proporcionar más que una simple evaluación del cumplimiento y ayudar a lograr una ciberseguridad mejorada. El enfoque global en la

transformación digital de la empresa abre nuevas áreas donde puede operar una auditoría interna, los proyectos tecnológicos estratégicos, incluida la modernización de la infraestructura, las iniciativas de mejora del rendimiento operativo y la digitalización de productos y servicios, van acompañados de la adopción de nuevas metodologías de desarrollo de software, como DevOps, que aceleran el ritmo del cambio, control de calidad y seguridad de la información a lo largo de todas las fases de los proyectos tecnológicos estratégicos, un equipo de auditoría interna puede identificar nuevos peligros y evaluar los procedimientos necesarios para los cambios en el entorno de control, en particular aquellos que afectan la segregación de funciones, las normas de auditoría actuales exigen que el auditor externo comprenda cómo la organización utiliza las tecnologías y cómo esa tecnología afecta los estados financieros, en la auditoría, se suele centrar especial atención en los controles de tecnologías de la información que están diseñados para garantizar el trabajo eficiente de los controles automatizados y la confiabilidad de los datos e informes realizados por la organización que se utilizan para generar sus estados financieros y divulgaciones externos, aunque los elementos de las habilidades de para la gestión de riesgos de ciberseguridad pueden actualmente estar más allá del alcance de una auditoría típica de estados financieros, los contadores públicos ya están en una posición sólida para informar y ayudar a los miembros de la junta directiva sobre el progreso de estas prácticas, ejecutar sus responsabilidades de supervisión más amplias, relacionados con los riesgos de ciberseguridad, la tecnología avanzada y el análisis de datos son prometedores para ayudar a las empresas a abordar los crecientes costos y la complejidad del cumplimiento de la ciberseguridad.

## 5.8 Operaciones Técnicas Ciberseguridad

Las exigencias de gestionar las operaciones de ciberseguridad están aumentando significativamente en casi todas las industrias, las tendencias de la digitalización y la privacidad de los datos y la disponibilidad de los servicios son cruciales, junto con el aumento de la frecuencia y complejidad de los ciberataques, han hecho que la necesidad de mejorar las operaciones de ciberseguridad sea más crítica que nunca.

La pandemia de COVID19 que inicio en el año 2020 ha acelerado el ritmo de digitalización de muchas industrias y ha agravado los riesgos de seguridad en TI, con un aumento en número y sofisticación de los ciberataques contra un modelo de trabajo cada vez remoto para muchas organizaciones, así como los delincuentes en el mundo físico buscan la forma más fácil de ingresar a un edificio, los ciberdelincuentes exploran el punto de entrada más fácil al sistema de una organización, tener un grupo de operaciones de ciberseguridad que inventaría todos los activos, como un minorista inventaría sus tiendas físicas o un banco, sus sucursales, es necesario en tiempo real para proporcionar protección a dichos activos, asignar propietarios y medir su cumplimiento de las medidas de prevención. El argumento para empoderar a un equipo central de operaciones de seguridad con la gestión y supervisión independientes del inventario de activos de una empresa y los controles generales de prevención, detección y respuesta se basa tanto en motivos de eficacia como de eficiencia, en primer lugar, desde la perspectiva de la eficacia, garantiza que sin importar dónde se desarrollen, agreguen y administren los activos (como en la organización del CIO o en una unidad de negocios individual), haya un grupo central encargado de garantizar que se cumplan los estándares, esto reduce la aparición de activos no autorizados y permite a un grupo empoderado medir y responsabilizar a toda la empresa por la buena higiene que solo se logra mediante el cumplimiento de altos estándares de defensa de ciberseguridad, en segundo lugar, desde la perspectiva de la eficacia, el equipo central independiente de operaciones de seguridad técnica puede ahorrar dinero al administrar los muchos controles y programas que componen la estrategia de defensa en profundidad de la empresa. A medida que las empresas emprenden el viaje de la transformación digital, se introducen nuevas metodologías y procesos para aumentar la validez y la eficacia de los proyectos tecnológicos y sus resultados, como la información que está en la nube, sin embargo, a medida que se introducen estas nuevas metodologías y tecnologías, las empresas deben identificar y abordar el riesgo de seguridad que acompañará a los cambios, para aprovechar plenamente el impacto de la transformación digital, los requisitos de seguridad deben abordarse adecuadamente desde el principio para que puedan construirse y respaldarse. La gestión de activos de TI es el conjunto de prácticas comerciales que unen funciones

financieras. Los activos de TI incluyen todos los componentes de software y hardware y direcciones de red en el entorno empresarial, contractuales y de inventario para respaldar el ciclo de vida y la toma de decisiones estratégicas para el entorno de TI e incluye políticas, gestión, gobernanza, monitoreo, informes y pruebas de control para activos de hardware y software, así como la gestión de todas las direcciones IP y URL de la empresa. Para mantener una gestión sólida de los activos de hardware, las empresas deben implementar programas de ciclo de vida de activos de red y servidores, gobernar y supervisar la incorporación, el mantenimiento, la gestión del final de su vida útil, la eliminación de los activos, la gestión de activos de software incluye la gestión de licencias de software en todo el mundo y el seguimiento y auditoría de los requisitos de utilización y licencia. Estrechamente interrelacionada con la gestión de activos empresariales está la primera de las áreas del dominio de la red que se están previniendo: la segmentación de activos, la segmentación consiste en identificar y domiciliar activos en función de su riesgo a través de una estrategia de contenedores bien diseñada que limite el acceso a cada entorno para evitar accesos innecesarios y separe los activos para reducir el impacto del acceso no autorizado en caso de que ocurra. Tradicionalmente, las operaciones de seguridad han sido una función reactiva, equiparada con un Centro de Operaciones de Seguridad, o SOC, donde los equipos técnicos de seguridad detectan, investigan y responden a los ciberataques, a medida que se amplía el papel de las operaciones para establecer una ciberseguridad eficaz a nivel empresarial, los Centros de Operaciones de Seguridad están asumiendo más responsabilidades, además de su función tradicional, los SOC están comenzando a actuar como centros de fusión, proporcionando datos de servicio y requisitos analíticos para otras funciones de gestión de riesgos en una organización, estas áreas incluyen detección de fraude, seguridad física, cumplimiento, para adaptarse a sus crecientes necesidades, el SOC está utilizando tecnología avanzada como el aprendizaje automático (ML) y la inteligencia artificial (IA) para mejorar y optimizar su función de prevención, detectar y responder a riesgos y ciberataques. No se puede subestimar la importancia de un SOC para identificar y defenderse contra ataques, sin embargo, el SOC en sí es solo un eslabón en una cadena de operaciones de seguridad que las empresas deben establecer,

gestionar y coordinar a nivel empresarial para garantizar un programa de ciberseguridad sólido y resiliente, corresponde a todas las organizaciones identificar y agrupar áreas claves de operaciones técnicas que deben trabajar juntas para gestionar el riesgo de ciberseguridad, se deben aplicar políticas comunes en todas las áreas y el desempeño se mide en función de esas políticas, independientemente de dónde se encuentren las actividades de control en la organización.

El Equipo de Respuesta a Incidentes de Seguridad (SIRT) es un grupo especializado que investiga, contiene, prioriza, mitiga y resuelve incidentes de seguridad reales y potenciales, cada empresa debe tener un SIRT, con la misión de gestionar de forma proactiva las amenazas e incidentes cibernéticos para mejorar la misión de seguridad de una organización, se debe alentar a los empleados de la empresa a que informen al SIRT de todos los posibles incidentes de seguridad y privacidad, estos incidentes incluyen violaciones de políticas, amenazas inminentes a la seguridad/privacidad de los datos, así como indicios de acceso o explotación inapropiada, las herramientas de seguridad también deberían enviar notificaciones automáticas al SIRT, los miembros del equipo SIRT deben tener habilidades y herramientas especializadas de investigación y respuesta para iniciar un estudio forense, estudio de malware, desarrollo de código y extracción de datos, los hallazgos del SIRT deben informarse a la gerencia y a las partes internas correspondientes, según sea necesario, luego, la gerencia debe entregar las comunicaciones requeridas a partes internas y externas adicionales, como el gerente ejecutivo, la junta de socios, los reguladores, los trabajadores y los clientes. Se debe establecer una Oficina del Programa de Continuidad dentro del Equipo de Operaciones de Seguridad y supervisar un ciclo continuo de evaluaciones, revisiones y ejercicios diseñados para gestionar el riesgo a un nivel aceptable, después de realizar una Evaluación de Impacto Empresarial (BIA), se debe realizar un análisis de brechas para determinar la aceptación del riesgo o si se necesitan esfuerzos de mitigación, se debe revisar una evaluación de amenazas para determinar alternativas para la mitigación de riesgos de continuidad y las estrategias para mitigar estos riesgos que se identifiquen, incluido el desarrollo de planes. Los planes de recuperación se ejercitan y evalúan para determinar su

eficacia y se realizan ajustes al BIA y al plan al menos una vez al año, los planes se desarrollan y redactan en el peor de los casos y pueden adaptarse a cualquier situación en la que se interrumpan las operaciones, los planes prevén el regreso a las funciones y el procesamiento normales lo antes posible después de un desastre.

## 5.9 Plan de Respuesta a Incidentes (IRP)

El enfoque formal de una organización para abordar y gestionar las consecuencias de una violación de seguridad o un ciberataque se conoce como plan de respuesta a incidentes, lo más importante es que un IRP es un enfoque pensado y publicado, en el que se informa de forma preventiva a las partes responsables, además un IRP es ordenado y sistemático, como un ejercicio que los empleados pueden seguir como si fuera a través de la memoria muscular, cuando se produce una infracción, una empresa puede entrar en pánico y sentirse demasiado abrumada para responder adecuadamente, a menos que esté bien preparada, una empresa mal preparada puede pasar directamente a controlar los daños y puede producirse el caos, el propósito de un IRP es combatir este tipo de reacciones impulsivas, los IRP bien diseñados abordan las infracciones de manera rentable y eficaz en términos de tiempo. Un IRP no es sólo un marco amplio de valores a recordar durante un incidente. Es un documento escrito con instrucciones paso a paso sobre exactamente cómo proceder y a quién contactar, en última instancia, los objetivos del IRPS son restaurar las operaciones, minimizar las pérdidas, corregir las vulnerabilidades de forma rápida y exhaustiva y fortalecer la seguridad para evitar incidentes futuros, los ataques cibernéticos han aumentado dramáticamente y es probable que sigan aumentando debido a las ventajas y beneficios que disfruta la comunidad de atacantes, los ataques pueden comenzar con campañas de phishing por correo electrónico dirigidas, pero terminar en una situación de ransomware en la que la organización ha quedado totalmente comprometida y ahora está a merced de una entidad cibercriminal desconocida, algunas organizaciones también han sido amenazadas con ataques de denegación de servicio que prometen dejar fuera de línea las capacidades de comercio electrónico de una organización, finalmente, la amenaza de una vulneración de datos en la que se puede robar cualquier cosa,

desde datos personales de los consumidores hasta planes de negocios corporativos, siempre está al acecho como una clara posibilidad, Desafortunadamente, a pesar de años de publicidad sobre la amenaza cibernética, todavía muchas empresas no planifican adecuadamente los inevitables ataques, según una encuesta de 2019 realizada por CS&A International y PR News y publicada en Forbes, solo alrededor del 62 % de las empresas tenían planes de crisis y no estaba claro cuántas los actualizaban periódicamente, casi el 60% de los directivos medios y altos encuestados dijeron que nunca habían realizado un ejercicio de crisis o no estaban seguros de con qué frecuencia sus empresas realizaban ejercicios. La respuesta a incidentes de ciberseguridad, al igual que otros aspectos de la ciberseguridad, es un tema de toda la empresa que trasciende a TI como el área responsable, una variedad de equipos en toda la organización deben participar en la respuesta a incidentes para que la respuesta sea efectiva y que haya gobernanza, capacidades de protección, detección, respuesta y recuperación (Gleason, 2022).

Un manual de respuesta a incidentes está diseñado para proporcionar un recorrido paso a paso por las amenazas cibernéticas más probables e impactantes para una organización, el manual garantizará que ciertos pasos del PIR se sigan adecuadamente y servirá como recordatorio si ciertos pasos de los planes no están implementados, la gestión de la ciberseguridad es un tema que afecta a toda la empresa y, por lo tanto, los componentes principales de un sólido manual de respuesta a incidentes incluyen la integración de funciones comerciales centrales y múltiples departamentos en el plan de respuesta, otro componente es un análisis de cómo la respuesta a incidente cibernético encajará en el plan general de crisis y recuperación empresarial de la empresa.

La capacidad de una organización para anticipar, prepararse, responder y adaptarse a cambios incrementales y perturbaciones repentinas para sobrevivir y prosperar se conoce como resiliencia organizacional, tan importante como la necesidad de tener una estrategia es tener la capacidad de implementarlas, la gobernanza de la seguridad eficaz es parte integral de una estrategia de ciberseguridad de alto funcionamiento, quizás el aspecto más importante de una gobernanza eficaz sea la

revisión y renovación continuas, ya que las mejores prácticas evolucionan rápidamente a medida que la tecnología cambia y los piratas informáticos buscan explotar las lagunas jurídicas abiertas. Modelar el impacto financiero de los riesgos cibernéticos identificados es necesario analizar y cuantificar los factores de riesgo, las vulnerabilidades y las consecuencias, esto debería incluir modelos de riesgo cibernético que puedan reflejar no sólo el impacto en el rendimiento del capital invertido de una empresa, sino también los resultados de la pérdida de ventajas competitivas, reparaciones costosas, multas y posiblemente años de litigios, dependiendo de lo que se perdió, una estimación inicial del impacto puede ser lo suficientemente material como para alentar a los equipos de estrategia a alterar la trayectoria de un acuerdo, la estimación se puede refinar a medida que continúa el proceso de transacción y se mitigan los riesgos, el paso más fundamental para gestionar los riesgos de información y privacidad relacionados con la transacción es comprender qué tipos de datos crea, recibe y recopila la organización objetivo como parte de sus procesos comerciales, sólo comprendiendo qué datos tiene el adquirente podrá determinar los requisitos legales y reglamentarios que debe cumplir después de la combinación, el cumplimiento de la privacidad en particular es imposible sin conocer los tipos de datos personales que recopila el destinatario.

# 6. MOODLE

Moodle es una plataforma de aprendizaje que permite a educadores, administradores y estudiantes crear ambientes de aprendizaje personalizados mediante un sistema integrado único, robusto y seguro. En términos técnicos, es un sistema web dinámico que administra entornos de enseñanza virtual con tecnología PHP y bases de datos MySQL. (moodle.org, s.f.).

Martin Dougiamas, un educador e informático australiano, creó la versión inicial en 2002. Su nombre original es el acrónimo de Entorno Modular de Aprendizaje Dinámico Orientado a Objetos.

Además, las plataformas de enseñanza en línea como Moodle se conocen como LMS, que significa Learning Management System (sistema de gestión de aprendizaje). Varios LMS como Chamilo, e-Doceo, Canvas, Sakai y FirstClass están disponibles en el mercado. Aunque hay una gran cantidad de opciones, Moodle es el mejor. Su gran cantidad de ventajas lo convierten en la plataforma de enseñanza en línea más utilizada en todo el mundo.

El principal beneficio de Moodle es que es un programa libre y está disponible bajo la licencia general pública. Esto significa que cualquier persona u organización puede usarlo y ajustarlo a sus necesidades sin pagar nada por el uso.

## 6.1 Ventajas al utilizar Moodle

Organizaciones de todo tipo, tamaños confían en esta herramienta confiable y estable para desarrollar sus planes de formación online.

Es simple de manejar y usar porque es intuitivo y fácil de usar. El panel de usuario tiene recursos bien documentados, una interfaz sencilla y característica de arrastrar y soltar.

Moodle es constantemente revisado y mejorado para adaptarse a las necesidades de los usuarios. Miles de usuarios de todo el mundo están involucrados en su desarrollo y se organizan en torno a comunidades online.

Gracias a su estructura de funcionamiento modular, Moodle se puede adaptar y adaptar a las necesidades individuales, ya que es un software de código abierto.

Es una plataforma escalable a cualquier tamaño que puede servir a miles de estudiantes en organizaciones pequeñas y grandes.

Moodle está disponible en línea, lo que significa que puede acceder a él desde cualquier dispositivo y en cualquier lugar del mundo. La interfaz funciona con todos los navegadores web y dispositivos móviles.

Los desarrolladores de Moodle están comprometidos con la protección de los datos y la privacidad de los usuarios, por lo que los controles de seguridad de la plataforma de Moodle se actualizan constantemente. Los sistemas de Moodle están diseñados para evitar el acceso no autorizado, la pérdida y el mal uso.

Moodle tiene una amplia gama de funcionalidades y ofrece una amplia gama de opciones. La instalación de plugins y complementos, creados por una gran comunidad global, permite ampliar sus funcionalidades.

Moodle está disponible en más de 120 idiomas diferentes. Otra de sus características más apreciadas es su habilidad para ofrecer múltiples idiomas.

Moodle satisface las necesidades de los tres roles principales en las actividades formativas online:

Profesores, su funcionamiento facilita al máximo las tareas del educador en línea. Su conjunto completo de herramientas le permite controlar todas las actividades del proceso de enseñanza-aprendizaje, desde un solo panel de administrador. (maximaformacion, s.f.).

Los alumnos, es práctico, fácil de usar y fácil de entender para los estudiantes. Esto les permite concentrarse en sus tareas de estudio y no tienen que preocuparse por aprender a usar una herramienta compleja. (maximaformacion, s.f.).

Su interfaz gráfica facilita la creación de aulas virtuales y cursos sin la necesidad de herramientas de programación. Es un sistema que puede adaptarse a cualquier entidad educativa, método de enseñanza, estructura de contenidos, formato de recursos didácticos texto, imágenes, videos, presentaciones, estética visual, etc. Para mejorar sus capacidades, se pueden instalar complementos. (maximaformacion, s.f.).

La plataforma Moodle permite:

- Controlar los usuarios, los accesos y los roles.
- Crear una estructura pedagógica que incluya actividades formativas.

- Controlar los recursos educativos y las actividades de capacitación.
- Controlar y monitorear el proceso de aprendizaje de los alumnos.
- Evaluar a los estudiantes y enviar informes.
- Establecer canales de comunicación entre maestros y alumnos.
- Construir entornos para el aprendizaje cooperativo (maximaformacion, s.f.).

Moodle se basa en el modelo pedagógico del Construccionismo Social, que pone énfasis en las actividades de aprendizaje en lugar de los contenidos o las herramientas.

El modelo pedagógico se basa en las siguientes condiciones:

Cuando interactuamos con nuestro entorno, generamos conocimiento. Todo lo que leemos, vemos, oímos, sentimos y tocamos contrasta con nuestro conocimiento previo y nos permite crear nuevo conocimiento que podemos usar con éxito en nuestro entorno. El conocimiento solo se puede construir y consolidar mediante la puesta en práctica de la experiencia. (maximaformacion, s.f.).

Cuando se construye algo que debe llegar a otros, el aprendizaje es más efectivo: Por ejemplo, es posible leer un artículo, libro o página web varias veces y, sin embargo, olvidarlo mañana, si tuvieras que explicárselo a otra persona, comprenderías mejor los nuevos conceptos y podrías combinarlos con tus propias ideas para crear nuevo conocimiento.

El conocimiento compartido impulsa el aprendizaje a niveles profundos. Cuando compartimos nuestro conocimiento con un grupo social (como compañeros de clase, compañeros de trabajo, etc.), formamos parte de una cultura de objetos de conocimiento compartidos con significados compartidos. Creemos que nuestras contribuciones benefician a la comunidad, lo que nos motiva a aprender más.

Enfoque conectado y separado: Moodle fomenta el comportamiento constructivo cuando una persona puede defender sus propias ideas usando la lógica mientras es empática, aplica la escucha activa y se esfuerza por comprender el punto de vista de los demás para hacer nuevas aportaciones y construir conocimiento.

# 7. Materiales y metodología

Para cumplir los objetivos mencionados y planteados anteriormente, se utilizó la siguiente metodología y los siguientes materiales:

Análisis de necesidades: Se realizó un análisis de necesidades para determinar las áreas de conocimiento en ciberseguridad que requieren los ejecutivos empresariales. Los riesgos cibernéticos a los que están expuestas las empresas se incluyen en el análisis y las mejores prácticas de seguridad informática que se deben adoptar, además se analizaron de una manera amplia estadísticas, recursos para mitigar ataques cibernéticos y así reducir la afectación de la información, recursos económicos y humanos.

Diseño de ambiente virtual de enseñanza: Una vez que se ha realizado el análisis de necesidad, se diseñó un ambiente virtual de enseñanza en la plataforma Moodle. Esto implica crear una estructura de módulos, establecer objetivos de aprendizaje y elegir herramientas de enseñanza como videos, infografías, cuestionarios, debates y evaluaciones, entre otras cosas.

Desarrollo de contenido educativo: Se generó el contenido educativo para la enseñanza de las mejores prácticas y conceptos fundamentales de ciberseguridad. El contenido es conciso y fácil de entender para los ejecutivos empresariales y personal de todas las áreas. Además, el contenido del curso está actualizado y relevante para cualquier institución.

Creación de materiales de concientización para ejecutivos: Se desarrolló material específico dirigido a los ejecutivos empresariales, empleados que destaque los riesgos cibernéticos y la importancia de la ciberseguridad para la empresa.

Implementación de la metodología: Una vez que se desarrolló el contenido educativo, se implementó la metodología en la plataforma Moodle. Esto incluye la

publicación de los módulos del curso, la creación de grupos de trabajo para los ejecutivos empresariales, empleados.

Evaluación y retroalimentación: Se implementó módulo de evolución del aprendizaje de los ejecutivos empresariales, empleados y proporcionar retroalimentación para mejorar el proceso de enseñanza. Esto es a través de pruebas y evaluaciones.

El curso de ciberseguridad para ejecutivos está diseñado con un enfoque netamente educativo, orientado a proporcionar conocimientos y habilidades prácticas que permitan a los participantes transformar, liderar y aplicar estrategias de ciberseguridad en sus empresas. La finalidad del curso es capacitar a los ejecutivos para que comprendan los riesgos y desafíos de la ciberseguridad en el entorno empresarial, y no está dirigido a obtener beneficios económicos directos.

La ciberseguridad es un campo en constante cambio, por lo que es esencial mantener el curso actualizado con las últimas tendencias y amenazas en el mundo digital. Revisar y actualizar el contenido periódicamente para garantizar la relevancia y la efectividad del curso, que se verá reflejado en las decisiones empresariales y mitigación de ataques a la empresa.

Los materiales utilizados se describen a continuación: plataforma Moodle, investigación Ciberseguridad para empresarios, laptop, máquinas virtuales.

# 8. Resultados y discusión

Los hallazgos de la investigación realizada son la creación de una Aula Virtual con la plataforma de código abierto Moodle donde consta el curso virtual para Enseñanza de Ciberseguridad para ejecutivos , la cual entre sus beneficios es brindar aprendizaje en línea de forma personalizada y flexible de acuerdo a las necesidades de cada organización o de quienes requieran utilizar la plataforma, Moodle brinda una amplia gama de beneficios tanto para los roles de estudiantes como para los roles de las personas que administran la plataforma, entre los beneficios más importantes que aporta al administrador están: organizar contenido, comunicación efectiva, seguimiento progreso del curso, evaluaciones flexibles, personalizar la plataforma, automatizar tareas, crear foros. Entre los principales beneficios que la plataforma brinda a estudiantes esta: acceso flexible según las necesidades, aprendizaje colaborativo entre instructor y estudiante, recursos adicionales, retroalimentación personalizada, aprendizaje autónomo.

Antes de implementar un curso de capacitación en ciberseguridad dirigido a líderes empresariales, se consideró fundamental evaluar el nivel de conocimiento previo de los participantes en este ámbito. Para ello, se llevó a cabo una encuesta a través de Google Forms, dirigida al personal clave que ocupa roles de liderazgo dentro de sus respectivas organizaciones o empresas.

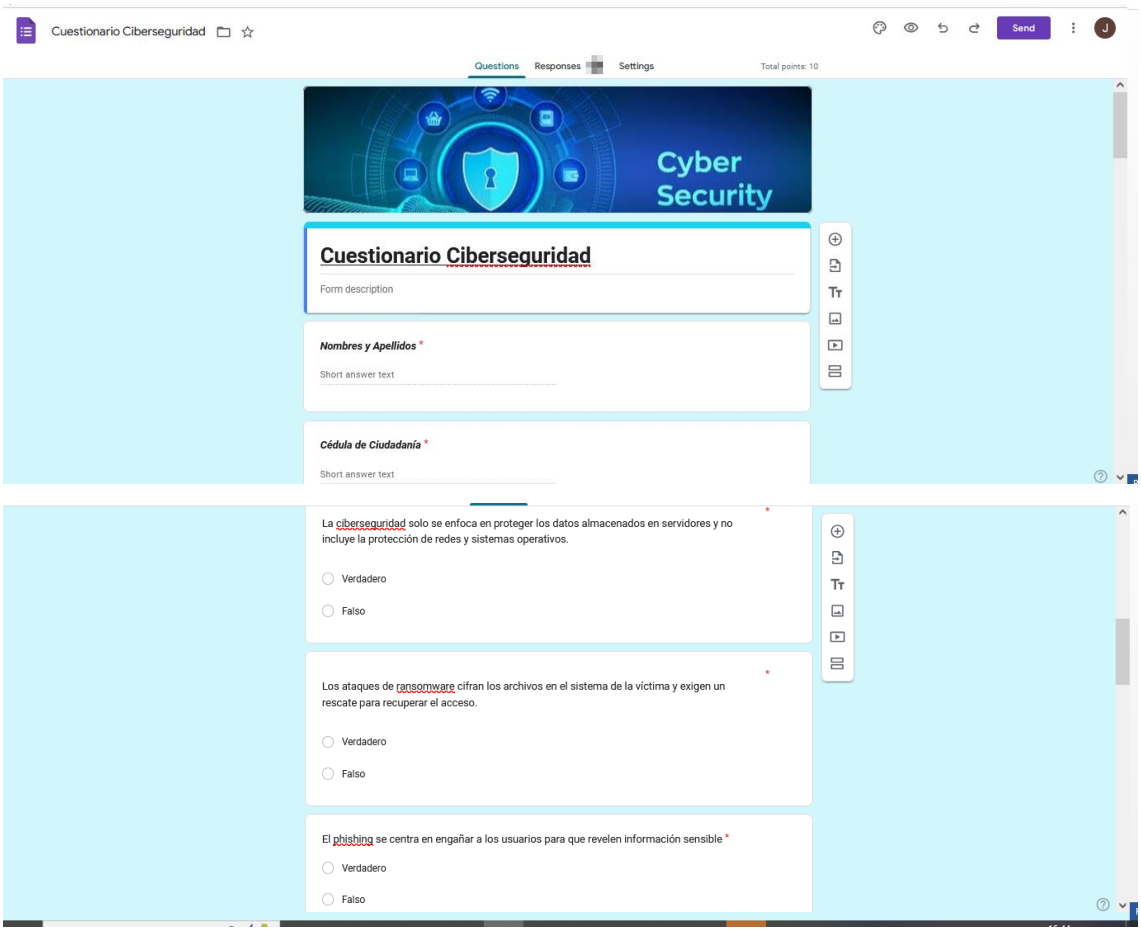
El objetivo principal de esta encuesta fue recopilar información detallada sobre el grado de familiaridad y comprensión que los líderes empresariales tienen en relación con temas críticos de ciberseguridad. Entre los temas se incluyeron:

- Conocimiento sobre amenazas cibernéticas como malware, phishing y ataques de denegación de servicio (DDoS).
- Prácticas de protección de datos y cumplimiento normativo.
- Capacidad de respuesta ante incidentes de seguridad, incluyendo la preparación para ataques y la gestión de crisis.

- Conciencia sobre políticas de seguridad interna y el uso seguro de tecnologías emergentes (inteligencia artificial).

La encuesta fue diseñada para ser concisa y eficiente, abarcando preguntas de V o F. En total, se incluyeron 10 preguntas claves, estructuradas para evaluar el nivel de conocimiento a líderes en diferentes áreas de ciberseguridad. Las preguntas abordaron tanto aspectos teóricos como prácticos, permitiendo identificar brechas de conocimiento y áreas de mejora.

En la figura 1 se observa la hoja de registro con los datos de los líderes que realizaran la encuesta previa para validar los conocimientos.



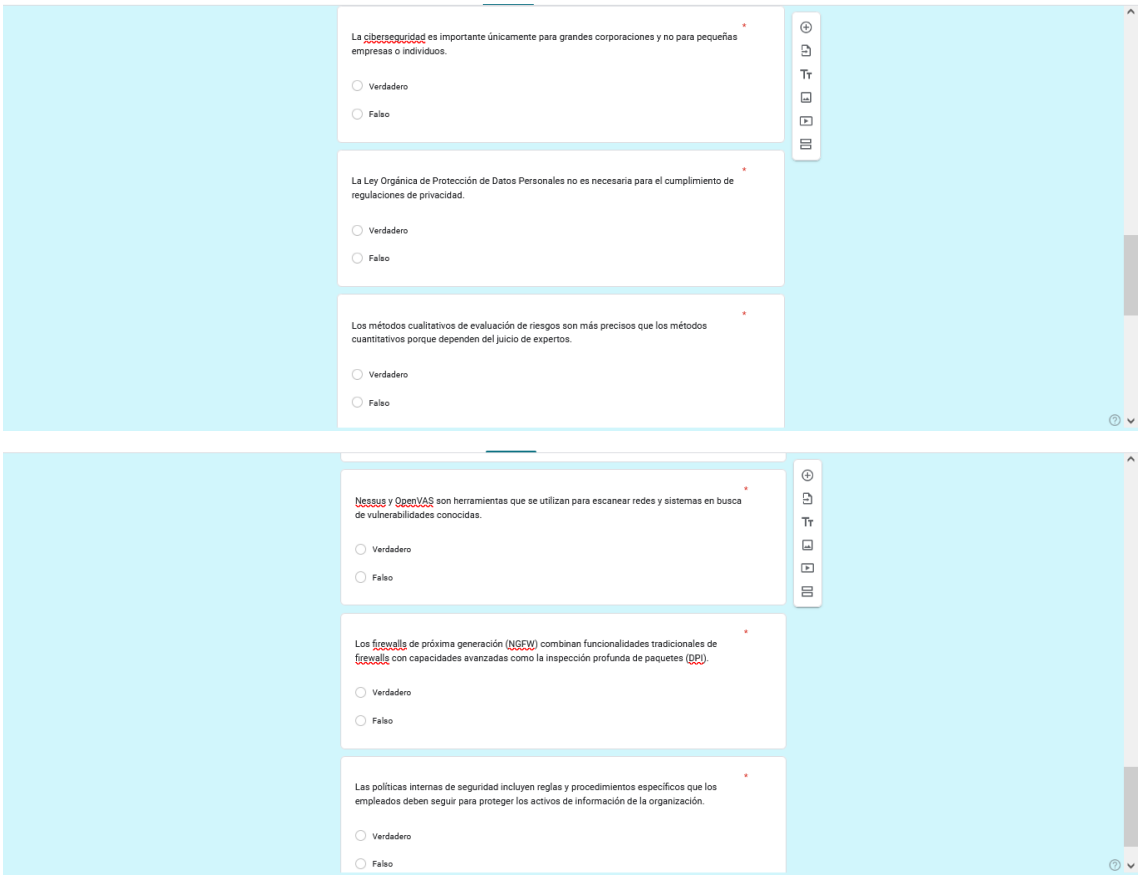



*Figura 1: Registro y Encuesta curso Ciberseguridad*

En la Figura 2, se presenta el total de personas que completaron la encuesta y registro de datos previa al inicio del curso Ciberseguridad para Ejecutivos. La encuesta fue diseñada para evaluar el nivel de conocimiento de los participantes en relación con temas de ciberseguridad antes de comenzar el curso. A partir de los resultados

obtenidos, se pudo identificar el grado de familiaridad y las áreas que los ejecutivos necesitaban reforzar durante la capacitación.

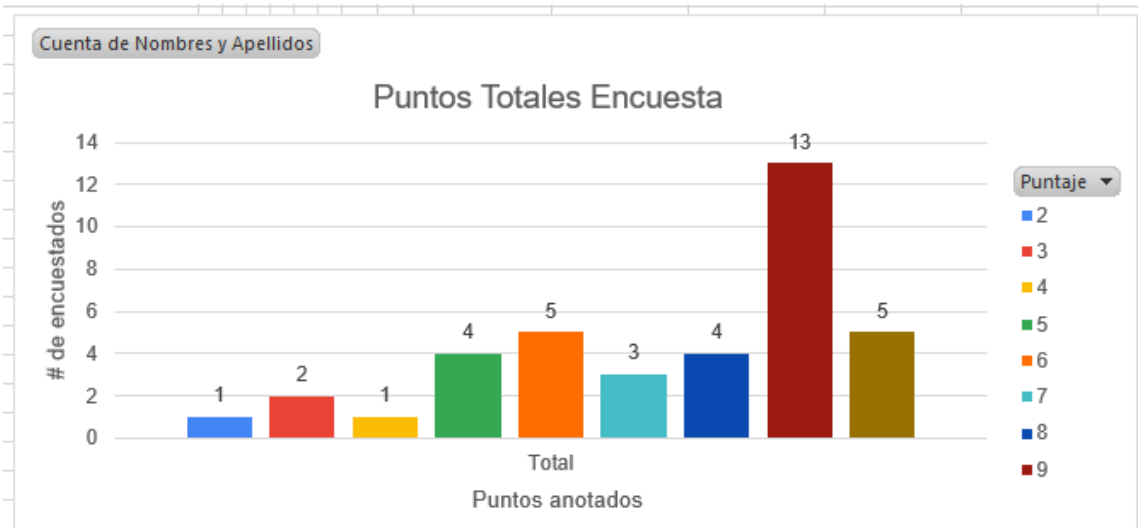



*Figura 2: Encuesta y Registro*

La sumatoria entre las personas que obtuvieron una nota entre 1 y 8 puntos es: 20 personas de un total de 38, que corresponde a 52,6%. Este grupo representa a los participantes con un nivel básico o moderado de conocimiento en ciberseguridad. Las notas en este rango indican una comprensión limitada de conceptos clave y un posible desconocimiento sobre las mejores prácticas en protección contra ciberamenazas.

La sumatoria entre las personas que obtuvieron una nota entre 8 y 9 puntos es: 18 personas de un total de 38, que corresponde al 47,4%. Los participantes en este grupo demostraron un conocimiento intermedio a avanzado, lo que sugiere una mayor familiaridad con los conceptos de ciberseguridad, aunque aún pueden necesitar profundizar en áreas especializadas o en la aplicación práctica de sus conocimientos.

Más de la mitad de los encuestados (52.6%) presentan un conocimiento limitado, lo que resalta la necesidad de un curso integral que cubra desde los fundamentos hasta las estrategias de ciberseguridad.

Casi la mitad (47.4%) de los participantes ya cuentan con un conocimiento más sólido, pero podrían beneficiarse de un enfoque en temas más complejos, como la gestión de incidentes y la ciberseguridad en tecnologías.

Con base en los hallazgos, el curso de Ciberseguridad para Ejecutivos se orientara en fortalecer las capacidades de respuesta ante incidentes, mejorar el cumplimiento normativo y proporcionar herramientas prácticas para proteger a sus organizaciones frente a amenazas emergentes.

Como parte del desarrollo del curso Enseñanza de Ciberseguridad para Ejecutivos, se llevó a cabo la creación completa de un aula virtual en la plataforma Moodle, la cual está publicada en internet. Este entorno virtual ha sido cuidadosamente configurado para proporcionar una experiencia de aprendizaje integral y accesible para los líderes empresariales. A continuación, se describen los elementos clave que fueron implementados, con detalles ilustrados en las siguientes figuras.

Se diseñó un curso específico titulado Ciberseguridad para Ejecutivos, estructurado en 6 módulos temáticos que abarcan desde los conceptos básicos hasta conceptos avanzados en ciberseguridad.

En la Figura 3 se puede observar la captura del acceso a la plataforma Moodle, el link de acceso publicado en internet es: https://ciberseguridadejecutivos.moodlecloud.com/login/index.php.

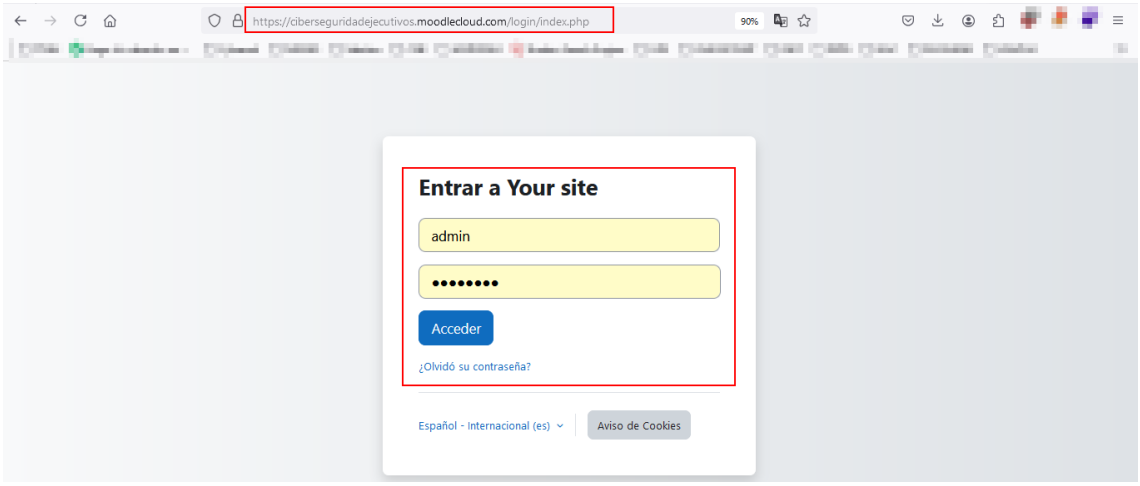



*Figura 3: Inicio de sesión Moodle*

Se realizó la configuración de la página de inicio del curso, incluyendo una descripción clara del contenido y a donde se enfoca, objetivos de aprendizaje y una guía de navegación para los participantes.

En la Figura 4 se puede observar el curso creado y disponible en la plataforma Moodle.

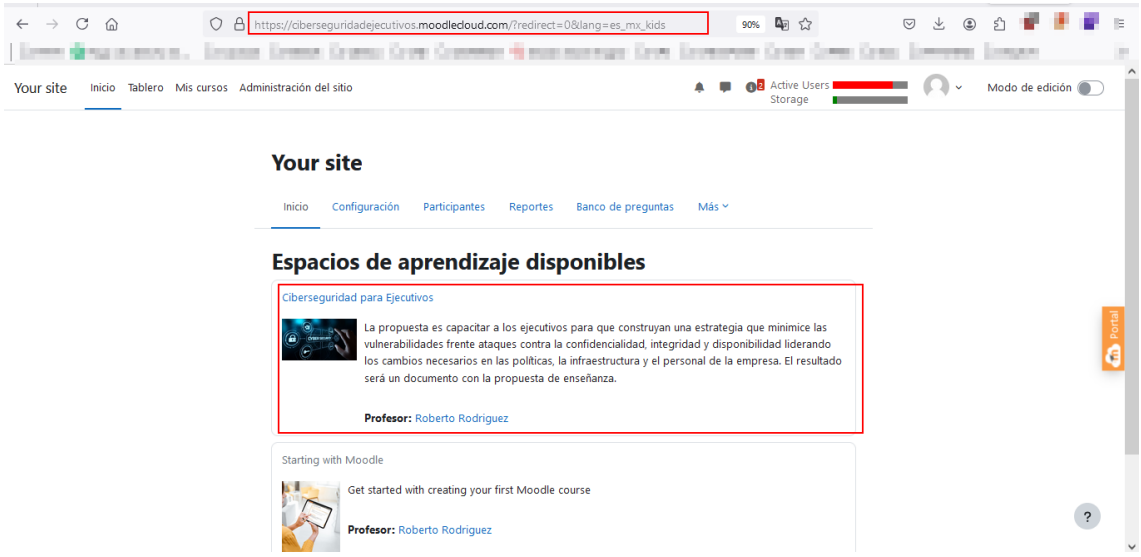



*Figura 4: Pagina Inicio y Curso Disponible*

Para la creación y configuración del usuario administrador, se establecieron permisos específicos para la administración del curso, facilitando la gestión de contenidos, seguimiento de usuarios, materia, etc.

En la creación de usuarios para los estudiantes o ejecutivos, se configuraron cuentas individuales para cada participante, asignándoles roles y permisos que les permitan acceder a los materiales, participar en actividades y visualizar sus calificaciones.

En la Figura 5 se observa que fueron creados 40 usuarios en la plataforma Moodle.

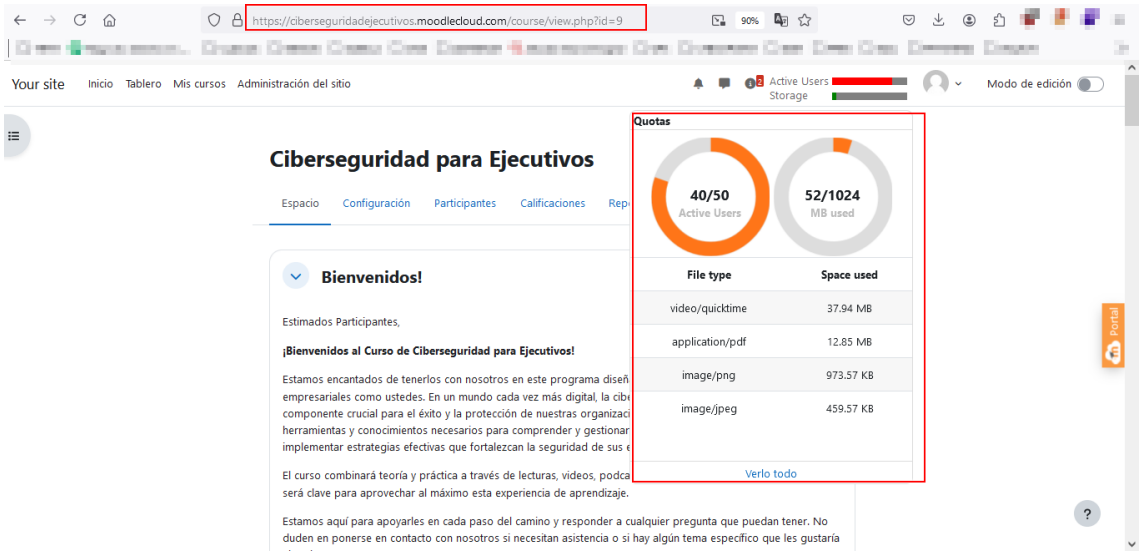



*Figura 5: Gestión de Usuarios*

En la Figura 6 se observa la creación de un total de 40 usuarios en la plataforma Moodle, como parte de la configuración del curso Enseñanza de Ciberseguridad para Ejecutivos. Los usuarios se dividen en dos categorías principales para facilitar la administración y el acceso al contenido:

- Usuarios Administradores o Profesores:

Se realizó la configuración con perfiles específicos para administradores y profesores encargados de gestionar el curso. Estos usuarios tienen permisos ampliados que les permiten:

- Crear y editar contenido del curso.
- Moderar foros y gestionar actividades interactivas.
- Evaluar pruebas y proporcionar retroalimentación a los estudiantes.

En total, 2 usuarios fueron asignados a este rol para asegurar una adecuada supervisión y soporte a los participantes.

- Usuarios Estudiantes o Ejecutivos

Se crearon 38 cuentas de estudiantes, enfocadas en líderes y ejecutivos de diversas organizaciones, quienes participarán en el curso.

Cada usuario cuenta con:

- Acceso personalizado a los materiales educativos (documentos PDF, videos, enlaces de recursos adicionales).
- Permisos para participar en foros de discusión y realizar pruebas en línea.
- Acceso al sistema de calificaciones para monitorear su progreso y recibir feedback.

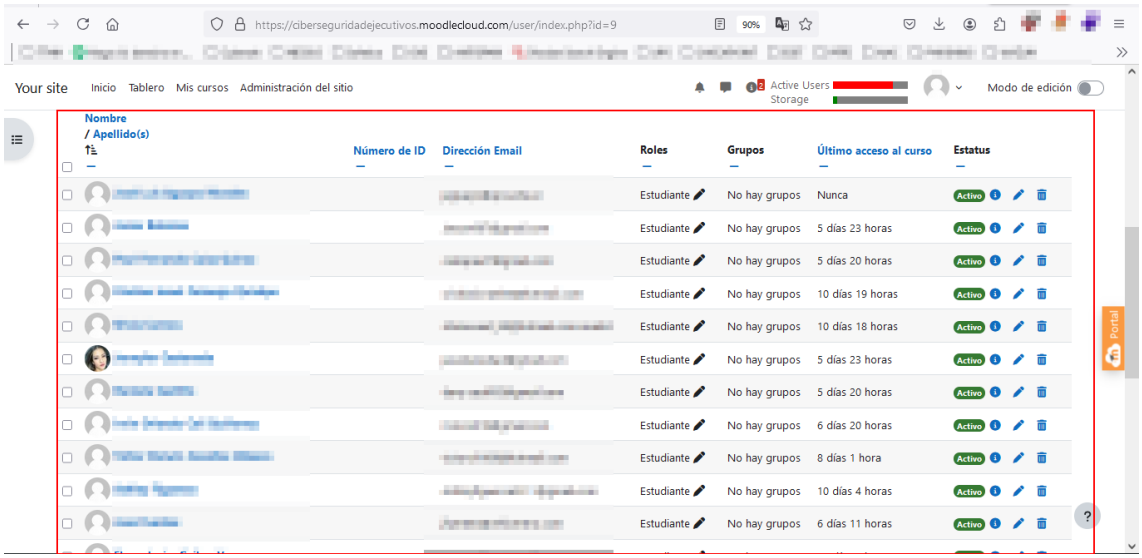



*Figura 6: Gestión de usuarios Administrador y Estudiantes*

En la Figura 7, se muestra la pantalla de bienvenida del curso Enseñanza de Ciberseguridad para Ejecutivos en la plataforma Moodle. La sección de bienvenida ha sido cuidadosamente diseñada para proporcionar a los participantes una introducción clara y acogedora al entorno de aprendizaje virtual, asegurando que se sientan orientados desde el primer momento.

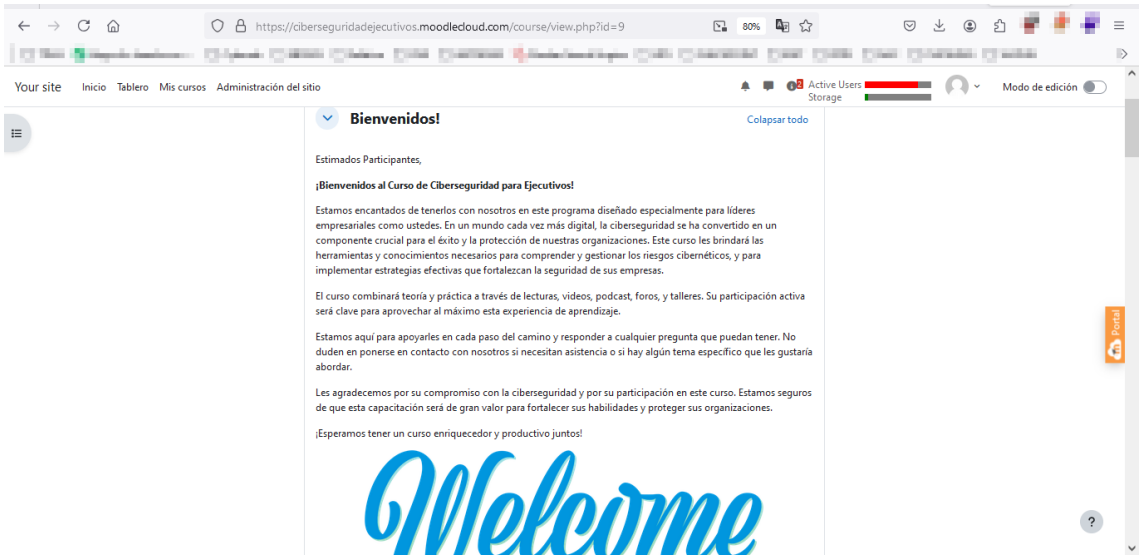



*Figura 7: Inicio Curso*

En la Figura 8, se muestran las redes sociales creadas para complementar el curso Enseñanza de Ciberseguridad para Ejecutivos. Las plataformas digitales han sido diseñadas para ofrecer un enfoque más interactivo y dinámico, facilitando el aprendizaje y la retención de conceptos clave en ciberseguridad de una manera accesible y atractiva. Se han creado perfiles específicos en: TikTok, YouTube, Spotify aprovechando el alcance y las características de cada red social para interactuar con los participantes.

Las plataformas permiten compartir contenido en tiempo real, fomentar discusiones y crear una comunidad activa de aprendizaje.

Los links de acceso a las plataformas de contenido se detallan a continuación:

TikTok: http://www.tiktok.com/@ciberseguridad_ejecutivo

Youtube: https://www.youtube.com/@CIberseguridadparaEjecutivos

Spotify: https://podcasters.spotify.com/pod/show/ciberseguridadejecutivos

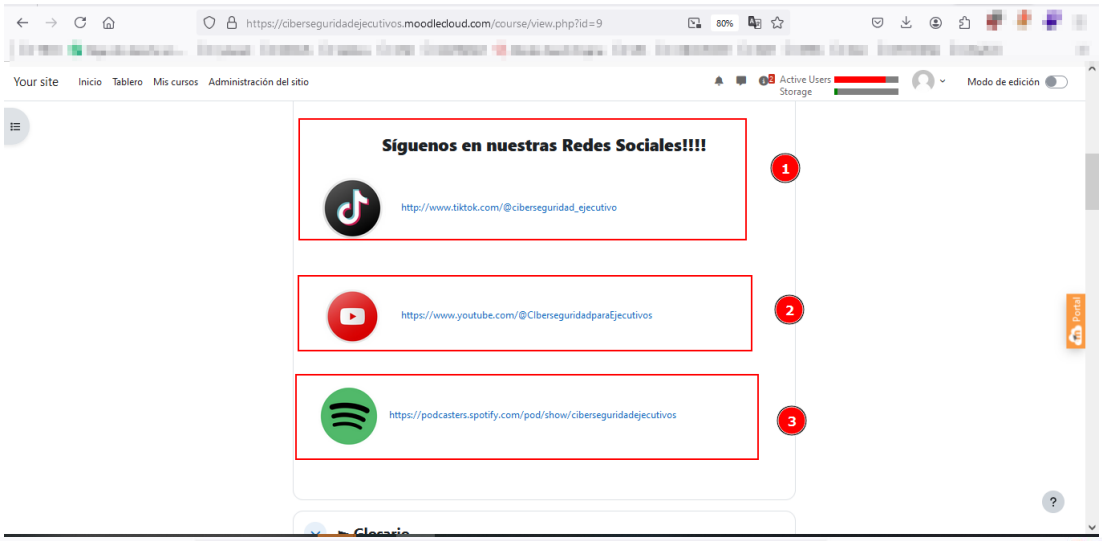
El uso de redes sociales y plataformas digitales como TikTok, YouTube y Spotify para el aprendizaje se ha vuelto cada vez más popular debido a sus múltiples beneficios,

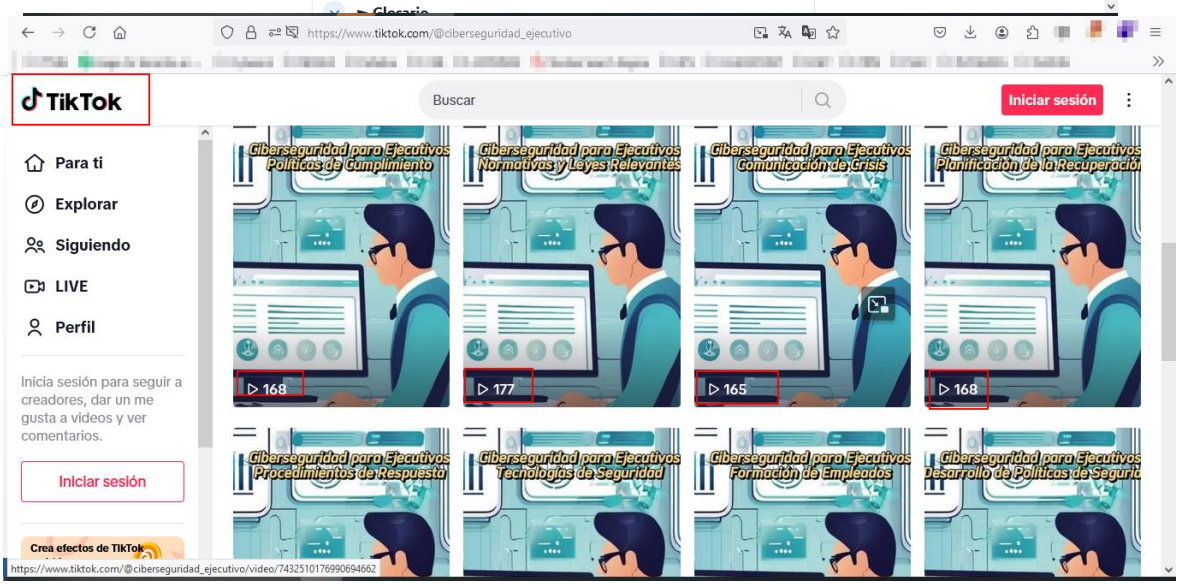
las plataformas ofrecen formas innovadoras y atractivas para adquirir conocimientos, especialmente en un entorno donde el aprendizaje auto dirigido y flexible es cada vez más valorado. A continuación, se describen los beneficios clave de utilizar estas herramientas para el aprendizaje

TikTok, YouTube y Spotify están disponibles en cualquier dispositivo con acceso a internet, lo que permite a los usuarios aprender en cualquier momento y lugar.

Ofrecen contenido gratuito, lo que hace que el aprendizaje sea accesible para una audiencia amplia, sin restricciones geográficas o financieras.

El uso de TikTok, YouTube y Spotify para el aprendizaje ofrece una manera innovadora y accesible de adquirir conocimientos, las plataformas de contenido redes sociales combinan contenido visual, auditivo e interactivo para hacer que el proceso de aprendizaje sea más atractivo y efectivo. Aprovechar las herramientas puede ser especialmente útil para desarrollar habilidades autodidactas, mantenerse al día con las últimas tendencias y explorar nuevos temas de manera dinámica y entretenida.


Your site
Inicio
Tablero
Mis cursos
Administración del sitio
Modo de edición
Síguenos en nuestras Redes Sociales!!!!
http://www.tiktok.com/@ciberseguridad_ejecutivo
https://www.youtube.com/@CIberseguridadparaEjecutivos
https://podcasters.spotify.com/pod/show/ciberseguridadejecutivos
1
2
3


TikTok
Buscar
Iniciar sesión
Para ti
Explorar
Siguiendo
LIVE
Perfil
Inicia sesión para seguir a creadores, dar un me gusta a videos y ver comentarios.
Iniciar sesión
Crea efectos de TikTok
Ciberseguridad para Ejecutivos Políticas de Cumplimiento
Ciberseguridad para Ejecutivos Normativas y Leyes Relevantes
Ciberseguridad para Ejecutivos Comunicación de Crisis
Ciberseguridad para Ejecutivos Planificación de la Recuperación
Ciberseguridad para Ejecutivos Procedimientos de Respuesta
Ciberseguridad para Ejecutivos Tecnologías de Seguridad
Ciberseguridad para Ejecutivos Formación de Empleados
Ciberseguridad para Ejecutivos Desarrollo de Políticas de Seguri
168
177
165
168
https://www.tiktok.com/@ciberseguridad_ejecutivo/video/7432510176990694662

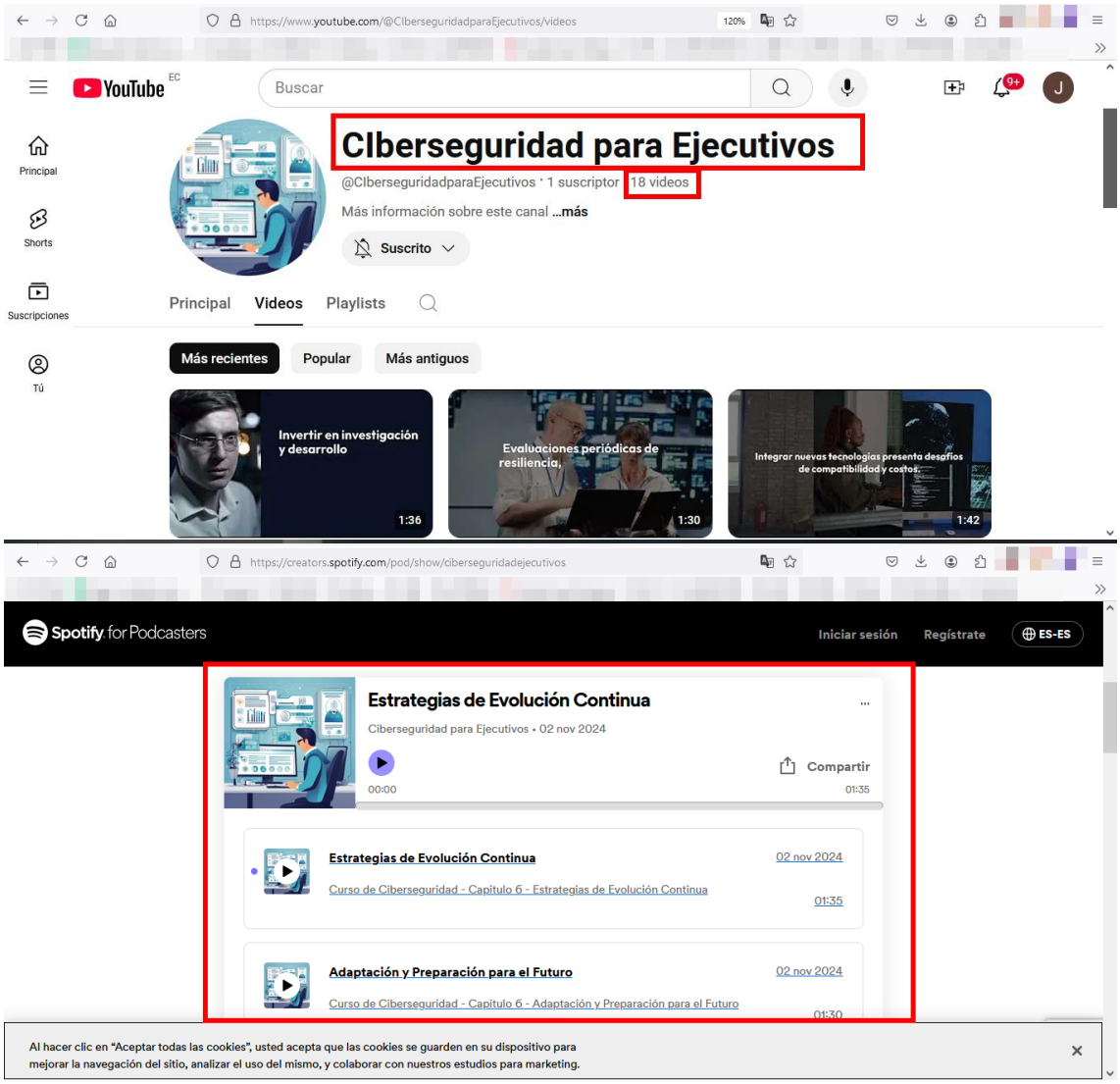



*Figura 8: Perfiles Redes Sociales*

En la Figura 9, se presenta una vista detallada del contenido de las actividades disponibles en la plataforma Moodle para el curso Enseñanza de Ciberseguridad para Ejecutivos. Las actividades han sido diseñadas y desarrolladas para proporcionar un aprendizaje integral, combinando teoría y práctica, y están estructuradas para adaptarse a las necesidades de los líderes empresariales que buscan fortalecer sus habilidades en ciberseguridad.

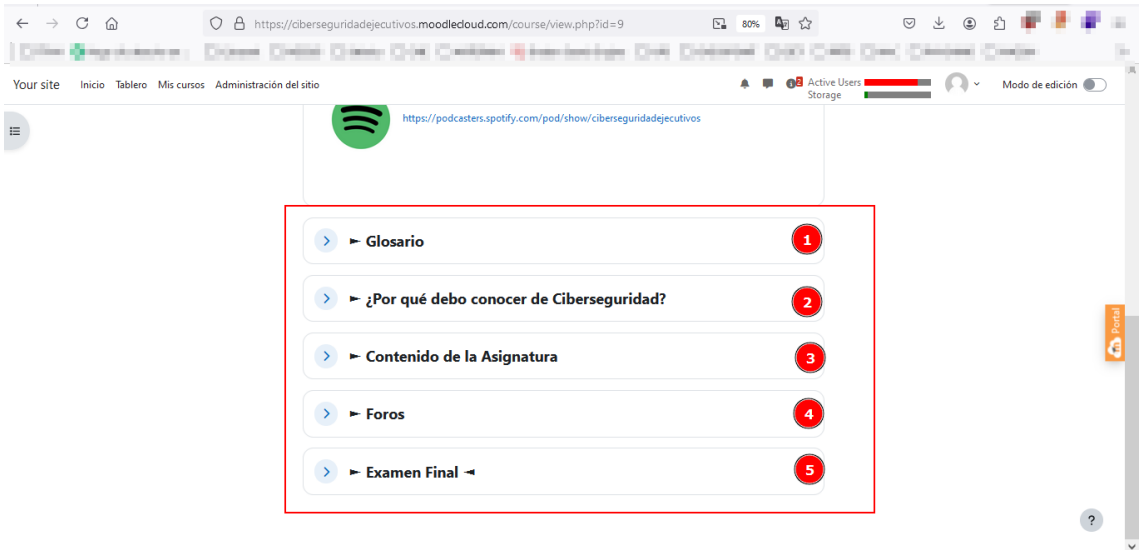



*Figura 9: Contenido Curso*

En la Figura 10 se puede observar el glosario de términos que contiene definiciones y explicaciones de palabras, conceptos y términos técnicos específicos referentes a los temas tratados. El propósito es ayudar a los participantes a comprender el significado de términos especializados que puedan no ser familiares.

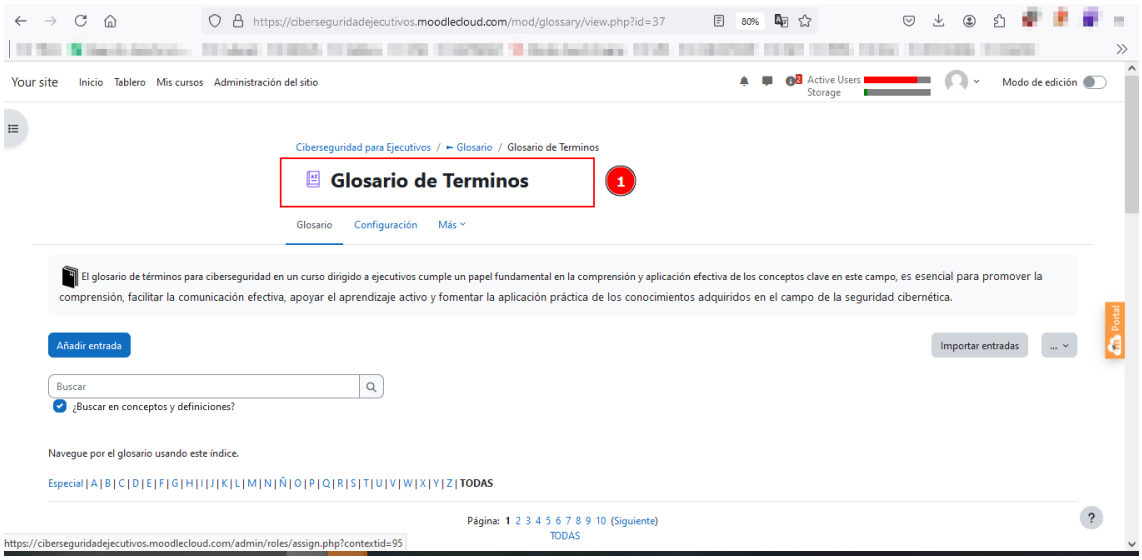



*Figura 10: Glosario de Términos*

En la Figura 11 se da a conocer una explicación, del por qué es importante conocer temas en ciberseguridad, en un mundo cada vez más digital, la ciberseguridad no

es solo un asunto técnico, sino un aspecto crítico para la toma de decisiones empresariales, los líderes empresariales deben estar informados y comprometidos con la ciberseguridad.

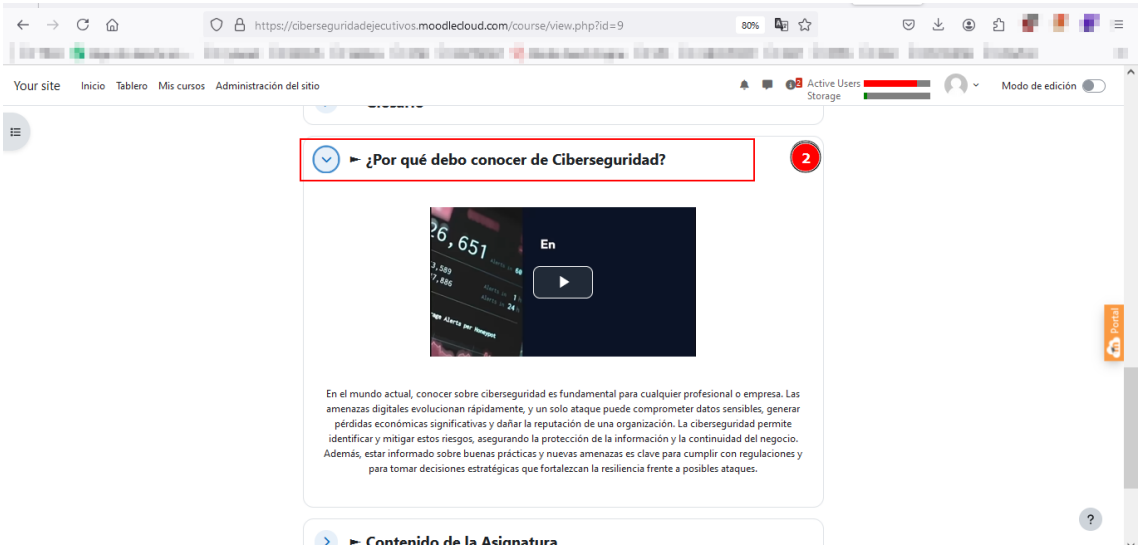



*Figura 11: Introducción Curso*

En la Figura 12 se puede observar el contenido del curso que está conformado por 6 capítulos, cada capítulo con definiciones, archivos para descargarse, una evaluación por capítulo, foros y 1 examen al final, son aspectos fundamentales que componen el curso, con el objetivo de proporcionar una visión clara de lo que los estudiantes aprenderán y cómo se estructurará el aprendizaje. Además se refleja un enfoque bien estructurado y centrado en el aprendizaje práctico, alineado con las necesidades de los líderes empresariales que buscan fortalecer sus habilidades en ciberseguridad. Esta metodología permite a los participantes adquirir conocimientos de forma progresiva, con una combinación de teoría, práctica y evaluación constante, asegurando una experiencia de aprendizaje completa y adaptada a los desafíos actuales del entorno digital.

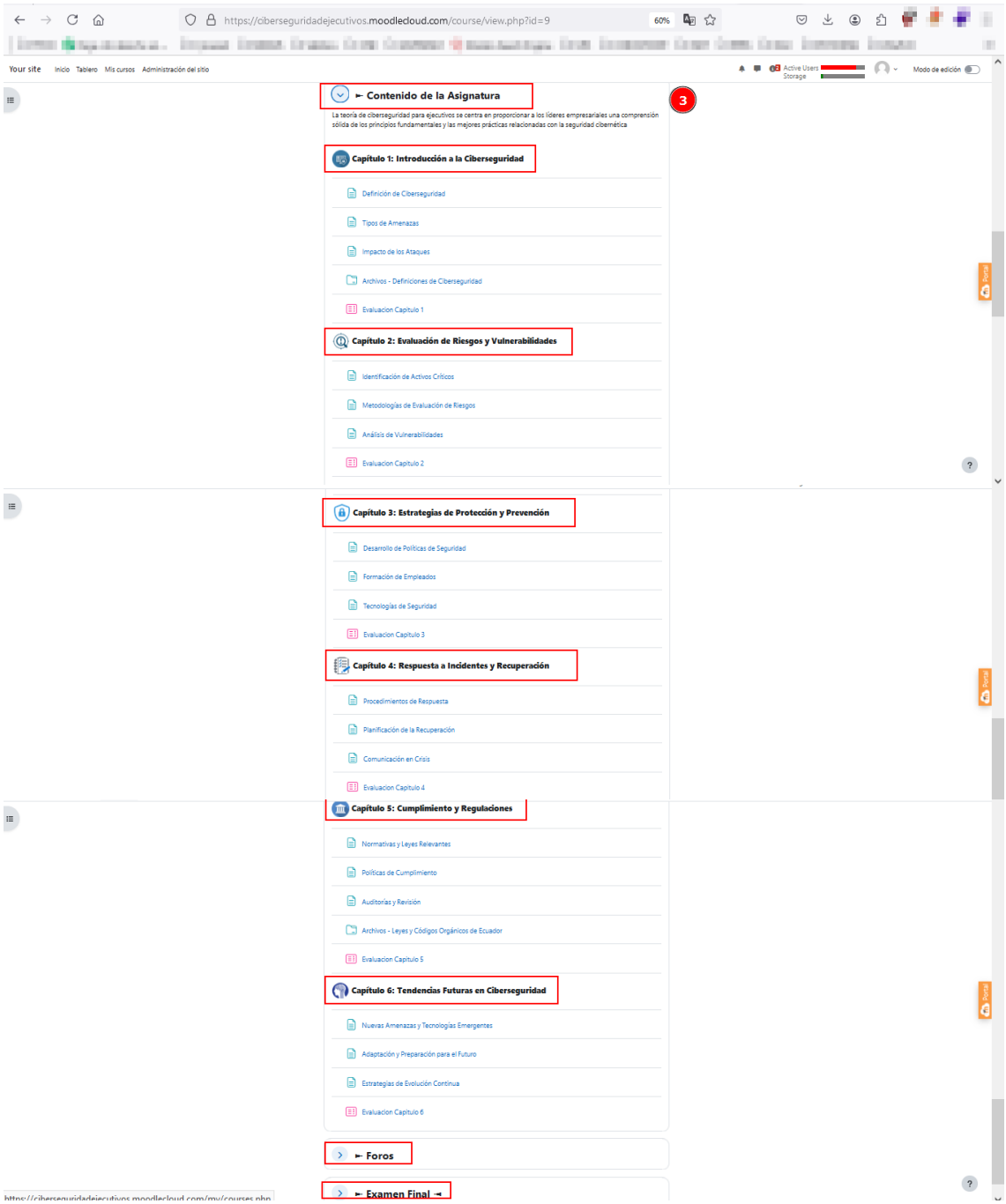



*Figura 12: Capítulos Curso CIberseguridad*

En la Figura 13 se puede observar el apartado de foros creados para facilitar la interacción, el intercambio de ideas y la colaboración entre estudiantes y docente, incluso cuando no están presentes en un aula, los foros creados permiten a los estudiantes y profesores publicar mensajes, compartir opiniones y debatir sobre diversos temas relacionados con el contenido del curso.

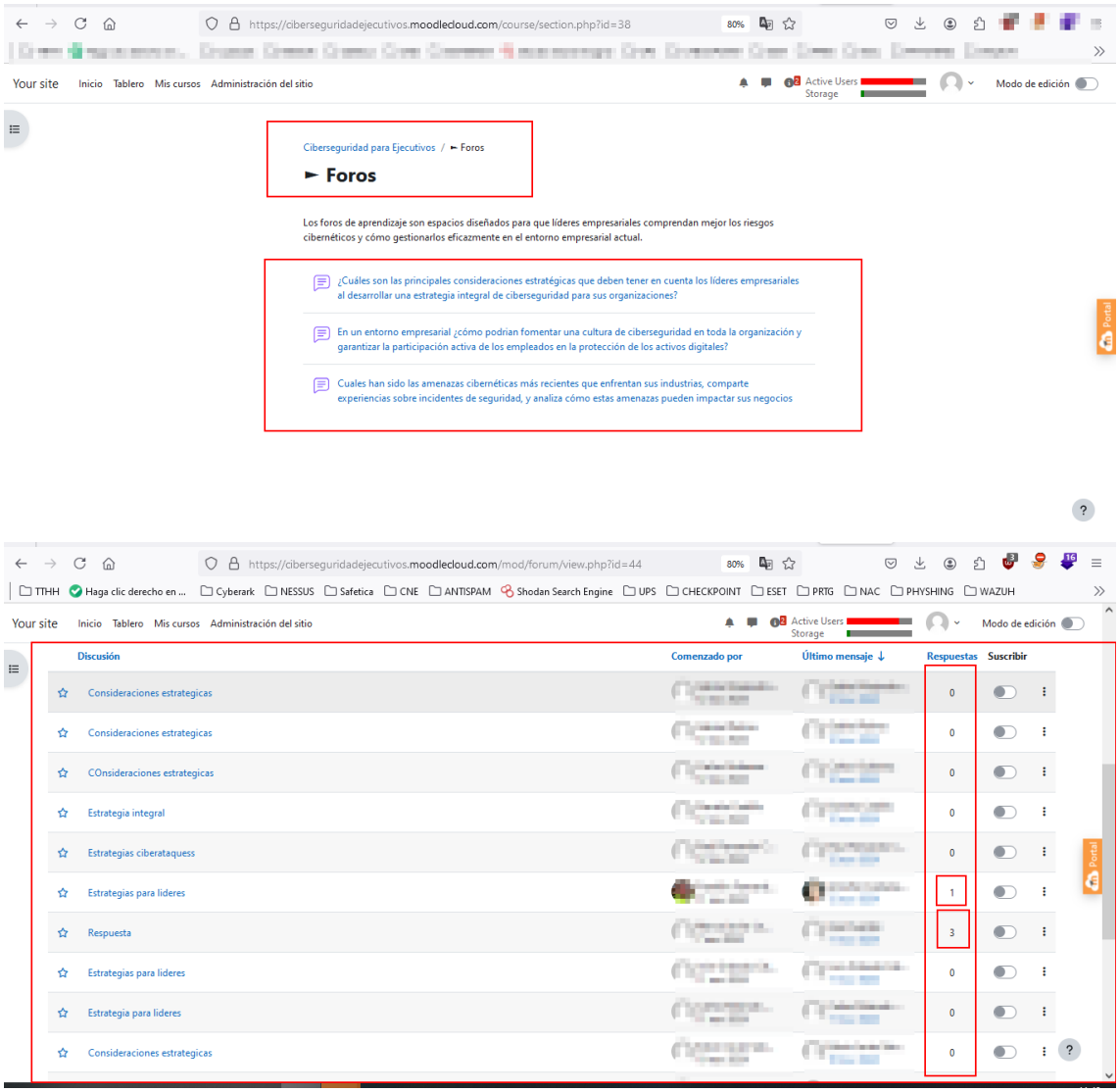



*Figura 13: Foros Curso Ciberseguridad*

En la Figura 14 se presenta un análisis de las interacciones en los 3 foros creados dentro del curso Enseñanza de Ciberseguridad para Ejecutivos en la plataforma Moodle. Los resultados demuestran un alto nivel de participación y una interacción satisfactoria entre los participantes, lo que indica un compromiso activo y un interés significativo en los temas discutidos.

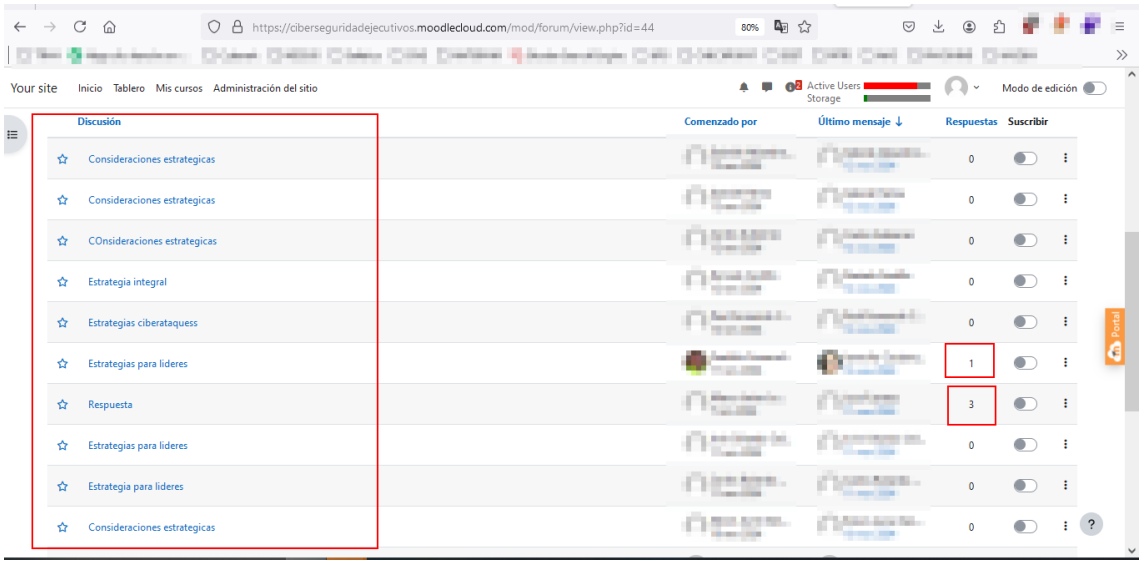



*Figura 14: Iteraciones Foros*

En la Figura 15, se presenta el examen final del curso Enseñanza de Ciberseguridad para Ejecutivos, el cual ha sido diseñado para evaluar de manera integral el nivel de comprensión y dominio de los estudiantes sobre los contenidos abordados a lo largo del programa. La evaluación tiene como objetivo principal medir la aplicación práctica de los conceptos adquiridos, asegurando que los participantes estén preparados para implementar estrategias de ciberseguridad en sus respectivos entornos empresariales.

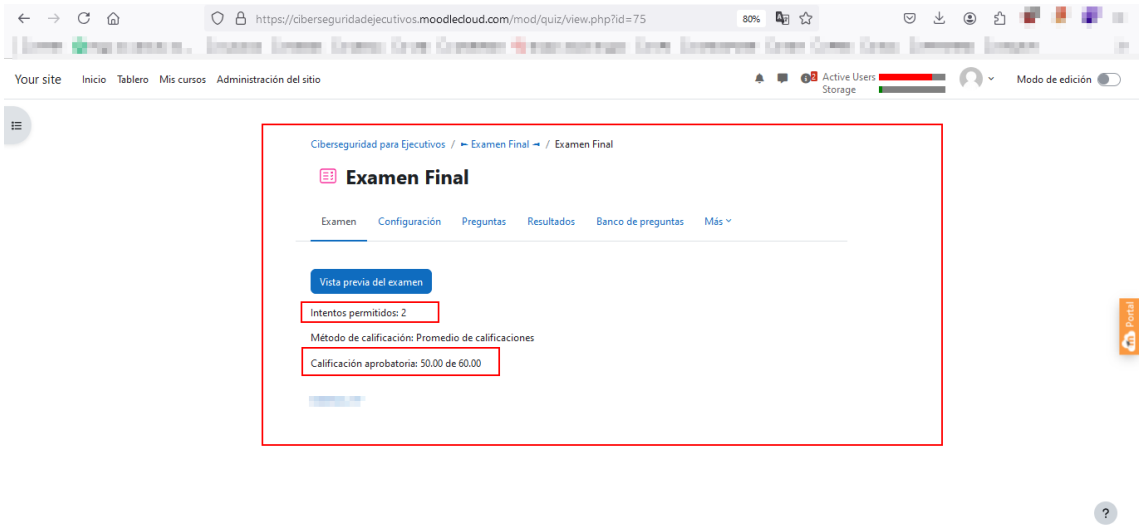



*Figura 15: Examen Final Curso Ciberseguridad*

En la Figura 16, se muestra el número de participantes matriculados en el curso de Enseñanza de Ciberseguridad para Ejecutivos en la plataforma Moodle. Se destaca el nivel de interés y compromiso de los líderes empresariales en mejorar sus competencias en ciberseguridad a través de este programa de formación.

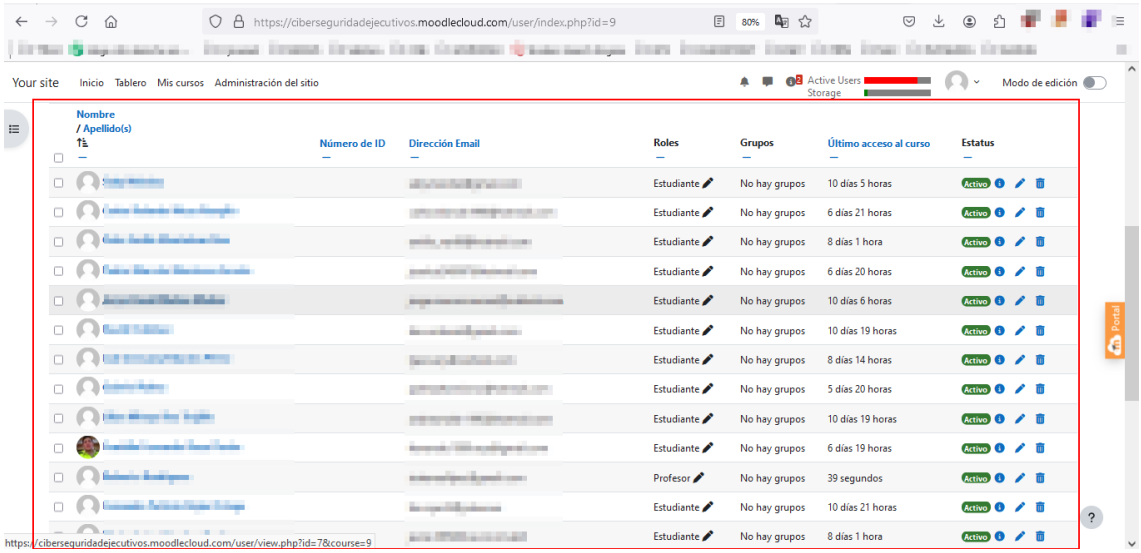



*Figura 16: Alumnos Matriculados*

En la Figura 17, se presentan las calificaciones obtenidas por los participantes tras la culminación del curso Enseñanza de Ciberseguridad para Ejecutivos en la plataforma, los resultados reflejan un desempeño sobresaliente por parte de los estudiantes, indicando un alto nivel de comprensión y dominio de los contenidos abordados a lo largo del curso.

Los estudiantes obtuvieron un promedio de 9.49 sobre 10 en las evaluaciones realizadas al final de cada capítulo. Este alto puntaje sugiere que los participantes comprendieron profundamente los temas cubiertos en cada módulo.

En el examen final, los participantes alcanzaron un promedio de 57.46 sobre 60, lo que equivale a un 95.77% de precisión en las respuestas.

Este resultado demuestra un excelente dominio global del contenido, destacando la capacidad de los ejecutivos para aplicar los conocimientos adquiridos en situaciones prácticas y casos reales.

El promedio acumulado de todo el curso, considerando tanto las evaluaciones por capítulos como el examen final, es de 114.41 sobre 120, lo que representa un 95.34% de aprovechamiento general.

Este alto promedio refleja no solo la dedicación y esfuerzo de los participantes, sino también la eficacia del diseño del curso, que ha logrado transmitir conocimientos clave de manera clara y efectiva.

Los resultados obtenidos indican que los ejecutivos que participaron en el curso están ahora mejor equipados para enfrentar los desafíos de ciberseguridad en sus organizaciones. La consistencia en las calificaciones altas sugiere que el enfoque pedagógico empleado que combina teoría, práctica, foros interactivos y autoevaluaciones, ha sido exitoso en facilitar un aprendizaje significativo.

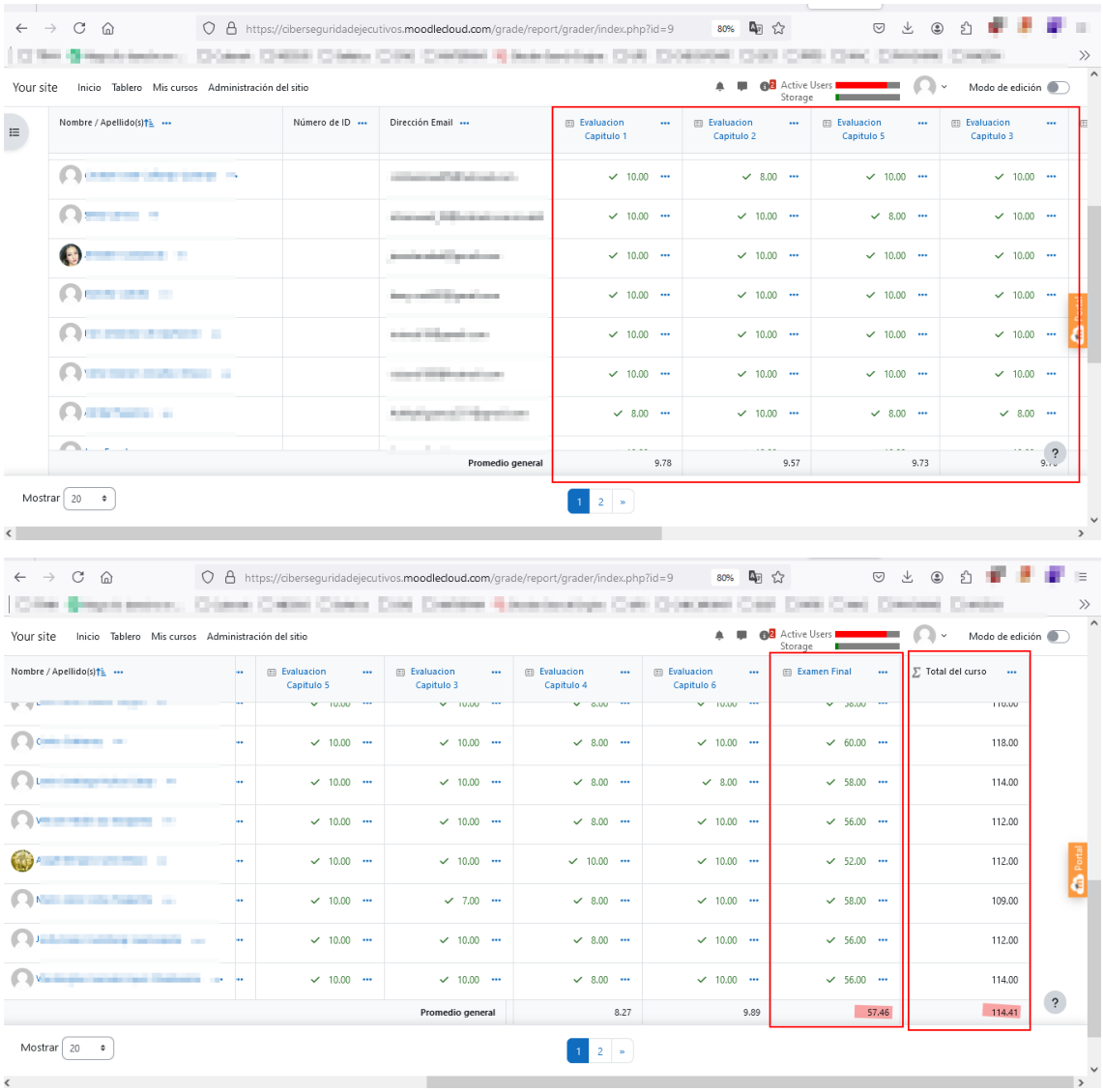



*Figura 17: Estadísticas del Curso*

La Figura 18 se destaca los logros académicos alcanzados por los participantes al finalizar el curso, subrayando que los ejecutivos han adquirido una comprensión sólida de la ciberseguridad. Los resultados reflejan tanto el esfuerzo de los estudiantes como la calidad educativa del curso, que ha sido exitoso en cumplir su propósito de formar líderes capaces de gestionar y proteger la información digital en sus empresas frente a riesgos cibernéticos.

| Evaluación Capitulo 1 | Evaluación Capitulo 2 | Evaluación Capitulo 3 | Evaluación Capitulo 4 | Evaluación Capitulo 5 | Evaluación Capitulo 6 | Evaluación examen | Promedio Curso |
|---|---|---|---|---|---|---|---|
| **9,78** | 9,57 | 9,73 | 9,7 | 8,27 | 9,89 | 57,46 | 114,41 |

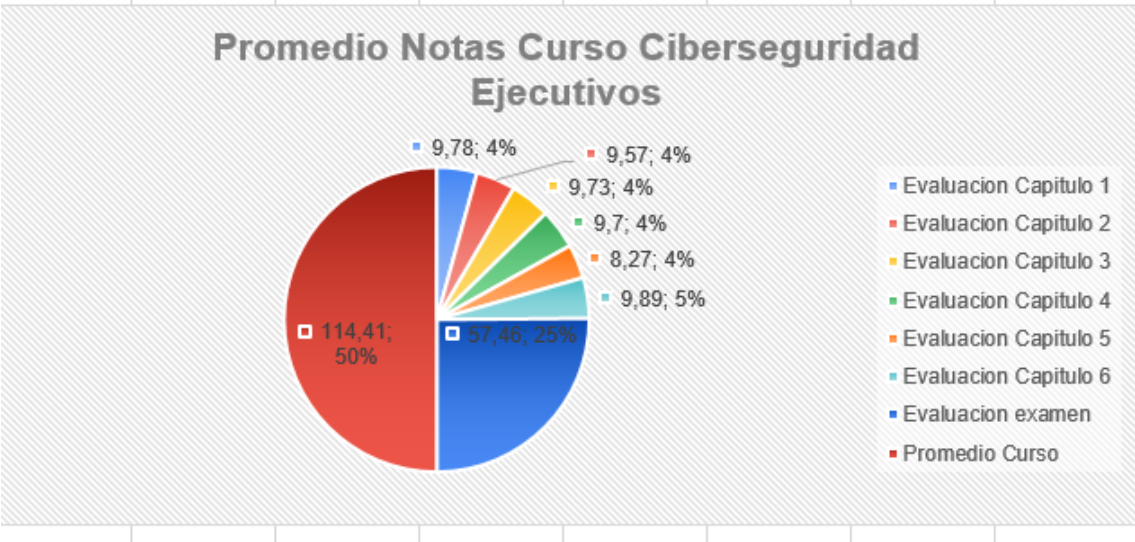



*Figura 18: Promedios Finales*

# 9. Conclusiones

La propuesta de enseñanza de ciberseguridad para ejecutivos debe centrarse en proporcionar no solo el conocimiento técnico necesario, sino también en desarrollar las habilidades estratégicas para que los líderes empresariales puedan identificar, gestionar y mitigar riesgos cibernéticos de manera efectiva. Al capacitar a los ejecutivos en los fundamentos de ciberseguridad, así como en la evaluación de riesgos, respuesta a incidentes, cumplimiento normativo y tendencias emergentes, se les prepara para liderar con confianza en un entorno digital cada vez más complejo. Este enfoque integral permitirá a los ejecutivos no solo entender las amenazas actuales, sino también anticiparse a las futuras, estableciendo una cultura de seguridad en toda la organización.

El verdadero valor de esta formación radica en la capacidad de los ejecutivos para transformar su aprendizaje en acción dentro de sus empresas. Al aplicar los conocimientos adquiridos, podrán liderar iniciativas de ciberseguridad efectivas, desarrollar políticas robustas, y fomentar una cultura organizacional donde la seguridad es una prioridad compartida. De esta manera, no solo protegen los activos críticos de la empresa, sino que también garantizan la continuidad del negocio y refuerzan la confianza de clientes y socios. Este tipo de liderazgo es esencial para mantener la competitividad y la resiliencia.

El uso de la plataforma Moodle para el curso, ofrece una plataforma flexible y robusta que facilita la enseñanza de conceptos complejos de manera estructurada y accesible. Con su capacidad para organizar contenidos en módulos específicos, como los planteados en esta propuesta, además permite una progresión lógica a través de temas fundamentales, como la introducción a la ciberseguridad, evaluación de riesgos, estrategias de protección, respuesta a incidentes, cumplimiento normativo y tendencias futuras. La plataforma también soporta una variedad de formatos de evaluación y actividades interactivas, lo que facilita el aprendizaje activo y la aplicación práctica de los conocimientos adquiridos.

Es ideal para fomentar la transformación y el liderazgo en ciberseguridad dentro de las empresas, a través de herramientas que ofrece la plataforma Moodle como foros de discusión, cuestionarios interactivos, y recursos multimedia, los ejecutivos pueden colaborar y compartir experiencias, lo que enriquece el proceso de aprendizaje. La flexibilidad de la plataforma permite a los participantes acceder a los contenidos en cualquier momento y lugar, lo que se adapta a sus agendas ocupadas. Al final del curso, los ejecutivos estarán mejor equipados para aplicar los conocimientos y habilidades en sus organizaciones, promoviendo una cultura de ciberseguridad sólida y liderando con confianza en un entorno digital en constante evolución.

La falta de capacitación en ciberseguridad contribuye significativamente a la vulnerabilidad de las empresas frente a los ataques cibernéticos. Dado el aumento de ataques de malware, ransomware y phishing, la capacitación regular y exhaustiva de los empleados es esencial para reducir el impacto de estos incidentes.

En síntesis, los resultados obtenidos por los participantes del curso Enseñanza de Ciberseguridad para Ejecutivos demuestran un desempeño excepcional, reflejando un sólido nivel de comprensión y dominio de los contenidos impartidos. El promedio general del 95.34% evidencia no solo el esfuerzo y la dedicación de los ejecutivos durante el proceso de aprendizaje, sino también la eficacia del diseño pedagógico del curso desarrollado en la plataforma Moodle. Estos resultados resaltan la capacidad de los participantes para aplicar los conocimientos adquiridos en escenarios prácticos y reales, lo que constituye un elemento clave para abordar los retos actuales en el ámbito de la ciberseguridad organizacional. Asimismo, la combinación de metodologías pedagógicas integradoras, que incluyen teoría, práctica, foros interactivos y herramientas de autoevaluación, ha sido determinante para fomentar un aprendizaje significativo. De este modo, el curso se consolida como una herramienta valiosa para mejorar las competencias ejecutivas en ciberseguridad, contribuyendo de manera tangible al fortalecimiento de la seguridad en las organizaciones.

# Referencias


(ENISA), E. U. (2021). Threat Landscape 2021: The Year in Review.

27001, I. (2013). Information Technology - Security Techniques - Information Security Management Systems - Requirements.

Abbott, J. (1 de Julio de 2019). Five Ways HR Can Improve Cyber Security.

Calles-García, J., & González-Pérez, P. (2011). *La Biblia del Footprinting.*

F Van der Oord, L. C. (25 de Enero de 2021). Principles to Unite Business for Cyber-resilience.

Gleason, P. (2022). *CYBERSECURITY FOR BUSINESS.* London, New York, Daryaganj: Kogan Page.

Institute, S. (2020). Incident Handler's Handbook.

Klemash, J. S. (7 de Agosto de 2020). What Companies are Disclosing about Cybersecurity Risk and Oversight, .

maximaformacion. (s.f.). *maximaformacion*. Recuperado el 04 de 01 de 2024, de https://www.maximaformacion.es/blog-teleformacion/que-es-la-plataforma-moodle-y-para-que-sirve-2/

moodle.org. (s.f.). *Moodle*. Recuperado el 04 de 01 de 2024, de https://docs.moodle.org/all/es/Acerca_de_Moodle

Picchi, A. (27 de Dicembre de 2013). After Security Breach, Target's Brand Takes a Hit, CBS News.

Seiersen, D. H. (2016). How to Measure Anything in Cybersecurity Risk, John Wiley & Sons Inc., . Hoboken, New Jersey.

Shameli-Sendi, A. A.-B. (2016). Taxonomy of Information Security Risk Assessment (ISRA).

Stallings, W. &. (2018). *Computer Security: Principles and Practice (4th ed.).* Pearson.

Technology), N. (. (2012). Guide for Conducting Risk Assessments .

Tipton, H. F. (2019). Information Security Management Handbook (7th ed.).

Whitman, M. E. (2017). Principles of Information Security (6th ed.).

www.elhacker.net. (s.f.). *www.elhacker.net*. Obtenido de https://www.elhacker.net/trucos_google.html