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 UNA SOLUCIÓN PARA MEJORAR EL CONTROL DE ACCESO DE LOS USUARIOS QUE UTILIZAN LOS SERVICIOS DE LA NUBE

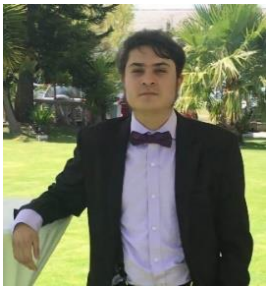
AUTORES:
RAFAEL GABRIEL SUQUINAHUA QUIROZ
CARLOS ALEJANDRO TORRES ALBÁN

DIRECTOR:
JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR
2024

Autores:

Rafael Gabriel Suquinahua Quiroz
Ingeniero en Telemática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
rafasuqui@gmail.com



Carlos Alejandro Torres Albán
Ingeniero en Sistemas mención Telemática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
ctorresa1@est.ups.edu.ec

Dirigido por:

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

Propuesta de una solución para mejorar el control de acceso de los usuarios que utilizan los servicios de la nube.

Autores:

RAFAEL GABRIEL SUQUINAHUA QUIROZ
CARLOS ALEJANDRO TORRES ALBAN

RESUMEN

El problema del acceso seguro a servicios en la nube ha aumentado en los últimos años a los usuarios que usan de manera frecuente esta opción.

La metodología para el desarrollo de la propuesta de solución se basa en tres puntos importantes: (i) recopilación de datos en la cual, se realizara un análisis en textos de fuentes certificadas en la tecnología con la finalidad de encontrar los aportes que se ha generado al actualidad y saber por qué es importante el capacitar a los usuarios mediante una herramienta de capacitación, (ii) encuesta aplicada para entender cómo se maneja el tema de seguridad en la nube así como el acceso a la misma, y (iii) la creación de una producto usando la herramienta Moodle para capacitar a los usuarios brindándoles el conocimiento adecuado para que ejecuten las buenas prácticas de acceso a los servicios en nube.

El resultado que se presenta es un producto curso de capacitación en Moodle que aumente la seguridad del acceso en la nube.

Palabras Claves: Autenticación, Control de Acceso, Seguridad en la Nube, Autenticación Multifactor, Protección de Datos.

ABSTRACT

The problem of secure access to cloud services has increased in recent years for users who frequently use this option.

The methodology for the development of the proposed solution is based on three important points: (i) data collection in which a text analysis of certified sources in the technology will be performed in order to find the contributions that have been generated to the present and to know why it is important to train users through a training tool, (ii) survey applied to understand how the issue of security in the cloud and access to it is handled, and (iii) the creation of a product using the Moodle tool to train users by providing them with the appropriate knowledge to execute good practices for access to cloud services

Keywords: Authentication, Access Control, Cloud Security, Multifactor Authentication, Data Protection.

1. INTRODUCCIÓN

Actualmente, en la era digital, los servicios de uso en nube se han convertido en una herramienta cada vez más relevante además de utilizada. Principalmente, el uso para los procesos de gestión y almacenamiento de datos, recursos e información en organizaciones [3]. La migración hacia los servicios de nube ha brindado innumerables beneficios como la flexibilidad operativa, escalabilidad y reducción de costos. Así también, la capacidad de acceder y administrar datos como aplicaciones de manera remota ha revolucionado la eficiencia y la productividad en una amplia variedad de sectores. Sin embargo, este avance tecnológico también ha planteado desafíos significativos centrándose sobre todo en la seguridad, particularmente en lo que refiere al control de acceso de los usuarios que trabajan con estos servicios [8].

Control de acceso a la nube

La supervisión continua del acceso a la información es fundamental no solo para mantener la seguridad empresarial, sino también para cumplir con las regulaciones legales. Normativas como Sarbanes-Oxley, PCI DSS, HIPAA y GDPR requieren revisiones periódicas del acceso de los usuarios. No cumplir con estos requisitos puede generar graves problemas para las empresas. Por lo tanto, el control de acceso es un elemento clave en los programas de cumplimiento de seguridad para salvaguardar la información sensible.

En entornos de TI dinámicos que combinan infraestructuras locales y servicios en la nube, gestionar el acceso puede ser un desafío. Es crucial comprender cómo se utiliza el acceso, detectar violaciones y corregirlas de manera automatizada. Algunas preguntas importantes que surgen en este contexto incluyen:

- ¿Quién tiene acceso?
- ¿A qué recurso en la nube?

- ¿Cómo obtuvieron el acceso?
- ¿Todavía lo necesitan?

Cuando los usuarios cuentan con acceso excesivo, las empresas se exponen al riesgo de violaciones internas. Para mitigar esto, es crucial aplicar la política de "mínimos privilegios", que restringe el acceso a los recursos en la nube únicamente a lo indispensable para el desempeño de sus funciones. Además de eliminar los privilegios innecesarios, es esencial gestionar y supervisar continuamente el acceso de aquellos usuarios que necesitan permisos especiales.

Llevar a cabo revisiones periódicas de las cuentas de usuario permite supervisar y auditar todo su ciclo de vida, desde su creación hasta su eliminación. Es importante detectar y dar prioridad a los arrastres de privilegios durante estas revisiones.

La mala configuración es responsable del 68% de los problemas (Fuente: Fortinet [29]).

Las organizaciones clasificaron las siguientes amenazas como las amenazas de seguridad más importantes para sus nubes públicas:

- Configuración incorrecta (68 %)
- Acceso no autorizado (58%)
- Interfaces inseguras (52%)
- Secuestro de cuentas (50%)

La mayoría de las aplicaciones cuentan con menos de tres certificaciones de seguridad, y las pertenecientes a TI suelen utilizar SSO. Además, muchas organizaciones no han dado prioridad a la ciberseguridad y el cumplimiento.

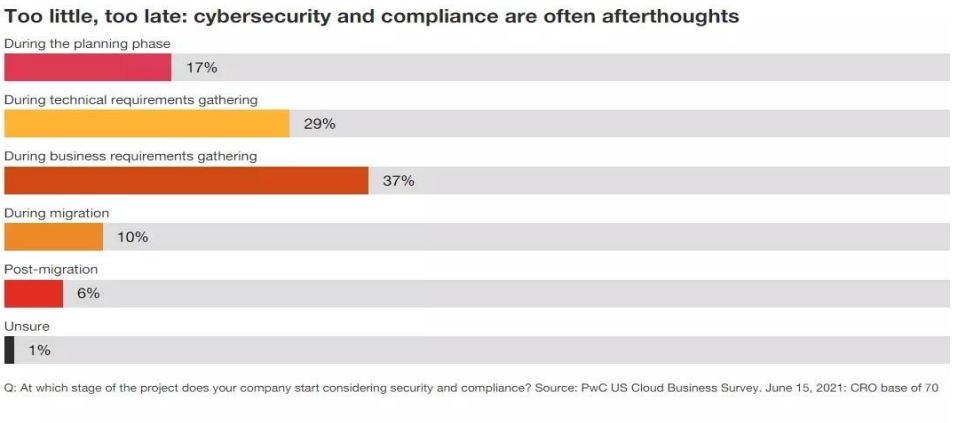


Fig 1. *Porcentajes de amenazas según Fortinet [29]*

Sin embargo, más organizaciones están implementando políticas de confianza cero para mejorar su seguridad en la nube, según Fortinet:

Fig 2. *Implementación zero trust para mejorar seguridad en nube [29]*

El modelo para la autenticación de estos servicios se ha convertido en un tema de alto riesgo, tanto a nivel nacional como internacional. La autenticación de usuarios es una herramienta crítica para la gestión y conservación de data; orientándose principalmente al establecimiento de la *integridad*, *privacidad* y la *disponibilidad* de los datos. La confianza en los servicios de nube como un medio seguro para el almacenamiento de datos y la eficacia del procesamiento de estos recursos en línea se encuentra estrechamente vinculada a la habilidad para autenticar y autorizar de manera apropiada a los usuarios que buscan acceder a ellos.

Problemas relacionados con el control de acceso a la nube

La computación en la nube se considera uno de los paradigmas más dominantes en la industria de la tecnología de la información en la actualidad, ofreciendo servicios rentables bajo demanda como Software como Servicio (SaaS), Infraestructura como Servicio (IaaS) y Plataforma como Servicio (PaaS). A pesar de sus beneficios, existen varios desafíos asociados, como la seguridad de los datos, el abuso de servicios en la nube, la amenaza de insiders maliciosos y ciberataques. Uno de los requisitos de seguridad más fundamentales en la computación en la nube es el control de acceso, que es esencial para evitar accesos no autorizados y proteger los activos de las organizaciones. Aunque se han desarrollado diversos modelos y políticas de control de acceso, como el Control de Acceso Mandatorio (MAC) y el Control de Acceso Basado en Roles (RBAC), estos pueden no satisfacer los requisitos específicos de la nube debido a su diversidad de usuarios y desafíos singulares como el alojamiento multiarrendatario [30].

Las limitaciones de las soluciones de acceso en la nube son similares a las de cualquier sistema de control de acceso: el elemento humano es impredecible y se debe gestionar con políticas y capacitación. Un sistema de seguridad puede ser muy avanzado, pero su efectividad se ve afectada si los usuarios no siguen las medidas básicas de seguridad, como no compartir credenciales o mantener cerradas las puertas. Por lo tanto, es esencial capacitar a las personas y asegurar el cumplimiento de las políticas para garantizar la seguridad, independientemente del nivel de avance tecnología del sistema [31].

Este proyecto se enfoca en abordar el problema del control de acceso existente actualmente en los servicios de la nube para proponer una solución integral que mejore las buenas prácticas de seguridad en este entorno digital moderno. A lo largo del presente trabajo, exploraremos las vulnerabilidades actuales en los sistemas de autenticación en la nube, examinaremos los riesgos únicos de seguridad asociados con los servicios de la nube, y presentaremos una metodología basada en la capacitación del usuario como el eslabón más débil del proceso de control de

acceso, con el objetivo de fortalecer y mejorar la autenticación en los servicios en la nube.

Según el modelo propuesto en 1991 por John McCumber desde el NIST, conocido como El Cubo de McCumber, presenta como contramedidas, controles o salvaguardas

- Tecnologías, dispositivos y productos que ayudan a proteger.
- Las políticas que se pueden establecer, procedimientos y continuidad en las prácticas.
- Actualización de forma constante del conocimiento requerido para enfrentar nuevas amenazas.

Un componente crucial de la solución propuesta es mejorar la capacitación de los involucrados en el control de acceso a la nube para aumentar la seguridad para lo cual se desarrollará una herramienta de capacitación basada en Moodle. Una plataforma de aprendizaje de fácil acceso, así como sin costo alguno que es lo que siempre busca el usuario. La herramienta ha sido seleccionada porque es ampliamente reconocida, y su sistema integrado de aprendizaje será utilizado para desarrollar módulos educativos que aborden las mejores prácticas de seguridad en el control de acceso a los servicios de nube [32].

Adicionalmente, el proyecto busca minimizar las brechas de seguridad causadas por errores humanos, lo cual es crucial, ya que el usuario es frecuentemente más débil en la cadena de seguridad [1]. Estas capacitaciones ayudarán a reforzar las defensas contra las amenazas cibernéticas, promoviendo un entorno más seguro, confiable para la gestión y el acceso a los servicios en la nube.

Conforme este proyecto avance, exploraremos a fondo las prácticas actuales de autenticación en los servicios de nube, identificaremos las amenazas clave y propondremos una solución basada en el marco de seguridad ISO 27001:2022, reconocido a nivel internacional como las normas a seguir por las organizaciones con el propósito de promover y aplicar las prácticas óptimas en cuanto a la

seguridad. Los mismos que serán integrados en la plataforma Moodle, como se ha descrito anteriormente, para respaldar la gestión de sistemas de seguridad en organizaciones de todos los tamaños y áreas.

El proyecto también realiza un análisis comparativo de frameworks que están ligados a las buenas prácticas. Información complementaria recogida mediante preguntas generales dirigidas al usuario, busca demostrar cuan necesario es tener una herramienta que concientice y capacite a usuarios para el mejoramiento de control de acceso como proceso de ingreso a dicho servicio. El objetivo de educar al usuario es la mejora del acceso a los servicios de nube, con lo cual todos los actores de la seguridad de la información estén cubiertos y así el ciclo de seguridad se complete teniendo una mejora sustancial en el proceso que conlleva a una organización a que sea más segura.

Los servicios de nube continúan evolucionando a medida que el mundo se digitaliza y opera sobre la automatización de procesos para dar mayor comodidad al usuario final. Este proyecto busca marcar una diferencia importante en la protección de datos y la integridad de sistemas en este entorno en constante cambio.

La pregunta de investigación que guía este proyecto es: ¿Cuál es el impacto de la implementación de las medidas sólidas de control de acceso, incluyendo la autenticación multifactor, en la seguridad de los servicios de nube y la prevención de brechas de seguridad?

2. DETERMINACIÓN DEL PROBLEMA

El crecimiento vertiginoso de la adopción de servicios que están alojados en la nube ha traído consigo una serie de desafíos, riesgos, amenazas además de vulnerabilidades en lo que respecta al control de acceso de los usuarios a dichos servicios. A pesar de los beneficios significativos que los servicios de nube ofrecen a las organizaciones en términos de flexibilidad, escalabilidad y la eficiencia de

costos, un problema crítico relacionado con la seguridad se ha detectado en el proceso de verificación de identidad de usuarios en los servicios de nube. [1]

El problema principal se centra en las debilidades de los sistemas de autenticación utilizados en los servicios en la nube. Estas debilidades incluyen, pero no se limitan a:

Contraseñas Débiles: Constituyen una significativa vulnerabilidad en el control de acceso a diversos servicios, especialmente en entornos remotos o no físicos. [2]

Falta de Autenticación Multifactor (MFA): La ausencia de MFA, que incorpora múltiples métodos de autenticación, deja las cuentas de usuario expuestas a accesos no autorizados. La autenticación que se basa exclusivamente en contraseñas es insuficiente ante la creciente sofisticación de las amenazas cibernéticas. [2]

Falta de Concienciación y Formación: La falta de educación y entrenamiento sobre prácticas de seguridad óptimas aumenta el riesgo de accesos no autorizados. Los usuarios pueden ser víctimas de phishing o ingeniería social por no estar familiarizados con las medidas de seguridad. [3]

Riesgos Únicos de Seguridad en la Nube: La seguridad en la nube enfrenta retos únicos, como la pérdida de visibilidad, incumplimiento normativo, amenazas internas, configuraciones erróneas y exposición de interfaces de programación de aplicaciones (API) inseguras. Estos factores pueden ser explotados para acceder a datos sensibles y recursos críticos. [4]

La consecuencia de una brecha de seguridad en el control de acceso en los servicios de nube puede ser catastrófica. Esto implica mayor posibilidad de pérdida de datos sensibles, daños a la reputación de la organización, sanciones regulatorias y repercusiones económicas significativas. Además, el incumplimiento de las regulaciones y estándares de seguridad de datos más significativas lo que puede acarrear consecuencias legales graves e irremediables.

3. MARCO TEÓRICO REFERENCIAL

Para abordar el marco teórico sobre el control de acceso en la seguridad en la nube, primero se establece una base conceptual que permite entender los fundamentos de la autenticación en servicios en la nube y el control de acceso de los usuarios. Posteriormente, se resaltan los conceptos teóricos clave para este proyecto:

Servicios en la Nube:

Los servicios en la nube son plataformas de cómputo y almacenamiento que proporcionan acceso a herramientas de computación a través de Internet. [6] Estos se dividen en tres categorías principales:

1. IaaS (Infraestructura como Servicio): Permite a los clientes utilizar recursos de cómputo, como procesamiento y almacenamiento, a través de un servicio externo, reduciendo la necesidad de invertir en infraestructura propia. [11]
2. PaaS (Plataforma como Servicio): Ofrece a los usuarios un entorno de desarrollo completo, incluyendo software de programación y un contenedor para alojar aplicaciones y servicios. [11]
3. SaaS (Software como Servicio): Facilita el acceso a aplicaciones a través de interfaces web, ocultando la complejidad de la infraestructura tecnológica subyacente. [11]

Autenticación: Es el proceso de verificar la identidad de un usuario mediante diversos métodos, incluidos contraseñas, autenticación multifactor (MFA), tarjetas inteligentes y biometría.[6]

MFA: Requiere múltiples pruebas de identidad para autenticar a un usuario**.** [2]

Ingeniería Social: Estrategia utilizada por atacantes para obtener información personal mediante la manipulación de personas.[7]

Riesgos de Seguridad en la Nube: Incluyen la pérdida de visibilidad sobre la infraestructura, violaciones de cumplimiento, amenazas internas, configuraciones incorrectas y exposiciones de interfaces web inseguras. Estos riesgos pueden comprometer la seguridad de los datos.[8]

ISO 27001:2002: Norma global que establece buenas prácticas para la gestión de la seguridad de la información, incluyendo un conjunto de controles y directrices para proteger dicha información. [9]

4. MATERIALES Y METODOLOGÍA

Se adopta un enfoque mixto que combina métodos cualitativos y cuantitativos para obtener una visión general sobre (i) la autenticación en la nube y (ii) el desarrollo y evaluación de la solución propuesta. Para comparar diferentes controles que mejoren el acceso de usuarios y fortalezcan la seguridad en sistemas en la nube, se analizarán las opciones según el cubo de McCumber, enfocándose en los pilares de Tecnología, Políticas y Personas. Finalmente, se elegirá al menos uno de estos pilares para abordar el problema del control de acceso en la nube.

Como punto de partida para la metodología, se llevará a cabo una revisión bibliográfica concisa, centrada en temas relacionados con el control de acceso en entornos de nube. Además, se buscará identificar patrones que demuestren que los usuarios bien capacitados tienden a gestionar de manera más eficiente el control de acceso, mejorando la seguridad y reduciendo riesgos.

Revisión Bibliográfica

Se analizan fuentes académicas, tales como revistas especializadas en seguridad informática, conferencias, y publicaciones científicas importantes en el campo de la seguridad y la autenticación de servicios alojados en la nube.

Además, se revisan informes técnicos provenientes de instituciones reconocidas en seguridad informática y documentos gubernamentales que aborden regulaciones y estándares en la autenticación en la nube. Estos artículos han sido analizados en

orden cronológico para explorar la evolución del control de acceso de los usuarios a la nube hasta la actualidad. En otras palabras, se ha llevado a cabo un seguimiento de cómo ha cambiado el acceso a los servicios de nube a lo largo del tiempo y de cómo se ha generado la necesidad de que los usuarios se capaciten mediante herramientas educativas que sean de fácil acceso y de bajo costo.

Research on cloud computing service based on trust access control (2019)

En este primer artículo se exploran tres escenarios diseñados para evaluar la confianza en los accesos a servicios en la nube. El primer escenario se basa en la metodología de confianza, utilizando contraseñas de manera simple y sin seguir buenas prácticas, todo ello centrado en la relación de confianza. En el segundo escenario, se introduce un algoritmo ponderado para mejorar la seguridad y reducir posibles brechas. Finalmente, se realiza una comparativa con dos modelos existentes en el tema, revelando que estos últimos gestionan de manera más efectiva la privacidad. [18]

El articulo concluye de manera clara y concisa explicando que el *usuario* tiene una alta participación en el control de accesos. El riesgo generado por el usuario se incrementa al no usar buenas prácticas o un conjunto de claves que no están bajo los estándares de seguridad. Por lo tanto, además del uso de algoritmos de protección de datos, es importante informar y capacitar a los usuarios de las organizaciones.

General Access Control Guidance for Cloud Systems (2020)

Este documento, elaborado por NIST, se presenta como una guía explicativa destinada a comprender los diversos modelos de control de acceso implementados hasta la fecha y su importancia en el contexto del control de acceso. Se enfoca en tres modelos los cuales son: IaaS, PaaS y SaaS. [19]

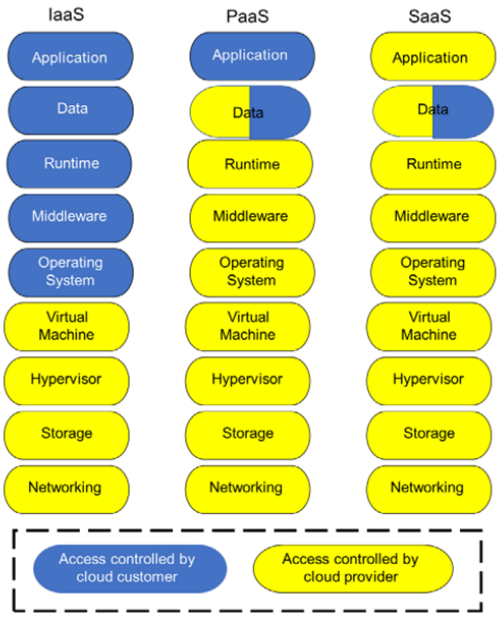


Fig 3. *Modelos de prestación de servicios en la nube: IaaS, PaaS y SaaS. [12]*

Teniendo en el año 2020 un tema de conmoción mundial, la mayoría de las organizaciones migraron sus sistemas al ecosistema de la nube. En consecuencia, la NIST realizo la implementación de nuevos documentos para dar un refuerzo a la capacitación y uso de las buenas prácticas para el control seguro de acceso para los servicios en la nube. La nueva versión destaca que el modelo IaaS está configurada netamente por el usuario o cliente final mientras que PaaS y SaaS están diseñadas por la parte técnica o el proveedor. En estas prácticas, independientemente de cada uno de los actores, predomina la necesidad de que los usuarios tengan conocimientos avanzados en temas de seguridad y en el acceso al ecosistema de nube.

Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review (2020)

La revisión se llevó a cabo utilizando los tres modelos fundamentales de control de acceso en la nube: IaaS, PaaS y SaaS. Estos modelos han sido pilares en la definición de directrices y proporcionan un marco para que los expertos en el tema desarrollen nuevos modelos futuros. La investigación se apoya en buenas prácticas y guías previamente establecidas, buscando evolucionar y mejorar los controles de acceso en la nube de manera efectiva. [13]

Debido al crecimiento y con el paso de los meses del 2020 año de cambios se decidió reforzar el tema de los modelos de acceso a la nube haciendo que estos modelos sean granulares es decir que tenga un crecimiento exponencial todo esto mediante el uso de nuevas tecnologías, así como tomar más medidas de seguridad por parte del proveedor, mediante el acompañamiento de equipos tecnológicos como firewalls de última tecnología o el uso recurrente de multi factor. Cabe destacar que se menciona como parte fundamental que el uso de buenas prácticas además del conocimiento del usuario en el acceso a nube, además de tener una capacitación adecuada será de gran ayuda para realizar una mejora en el proceso de la seguridad de los servicios en nube.

Dual Access Control for Cloud-Based Data Storage and Sharing (2020)

Este artículo aborda el progreso tecnológico en el contexto del control de acceso, destacando la transición desde la dependencia exclusiva de un solo control de acceso vinculado al cifrado AES. En lugar de ello, se busca una dualidad, incorporando un enfoque adicional que mitigue los riesgos de ataques de denegación de servicio que podrían perjudicar los servicios en la nube.

El mecanismo propuesto implica un control integral, abarcando tanto el acceso a los datos mediante buenas prácticas de contraseñas seguras como la limitación del intercambio innecesario de información. Teniendo como premisa principal que tanto la tecnología como el cifrado y el alto conocimiento del usuario de las buenas prácticas todo esto bajo una buena capacitación hacen que el acceso a la nube sea un pilar, para su uso en las organizaciones.

Access Control Model for Google Cloud IoT (2020)

El artículo aborda la carencia de enfoque adecuado en el uso correcto de medidas de seguridad, especialmente en cuanto a lo que tiene que ver con el ámbito del acceso a servicios en la nube. Se destaca la falta de concesión y la necesidad de abordar este aspecto de manera seria y efectiva. El artículo propone una solución específica para mejorar el acceso a la plataforma de nube de Google, denominada GCPAC. [16]

El modelo de Google resulta ser uno de los más interesantes debió a que se basa en la importancia del uso de multifactor en el acceso a la nube, pero es claro que se menciona al usuario en un apartado en el cual sin el conocimiento adecuado del mismo no se podría tener una plataforma segura y que de la rentabilidad para con el usuario.

Security and privacy preservation using constructive hierarchical data-sharing approach in cloud environment (2024)

Este último artículo se centra en mejorar la seguridad del control de acceso mediante el uso del cifrado, proponiendo un paradigma basado en un modelo jerárquico. El objetivo es garantizar un funcionamiento adecuado y libre de brechas de seguridad en este contexto.[17]

En el artículo más reciente en el año en curos se presente seguir por el camino de que el proveedor es aquel que debe buscar cómo garantizar que el control de acceso a la nube sea más seguro, en un apartado de este documento también se hace relación con el usuario donde se destaca que la falta de conocimiento en la actualidad con tantas medidas de seguridad sigue siendo el eslabón que puede fallar el ciclo de seguridad por ser humando y estar tentado a los fallos, es decir que no tenga buenas prácticas o no esté capacitado en estos temas tan recientes o de actualidad tecnológica.

A continuación, se resume la contribución de los artículos analizados en referencia con el tema central del estudio – Tabla 1.

Tabla 1. *Contribución de los artículos incluidos en la revisión bibliográfica*

AÑO	TÍTULO	CONTRIBUCIÓN
2019	**Research on cloud computing service based on trust access control**	En resumen, el fortalecimiento y la optimización de los sistemas de control de acceso contribuyen significativamente a mejorar la seguridad en entornos de computación en la nube

2020	**General Access Control Guidance for Cloud Systems**	Se logró establecer que son tres modelos de prestación de servicios de control de acceso en nube tales como Iaas, Paas, Saas, estos tres modelos son los más comúnmente empleados para gestionar el control de acceso y garantizar la seguridad en entornos de computación en la nube.
2020	**Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review**	Los tres controles de acceso en la nube los cuales son: Iaas, Paas, Saas, estos dan los lineamientos para que los diferentes expertos logren obtener nuevos modelos con vistas al futuro a base de buenas prácticas y guías que se han escrito con anterioridad.
2020	**Access Control Model for Google Cloud IoT**	Se ha demostrado la relevancia de dos escenarios dominantes IoT: el caso de uso de la sanidad electrónica y el caso de uso del hogar inteligente. En otras palabras, se ha evidenciado la importancia y el impacto significativo de estos dos escenarios en el ámbito del IoT.
2024	**Security and privacy preservation using constructive hierarchical data-sharing approach in cloud environment**	El análisis muestra que los modelos de seguridad para el acceso a la nube han evolucionado positivamente. Destaca la importancia del cifrado y de prácticas de contraseñas seguras, incluyendo la autenticación de doble factor, para garantizar una seguridad sólida en esta tecnología en constante crecimiento.

Dado que los avances tecnológicos y de seguridad subrayan la importancia de que los usuarios estén capacitados para comprender los riesgos asociados con un control de acceso inadecuado, tanto dentro como fuera de las organizaciones, se buscará validar los lineamientos más adecuados a seguir. Para ello, se realizará una comparativa exhaustiva de los controles de los marcos de seguridad más reconocidos: ISO 27001:2022, NIST, CIS y zero trust, detallados a continuación:

Marcos de Seguridad

El control de acceso de usuarios es un componente fundamental de la seguridad en la nube, que permite gestionar *quién* puede acceder a los recursos de la nube y qué acciones pueden realizar, a su vez ayuda a proteger los datos confidenciales, prevenir el acceso no autorizado y cumplir con las regulaciones.

Para proporcionar un análisis exhaustivo de varios marcos de seguridad que pueden aplicarse para mejorar el control de acceso de los usuarios, es crucial detallar cada uno de ellos. Este enfoque permitirá entender las características distintivas, ventajas, desventajas y la aplicabilidad específica de cada uno en el contexto de la seguridad en la nube. A continuación, se procederá a desglosar de manera sistemática cada marco:

ZERO TRUST

El enfoque de seguridad holístico de Microsoft se fundamenta en el modelo de zero trust, que se centra en la identificación y protección de activos digitales y control de acceso a la nube. Este enfoque busca detectar y responder a amenazas desde el Centro de Operaciones de Seguridad (SOC), integrar la seguridad en el desarrollo de aplicaciones, incluido DevOps, y extender estas medidas a dispositivos IoT.

El modelo zero trust, elimina la noción de un perímetro seguro, asumiendo que los atacantes pueden estar dentro de la organización. Por esta razón, se intensifican los procesos de verificación y se implementan accesos con privilegios mínimos. Este modelo se ha convertido en esencial para gestionar riesgos, abarcando desde la identidad hasta la red, los datos, las aplicaciones y la infraestructura. [33]

La evaluación de riesgos es continua, con un enfoque en la monitorización y generación de informes que permiten una respuesta automatizada a amenazas. El objetivo es lograr una visibilidad detallada en todos los niveles de la organización.

ISO 27001:2022

Políticas para la seguridad de la información (5.1.1)

Este primer control en el apartado de seguridad de la información requiere que se definan políticas de seguridad para la organización, las cuales serán de gran utilidad durante las auditorías. Para este control, se pueden considerar las siguientes opciones: [21]

- Política de control de acceso a nube
- Política de controles criptográficos
- Política de contraseñas seguras
- Política de uso de doble factor para accesos.

Políticas de control de acceso (9.1.1)

Se enfoca en la definición de reglas para el control de acceso, basadas en los siguientes principios fundamentales: asignar la menor cantidad de privilegios necesarios para realizar una tarea, otorgar estos privilegios solo por el tiempo estrictamente necesario y garantizar que no se abuse de ellos. [22]

Gestión de acceso a los usuarios (9.2.2)

Este control se refiere al registro de la gestión de autorizaciones para los usuarios que acceden a los sistemas en la nube. Es necesario identificar la red y los servicios de nube a los que se tiene acceso, así como los medios utilizados por los usuarios para acceder al entorno de la nube. También se deben establecer los diferentes requisitos para el acceso de los usuarios. [23]

Sistema de gestión de contraseñas (9.4.3)

Organizar y aplicar contraseñas seguras, evitando el uso de contraseñas débiles, y reforzar el control de acceso mediante la implementación de sistemas de autenticación multifactor. [24]

Gestión de claves (10.1.2)

Los métodos de cifrado implican gestionar las claves de los usuarios que utilizan medios cifrados, especialmente dentro de la infraestructura en la nube. Esto requiere la implementación de políticas específicas. [25]

- La generación del cifrado.
- El uso y protección de estas.
- La renovación o destrucción del uso del cifrado en el acceso a nube.

Seguridad de la información para el uso de servicios en la nube (5.23)

El principal control de acceso relacionado con la nube establece los servicios en la nube para lograr una mejor y más completa protección, así como un control de acceso más efectivo. En su mayoría, el único cambio necesario será utilizar de manera más exhaustiva las funciones de seguridad existentes en la nube. [26]

NIST Cybersecurity Framework (CSF)

Se trata de un conjunto de guías prácticas y prescriptivas para ayudar a las organizaciones a gestionar y mejorar la ciberseguridad de sus sistemas de información, incluyendo la nube. [27]

- **ID.AM-1: Definir roles y responsabilidades:** Establecer roles y responsabilidades claras para la gestión de identidades y accesos en la nube. Asignar usuarios a roles en función de sus necesidades laborales y nivel de acceso requerido.
- **ID.AM-3: Evaluar los riesgos de acceso:** Evaluar los riesgos de acceso a los activos de información en la nube. Identificar amenazas potenciales como ataques de phishing, malware y accesos no autorizados.

- **PR.AC-1: Implementar MFA:** Exigir MFA para todos los accesos a cuentas de usuario en la nube. Utilizar métodos de autenticación adicionales como códigos de un solo uso (OTP), tokens de seguridad o biometría.
- **PR.AC-2: Aplicar el principio de mínimo privilegio:** Otorgar a los usuarios solo los permisos necesarios para realizar sus tareas. Evaluar los requisitos de acceso para cada rol y asignar solo los permisos esenciales.
- **PR.AC-3: Gestionar contraseñas de forma segura:** Implementar políticas de contraseñas sólidas y almacenar las contraseñas de forma segura.
- **PR.AC-5: Monitorizar y registrar las actividades de acceso:** Registrar y monitorizar las actividades de acceso a los recursos en la nube. Establecer alertas para notificar a los administradores sobre eventos de acceso de alto riesgo.
- **RS.AC-1: Definir un plan de respuesta a incidentes:** Establecer un plan de respuesta a incidentes para gestionar las brechas de seguridad y los accesos no autorizados.

CIS Controls (Center for Internet Security)

Son un conjunto de recomendaciones de seguridad prescriptivas y de mejores prácticas diseñadas para ayudar a las organizaciones a protegerse contra los ciberataques más comunes y peligrosos. Estos controles incluyen directrices específicas para el control de acceso de usuarios en la nube. [28]

- **Control 1: Inventario de software:** Este control exige la creación y mantenimiento de un inventario de todo el software que se ejecuta en los entornos de nube. Esto ayuda a identificar posibles vulnerabilidades y riesgos de seguridad.
- **Control 3: Protección de datos:** Este control exige la protección de los datos confidenciales en la nube mediante medidas como el cifrado y el control de acceso.

- **Control 5: Control de acceso a la red:** Este control exige la implementación de controles de acceso a la red para restringir el acceso a los recursos de la nube. Esto incluye el uso de firewalls, listas de control de acceso (ACL).

Tras analizar detalladamente los diferentes marcos de seguridad y sus controles relacionados con el control de acceso tanto en general como específicamente en entornos de nube, se presenta el siguiente cuadro comparativo.

Tabla 2. *Comparativa de Frameworks basada en controles de acceso a la nube y desventajas localizadas*

FRAMEWORK	CONTROLES DIRIGIDOS ACCESO A NUBE	DESVENTAJA LOCALIZADA
ZERO TRUST	El enfoque de seguridad holístico de Microsoft	Se requiere del trabajo de la mano de un SOC, para obtener resultados esto es un gasto de presupuesto para las empresas.
ISO 27001:2022	Seguridad de la información para el uso de servicios en la nube (5.23)	El control de acceso en nube depende de las buenas prácticas del usuario, así como del servicio en nube para que funcione de manera correcta.
NIST Cybersecurity Framework (CSF)	Posee controles de acceso seguro, así como buenas prácticas de contraseñas	Controles de relacionados con las buenas prácticas de los usuarios, así como los métodos óptimos para el control de acceso en general
CIS Controls (Center for Internet Security)	Posee controles de acceso seguro, así como buenas prácticas de contraseñas	Controles de relacionados con las buenas prácticas de los usuarios, así como los métodos óptimos para el control de acceso en general

Después de comparar varios marcos de referencia, elegimos la ISO 27001:2022 debido a que abarca más controles específicos relacionados con el control de acceso, especialmente en entornos de nube. Además, hemos observado que el eslabón más débil en todos los controles analizados suele ser la falta de buenas prácticas o el desconocimiento. Para abordar esta brecha de conocimiento, desarrollaremos módulos dentro de la plataforma Moodle que enseñarán a los usuarios cómo mejorar el control de acceso en la nube utilizando la ISO 27001:2022. Por lo tanto, para continuar con nuestra metodología, planeamos realizar encuestas generales a los usuarios de servicios en la nube. El objetivo es entender su nivel de conocimiento sobre este tema y evaluar su capacidad en este ámbito.

Encuesta

El conjunto de preguntas seleccionadas, son seleccionadas después de haber entendido en contexto en cual se maneja el control de acceso en nube mediante la recolección de datos de las fuentes bibliográficas además de que realizara la comparativa de los frameworks se tiene como idea principal el que el usuario es eslabón más débil a cubrir y que es importante generar una herramienta de capacitación para que dicho eslabón sea cubierto y de esta manera obtener una mejora en el control de acceso a los servicios ya mencionados.

Se diseñó y administró una encuesta a profesionales en TI, estudiantes de la UPS, administradores de sistemas y usuarios de servicios en la nube para obtener las nociones más importantes acerca de las vulnerabilidades y necesidades en cuanto a autenticación que se han presentado hasta la actualidad.

La encuesta consta de las siguientes preguntas:

1. **¿Qué métodos de autenticación utilizan actualmente en los servicios de nube?**
2. **¿Qué tan conscientes están los usuarios finales de la importancia de contraseñas seguras?**
3. **¿Han experimentado brechas de seguridad relacionadas con la autenticación en la nube en el pasado?**

4. **¿Consideran que las contraseñas únicas y robustas son suficientes para garantizar la seguridad en la nube?**
5. **¿Cuál creen que es el nivel de riesgo asociado a la falta de autenticación multifactor?**
6. **¿Cuáles son las principales preocupaciones o desafíos relacionados con la autenticación en la nube en su organización?**
7. **¿Estarían dispuestos a adoptar una solución de autenticación multifactor más avanzada?**
8. **¿Qué barreras creen que podrían obstaculizar la implementación de medidas más sólidas de autenticación en la nube?**

A continuación, se presenta que datos relevantes se obtuvieron al realizar esta encuesta los cuales sumados a todo lo antes revisado como la revisión bibliográfica y la comparativa además de la elección de cuáles serán los controles que usar para con ello realizar el diseño de la solución.

Pregunta 1: ***¿Qué métodos de autenticación utilizan actualmente en los servicios de nube?***

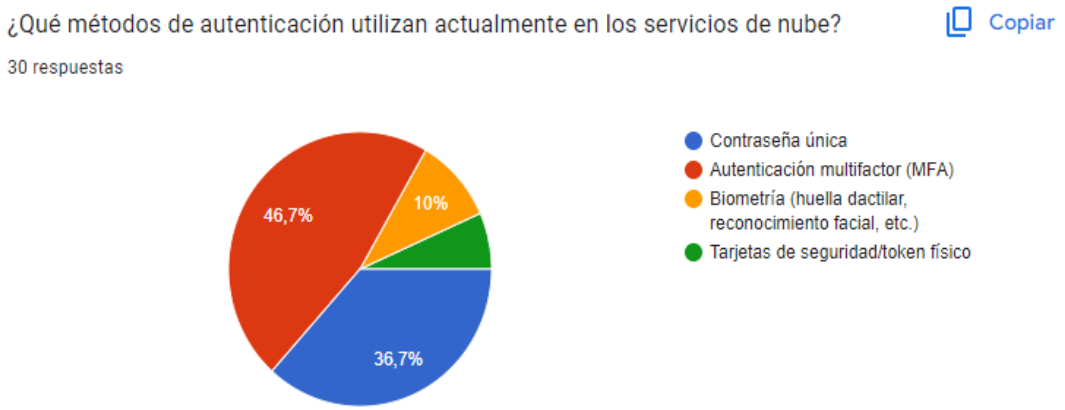


Fig 4. *Porcentaje de distribución de respuesta opción múltiple – Pregunta 1*

Conclusión

La variedad en las respuestas revela que las organizaciones optan por una combinación de métodos en lugar de depender exclusivamente de uno. Esta

estrategia diversificada podría ser una medida proactiva para abordar diferentes tipos de amenazas. La Autenticación multifactor (MFA)" destaca un enfoque claro en la autenticación fuerte. Esto puede deberse a la conciencia de la vulnerabilidad de las contraseñas tradicionales.

Pregunta 2: ¿Qué tan conscientes están los usuarios finales de la importancia de contraseñas seguras?

Fig 5. *Porcentaje de distribución de respuesta opción múltiple – Pregunta 2*

Conclusión

La variedad de respuestas indica la necesidad de estrategias diferenciadas para abordar niveles variados de conocimiento.

Es necesario la concientización que aborden tanto los conceptos básicos como los detalles específicos sobre la creación y gestión de contraseñas.

Pregunta 3: ¿Han experimentado brechas de seguridad relacionadas con la autenticación en la nube en el pasado?

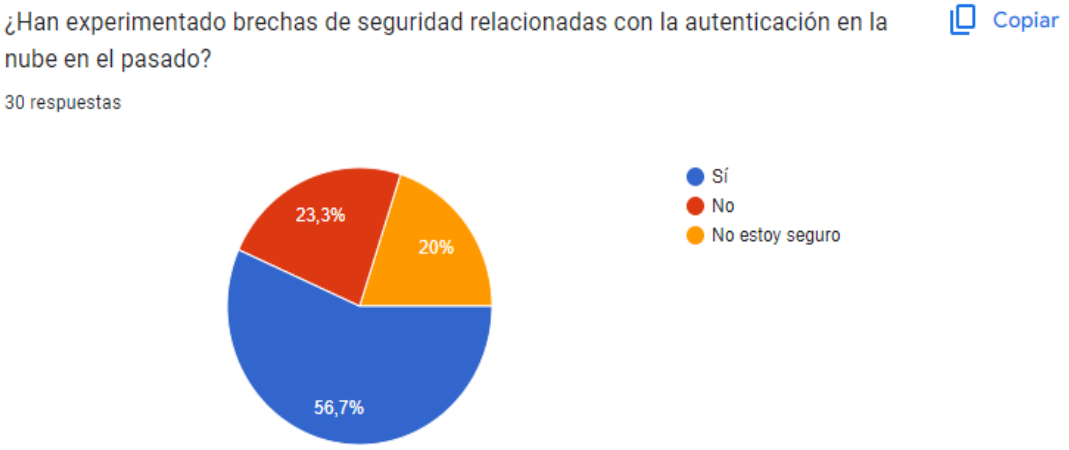


Fig 6. *Porcentaje de distribución de respuesta opción múltiple – Pregunta 3*

Conclusión

La mayoría ha experimentado brechas de seguridad relacionadas con la autenticación en la nube, indicando una preocupación significativa.

La experiencia diversa subraya la necesidad de enfoques personalizados para mejorar la postura de seguridad.

Compartir experiencias y adoptar medidas preventivas son esenciales para fortalecer la seguridad en la autenticación en la nube.

Pregunta 4: ¿Consideran que las contraseñas únicas y robustas son suficientes para garantizar la seguridad en la nube?

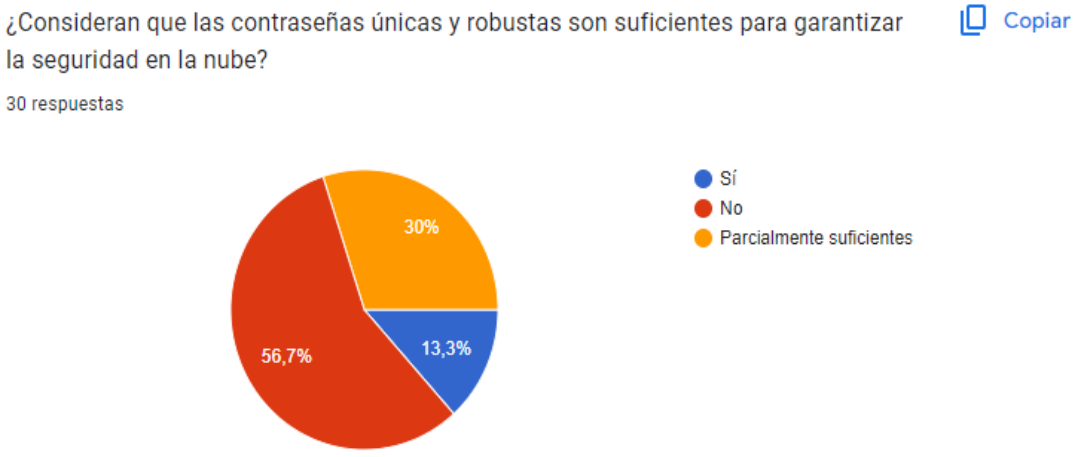


Fig 7. *Porcentaje de distribución de respuesta opción múltiple – Pregunta 4*

Conclusión

La mayoría percibe que las contraseñas únicas y robustas no son suficientes para garantizar la seguridad. Una minoría que considera que son parcialmente suficientes podría indicar una comprensión de su papel complementario en una estrategia de seguridad más amplia.

Pregunta 5: ¿Cuál creen que es el nivel de riesgo asociado a la falta de autenticación multifactor?

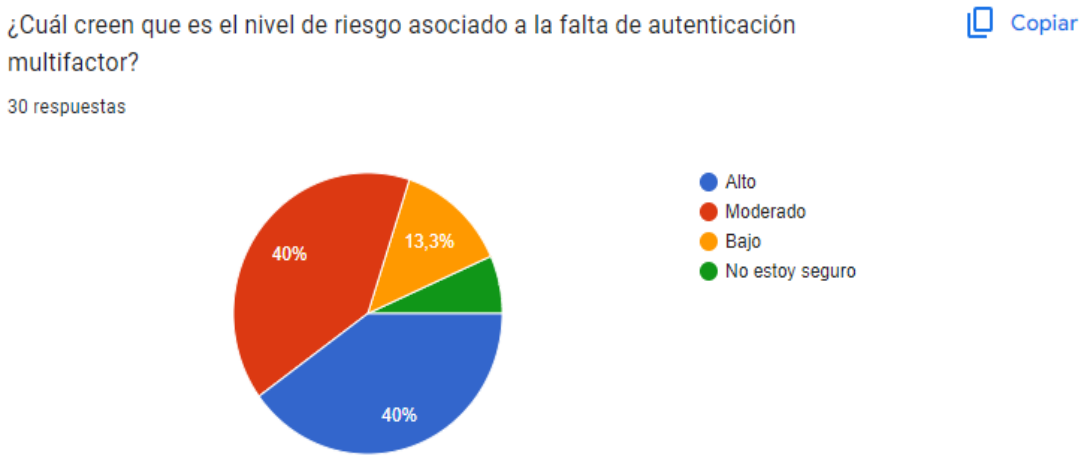


Fig 8. *Porcentaje de distribución de respuesta opción múltiple – Pregunta 5*

Conclusión

La mayoría percibe un alto riesgo asociado a la falta de autenticación multifactor.

La variabilidad en las respuestas sugiere la necesidad de enfoques personalizados para la mejora de la seguridad.

La implementación de MFA es crucial para atender las inquietudes de seguridad y reducir el riesgo percibido.

Pregunta 6: ¿Cuáles son las principales preocupaciones o desafíos relacionados con la autenticación en la nube en su organización?

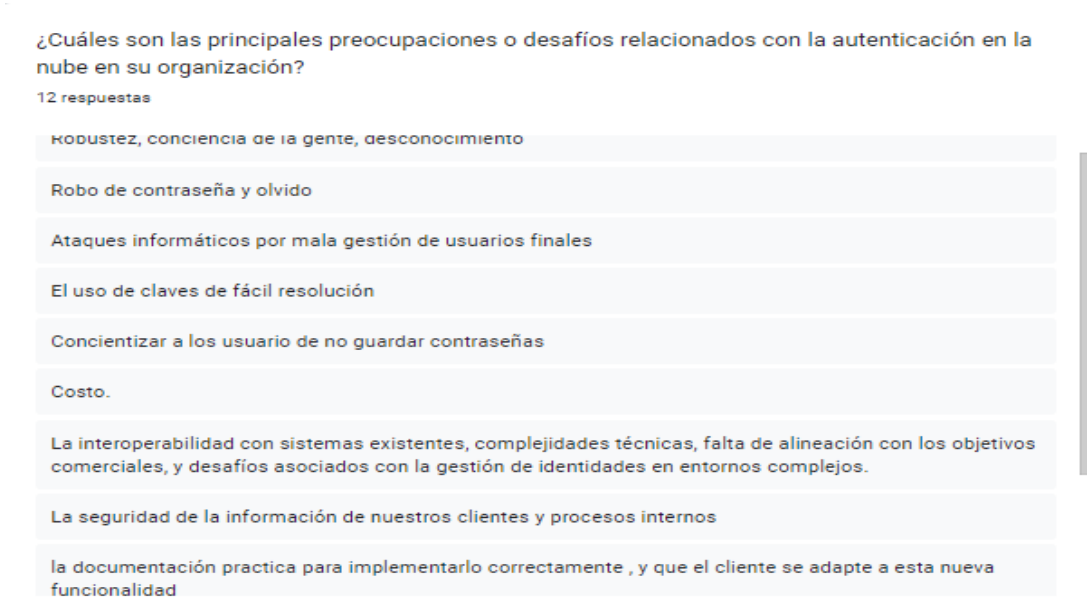


Fig 9. *Resumen respuesta abierta – Pregunta 6*

Conclusión

Las preocupaciones abordadas reflejan la complejidad de la gestión de la autenticación en la nube.

La implementación efectiva de soluciones debe abordar aspectos técnicos, educativos y financieros de manera integrada.

La adaptabilidad y la consideración de las necesidades específicas de cada organización son fundamentales para superar estos desafíos.

Pregunta 7: ¿Estarían dispuestos a adoptar una solución de autenticación multifactor más avanzada?

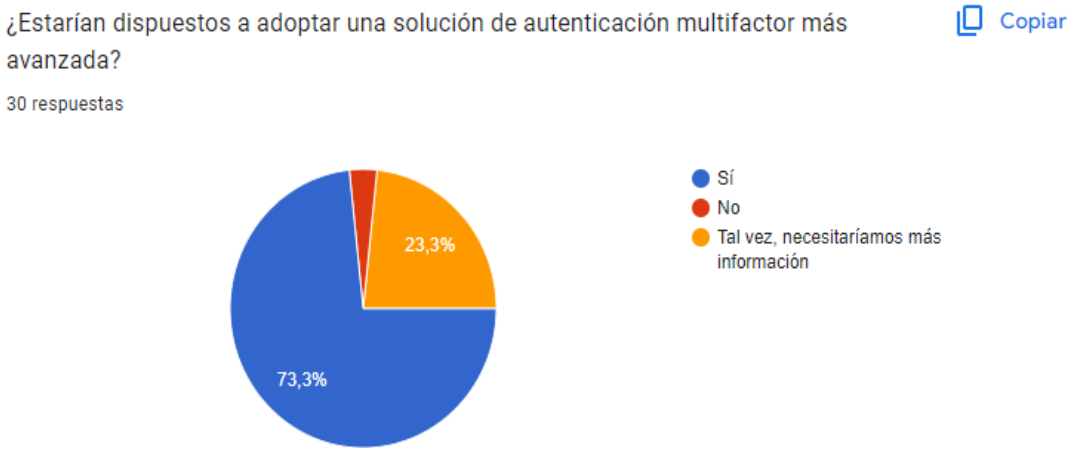


Fig 10. *Porcentaje de distribución de respuesta opción múltiple – Pregunta 7*

Conclusión

La disposición general a adoptar una solución más avanzada es positiva.

El éxito de la implementación dependerá de una comunicación efectiva y del abordaje proactivo de posibles inquietudes a través de la información y el soporte adecuados.

Pregunta 8: ¿Qué barreras creen que podrían obstaculizar la implementación de medidas más sólidas de autenticación en la nube?

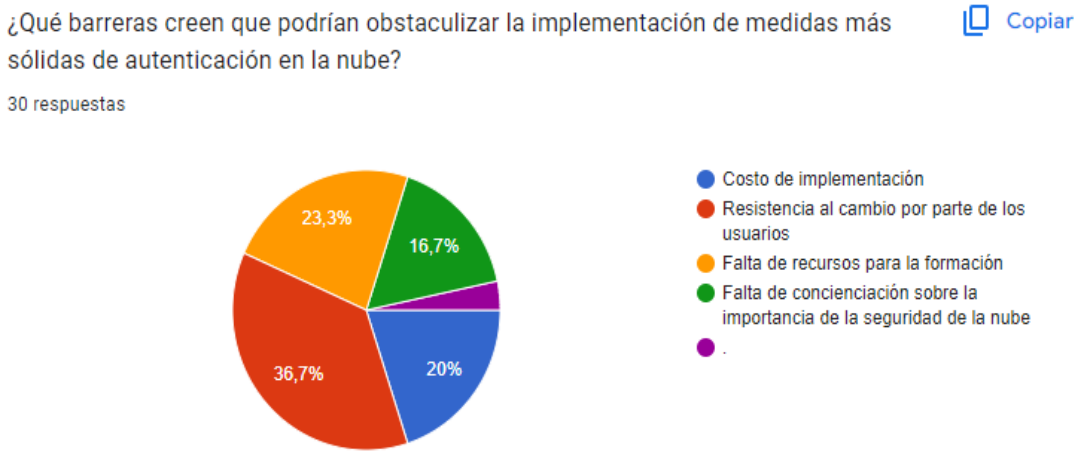


Fig 11*. Porcentaje de distribución de respuesta opción múltiple – Pregunta 8*

Conclusión

- **Estrategias de Gestión del Cambio:**

Desarrollar estrategias efectivas de gestión del cambio con la finalidad de abordar a la resistencia, como sesiones de concientización, comunicación clara de beneficios y demostraciones prácticas.

- **Asignación de Recursos para la Formación:**

Destinar recursos específicos para programas de formación que aborden la falta de conocimiento y aseguren una transición suave hacia las medidas de autenticación más sólidas.

- **Involucramiento de stakeholders:**

Involucrar a los usuarios, en el proceso de toma de decisiones puede contribuir a una mayor aceptación y colaboración.

Cubo de ciberseguridad de McCumber

Tomando como base el modelo planteado por John McCumber, plantea como opciones de contramedidas:

1) Tecnología

2) Políticas y prácticas

3) Personas

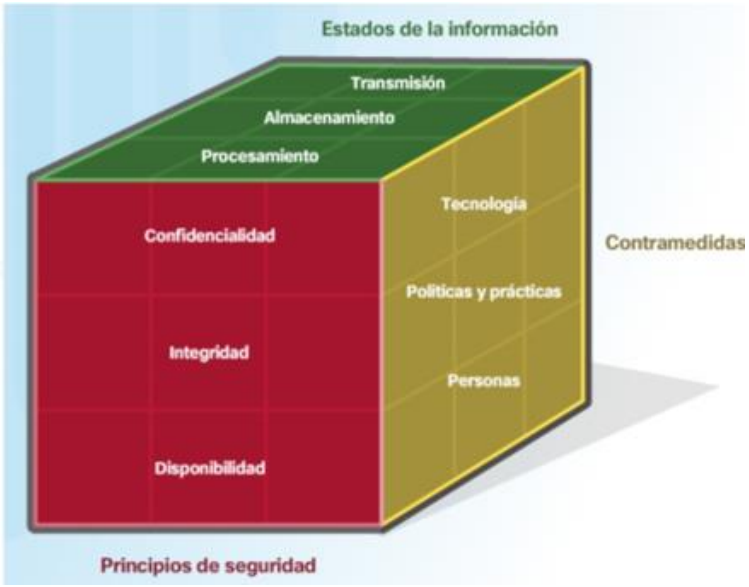


Fig 12. *Cubo contramedidas entre (Personas-Capacitación) [9]*

- **Contramedida en Tecnologías para mejorar la Seguridad**:

Para mejorar el control de acceso en entornos de nube, es fundamental implementar tanto hardware como softwares específicos que fortalezcan la seguridad de la infraestructura.

Hardware: Se recomienda el uso de dispositivos de autenticación multifactor (MFA) como tokens de hardware o dispositivos de biometría. Estos dispositivos permiten asegurar que solo los usuarios autorizados puedan acceder a los recursos en la nube, añadiendo una capa adicional de seguridad más allá de las contraseñas.

Software: Es fundamental implementar soluciones de gestión de identidad y acceso (IAM) que permitan controlar quién tiene acceso a qué recursos en la nube. Estas soluciones permiten establecer políticas de acceso basadas en roles (RBAC) y grupos de usuarios, asegurando que cada persona tenga sólo el acceso necesario según sus funciones laborales. También es recomendable utilizar softwares con capacidades de monitoreo y auditoría que registren y analicen los intentos de acceso, así como detectar comportamientos sospechosos.

Además, la implementación de soluciones de Single Sign-On (SSO) puede facilitar la experiencia del usuario al permitirle autenticarse una sola vez para acceder a múltiples aplicaciones en la nube, simplificando la gestión de credenciales y reduciendo el riesgo de uso de contraseñas débiles o repetidas.

- **Contramedida Políticas de Seguridad**

Las políticas de seguridad son fundamentales para mejorar el control de acceso y proteger los recursos en entornos de nube. Según la literatura, se recomienda implementar las siguientes políticas para fortalecer el control de acceso en la nube:

1. **Autenticación Multifactor (MFA):** La implementación de MFA es crucial para garantizar que solo los usuarios autorizados puedan acceder a los recursos. Esto implica requerir múltiples formas de verificación, como contraseñas, tokens de hardware o aplicaciones de autenticación.

2. **Principio del Menor Privilegio:** Esta política sugiere que los usuarios deben tener solo los permisos necesarios para llevar a cabo sus funciones laborales. Limitar el acceso a la información sensible y los recursos críticos minimiza el riesgo de exposiciones o brechas de seguridad.

3. **Control de Acceso Basado en Roles (RBAC):** Asignar permisos según los roles de los usuarios dentro de la organización permite un manejo más eficiente de quién tiene acceso a qué. Esto también facilita la auditoría y el seguimiento de accesos.

4. **Políticas de Gestión de Identidades y Acceso (IAM):** Implementar soluciones de IAM permite administrar de manera centralizada las credenciales de usuario y mejorar la seguridad del acceso. La monitorización y gestión de identidades ayudan a prevenir accesos no autorizados.

5. **Auditorías y Monitoreo Continuo:** Realizar auditorías periódicas y monitorear continuamente el acceso a los recursos en la nube permite identificar comportamientos inusuales o no autorizados, facilitando una respuesta rápida ante amenazas potenciales.

6. **Educación y Concienciación del Usuario:** Capacitar a los empleados sobre las mejores prácticas de seguridad en la nube y la importancia de la protección de datos es esencial. Esto incluye la detección de intentos de phishing y el uso adecuado de contraseñas seguras.

7. **Gestión de Contraseñas:** Implementar políticas para la complejidad y renovación regular de contraseñas, así como el uso de herramientas de gestión de contraseñas, ayuda a mantener un control más estricto sobre el acceso de usuarios.

8. **Revisión y Revocación de Accesos:** Establecer procedimientos para la revisión regular de los accesos de los empleados, especialmente tras cambios en el empleo, y revocar el acceso cuando ya no sea necesario, ayuda a prevenir accesos indebidos.

9. **Protección de Datos y Cifrado:** Aplicar políticas que garanticen el cifrado de datos en reposo y en tránsito, asegurando que incluso si se produce un acceso no autorizado, la información permanezca protegida.

10. **Políticas de Seguridad por Énfasis en la Nube:** Dado que las arquitecturas en la nube son diferentes de las locales, es importante adaptar las políticas de seguridad a estas realidades, considerando aspectos como el acceso remoto, las API, y la colaboración con terceros.

- **Contramedida en Capacitación de las Personas**

Para mejorar el control de acceso en entornos de nube, es esencial capacitar a las personas en las siguientes buenas prácticas de seguridad:

1. **Autenticación Fuerte**: Instruir a los usuarios sobre la importancia de utilizar métodos de autenticación robustos, como la autenticación multifactor (MFA), que proporciona una capa adicional de seguridad más allá de las contraseñas.

2. **Gestión de Contraseñas**: Promover el uso de contraseñas seguras y la implementación de políticas de cambio regular de contraseñas. También se debe enseñar a utilizar gestores de contraseñas para almacenar y generar claves complejas.

3. **Principio de Mínimos Privilegios**: Capacitar a los usuarios en la necesidad de otorgar solo los permisos estrictamente necesarios para realizar su trabajo, así como revisar periódicamente los accesos concedidos.

4. **Revisión Regular de Accesos**: Fomentar la práctica de realizar auditorías periódicas de los accesos a la nube para identificar y revocar permisos no utilizados o innecesarios.

5. **Sesiones y Accesos Temporales**: Instruir sobre cómo implementar sesiones temporales y accesos limitados en el tiempo para tareas específicas, minimizando el tiempo durante el cual las credenciales son válidas.

6. **Concienciación sobre Phishing**: Capacitar a los usuarios en la identificación y prevención de ataques de phishing, que suelen ser utilizados para robar credenciales de acceso.

7. **Uso de APIs Seguras**: Enseñar la importancia de utilizar APIs seguras y el manejo adecuado de las claves de acceso a los servicios en la nube, evitando la exposición innecesaria.

8. **Monitoreo y Alerta de Actividades Sospechosas**: Capacitar a los equipos sobre cómo monitorear accesos y actividades inusuales en la nube, así como la respuesta a incidentes que puedan comprometer la seguridad.

9. **Formación Continua**: Establecer programas de formación continua y actualizaciones regulares sobre nuevas amenazas y prácticas de seguridad, asegurando que el personal esté al día con las mejores prácticas.

10. **Documentación y Procedimientos Estándar**: Proporcionar a los usuarios documentación clara y accesible sobre los procedimientos de seguridad, incluidas las responsabilidades en el uso de servicios en la nube.

En este trabajo de titulación, se propone mejorar el control de acceso a la nube mediante la capacitación de usuarios a través de un producto educativo en la plataforma Moodle. La investigación revela que la seguridad multifactor y la capacitación del usuario final son fundamentales para el correcto funcionamiento de los servicios en la nube. Dado que los proveedores se encargan de la implementación de la tecnología multifactor, se sugiere la creación de un recurso de formación en Moodle que fomente buenas prácticas entre los usuarios

Diseño de la solución

La creciente adopción de servicios en la nube ha generado una serie de desafíos en términos de seguridad, especialmente en lo que respecta al control de acceso de los usuarios. Basándose en la revisión bibliográfica, comparativa de los controles de los frameworks, se identificaron varios problemas clave en el acceso a servicios en la nube, que incluyen contraseñas débiles, falta de conciencia sobre buenas prácticas

de seguridad, dejando en claro que es necesarios la capacitación de los usuarios y por ello una herramienta de capacitación ayudaría a mejorar este apartado.

Moodle ofrece una plataforma educativa robusta que puede integrar módulos específicos para la formación en seguridad de la autenticación en la nube. Proporciona una solución educativa efectiva y accesible, ideal para mejorar el control de acceso en la nube a través de la capacitación continua y la concienciación sobre seguridad. Sin embargo, para necesidades empresariales específicas y soluciones de seguridad de nivel empresarial, las alternativas mencionadas pueden ofrecer capacidades más avanzadas y especializadas en gestión de accesos y seguridad.

Justificación Metodológica

La revisión bibliográfica ofrece una visión teórica detallada de este tema, mediante la identificación de tendencias, desafíos y soluciones propuestas por expertos, así como por estudios previos. Por otro lado, las encuestas permiten capturar las percepciones y experiencias reales de profesionales y usuarios, revelando prácticas comunes, debilidades percibidas y desafíos prácticos en la autenticación en la nube. Esta combinación de métodos garantiza la cobertura tanto teórica como práctica de la problemática, permitiendo una comprensión completa además de la identificación correcta de soluciones y buenas prácticas para el tema estudiado.

No solo proporciona un respaldo teórico al estudio, sino que también ofrece un análisis detallado de las prácticas actuales y las últimas tendencias en seguridad de la autenticación en la nube. Identifica los marcos conceptuales, normativas de la industria y las recomendaciones de seguridad más actualizadas, respaldando así la propuesta de solución planteada en base a prácticas validadas y reconocidas

Las encuestas proporcionan una ventana directa a la realidad operativa y las experiencias de los profesionales y usuarios involucrados en la autenticación en la nube. Estas respuestas prácticas ofrecen una comprensión detallada de los desafíos reales que enfrentan las organizaciones en términos de métodos de autenticación, percepciones sobre riesgos y brechas de seguridad experimentadas. Permiten

identificar patrones, problemas comunes y áreas de mejora percibidas desde una perspectiva práctica, enriqueciendo así la investigación con datos concretos y experiencias reales.

La elección de ISO 27001:2022 como base para el análisis y comparación de controles de acceso en la nube está justificada por su reconocimiento global, enfoque integral, relevancia actualizada, flexibilidad, promoción de la mejora continua y esta norma proporciona un marco robusto y probado para gestionar y mejorar la seguridad de la información en entornos de nube, garantizando que las organizaciones puedan proteger eficazmente sus datos y sistemas contra amenazas y vulnerabilidades.

La creación de una plataforma de capacitación, como se propone en el estudio, representa una estrategia activa y eficiente para difundir las prácticas más efectivas de seguridad adoptadas por los usuarios finales. Esta plataforma, basada en Moodle o un sistema similar, puede ofrecer módulos interactivos, recursos educativos y pruebas prácticas con el fin de aumentar la conciencia, comprensión de la autenticación sólida en la nube. Además, proporciona un entorno controlado para simular situaciones de seguridad, ofreciendo a los usuarios oportunidades prácticas para aprender y aplicar directamente las medidas de seguridad recomendadas.

Plataforma de Capacitación Moodle:

Moodle es un sistema de gestión del aprendizaje de código abierto que permite crear entornos de capacitación en línea de manera efectiva. En este proyecto, se implementará Moodle para desarrollar una plataforma dedicada a la formación en seguridad en la nube. [10]

5. RESULTADOS Y DISCUSIÓN

Se presentan los cursos creados en relación con la norma ISO 27001:2022. Los cuales abarcan temas que son de alta relevancia para que el usuario se capacite en el tema, así como este al tanto de los temas más importantes y de esta manera logre un mejor acceso al servicio de nube el cual utilice.

Temas referentes a los cursos

A continuación, se presentan en detalle los módulos de los cursos:

Curso 1: Fortalecimiento de la Autenticación en la Nube

El curso "Fortalecimiento de la Autenticación en la Nube", ofrece una visión integral de los fundamentos y las mejores prácticas relacionadas con la autenticación en entornos de nube. Este curso está diseñado para equipar a los profesionales con las habilidades necesarias para implementar y gestionar de manera efectiva la autenticación multifactor (MFA) en conformidad con los estándares de seguridad de la norma ISO 27001:2022.

Módulo 1: Fundamentos de la Autenticación en la Nube

1. **Introducción a la Autenticación en la Nube:**
    - Definición y relevancia en el contexto actual.
    - Evolución de los métodos de autenticación y su adaptación a entornos de nube.
2. **Desafíos Actuales en la Autenticación:**
    - Análisis detallado de riesgos y vulnerabilidades.
    - Estudio de casos reales de brechas de seguridad asociadas con la autenticación en la nube.

Módulo 2: Mejores Prácticas en Autenticación Multifactor (MFA)

1. **Conceptos Básicos de MFA:**
    - Exploración de diferentes factores de autenticación.
    - Casos de uso y ejemplos prácticos de implementación.
2. **Implementación Efectiva de MFA con ISO 27001:2022:**
    - Integración de MFA según las directrices de la norma ISO 27001.
    - Herramientas y plataformas compatibles con los estándares de seguridad.

Módulo 3: Estrategias de Gestión del Cambio

1. **Abordando la Resistencia al Cambio en la Implementación de MFA:**
    - Estrategias efectivas de gestión del cambio aplicadas a la seguridad.

- Comunicación y concientización sobre la importancia de la autenticación multifactor.

2. **Involucramiento de los Usuarios en Prácticas Seguras:**
   - Métodos para motivar y educar a los usuarios.
   - Creación de una cultura organizacional centrada en la seguridad.

Módulo 4: Evaluación y Mejora Continua

1. **Monitoreo y Evaluación de la Autenticación:**
   - Utilización de métricas clave para evaluar la efectividad.
   - Identificación temprana de posibles problemas y ajustes necesarios.
2. **Mejoras Continuas y Adaptación según ISO 27001:2022:**
   - Actualización de políticas y procedimientos en línea con ISO 27001:2022.
   - Incorporación de nuevas tecnologías y enfoques para mantener la seguridad.

Creación del curso 1, en la plataforma de Moodle

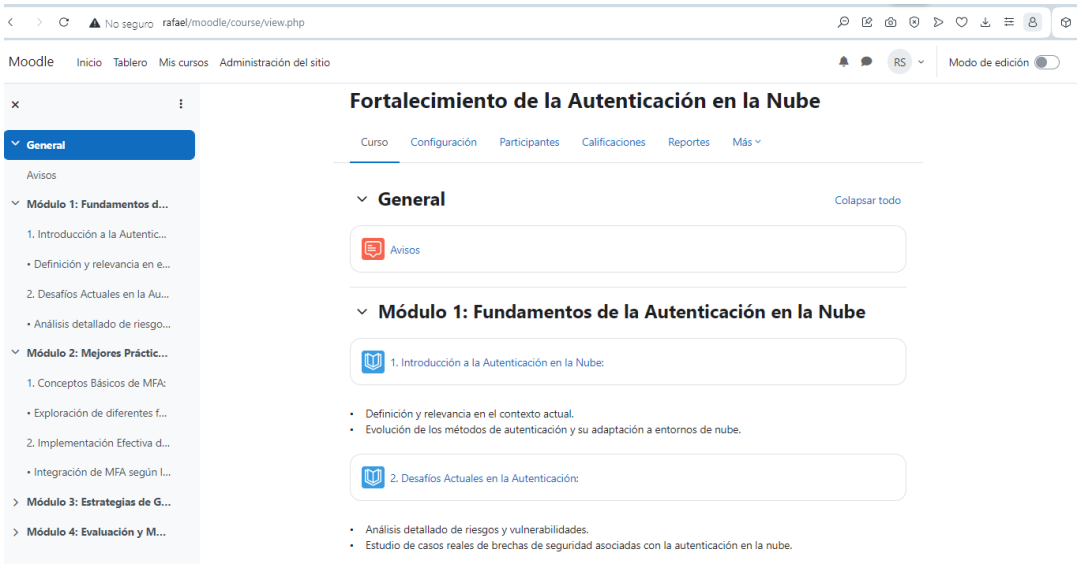


Fig 13. *Creación del curso 1 en Moodle, visualización del módulo 1.*

Fig 14. *Creación del curso 1 en Moodle, visualización del módulo 2.*

Fig 15. Creación del curso 1 en Moodle, visualización del módulo 3 y 4.

Curso 2: Seguridad Integral en Servicios de Nube

El curso "Seguridad Integral en Servicios de Nube", se centra en la evaluación de riesgos, el cumplimiento legal además de la implementación de soluciones avanzadas en servicios de nube. Este curso aborda las barreras organizacionales y

proporciona estrategias para superarlas, garantizando la adopción de medidas sólidas de autenticación en conformidad con ISO 27001:2022.

Módulo 1: Evaluación de Riesgos y Cumplimiento Legal

1. **Análisis de Riesgos Específicos de la Nube según ISO 27001:2022:**
    - Identificación y evaluación de riesgos en línea con la norma ISO 27001.
    - Cómo prevenir amenazas y garantizar la seguridad de la información.
2. **Cumplimiento Legal en la Nube con ISO 27001:2022:**
    - Guía para el cumplimiento con las regulaciones y estándares de seguridad.
    - Evitar sanciones, proteger la integridad legal de la organización.

Módulo 2: Estrategias para Superar Barreras Organizacionales

1. **Abordaje de la Resistencia al Cambio en la Seguridad de la Nube:**
    - Estrategias prácticas para superar la resistencia al cambio.
    - Implementación de políticas que fomenten la aceptación de nuevas medidas.
2. **Gestión de Recursos para Formación y Cumplimiento Normativo:**
    - Asignación efectiva de recursos para la formación y cumplimiento normativo.
    - Desarrollo de programas adaptados a las necesidades y requerimientos de la norma ISO 27001:2022.

Módulo 3: Implementación de Soluciones Avanzadas

1. **Adopción de Medidas Sólidas de Autenticación en Conformidad con ISO 27001:2022:**
    - Pasos prácticos y consideraciones para implementar medidas avanzadas.
    - Casos de éxito y lecciones aprendidas.
2. **Desarrollo de Plataformas de Capacitación en Moodle:**
    - Utilización efectiva de la plataforma Moodle para la formación en seguridad.
    - Creación de cursos y contenido alineado con ISO 27001:2022.

Módulo 4: Seguimiento y Mejora Continua

1. **Monitoreo de Seguridad en la Nube según ISO 27001:2022:**
    - Herramientas y mejores prácticas para el monitoreo constante.
    - Respuesta a incidentes y gestión de crisis siguiendo las directrices de ISO 27001:2022.
2. **Evaluación Periódica y Actualización de Políticas:**
    - Revisión regular de políticas y procedimientos según ISO 27001:2022.
    - Mantenimiento de la seguridad en un entorno dinámico y en evolución.

Creación del curso 2, en la plataforma de Moodle

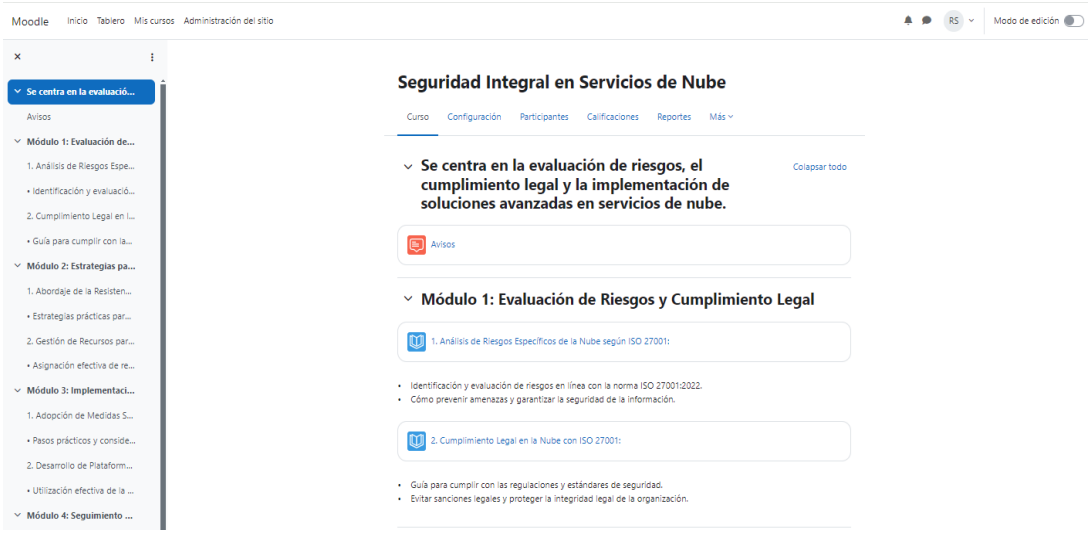


Fig 16. *Creación del curso 2 en Moodle, visualización del módulo 1.*

Fig 17. *Creación del curso 2 en Moodle, visualización del módulo 2 y 3.*

Fig 18. *Creación del curso 2 en Moodle, visualización del módulo 4.*

Plan de Capacitación para Usuarios Finales en Autenticación en la Nube

Creación de un plan de capacitación de un mes dirigido a usuarios finales, enfocado en prácticas seguras de autenticación en entornos en la nube. El propósito principal es mejorar la conciencia de seguridad entre los usuarios y disminuir los riesgos asociados con los procesos de autenticación en este contexto específico.

Concienciación sobre Autenticación en la Nube

Día 1-3: Sesiones Iniciales de Concienciación

- Presentación del concepto de autenticación en la nube.
- Importancia de la autenticación segura en la protección de datos.
- Estadísticas y ejemplos de brechas de seguridad relacionadas con la autenticación.

Día 4-7: Webinars y Charlas Interactivas

- Exploración de diferentes métodos de autenticación en la nube.
- Casos de estudio sobre la relevancia de contraseñas fuertes y autenticación multifactor.
- Participación de los usuarios en preguntas y respuestas.

Entrenamiento Práctico en Autenticación

Día 8-14: Talleres Prácticos

- Sesiones prácticas sobre la creación de contraseñas seguras.
- Simulacros de autenticación multifactor utilizando herramientas de capacitación.
- Ejercicios de identificación de posibles amenazas y vulnerabilidades.

Implementación de Buenas Prácticas

Día 15-21: Implementación y Uso Diario

- Guía paso a paso sobre la implementación de autenticación multifactor.
- Pruebas en entornos simulados para garantizar la comprensión.
- Sugerencias para el uso diario y la gestión segura de credenciales.

Evaluación y Reforzamiento

Día 22-28: Evaluación Final y Reforzamiento

- Evaluación de conocimientos adquiridos a través de pruebas cortas.
- Sesiones de preguntas y respuestas finales.

- Entrega de recursos adicionales para referencia futura.

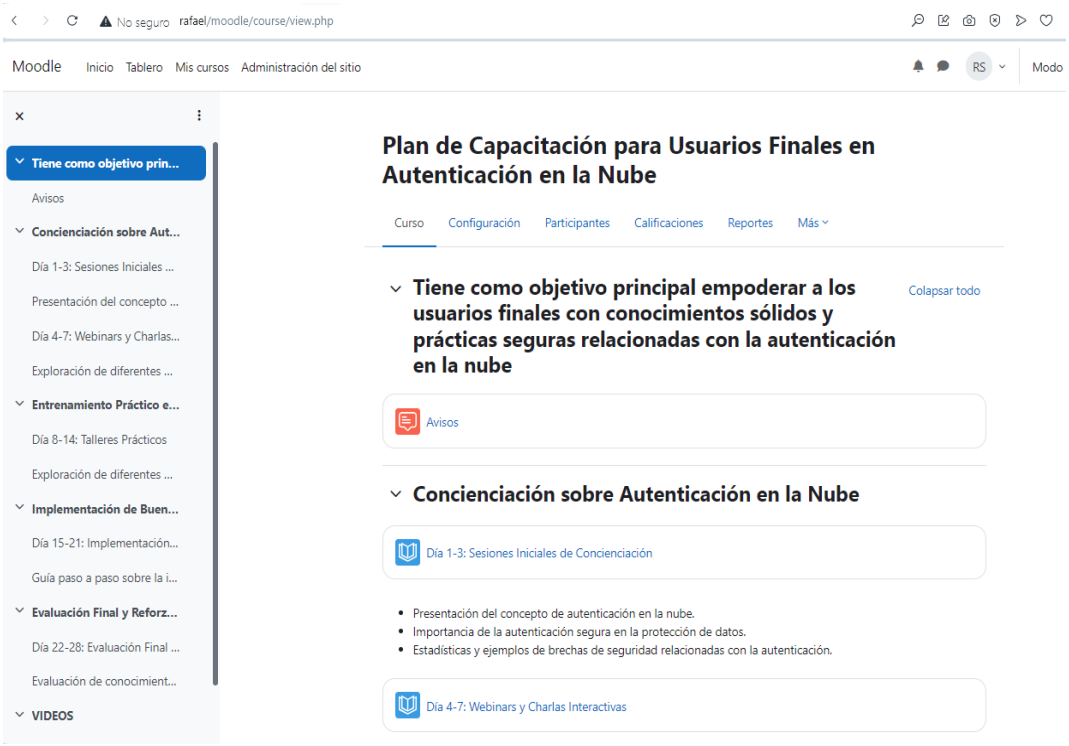


Fig 19. *Creación del plan de capacitación en Moodle, visualización del módulo 1.*

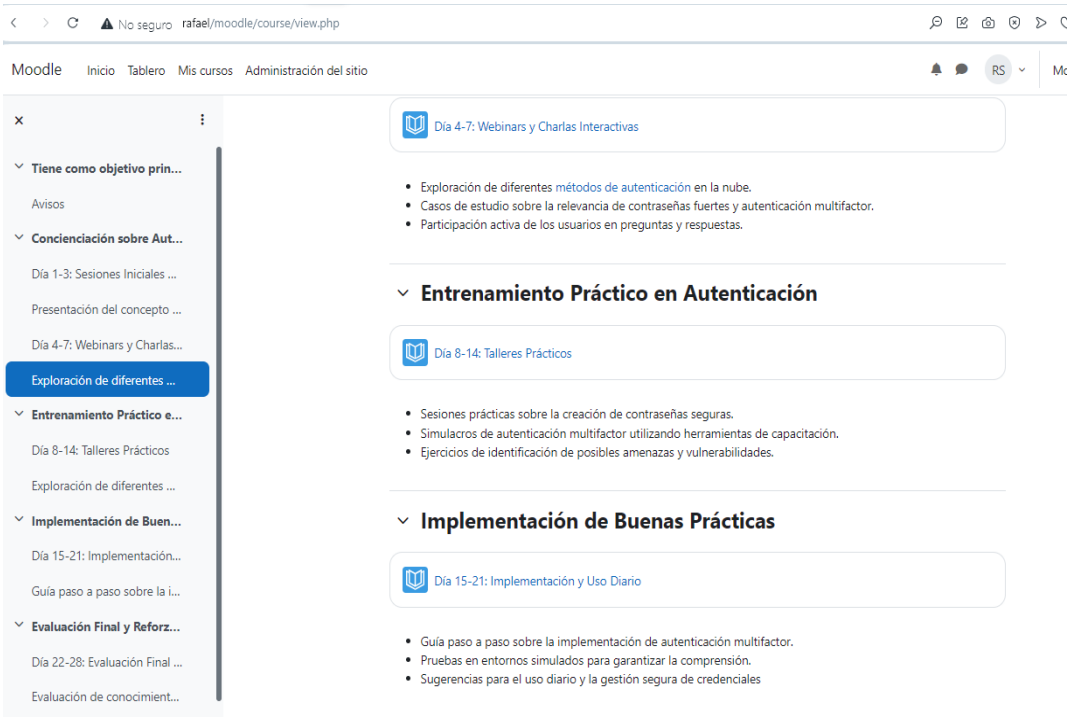


Fig 20. *Creación del plan de capacitación en Moodle, visualización del módulo 2 y 3.*

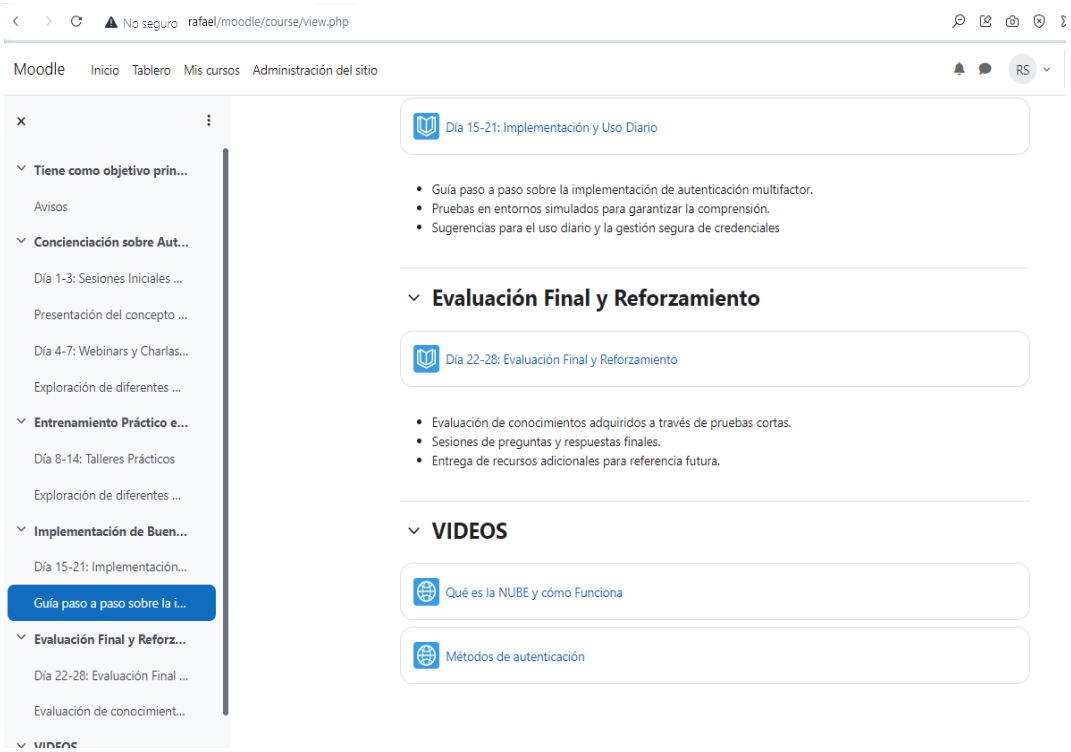


Fig 21. *Creación del plan de capacitación en Moodle, visualización del módulo 4.*

Resultados de la plataforma Moodle acerca de los cursos planificados

Para un tamaño de muestra de 30 personas para validar la plataforma Moodle como herramienta de capacitación, se utilizó la fórmula para el cálculo del tamaño de muestra en estudios de investigación. Esta fórmula se basa en tres parámetros principales: el nivel de confianza, el margen de error y la variabilidad esperada en los datos.

Nivel de confianza:

- Dado que la muestra es relativamente pequeña, se utiliza un nivel de confianza del 95%, que proporciona un equilibrio razonable entre confianza en los resultados y la precisión.
- Utilizaremos un nivel de confianza del 95% para este cálculo.

Margen de error:

- Para un tamaño de muestra de 30 personas, un margen de error típico podría ser del 10%.

La revisión se centró en evaluar la idoneidad de Moodle como una herramienta eficaz para la capacitación de usuarios en el ámbito de la autenticación en la nube. Se realizaron varias evaluaciones para validar su eficacia y resolver los problemas identificados:

Facilidad de Uso y Accesibilidad: Se evaluó la interfaz que sea intuitiva permite a los usuarios navegar por Moodle sin problemas y encontrar rápidamente lo que están buscando. Esto reduce la curva de aprendizaje y hace que la plataforma sea más amigable para usuarios de todos los niveles de habilidad.

Fig 22. *Vista general de los cursos.*

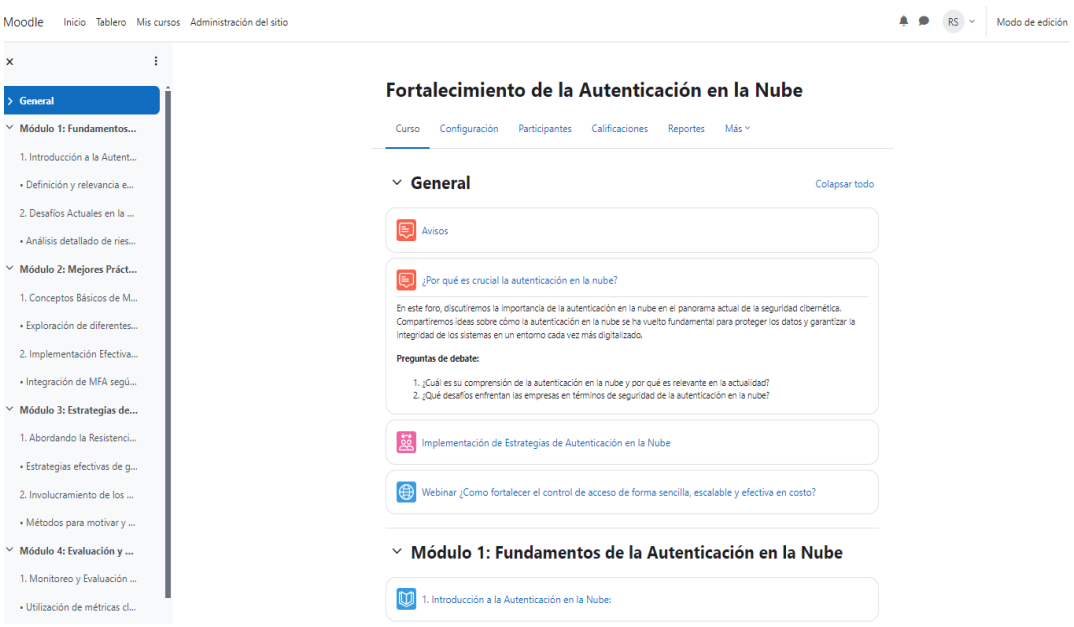


Fig 23. *Segmentación de los módulos de cada curso.*

Funcionalidades de Aprendizaje Interactivo: Se revisaron las características de Moodle relacionadas con el aprendizaje interactivo, como foros de discusión, talleres y actividades prácticas (videos, encuestas, etc.). Estas herramientas se utilizaron para fomentar la participación de los usuarios y facilitar la comprensión de los conceptos de autenticación en la nube.

- **Foros de discusión:** Los foros permiten a los estudiantes discutir temas relacionados con el aprendizaje, compartir sus perspectivas y experiencias, y hacer preguntas. Al participar en discusiones grupales, los estudiantes pueden aprender unos de otros, resolver problemas juntos y construir conocimiento de manera colectiva.

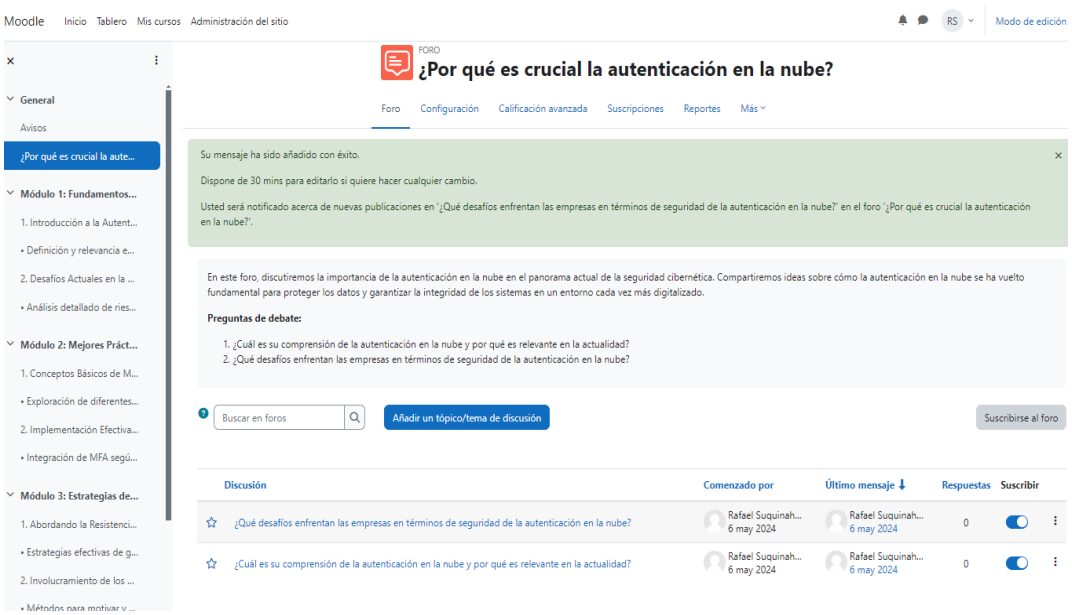


Fig 24. *Creación de foros de acuerdo con los cursos.*

- **Talleres:** Los talleres proporcionan oportunidades para que los estudiantes apliquen activamente lo que han aprendido en situaciones prácticas y realistas. Incluir una fase de revisión y retroalimentación, donde los estudiantes pueden recibir comentarios detallados sobre su trabajo y mejorar sus habilidades.

Fig 25. *Creación de talleres de acuerdo con los cursos.*

- **Actividades prácticas (videos, encuestas, etc.)** Las actividades prácticas, como videos explicativos, demostraciones en línea o encuestas interactivas, pueden

ayudar a los estudiantes a comprender mejor los conceptos difíciles al visualizarlos o experimentarlos de manera práctica.

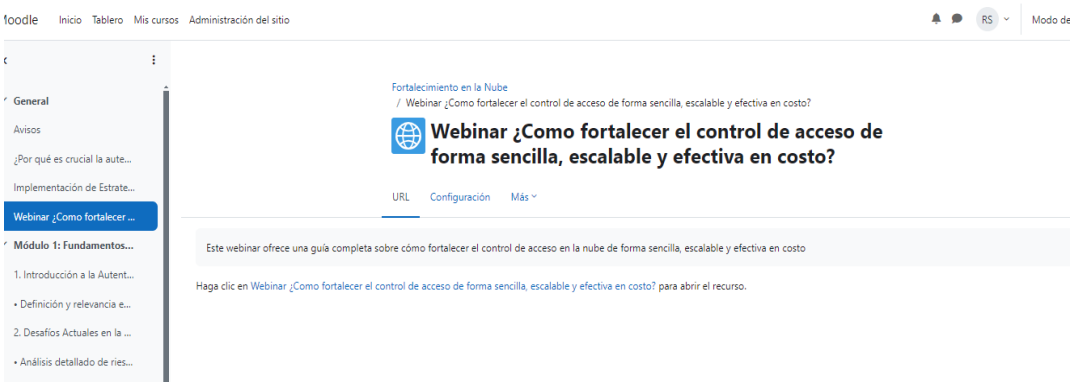


Fig 26. *Creación de talleres de acuerdo con los cursos.*

Seguridad y Protección de Datos: Se analizaron los protocolos de seguridad de Moodle para garantizar la protección de los datos sensibles de los usuarios durante el proceso de capacitación. Se implementaron medidas de seguridad adicionales como:

- **Configuraciones de usuario:** establecer requisitos de contraseña para los usuarios, como la longitud mínima, caracteres especiales requeridos, y la expiración de contraseñas periódicas para garantizar una mayor seguridad de las cuentas de usuario.

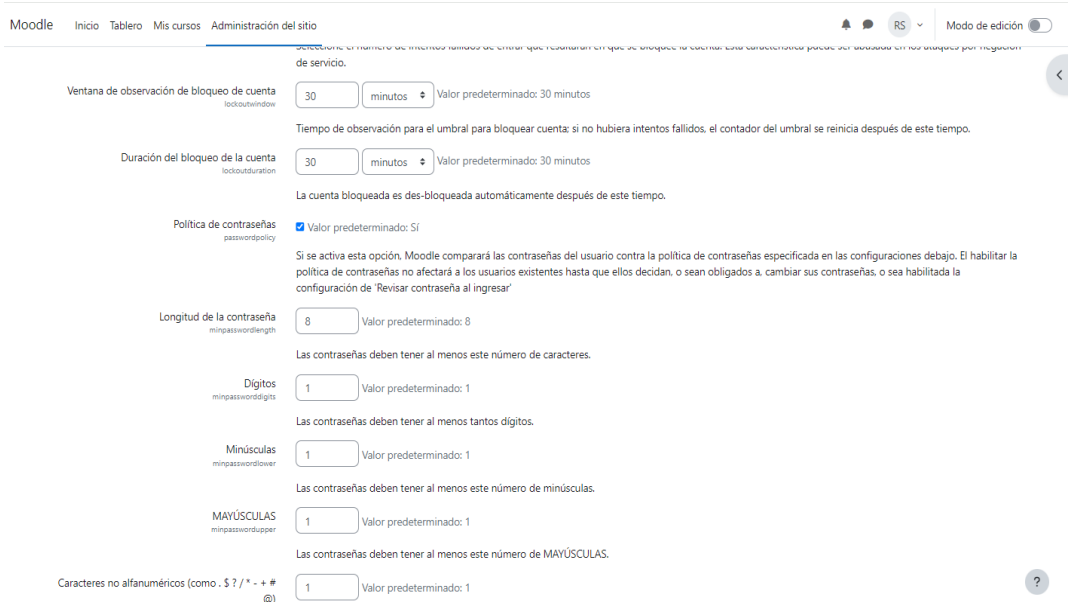


Fig 27. Administración de contraseñas.

- **Gestión de roles y permisos:** permite asignar roles específicos a los usuarios, lo que determina qué acciones pueden realizar en el sistema. Revisa y ajusta los permisos de cada rol para garantizar que los usuarios solo tengan acceso a la información que necesitan.

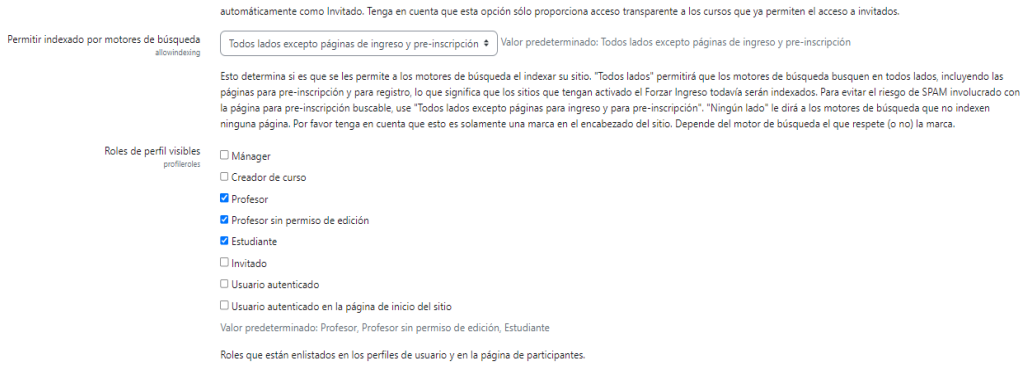


Fig 28. Administración de roles de perfil.

- **Cookies:** Las cookies pueden almacenar preferencias de los usuarios, como el idioma preferido o la configuración de visualización, lo que permite personalizar la experiencia de cada usuario en Moodle según sus necesidades y preferencias.

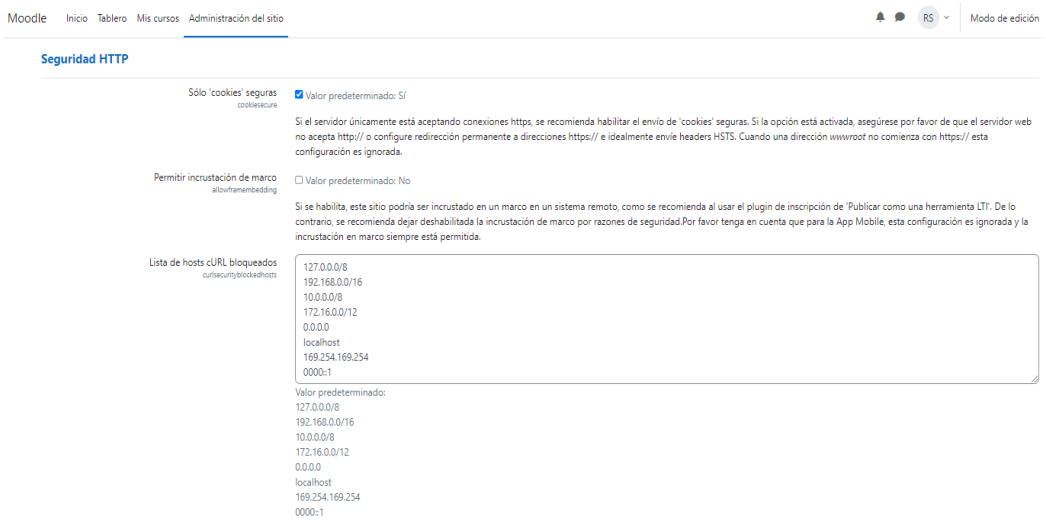


Fig 29. Administración de cookies seguras.

Flexibilidad y Personalización: Se exploraron las capacidades de personalización de Moodle para adaptar el contenido del curso a las necesidades específicas de los usuarios y organizaciones. Se crearon módulos de aprendizaje personalizados que abordaban los desafíos particulares relacionados con la autenticación en la nube y se adaptaban a diferentes niveles de habilidad y experiencia.

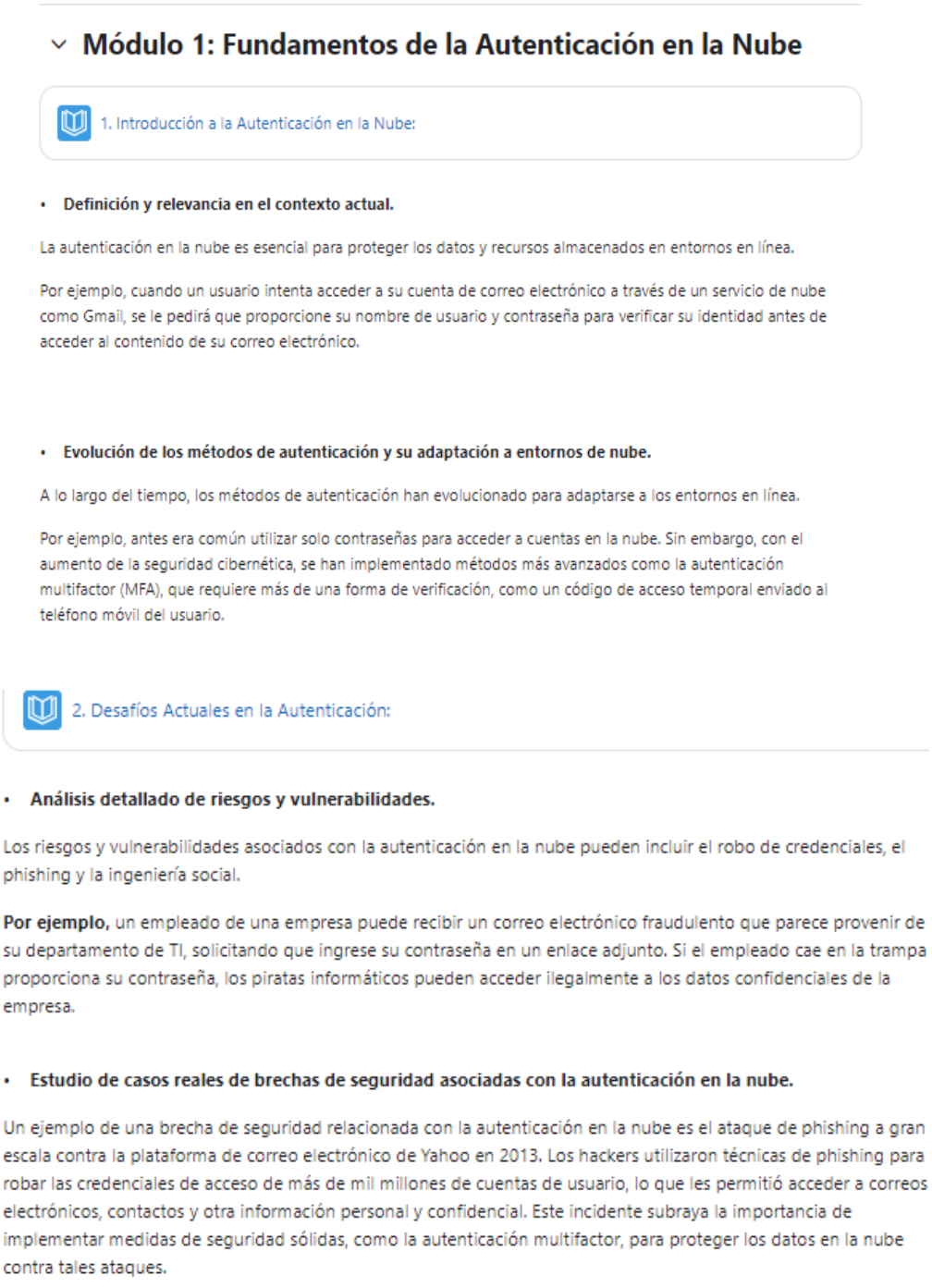


Fig30. Elaboración de conceptos y ejemplos del módulo 1.

Módulo 2: Mejores Prácticas en Autenticación Multifactor (MFA)

1. Conceptos Básicos de MFA:

- **Exploración de diferentes factores de autenticación.**

La autenticación multifactor (MFA) utiliza múltiples factores para verificar la identidad de un usuario. Estos factores pueden incluir algo que el usuario sabe (contraseña), algo que el usuario tiene (teléfono móvil) y algo que el usuario es (escaneo de huellas dactilares).

Por ejemplo, al acceder a una cuenta bancaria en línea, el usuario puede necesitar proporcionar una contraseña (algo que sabe) y luego recibir un código de verificación en su teléfono móvil (algo que tiene) para completar el proceso de inicio de sesión.

- **Casos de uso y ejemplos prácticos de implementación.**

La autenticación multifactor se utiliza en una variedad de contextos, desde aplicaciones financieras hasta plataformas de redes sociales.

Por ejemplo, muchas empresas implementan MFA para proteger las cuentas de correo electrónico corporativo, donde los empleados deben proporcionar una contraseña y luego confirmar su identidad a través de un mensaje de texto enviado a su teléfono móvil.

2. Implementación Efectiva de MFA con ISO 27001:2022:

- **Integración de MFA según las directrices de la norma ISO 27001:2022.**

La norma ISO 27001 proporciona directrices para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Al integrar MFA según las directrices de ISO 27001, las organizaciones pueden fortalecer aún más su postura de seguridad cibernética y garantizar que sus sistemas y datos estén protegidos contra amenazas potenciales.

Por ejemplo, una empresa puede seguir los controles y procedimientos recomendados por ISO 27001 para implementar una solución MFA que cumpla con los estándares de seguridad reconocidos internacionalmente.

- **Herramientas y plataformas compatibles con los estándares de seguridad.**
  - La elección de la herramienta o plataforma adecuada para la implementación de la autenticación multifactor (MFA) es crucial para garantizar la seguridad y la compatibilidad con los estándares de seguridad, como ISO 27001:2022. Algunas de las herramientas y plataformas populares que cumplen con estos estándares incluyen:
    - **Google Authenticator:** Una aplicación de autenticación que genera códigos de seguridad de dos pasos en su dispositivo móvil.
    - **Microsoft Azure Multi-Factor Authentication:** Una solución MFA basada en la nube que proporciona una capa adicional de seguridad para el inicio de sesión.
    - **Duo Security:** Una plataforma MFA que ofrece opciones de autenticación múltiple, incluidos mensajes push, códigos de un solo uso y tokens de hardware.
    - **RSA SecurID:** Un sistema de autenticación MFA que utiliza tokens físicos o virtuales para verificar la identidad del usuario.

Fig31. Elaboración de conceptos y ejemplos del módulo 2.

Módulo 3: Estrategias de Gestión del Cambio

1. Abordando la Resistencia al Cambio en la Implementación de MFA:

- **Estrategias efectivas de gestión del cambio aplicadas a la seguridad.**

Las estrategias efectivas de gestión del cambio son enfoques estructurados que ayudan a las organizaciones a gestionar las transiciones de manera exitosa, incluyendo la implementación de medidas de seguridad, como la autenticación multifactor.

Ejemplo: Antes de implementar la autenticación multifactor, la empresa lleva a cabo sesiones de información y talleres para los empleados donde se explica por qué se está realizando el cambio, los riesgos de seguridad asociados con las contraseñas tradicionales y cómo la autenticación multifactor puede mitigar estos riesgos. Se establece un equipo de soporte dedicado para ayudar a los empleados con cualquier pregunta o problema que puedan tener durante la transición.

- **Comunicación y concientización sobre la importancia de la autenticación multifactor.**

La comunicación efectiva y la concientización son fundamentales para asegurar que los empleados comprendan la importancia de la autenticación multifactor y estén motivados para adoptarla.

Ejemplo: La empresa envía correos electrónicos informativos, organiza sesiones de capacitación y crea materiales educativos (como carteles y folletos) para comunicar a los empleados sobre la importancia de la autenticación multifactor y cómo pueden configurarla en sus dispositivos.

2. Involucramiento de los Usuarios en Prácticas Seguras:

- **Métodos para motivar y educar a los usuarios.**

Motivar y educar a los usuarios es fundamental para garantizar que comprendan la importancia de la seguridad y estén comprometidos con prácticas seguras. Esto implica:

- Utilizar enfoques de aprendizaje activo y participativo para hacer que la educación en seguridad sea más efectiva y relevante.

Ejemplo: La empresa implementa un programa de incentivos donde los empleados que completen con éxito la capacitación en seguridad y demuestren un buen comportamiento en materia de seguridad son elegibles para recibir bonificaciones o reconocimientos.

- **Creación de una cultura organizacional centrada en la seguridad.**

La creación de una cultura organizacional centrada en la seguridad implica establecer valores, normas y comportamientos que prioricen la seguridad de la información en todos los niveles de la organización.

Ejemplo: La alta dirección de la empresa lidera con el ejemplo al adherirse y promover activamente las políticas de seguridad de la empresa. Se establecen canales de comunicación abiertos y accesibles para que los empleados puedan informar sobre incidentes de seguridad o plantear inquietudes sin temor a represalias.

Fig32. Elaboración de conceptos y ejemplos del módulo 3.

Módulo 4: Evaluación y Mejora Continua

1. Monitoreo y Evaluación de la Autenticación:

- **Utilización de métricas clave para evaluar la efectividad.**

La utilización de métricas clave implica seleccionar indicadores cuantificables que permitan medir la efectividad del sistema de autenticación en la nube. Estas métricas pueden incluir:

- Tasa de éxito de inicio de sesión: Proporción de intentos de inicio de sesión exitosos en relación con el total de intentos.
- Tiempo medio de respuesta del sistema de autenticación: El tiempo promedio que tarda el sistema en autenticar a un usuario.

Ejemplo: Una empresa utiliza la métrica de tasa de éxito de inicio de sesión para evaluar la efectividad de su sistema de autenticación en la nube. Durante un período de prueba de un mes, registra 9000 intentos de inicio de sesión, de los cuales 8500 tienen éxito.

- **Identificación temprana de posibles problemas y ajustes necesarios.**

La identificación temprana de problemas implica el uso de herramientas de monitoreo y alerta para detectar anomalías o patrones inusuales en el sistema de autenticación en la nube. Esto permite a los administradores de seguridad tomar medidas correctivas de manera oportuna y realizar ajustes necesarios para mejorar la seguridad.

Ejemplo: Una empresa utiliza un sistema de monitoreo continuo que alerta automáticamente a los administradores de seguridad cuando detecta un aumento inusual en el número de intentos de inicio de sesión fallidos en un corto período de tiempo. Al recibir la alerta, los administradores investigan el incidente y descubren un intento de ataque de fuerza bruta.

2. Mejoras Continuas y Adaptación según ISO 27001:2022:

- **Actualización de políticas y procedimientos en línea con ISO 27001:2022.**

La ISO 27001 es una norma internacional para la gestión de la seguridad de la información que proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).

Ejemplo: Una empresa revisa y actualiza regularmente sus políticas de seguridad de la información para garantizar que cumplan con los requisitos de la ISO 27001. Esto incluye políticas relacionadas con el acceso a datos confidenciales, la gestión de contraseñas, la clasificación de la información y los controles de acceso físico y lógico.

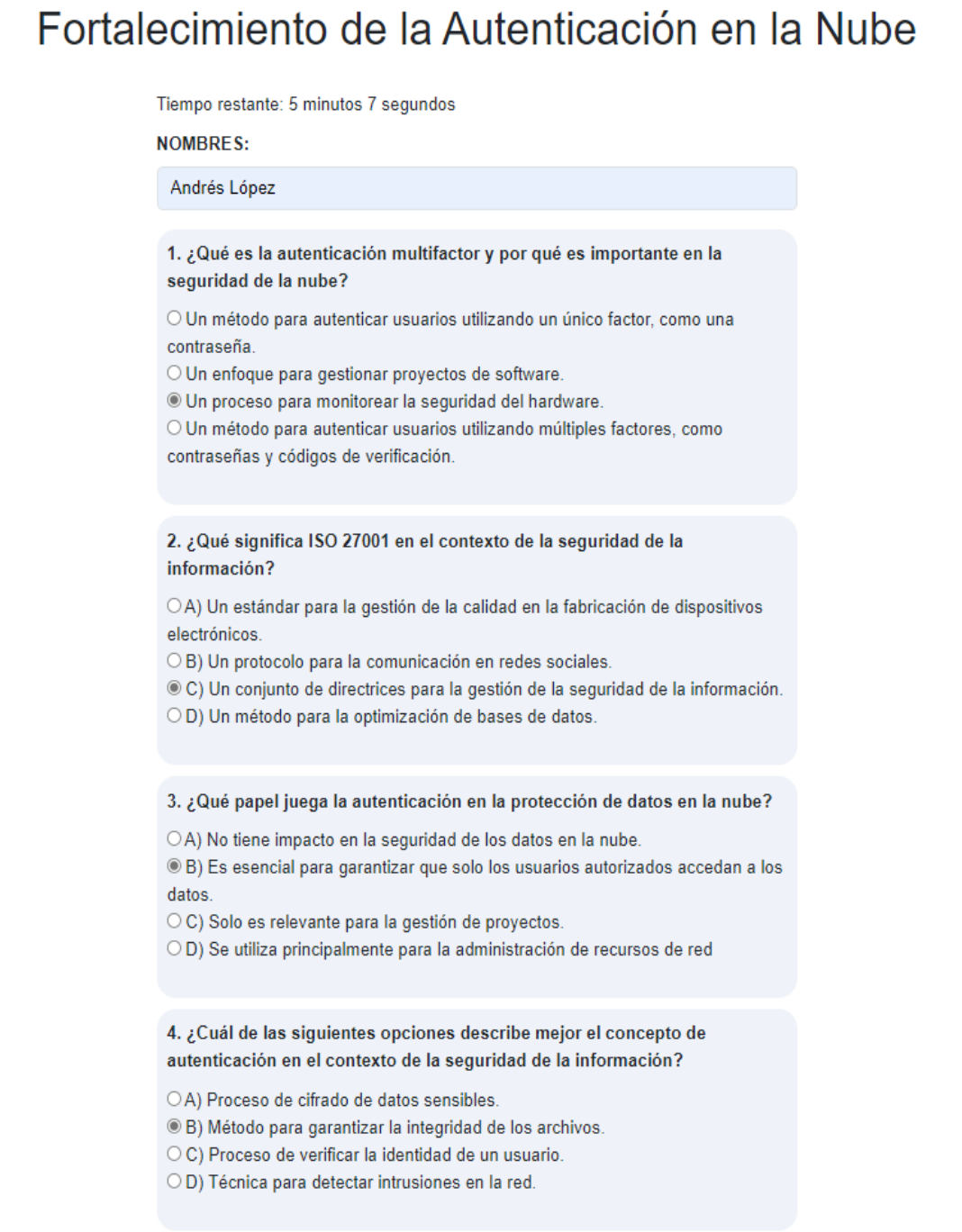
- **Incorporación de nuevas tecnologías y enfoques para mantener la seguridad.**

El campo de la seguridad de la información está en constante evolución, con nuevas tecnologías y enfoques emergentes para hacer frente a las amenazas en constante cambio. La incorporación de nuevas tecnologías y enfoques implica adoptar herramientas, prácticas y metodologías innovadoras que mejoren la seguridad y protejan los activos de información de la organización.

- **Ejemplo:** Una empresa decide implementar un sistema de autenticación biométrica para mejorar la seguridad de sus sistemas en la nube. Esta tecnología utiliza características físicas únicas, como huellas dactilares o reconocimiento facial, para verificar la identidad de los usuarios. Al adoptar esta nueva tecnología, la empresa fortalece la autenticación de sus usuarios y reduce el riesgo de accesos no autorizados.

Fig33. Elaboración de conceptos y ejemplos del módulo 4.

Evaluaciones: A continuación, se presenta muestras de dos personas que realizaron evaluaciones, después de realizar las capacitaciones como se puede ver se obtuvo los resultados esperados, que es de gran ayuda para entender el tema de la investigación.



Fortalecimiento de la Autenticación en la Nube

Tiempo restante: 5 minutos 7 segundos

NOMBRES:

Andrés López

1. ¿Qué es la autenticación multifactor y por qué es importante en la seguridad de la nube?

- ○ Un método para autenticar usuarios utilizando un único factor, como una contraseña.
- ○ Un enfoque para gestionar proyectos de software.
- ◉ Un proceso para monitorear la seguridad del hardware.
- ○ Un método para autenticar usuarios utilizando múltiples factores, como contraseñas y códigos de verificación.

2. ¿Qué significa ISO 27001 en el contexto de la seguridad de la información?

- ○ A) Un estándar para la gestión de la calidad en la fabricación de dispositivos electrónicos.
- ○ B) Un protocolo para la comunicación en redes sociales.
- ◉ C) Un conjunto de directrices para la gestión de la seguridad de la información.
- ○ D) Un método para la optimización de bases de datos.

3. ¿Qué papel juega la autenticación en la protección de datos en la nube?

- ○ A) No tiene impacto en la seguridad de los datos en la nube.
- ◉ B) Es esencial para garantizar que solo los usuarios autorizados accedan a los datos.
- ○ C) Solo es relevante para la gestión de proyectos.
- ○ D) Se utiliza principalmente para la administración de recursos de red

4. ¿Cuál de las siguientes opciones describe mejor el concepto de autenticación en el contexto de la seguridad de la información?

- ○ A) Proceso de cifrado de datos sensibles.
- ◉ B) Método para garantizar la integridad de los archivos.
- ○ C) Proceso de verificar la identidad de un usuario.
- ○ D) Técnica para detectar intrusiones en la red.

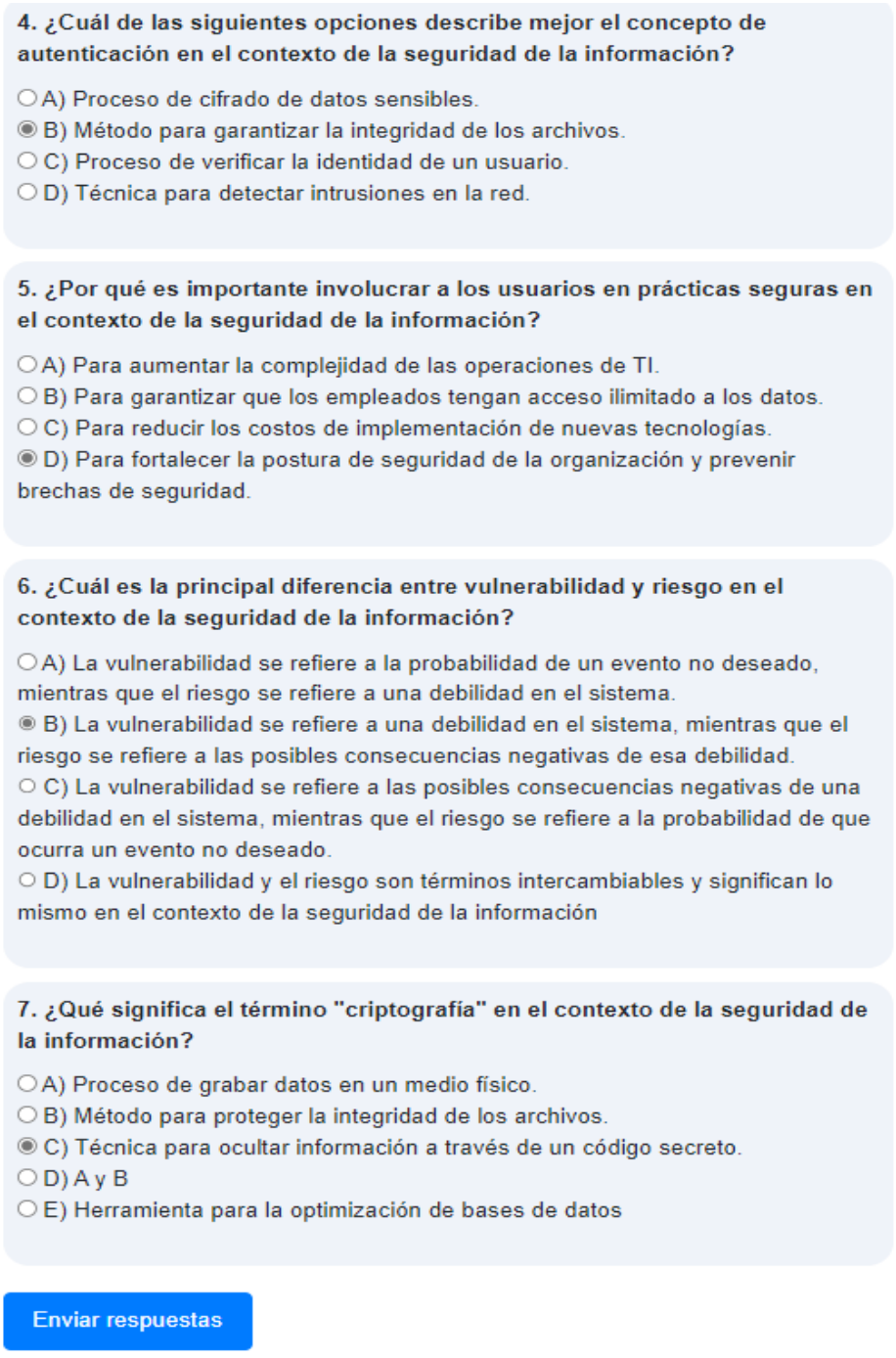


Fig34. Evaluación de lo aprendido en las capacitaciones.

La mejora del acceso a servicios de nube se ven en los resultados de los capacitados que lograron obtener un resultado positivo en la evaluación que se les planteo. Gracias a ello se brindará una solución de manera óptima a la problemática tratada en el documento.

RESULTADOS

NOMBRES: Andrés López
PREGUNTA1: **D**
PREGUNTA2: **C**
PREGUNTA3: **B**
PREGUNTA4: **B**
PREGUNTA5: **D**
PREGUNTA6: **B**
PREGUNTA7: **C**

Fig35. Respuestas Correctas de la evaluación.

6. RECOMENDACIONES

- Se optará por fuentes bibliográficas provenientes de la universidad, asegurándose de que sean reconocidas y de importancia académica. La elección de fuentes confiables respaldará la calidad y validez.
- La búsqueda de información se ceñirá a un intervalo máximo de 5 años (2019-2024). Este enfoque temporal garantiza la actualidad y relevancia de los datos recopilados, alineándose con las tendencias y desarrollos más recientes.
- Para las encuestas, se emplearán preguntas abiertas con el objetivo de facilitar la tabulación y obtener resultados detallados y cualitativos.
- Al diseñar los módulos del curso, se abordarán de manera exhaustiva todos los puntos relacionados con las buenas prácticas en el acceso a servicios de nube. Cada módulo se estructurará de manera lógica y se basará en información actualizada y aplicaciones prácticas para garantizar una comprensión integral del tema.

7.CONCLUSIONES

- El cifrado, ya sea utilizando métodos simétricos o asimétricos, es indiscutiblemente esencial como un componente fundamental en las buenas prácticas de seguridad para el acceso a servicios. Es crucial tener en cuenta que la confidencialidad, disponibilidad e integridad deben ser siempre consideradas como la máxima prioridad en este contexto.

  A lo largo de los años, se ha observado un esfuerzo constante en la búsqueda de métodos para preservar estos principios fundamentales mediante la implementación de controles y la exploración de alternativas de seguridad. Este enfoque se ha llevado a cabo a través de experimentación y estudios continuos, reflejando una dedicación continua a la mejora y adaptación de las medidas de seguridad en el acceso a servicios.
- La gestión del acceso en los servicios de nube son un componente esencial en la evolución de esta tecnología en constante crecimiento. Más allá de la formulación de políticas y buenas prácticas, se ha avanzado hacia la implementación de Acuerdos de Nivel de Servicio (SLA), los cuales son fundamentales para garantizar una respuesta robusta en términos de seguridad ante posibles interrupciones en esta infraestructura dinámica y sin una ubicación estática específica. En resumen, la seguridad en el acceso a servicios de nube se ha elevado a un nivel en el que la implementación de SLA se convierte en una pieza clave para la continuidad y confiabilidad del servicio.
- La adopción de la autenticación de doble factor se ha vuelto una práctica habitual para reforzar la seguridad en el acceso a servicios en la nube. Las organizaciones, cada vez más, imponen políticas que requieren este nivel adicional de verificación, mientras que las contraseñas estándar, utilizadas en entornos personales, están siendo relegadas. Es importante señalar que el uso de tokens para

autenticación adicional puede ser más complejo, ya que implica un proceso que lleva más tiempo. Esto refleja cómo, con el tiempo, el acceso a los servicios en la nube ha evolucionado y se ha actualizado para convertirse en una parte integral y segura de la infraestructura tecnológica.

- La creación de cursos en plataformas fortalece la comprensión y aplicación de buenas prácticas, así como el uso adecuado del acceso a servicios en la nube. El objetivo principal es promover la adopción de procesos seguros y asegurar la integridad de la información contenida en estos servicios. Estos cursos proporcionan una base sólida para que los usuarios adquieran conocimientos y habilidades esenciales, contribuyendo así a un entorno más seguro y confiable en el uso de servicios en la nube.

REFERENCIAS

[1]«CEDIA: Eficiencia y seguridad en la nube» 20 de julio del 2023. [En línea]. Disponible: https://itahora.com/2023/07/20/cedia-eficiencia-y-seguridad-en-la-nube/

[2]«ACCESS CONTROL WEAKNESSES» 09 de marzo del 2023. [En línea]. Disponible: https://cqr.company/web-vulnerabilities/access-control-weaknesses/

[3]« Ingeniería social, claves y precauciones desde la seguridad informática» 14 de mayo del 2023. [En línea]. Disponible: https://www.unir.net/ingenieria/revista/ingenieria-social/

[4]« CLOUD SECURITY, These Are the Top Five Cloud Security Risks, Qualys Says

» 03 de agosto del 2023. [En línea]. Disponible: https://www.securityweek.com/these-are-the-top-five-cloud-security-risks-qualys-says/

[5]«¿Cuáles son los pilares de la seguridad de la información?» 24 de agosto del 2021. [En línea]. Disponible: https://www.docusign.mx/blog/seguridad-de-la-informacion

[6]« A Comprehensive Guide to Cloud Security in 2023 (Risks, Best Practices, Certifications) » 11 de agosto del 2023. [En línea]. Disponible: https://kinsta.com/blog/cloud-security/

[7]«Ingeniería social y cómo protegerse» 29 de octubre del 2020. [En línea]. Disponible: https://www.avast.com/es-es/c-social-engineering

[8]«¿Cuáles son las principales amenazas a la ciberseguridad en 2023? Informe exclusivo» 21 de septiembre del 2023. [En línea]. Disponible: https://www.cryptopolitan.com/es/%C2%BFcuales-son-las-principales-amenazas-a-la-ciberseguridad-en-2023-/

[9]«¿Qué es la norma ISO 27001 y para qué sirve?» 20 de julio del 2023. [En línea]. Disponible: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

[10]«Acerca de MOODLE » 26 de diciembre del 2022. [En línea]. Disponible: https://docs.moodle.org/all/es/Acerca_de_Moodle

[11]«Principales modelos de servicio cloud: IaaS, PaaS y SaaS» 01 de febrero del 2023. [En línea]. Disponible: https://www.stackscale.com/es/blog/modelos-de-servicio-cloud/

[12]«General Access Control Guidance for Cloud Systems» julio del 2020. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf?ref=julien.io

[13]«Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review

» 12 de marzo del 2020. [En línea]. Disponible: https://ieeexplore.ieee.org/abstract/document/9031179

[14]«Research on cloud computing service based on trust access control» 26 de enero del 2020. [En línea]. Disponible: https://journals.sagepub.com/doi/full/10.1177/1847979019897444

[15]«Dual Access Control for Cloud-Based Data Storage and Sharing» 23 de julio del 2020. [En línea]. Disponible: https://ieeexplore.ieee.org/abstract/document/9146722

[16]«Access Control Model for Google Cloud IoT» 23 de junio del 2020. [En línea]. Disponible: https://ieeexplore.ieee.org/abstract/document/9123054

[17]«Security and privacy preservation using constructive hierarchical data-sharing approach in cloud environment» 17 de octubre del 2022. [En línea]. Disponible: https://www.tandfonline.com/doi/abs/10.1080/19393555.2022.2128942

[18]«5 consejos para implementar seguridad en la nube » 19 de noviembre del 2018. [En línea]. Disponible: https://www.ilimit.com/blog/consejos-implementar-seguridad-nube/

[19]«Best Practices for Cloud Security in 2023 » 17 de mayo del 2023. [En línea]. Disponible: https://blog.rsisecurity.com/best-practices-for-cloud-security-in-2023/#more-13688

[20]«Dual Access Control for Cloud Based Data Storage and Sharing» 25 de febrero del 2023. [En línea]. Disponible: https://blog.rsisecurity.com/best-practices-for-cloud-security-in-2023/#more-13688

[21]«A5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN». [En línea]. Disponible: https://normaiso27001.es/a5-politicas-de-seguridad-de-la-informacion/

[22]«A9 CONTROL DE ACCESO». [En línea]. Disponible: https://normaiso27001.es/a9-control-de-acceso/

[23]«A9 CONTROL DE ACCESO». [En línea]. Disponible: https://normaiso27001.es/a9-control-de-acceso/

[24]«A9 CONTROL DE ACCESO». [En línea]. Disponible: https://normaiso27001.es/a9-control-de-acceso/

[25]«A9 CONTROL DE ACCESO». [En línea]. Disponible: https://normaiso27001.es/a9-control-de-acceso/

[26]¿Cuáles son los 11 nuevos controles de seguridad en ISO 27001:2022?» [En línea]. Disponible: https://www.solucionesdetecnologia.com/controles-de-seguridad/#:~:text=sobre%20las%20amenazas.-,A.,su%20informaci%C3%B3n%20en%20la%20nube.

[27]Prácticas operativas recomendadas para el NIST Privacy Framework v1.0» [En línea]. Disponible: https://docs.aws.amazon.com/es_es/config/latest/developerguide/operational-best-practices-for-nist_privacy_framework.html

[28]CIS Controls Spanish Translation» [En línea]. Disponible: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

[29]Fortinet» [En línea]. Disponible: Líder global en soluciones y servicios de ciberseguridad | Fortinet

[30] An access control model for cloud computing [En línea]. Disponible: https://www.sciencedirect.com/science/article/abs/pii/S2214212614000222?via%3Dihub

[31] Challenges of Cloud Access Control [En línea]. Disponible: Challenges Of Cloud Access Control | SEN.news - No. 1

[32] The McCumber Cube and Cybersecurity [En línea]. Disponible: The McCumber Cube and Cybersecurity - Rberny

[33] Una visión holística de la seguridad garantizar la protección de sistemas, datos y aplicaciones [En línea]. Disponible: https://www.digitalbizmagazine.com/wp-content/uploads/2022/07/especial-seguridad-microsoft.pdf