Implementar MultiFactor de Autenticación con Microsoft 365 como estrategia de mejora en la ciberseguridad.

Dr. José Antonio Navarrete Prieto, MPEDT Hilda, Díaz Rincón, M. A. Iliana G. Laguna López de Nava, Allende Ortiz Nancy Anayelli, MTI José Antonio Gallardo Godínez

[a] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, posgrado_ittla@yahoo.com.mx, Tlalnepantla de Baz, Estado de México, México

[b] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, c_computo_sie@hotmail.com, Tlalnepantla de Baz, Estado de México, México

[c] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, ilianaxim@hotmail.com, Tlalnepantla de Baz, Estado de México, México.

[d] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, msistemasdiaz@gmail.com, Tlalnepantla de Baz, Estado de México, México.

[e] Tecnológico Nacional de México /Instituto Tecnológico de Tlalnepantla, jose.gg@tlalnepantla.tecnm.mx, Tlalnepantla de Baz, Estado de México, México.

Resumen

La importancia actual de la ciberseguridad ante los inminentes ataques que día a día surgen dentro del uso de las nuevas tecnologías hace necesario que se adopten política, mecanismos y técnicas, que permitan fortalecer el proceso de autenticación de identidades a los usuarios que utilicen los sistemas o dispositivos pertenecientes a una organización en la realización de sus actividades. Por ello uno de los objetivos primordiales en estos procesos es la autenticación que permita identificar qué personas u objetos pertenecen al dominio organizacional, para que en base a ello se les asignen permisos que requieren para el uso de los sistemas de información, correos electrónicos, sitios de colaboración y cualquier aplicación que se utilice por parte de los activos de la organización.

Como una necesidad de mejorar la seguridad, la empresa decide implementar el multifactor de autenticación (MFA) considerando que se tiene la licencia de Microsoft 365 y que está incluye como una herramienta de seguridad en combinación Azure a fin de prevenir los incidentes de seguridad que se tienen dentro de la organización como son: el manejo de contraseñas, comprobación de identidad de los usuarios y minimizar el robo de información. Se realizo la implementación a nivel corporativo y nacional logrando implementar el MFA y generando una primera etapa de concientización al usuario a través de la elaboración de infografías, capacitación, presentaciones virtuales haciendo énfasis en los beneficios de la MFA.

Palabras clave—aplicación móvil, conectividad, mejora, servicios.

Abstract

The current importance of cybersecurity in the face of the imminent attacks that arise every day in the use of new technologies makes it necessary to adopt policies, mechanisms and techniques to strengthen the process of authentication of identities of users who use systems or devices belonging to an organization in carrying out their activities. Therefore, one of the main objectives in these processes is the authentication that allows to identify which persons or objects belong to the organizational domain, so that based on this they can be assigned permissions required for the use of information systems, e-mails, collaboration sites and any application used by the organization's assets.

As a need to improve security, the company decided to implement the multifactor authentication (MFA) considering that it has the Microsoft 365 license and that it is included as a security tool in Azure combination in order to prevent security incidents that occur within the organization such as: password management, identity verification of users and minimize information theft. The implementation was carried out at corporate and national level, achieving the implementation of MFA and generating a first stage of awareness to the user through the development of infographics, training, virtual presentations emphasizing the benefits of MFA.

Keywords- mobile application, connectivity, enhancement, services

1. INTRODUCCIÓN

[1] Afirma que hoy más que nunca, en la era de la inmensidad del internet, valoramos la sensibilidad de la información. La data generada por las empresas, en este sentido, se ha convertido en un activo que debe ser protegido por las compañías tecnológicas que brindan soporte a diferentes industrias. La confidencialidad de los datos de los clientes (especialmente en rubros tan cruciales para el movimiento del mundo, como la logística) es imperativa, y los desarrollos tecnológicos que se hagan en esta línea deben velar exhaustivamente por la seguridad digital, puesto que cualquier interrupción en la operatividad comercial puede causar un problema mucho más grande a nivel cadena. En donde sin duda la transformación digital ha beneficiado y potenciado ampliamente a la industria logística a nivel global, permitiéndole responder a tiempo y en buena forma a las demandas operativas generadas en cada contexto, particularmente durante los últimos dos años con la pandemia. Sin embargo, este mismo auge ha posicionado a la industria logística como un blanco atractivo para los delincuentes cibernéticos, quienes, no solo “secuestran” y roban la información, sino que también la comercializan, extorsionan e incluso hasta arman planes para sacar provecho de la información sensible.

También [1] indica que según el reporte más reciente de la Comisión Económica para América Latina y el Caribe (CEPAL) titulado Estado de la ciberseguridad en la logística de América Latina y el Caribe, durante los últimos 5 años se han registrado 30 incidentes de ciberseguridad (de conocimiento público) donde se vieron involucradas organizaciones relacionadas con la cadena logística, en donde Gartner estima que para el año 2025 cerca del 45 % de las organizaciones a nivel mundial habrán experimentado algún

ataque en el software en sus cadenas de suministro. La firma consultora afirma que en la medida en que se use una malla de ciberseguridad, es decir, una infraestructura escalable y flexible para mantener la seguridad de IT, se reduciría el impacto financiero de los incidentes individuales de seguridad hasta en un 90%.[1]

Dentro de los problemas tecnológicos que enfrentan las organizaciones es la diversidad de mecanismos de autenticación para el acceso a los servicios que son utilizados por el usuario. Esto complica el proceso de mantenimiento, creación y eliminación de las identidades para los administradores de tecnología de información (TI). Por lo que las organizaciones deben buscar herramientas que les permitan estandarizar y mejorar la administración de identidades, considerando que la autenticación es el acto de probar la identidad a una aplicación o recurso de red. Normalmente, la identidad se demuestra mediante una operación criptográfica que utiliza una clave que solo el usuario conoce como con la criptografía de clave pública o una clave compartida. La parte del servidor del intercambio de autenticación compara los datos firmados con una clave criptográfica conocida para validar el intento de autenticación. [2]

La identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema. La autenticación es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser. Por ejemplo, considere el caso de un usuario que se conecta a un sistema especificando un ID de usuario y una contraseña. El sistema utiliza el ID de usuario para identificar al usuario y autentifica al usuario en el momento de la conexión comprobando que la contraseña proporcionada es correcta [3]

[4] Indica que los equipos que ejecutan una versión compatible de Windows pueden controlar el uso de recursos del sistema y de red a través de los mecanismos interrelacionados de autenticación y autorización. Una vez autenticado un usuario, el sistema operativo Windows usa tecnologías integradas de autorización y control de acceso para implementar la segunda fase de protección de recursos: determinar si un usuario autenticado tiene los permisos correctos para acceder a un recurso. Continuando con [5] indica que los recursos compartidos están disponibles para usuarios y grupos distintos del propietario del recurso y deben protegerse frente a usos no autorizados. En el modelo de control de acceso, los usuarios y grupos (también conocidos como entidades de seguridad) se representan mediante identificadores de seguridad únicos (SID). Se les asignan derechos y permisos que informan al sistema operativo de lo que cada usuario y grupo puede hacer. Cada recurso tiene un propietario que concede permisos a las entidades de seguridad. Durante la comprobación del control de acceso, estos permisos se examinan para determinar qué entidades de seguridad pueden acceder al recurso y cómo pueden acceder a él. [4]

Es importante considerar lo que los autores indican en los párrafos anteriores ya que se toma como base para el desarrollo de la implementación considerando lo que menciona el pedagogo, filósofo, sociólogo y ensayista argentino Ezequiel Ander-Egg Hernández quien indica que la investigación aplicada es una solución eficiente y con fundamentos a un problema que se ha identificado.[5]

2. CONTENIDO

Los programas empresariales de concientización de seguridad de la información son actualmente un elemento fundamental para garantizar la estabilidad en las operaciones de una empresa, por lo que es realmente preocupante que muchas empresas sigan sin brindarles estas herramientas a sus empleados; además, aunque una empresa cuente con cursos de concientización en ciberseguridad, no siempre se encuentran actualizados ni son impartidos de la manera apropiada. Por lo que, a pesar de los esfuerzos y recursos invertidos durante los años más recientes, los errores del factor humano siguen siendo una de las principales causas de incidentes de seguridad en las empresas. Es por esto que han sido diseñados cursos de concientización en ciberseguridad que contemplan a los usuarios finales dentro de una empresa como una vulnerabilidad, pensando en las aptitudes necesarias para mitigar los riesgos de seguridad generados por los empleados. [6]

Los hackers están desarrollando mecanismos de ataques más sofisticados para atacar a las organizaciones, los cuales resultan en grandes pérdidas monetarias y en efectos negativos a la reputación de la entidad. El robo de credenciales es cada vez más frecuente, aumentando los riesgos de robo de información. Estas vulnerabilidades no se deben de convertir en un obstáculo para el desarrollo de las actividades de las empresas, y para el trabajo diario de sus empleados, los cuales necesitan tener acceso a diferentes herramientas y cuentas para desarrollar sus actividades, como a sus cuentas de correo corporativas o a servicios en nube. Es aquí cuando las personas de TI y Seguridad Informática de las empresas se preguntan ¿Cómo permitir los accesos seguros a estos servicios evitando riesgos de intercepción de correos electrónicos o cuentas corporativas? La respuesta está en implementar una solución de Autenticación de usuarios por medio de Identidades Digitales (comprobadas mediante un Certificado Digital). Así los empleados pueden usar estos certificados para verificar su identidad y desarrollar tareas como firma y cifrado de correos electrónicos, de igual manera les permite tener accesos a sus cuentas corporativas entregando un nivel de seguridad más fuerte.[7]

Así [8] indica: “La autenticación multi-factor es un método que requiere más de una forma de verificación y agrega una segunda capa de seguridad al acceso de los usuarios. Funciona requiriendo dos o más métodos de verificación: algo conocido por el usuario, algo que posea el usuario y características físicas específicas que tenga el usuario”. Con el uso de esta en el proceso de autenticación de usuarios en

las organizaciones, se rompe el paradigma de utilizar solamente la contraseña como único factor de autenticación. MFA busca que la persona que utiliza el servicio sea quien dice ser, prácticamente se acerca a la metodología confianza cero, su nombre en inglés Zero Trust.

En [9] establece: La autenticación adaptativa es, a la vez, una forma de configurar e implementar la MFA y un método para determinar los factores de autenticación correctos, basados en el perfil de riesgo de un usuario en particular. En otras palabras, la autenticación adaptativa determina qué factores de autenticación se presentan al usuario durante el proceso de inicio de sesión. El proceso de autenticación debe ser algo simple, pero fuerte. Este tipo de metodologías permite fortalecerlo, de tal forma si un hacker obtiene una contraseña de cualquier usuario va a necesitar estrictamente el mecanismo de segundo factor el cual utiliza la persona vulnerada para poder acceder a los servicios asociados con el perfil.
A pesar de las divisiones de mecanismos de autenticación que existen, todos ellos siguen una serie de pasos en general como son:

1. El usuario pide acceso a un recurso
2. El sistema le solicita el usuario su medio de autenticación
3. El usuario entrega sus credenciales de autenticación
4. El sistema verifica las credenciales del usuario
5. El sistema niega o proporciona al usuario el acceso al recurso.

Con base en todo lo anterior, se determinaron las siguientes actividades estratégicas que son las siguientes:

- Detección de problemática
- Reunión con el proveedor de Microsoft
- Ejecución de pruebas del MFA y liberación de usuario en la nube en el área de TI
- Desarrollo de difusiones
- Desarrollo del Plan de trabajo
- Capacitación para el personal de la empresa
- Activación de MFA
- Elaboración de Manual de usuario
- Evaluación de resultados

La Detección de problemática, se realizó con la aplicación de un cuestionario considerando una muestra representativa de 100 usuarios. El cuestionario contenía preguntas como son:

¿Realizas Home Office actualmente?
¿Cuentas con algún mecanismo de seguridad para uso de tu equipo?
¿Consideras que la contraseña de tu cuenta es segura?
¿Utilizas OneDrive para seguridad de tu información?
¿Sabes que es un ciberataque?
¿Conoces como generar una contraseña más segura?
¿Conoces algún método de autenticación?

Como resultado de la aplicación del cuestionario se observo que la mayoría del personal (85%) no tenia mecanismos de seguridad en sus equipos, un (90%) utilizaban la misma contraseña sin realizar actualizaciones y no realizaba combinación de caracteres, además que un (77%) utilizaba el almacenamiento de OneDrive para guardar su información, con respecto a los ciberataques un (90%) conoce solo los ataque que se dan por el uso de redes sociales y algunos que conocen por noticias.

La Reunión con el proveedor de Microsoft, fue esencial y con ello se estableció el contacto directo con los jefes de infraestructura para presentar y generar la propuesta del proyecto, en esta además se explicaron los beneficios de la aplicación del MFA indicando el proveedor que se tendría el apoyo durante todo el proceso de implementación y activación del MFA. Como parte de la plática que se tuvo con el proveedor este mostro mediante una serie de pruebas como se realizaría y cuál sería el resultado de aplicar el MFA en los activos que pertenecen a la organización. Como parte de la ejecución de pruebas del MFA la cual incluye la liberación de usuario en la nube en el área de TI se concluyó que toda vez que es que aprobado el proyecto se iniciaría apoyándose del personal interno de la organización siendo el equipo de soporte técnico, personal de infraestructura y desarrollo de software quienes comprobarían y verificarían el funcionamiento de los cambios realizados de la identificación del acceso.

Para el desarrollo difusiones y para que exista una comunicación visual se elaboran infografías como se muestran en la figura 1, además se genera una presentación específica para el personal que labora en la organización donde se explica ¿qué es? ¿para qué sirve? la autenticación del MFA como temas principales, ver figura 1.

Figura 1. Infografías realizadas con base en la información de Microsoft 365. Fuente: Elaboración propia

Continuando con las actividades estratégica, se desarrolló un Plan del trabajo, donde se consideran el total de usuarios y equipos que se tienen en plantas y corporativo los cuales deben contar con licencia de Microsoft 365, ver tabla 1.

Tabla 1. Equipos totales para implementar con el MFA

IMPLEMENTACION DEL MFA Y DESBLOQUEO DE USUARIOS DE WINDOWS														
PLANTA	TOTAL DE EQUIPO	AREAS	Total de Maquina	Equipos completa	AREAS	Total de Maquina	Equipos completa	AREAS	Total de Maquina	Equipos completa	AREAS	Total de Maquina	Equipos completa	AREAS
AGS	2				Producción	2								
ALT	15	Administración	3		Compras	2		Planta	4					
		Almacen	1		Distribución	2		SeguridadInd	1					
		CCI	2		Enfermeria	1								
CAR	6	Administración	1		Mtto Criogenico	1								
		Distribución	3		Planta	2								
CDJ	6	Administración	1		Compras	1								
		SeguridadInd.	2		Produccion	2								
CEL	22	Administración	4		Distribución	5		Produccion	2		Planta	2		
		Almacen	2		Mtto Criogenico	2		SeguridadInd	3		Compras	1		
											CCI	1		
CDA II	13	Distribución	4		Produccion	6		SeguridadInd	2		Recepcion	1		
CDA	12	Administración	3		Mtto Criogenico	3		Compras	2					
		Almacen	1		SeguridadInd.	1		Produccion	2					
CORP	190	Activos	2		Contraloria	6		Contabilidad	13		Facturacion	2		Plan y Aud
		Caja	1		Comercial y SE	15		CVC	5		Ingenieria	29		Tesoreria
		Compras	14		Impuestos	7		Direccion FIN	6		Presupuestos	5		TI
		RH	24		Mejora Continu	7		Dir General	2		Riesgos	3		
CDS	1	Produccion	1											
GDL	13	Administración	3		Distribución	2		Ventas	3					
		CCI	1		Mtto Criogenico	4								
GEI	48	Administración	4		Produccion	14		Ingenieria	1		Recepcion	1		
		Contabilidad	1		Dir Fin	2		Tesoreria	1		Ventas	5		

Fuente: Elaboración propia con base en los datos de la organización.

Ya establecido el total de activos a implementar, se procede a realizar la capacitación en forma virtual con la finalidad de tener un mayor número de usuarios en la misma, en esta se les explica la importancia del MFA y la facilidad de utilizar este para el inicio de sesión en sus equipos, además de mostrarles los beneficios que involucra el tener el MFA para el resguardo de su información y de las actividades que realizan en los mismos.

Al término de la capacitación, se procede a realizar la activación del MFA para los activos de la organización siguiendo la serie de pasos que requiere para ello, en este apartado se muestran algunos como so los siguientes:

- Seleccionar el siguiente enlace: https://admin.microsoft.com/adminportal/home/logout
- Ya en el enlace seleccione la opción mostrar todos y elija el centro de administración de Azure Active Directory, ver figura 2.

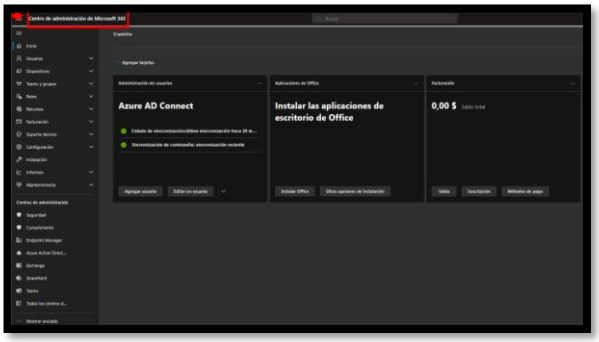

Figura 2. Selección en el Centro de Administración. Fuente: Elaboración propia con base en lo muestra Azure Microsoft

Posteriormente a la selección del centro, se procede a crean los grupos que correspondan para las diversas áreas de la organización, como se puede visualizar en la figura 3.

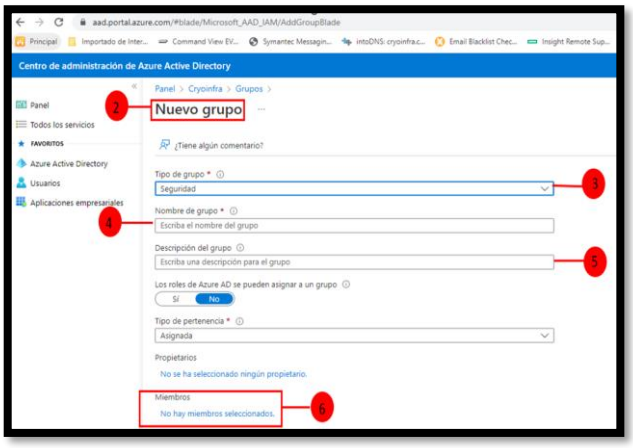

Figura 3. Creación de grupo. Fuente: Elaboración propia con base en lo muestra Azure Microsoft

Continuando con el procedimiento, se establece la seguridad a través de Azure, ingresando al apartado de seguridad y en este se selecciona "Acceso condicional de Azure AD", se crean su directiva de MFA en la opción de Tareas, seleccionando el grupo de usuarios que creó para aplicarle la política, como se visualiza en la figura 4, se le indican las aplicaciones que requieren tener el MFA (se recomienda que sean a todas las aplicaciones en la nube) y posteriormente se seleccionan las condiciones para el control de acceso de los usuarios (recomendado seleccionarlos todos), ver figura 4.

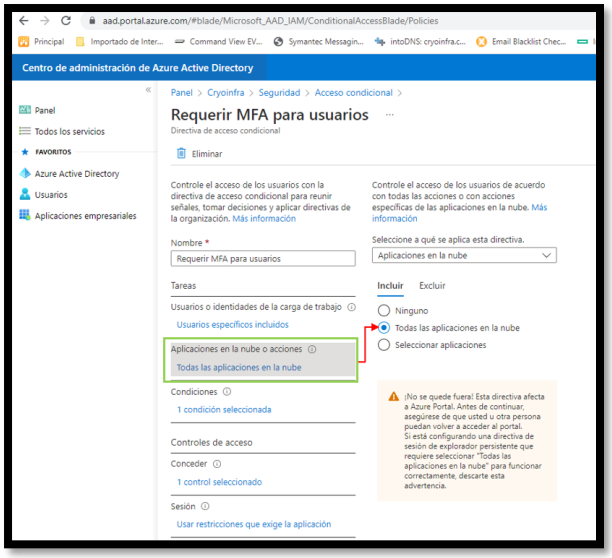

Figura 4. Configuración de MFA para usuarios. Fuente: Elaboración propia con base en lo muestra Azure Microsoft

En esta parte donde se concluye la configuración del MFA al habilitar la directiva y configurar la autentificación multifactorial dentro de las opciones que proporciona Azure, esto se visualiza en la Figura 5.

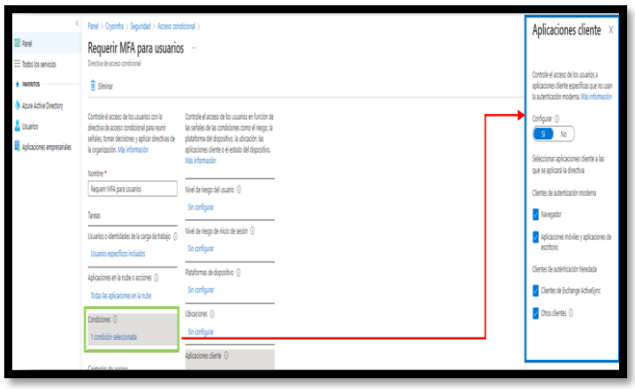

Figura 5. Configuración de MFA con autentificación multifactorial
Fuente: Elaboración propia con base en lo muestra Azure Microsoft

Como parte del trabajo de implementación, se consideró la elaboración de manuales básicos y que servirán de guía en cualquier situación que se pueda presentar durante la implementación del MFA, el contenido de estos es básico y sencillo, como se puede ver en la Figura 6.

Finalmente se llego al resultado esperado, logrando reducir contraseñas vulnerables y un aumento considerable en la seguridad de la cuenta de cada usuario perteneciente a la empresa con un mayor grado de seguridad en su información.

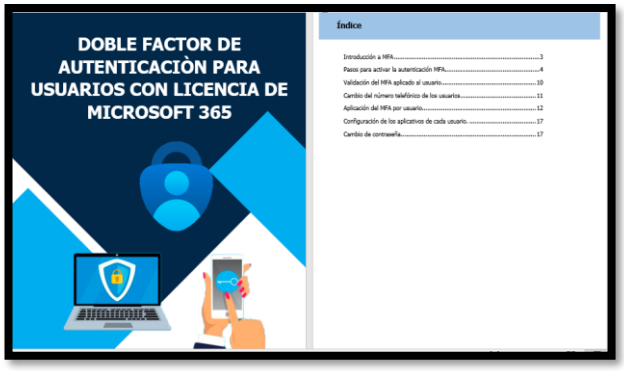

Figura 6. Manual de Usuario. Fuente: Elaboración propia

En la organización se observó una mejora del 89% en lo que se refiere a la autentificación de los usuarios en los aplicativos seleccionados, al implementar el MFA en plantas y áreas indicadas por esta, como se muestra en la Tabla 1.

Tabla 1. Comparación de verificación con MFA

	Sin aplicación del MFA	Con aplicación del MFA
Contraseñas seguras	Se cuenta con contraseña débil ya que usan contraseñas muy fáciles de adivinar.	Contraseña con restricción a colocar nombre, empresa, mes, año, etc.
Cuenta protegida	Cualquiera podía ingresar a cuenta	Se requiere de código de verificación que llega al celular y que únicamente tiene el usuario de dicha cuenta.
Verificación de identidad	No se cuenta con ninguna	Se pide código de verificación al iniciar sesión en aplicativos.
Capacitación del riego informático	Ninguno	El personal esta consciente de los riesgos y amenazas a os que esta expuesto y como debe actuar.

Fuente: Elaboración propia

Finalmente, en la figura 7 permite observar como se realiza la verificación del MFA ya en funcionamiento vinculando aplicaciones con el dispositivo del usuario.

Es importante comentar que se está terminando de implementar esto en la totalidad de las áreas además de que se están incluyendo más aplicativos en la selección para que la seguridad este mejor gestionada y se minimice el riesgo de ataques por el acceso de aplicaciones que no estén integradas en las configuraciones del MFA.

En ella se puede visualizar como se realiza la comprobación de la identificación del usuario a través del envió de un mensaje a su número telefónico.

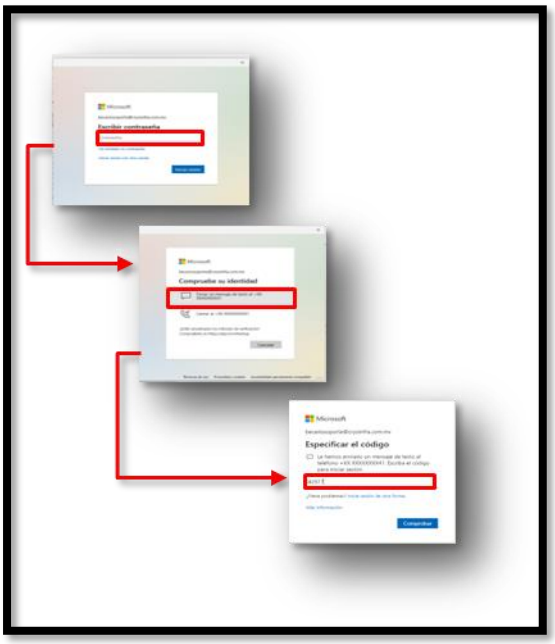

Figura 7. Comprobación de identidad del usuario. Fuente: Elaboración propia con base en lo que muestra Microsoft 365.

3. CONCLUSIONES Y RECOMENDACIONES

Considerando que el objetivo del MFA es poder crear una defensa en capas para dificultar que una persona que no esté autorizada pueda ingresar a un sitio, ya sea una ubicación física, algún dispositivo informático, una red o una base de datos, en la organización se logró con el esfuerzo y apoyo de cada una de las áreas involucradas y en conjunto con la participación de los usuarios quienes consideraron que el cambio para ellos al autentificarse con el dispositivo móvil para el acceso a equipos y aplicaciones les permitía apreciar que existía un medio para verificar si alguien accedía a su aplicación y/o dispositivo.
Aplicar la ciberseguridad con el uso de herramientas sencillas como es Microsoft 365 en combinación con herramientas como es Azure permitió a la organización disminuir el riesgo y mejorar la gestión de los usuarios en lo que respecta a las aplicaciones que se utilizan dentro de la organización.

Y [10] indica que a medida que las organizaciones digitalizan su funcionamiento y adquieren una mayor responsabilidad por almacenar los datos de los clientes y los suyos propios, los riesgos y la necesidad de seguridad también aumentan. Dado que los atacantes han explotado durante mucho tiempo los datos de inicio de sesión de usuario para obtener entrada a cualquier sistema, la comprobación de la identidad del usuario ha adquirido una importancia vital para las empresas. MFA requiere medios de verificación que los usuarios no autorizados no tendrán. Dado que las contraseñas son insuficientes para verificar la identidad, MFA requiere de varias pruebas para verificar la identidad. La variante más común de MFA es la autenticación de dos factores (2FA).

El MFA es una metodología que al implementarla mejora la seguridad al existir la autentificación para los usuarios de la organización, ya que les ayuda a proteger el acceso a los datos y aplicaciones de una forma sencilla y rápida lo que hace que se minimice el riesgo de amenazas, sin embargo, se debe tener configurada la seguridad activa debido a que en cualquier momento puede haber vulnerabilidades existentes en cualquier software que se esté utilizando y este se convierta en una amenaza. Es por ello que la seguridad siempre debe estar de forma activa para no tener que estar de forma considerando la reactiva y que se generen en algunos casos gastos extras para realizarla.

Trabajo a Futuro.

Se recomienda que se implemente más medidas de seguridad informática y ciberseguridad utilizando herramientas ye instrumentos de monitoreo constante ya que como Microsoft indica, las aplicaciones y servicios web son vulnerables ya que son accesibles desde cualquier parte del mundo, además de que no se tiene control sobre el cliente que ni de los recursos que utiliza para acceder a la aplicación, ni del entorno en donde se encuentra, por lo que es importante concientizar y establecer estrategias de control para minimizar el riesgo probable de fallas y amenazas que puedan intervenir en el desarrollo de los procesos de la organización.

4. REFERENCIAS

[1] AMVO - Asociación Mexicana de Venta Online. (2022), “Seguridad digital: el rol de las empresas de tecnología en la protección de los datos dentro de la industria logística”, [En línea] Disponible: https://www.amvo.org.mx/blog/seguridad-digital-el-rol-de-las-empresas-de-tecnologia-en-la-proteccion-de-los-datos-dentro-de-la-industria-logistica/, [Último acceso: 17 de marzo 2023].

[2] Microsoft. (2019). “LA Clippers secure company data and eliminate shadow IT with Microsoft Enterprise Mobility + Security”.[En línea] Disponible: https://customers.microsoft.com/es-es/story/la-clippers-media-entertainmentmicrosoft-36, [Último acceso: 10 agosto 2022].

[3] IBM, (2021), “Identificación y autenticación”, [En línea] Disponible https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm, [Último acceso: 14 junio 2022]

[4]Microsoft, (2023), “Introducción a Access Control”, [En línea] Disponible: https://learn.microsoft.com/es-es/windows/security/identity-protection/access-control/access-control, [Último acceso: 07 mayo 2022]

[5] Lifeder. (17 de septiembre de 2020). Investigación aplicada: características, definición, ejemplos. [En línea [Disponible: https://www.lifeder.com/investigacion-aplicada/. [Último acceso: 18 Octubre 2022]

[6] International Institute of Cyber Security. (2021), “Concientización de ciberseguridad”, [En línea] Disponible: Concientización de ciberseguridad seguridad informática de información (iicybersecurity.com), [Ultimo acceso: 17 marzo 2023].

[7] Toms, L. (2016), "La importancia de la Autenticación en el Internet de Todas las Cosas", [En línea] Disponible: https://www.globalsign.com/es/blog/importance-of-authentication-in-iot

[8] Sevilla, B. (2018, “Análisis de Factibilidad de procedimiento de autenticación única para acceder a los servicios informáticos de la Pontificia Universidad Católica del Ecuador. Sede Esmeralda”. [En línea] Disponible en : https://repositorio.pucese.edu.ec/bitstream/123456789/1467/1/SEVILLA%20DELGADO%20BRYAN%20ALEXANDER%20.pd, [Último acceso: 05 junio 2022]

[9] ChakRay. (2019), ”Mejore su seguridad con la autenticación adaptativa - Taller en Singapur – Chakray” [En línea] Disponible : https://www.chakray.com/es/mejore-su-seguridad-con-la-autenticacion-adaptativataller-en-singapur/, [Último acceso: 03 julio 2022]

[10] Gómez, P. (2020), “Qué es la autenticación multifactor (MFA)” [En línea] Disponible: https://www.icm.es/2020/12/30/que-es-autenticacion-multifactor/, [Último acceso: 28 abril 2022]