NOMBRE DEL TRABAJO

Hilary Fatima Inquil Villegas PTMTSP.pdf

AUTOR

Hilary Fatima Inquil Villegas

RECUENTO DE PALABRAS

9853 Words

RECUENTO DE CARACTERES

59707 Characters

RECUENTO DE PÁGINAS

57 Pages

TAMAÑO DEL ARCHIVO

1.5MB

FECHA DE ENTREGA

Mar 7, 2024 12:32 AM GMT-5

FECHA DEL INFORME

Mar 7, 2024 12:33 AM GMT-5

18% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 17% Base de datos de Internet
- 3% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45º de la ley Nº 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10º del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (x)

DATOS PERSONALES

Apellidos y Nombres: INQUIL VILLEGAS HILARY FATIMA
D.N.I.: 75184404
Otro Documento:
Nacionalidad: PERUANA
Teléfono: 995501977
e-mail: 2016100002@untels.edu.pe

DATOS ACADÉMICOS

Pregrado

Facultad: FACULTAD DE INGENIERÍA Y GESTIÓN
Programa Académico: TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado: INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Postgrado

Universidad de Procedencia:
País:
Grado Académico otorgado:

Datos de trabajo de investigación

Título: "IMPLEMENTACIÓN DE LA AUTENTICACIÓN MULTIFACTOR MEDIANTE EL LENGUAJE MARCADO DE AFIRMACIÓN DE SEGURIDAD SAML PARA EL SSO DE LOS USUARIOS EN UNA ENTIDAD DEL ESTADO"
Fecha de Sustentación: 17 DE DICIEMBRE DEL 2023
Calificación: APROBADO POR UNANIMIDAD
Año de Publicación: 2024

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo _____ No autorizo X

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	( )

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva Nº 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	(x)
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:
info:eu-repo/semantics/restrictedAccess

Motivos de la elección del acceso restringido:
La selección del acceso restringido al trabajo de suficiencia profesional se fundamenta en la presencia de información proveniente de la empresa, que protege en reserva y confidencialidad para garantizar la protección adecuada de dicha información.

INQUIL VILLEGAS HILARY FATIMA

APELLIDOS Y NOMBRES

75184404

DNI

Firma y huella:

Lima, 08 de MARZO del 2024

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“IMPLEMENTACIÓN DE LA AUTENTICACIÓN MULTIFACTOR MEDIANTE EL LENGUAJE MARCADO DE AFIRMACIÓN DE SEGURIDAD SAML PARA EL SSO DE LOS USUARIOS EN UNA ENTIDAD DEL ESTADO”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

INQUIL VILLEGAS, HILARY FATIMA
ORCID: 0009-0006-5814-480X

ASESOR

YAURI RODRIGUEZ, RICARDO
ORCID: 0000-0001-9884-9317

Villa El Salvador
2023

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

"Año de la unidad, la paz y el desarrollo"

VI Programa de Titulación por la Modalidad de Trabajo de SuficienciaProfesional
Decanato de la Facultad de Ingeniería y Gestión

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 17:27 horas del día 17 de diciembre de 2023, se reunieron en las instalaciones de la Universidad Nacional Tecnológica de Lima Sur, los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	:	MG. JOSÉ AMBROSIO MACHUCA MINES	CIP Nº 158894
Secretario	:	MG. DANIEL LÉVANO RODRIGUEZ	CIP Nº 155059
Vocal	:	DR. JULIO ENRIQUE QUISPE TUESTA	CIP Nº 150139

Designados con Resolución de Decanato de la Facultad de Ingeniería y Gestión N° 984-2023-UNTELS-R-D de fecha 13 de diciembre del 2023.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de **Ingeniero Electrónico y Telecomunicaciones**, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional (Resolución de Consejo Universitario Nº 065-2023-UNTELS-CU de fecha 08 de agosto del 2023), en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur" ; siendo que el Art. 4º del precitado Reglamento establece que: **"La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo deSuficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otras modalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar un mínimo de dos (02) años de experiencia laboral, de acuerdo a lo establecido en la Resolución Nº 174-2019- SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)..."**, en el cual;

La Bachiller **HILARY FATIMA INQUIL VILLEGAS**
Sustentó su Trabajo de Suficiencia Profesional: **IMPLEMENTACIÓN DE LA AUTENTICACIÓN MULTIFACTOR MEDIANTE EL LENGUAJE MARCADO DE AFIRMACIÓN DE SEGURIDAD SAML PARA EL SSO DE LOS USUARIOS EN UNA ENTIDAD DEL ESTADO**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición Aprobado por unanimidad Equivalencia Bueno de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las 18:00 horas del día 17 de diciembre de 2023 se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado.

PRESIDENTE
MG. JOSÉ AMBROSIO MACHUCA MINES
CIP N° 158894

SECRETARIO
MG. DANIEL LÉVANO RODRIGUEZ
CIP N° 155059

VOCAL
DR. JULIO ENRIQUE QUISPE TUESTA
CIP N° 150139

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del presidente del jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del jurado, la sustentación será reprogramada durante los 05 días siguientes.

DEDICATORIA

A Dios y a mis padres.

Quienes son fuente constante de inspiración y ejemplo de sacrificio. Su aliento y confianza en mí siempre fue la fuerza impulsadora que me sostuvo.

AGRADECIMIENTO

A mi familia y mi asesor Ricardo Yauri cuya orientación y apoyo fueron fundamentales para el desarrollo y éxito de este proyecto.

INDICE

LISTADO DE FIGURAS

RESUMEN

El presente Trabajo de Titulación aborda la implementación de una solución de autenticación Multifactor RSA SecurID Access a través del lenguaje marcado de afirmación de seguridad SAML para el inicio de sesión único (SSO) de todos los usuarios de una entidad estatal.

Este proyecto se llevó a cabo durante mi empleo en la empresa Securesoft, una compañía especializada en ciberseguridad que ofrece servicios y soluciones de seguridad informática a diversas organizaciones en el país. Mi función en dicha empresa fue la de ingeniero residente para una entidad estatal peruana.

En la actualidad, la entidad estatal enfrenta diversos desafíos relacionados con la seguridad de sus sistemas de inicio de sesión. Se ha comprobado que los métodos de autenticación basados en contraseñas tradicionales son vulnerables a diversas amenazas, como ataques de fuerza bruta, suplantación de identidad y filtraciones de contraseñas. Esta situación representa una amenaza significativa para la seguridad de los datos sensibles y confidenciales gestionados por la entidad.

La implementación de un sistema de inicio de sesión único contribuye a la unificación de aplicaciones a través de un portal central. Este enfoque no solo mejora la experiencia del usuario al proporcionar acceso a múltiples servicios sin necesidad de volver a iniciar sesión, sino que también implica la necesidad de incorporar una segunda autenticación para fortalecer significativamente la seguridad.

INTRODUCCIÓN

En los últimos años, ha sido evidente el crecimiento del trabajo remoto, donde las organizaciones se ven obligadas a garantizar la protección de sus accesos. Por lo tanto, enfrentan la necesidad de reestructurar su infraestructura tecnológica y adoptar medidas de seguridad frente a diversos ataques informáticos que buscan explotar vulnerabilidades o debilidades, a menudo desconocidas para los usuarios respecto al impacto que pueden ocasionar.

La empresa de ciberseguridad Fortinet ha recopilado datos a través de su laboratorio de inteligencia de amenazas, destacando que la región de América Latina y el Caribe experimentó 137 millones de intentos de ciberataques de enero a junio de 2022, representando un aumento del 50% en comparación con 2021. En este contexto, Perú registró 15 mil millones de intentos de ataques (Fortinet, 2022).

Los usuarios acceden a un número relevante de activos corporativos desde fuera de los límites de la red gobernada por la empresa. Esta nueva estructura de trabajo ha planteado considerables retos de seguridad a las empresas unos de los cuales son las “amenazas basadas en la identidad” (Dasu et al., 2023).

Las amenazas basadas en la identidad surgen cuando se cuenta con poca protección de los recursos informáticos al no contar con un sistema robusto de autenticación e identificación, una baja complejidad de contraseñas sin ningún método de autenticación sumado, puede permitir a los ciberdelincuentes realizar ataques de fuerza bruta (varios intentos forzosos de acceso mediante combinaciones de letras y números) o diccionario (mediante una lista de contraseñas simples de uso común) teniendo acceso tanto la información personal o empresarial.

La entidad del Estado Peruano en la cual se desarrolló el trabajo cuenta con aplicaciones e interfaces de administración de plataformas perimetrales para el desempeño de las funciones de colaboradores quienes son empleados de la institución así mismo al tener conocimientos sobre estos riesgos informáticos, optó por adquirir la solución de autenticación RSA SecurID, solución que permite

configurar conexiones entre un Proveedor de servicios como aplicaciones web o SaaS (software como servicio) y el enrutador de identidad (Proveedor de identidad) que son habilitadas mediante SAML (lenguaje de marcado de afirmación de seguridad). Estas conexiones brindan a los usuarios acceso SSO (inicio de sesión único) a esas aplicaciones a través del portal de aplicaciones.

CAPÍTULO I. ASPECTOS GENERALES

1.1. Contexto

Securesoft, una compañía peruana dedicada a la ciberseguridad cuenta con certificaciones en ISO 9001:2015, ISO 27001:2013 y PCI DSS 3.2. Se especializa en proporcionar servicios y soluciones de seguridad informática con el propósito de proteger la integridad de la información empresarial. Su equipo de ingenieros altamente capacitados posee certificaciones en diversos productos y soluciones que la empresa ofrece. La firma ha acumulado valiosa experiencia en la implementación de soluciones de gran escala, asegurando el éxito de sus servicios. Su visión es liderar el ámbito de la ciberseguridad en Latinoamérica para el año 2023, mientras que su misión se centra en respaldar la transformación digital de los clientes mediante la oferta de productos y servicios especializados en ciberseguridad (Securesoft, 2023).

Cada solución puede ser adaptada a los parámetros de las organizaciones. Por lo que, ofrece categorías de soluciones para los diferentes requerimientos tales como: Seguridad de datos (Data Security), seguridad de puntos finales (Endpoint Security), Seguridad en la nube (Cloud Security), Seguridad de las aplicaciones (Application Security), seguridad de las redes (Networking Security) y Ciber inteligencia (Securesoft, 2023).

1.2. Delimitación temporal y espacial del trabajo

1.2.1 Delimitación temporal

El presente trabajo de Suficiencia Profesional se desarrolló en un periodo de 4 meses entre abril y julio del año 2023.

1.2.2 Delimitación espacial

Este trabajo de Suficiencia Profesional se desarrolló en la entidad del estado ubicado en el distrito del Cercado de Lima del departamento de Lima, Perú.

1.2.3 Proceso de despliegue

En este trabajo se dividieron las actividades de despliegue en etapas. Estas

son: la etapa de planificación, implementación y confirmación.

- Etapa de planificación, tiene como propósito realizar la viabilidad de la implementación, además de plasmar el plan de ejecución de las actividades previas, durante y finales mediante el Plan de trabajo.
- Etapa de Implementación en donde se procede con el despliegue de la integración SAML a los usuarios.
- Etapa de Confirmación, en donde la empresa valida la correcta funcionalidad del cambio realizado.

1.3. Objetivos

Los objetivos del presente trabajo son:

1.3.1. Objetivo General

Implementar la autenticación Multifactor mediante el lenguaje marcado de afirmación de seguridad para el inicio de sesión único de los usuarios en una entidad del estado.

1.3.2. Objetivo Específicos

- Establecer y aplicar políticas de acceso específicas que necesiten autenticación multifactor durante el proceso del inicio de sesión único.
- Configurar el protocolo SAML que admita la autenticación multifactor garantizando su compatibilidad con los sistemas existentes en la entidad gubernamental.
- Implementar el portal web seguro basado en la nube para acceder a las aplicaciones mediante el inicio de sesión único.
- Verificar la operatividad de la configuración asegurando la efectividad de la autenticación multifactor y el inicio de sesión único.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

Dentro de los temas referidos a la investigación para la verificación de identidad de los usuarios a través de la implementación de una solución de autenticación, de las cuales se tomaron las siguientes:

2.1.1. Antecedentes Nacionales

Según Ñique (2016), en su trabajo de investigación para obtener el Título Profesional de Ingeniero Informático y de Sistemas, titulada “Implementación de Solución de autenticación segura basada en doble factor en una entidad del estado”. Universidad San Ignacio de Loyola.

- Mediante la incorporación de la solución de RSA Authentication Manager y la aplicación de autenticación de doble factor, se alcanzó una significativa disminución, aproximadamente del 45%, en el riesgo de accesos no autorizados a información valiosa y recursos empresariales. Esta implementación ha posibilitado establecer un proceso de autenticación sólido y seguro. Es fundamental destacar que este enfoque no solo contribuye a salvaguardar los activos empresariales, sino que también se traduce en el cumplimiento efectivo de los requisitos establecidos por la Norma Técnica Peruana ISO/IEC 27001. La combinación de la tecnología RSA Authentication Manager con la autenticación de doble factor ha demostrado ser una estrategia eficaz para fortalecer la seguridad, garantizando la integridad y confidencialidad de la información crítica de la organización (Ñique, 2016).

Según Vásquez (2019), en su trabajo para conseguir el Título Profesional de Ingeniero de Sistemas e Informática, titulada “Implantación de EMS (Enterprise Mobility + Security) contra amenazas avanzadas en infraestructura hibrida”. Universidad Tecnológica del Perú.

- A través de la adopción de la suite de seguridad Enterprise Mobility + Security (EMS), se llevó a cabo la configuración del inicio de sesión único

(SSO) mediante la integración de credenciales de acceso a diversas aplicaciones. Este proceso se ejecutó de manera centralizada mediante una consola de administración de identidad unificada. La implementación de esta solución no solo permitió la simplificación y eficiencia en el acceso a múltiples plataformas, sino que también desempeñó un papel fundamental en la salvaguarda de la identidad del usuario final. Este enfoque estratégico contribuyó significativamente a mitigar los riesgos asociados con la pérdida u olvido de credenciales de acceso, problemáticas que previamente impactaban la productividad de los usuarios. Al consolidar la gestión de identidad a través de EMS y la integración del estándar de autenticación SAML, se logró establecer un entorno de trabajo más seguro y eficaz. Este avance no solo se tradujo en la protección de la información sensible, sino que también optimizó la experiencia del usuario al proporcionar un acceso sencillo y seguro a las aplicaciones esenciales para su labor diaria (Vásquez, 2019).

Según el estudio llevado a cabo por Bernal y Echevarría (2019), titulado "Modelo de Niveles de Seguridad para Pruebas de Intrusión en Aplicaciones Web para PYMES en el Perú".

- El propósito del estudio era evaluar y mejorar la seguridad de las aplicaciones web utilizadas por las PYMES en el Perú. Se buscaba establecer un modelo de niveles de seguridad que permitiera llevar a cabo pruebas de intrusión de manera efectiva, identificando posibles vulnerabilidades y proponiendo soluciones. La metodología se basó en la evaluación exhaustiva de las aplicaciones web utilizadas por las PYMES, utilizando técnicas de pruebas de intrusión. Se diseñó un modelo de niveles de seguridad específico, adaptado a las características y desafíos particulares de las pequeñas y medianas empresas. Los resultados proporcionaron un panorama claro del estado de seguridad de las aplicaciones web en las PYMES, identificando áreas de mejora y posibles amenazas. Esto permitió desarrollar estrategias de fortalecimiento de la seguridad informática en un entorno empresarial vulnerable. El estudio concluyó que la implementación de un Modelo de

Niveles de Seguridad adaptado a las PYMES en el Perú es esencial para mitigar riesgos de seguridad en aplicaciones web. La detección temprana de vulnerabilidades mediante pruebas de intrusión contribuye a fortalecer la ciberseguridad en un contexto empresarial específico (Bernal & Echevarría, 2019).

2.1.2. Antecedentes Internacionales

Según el estudio llevado a cabo por Sepúlveda Marín (2022), titulado "Análisis de la Efectividad de los Modelos de Autenticación 2FA y MFA de acuerdo con los Algoritmos y Protocolos Aplicados en la Seguridad de Cuentas de Servicios y Plataformas Online en Colombia".

- La investigación se propuso evaluar la eficacia de los modelos de autenticación de doble factor (2FA) y autenticación multifactor (MFA) en el contexto de la seguridad de cuentas de servicios y plataformas online en Colombia. El objetivo principal consistió en determinar la efectividad de estos modelos mediante la aplicación de diferentes algoritmos y protocolos. La metodología incluyó un análisis exhaustivo de casos de uso, simulaciones de ataques y la recopilación de datos de incidentes de seguridad. Los resultados revelaron que la autenticación MFA demostró ser más robusta en la prevención de accesos no autorizados en comparación con la autenticación 2FA. Con algoritmos y protocolos adecuados, se logró una reducción significativa en los incidentes de seguridad. En conclusión, la implementación de la autenticación MFA, respaldada por algoritmos y protocolos efectivos, se presenta como una estrategia más sólida y eficaz para salvaguardar la seguridad de las cuentas en entornos online en el contexto colombiano (Sepúlveda, 2022).

Según Gutiérrez (2023), en su trabajo final del máster universitario en ciberseguridad y privacidad titulado “Implantación de un SSO en un entorno empresarial” (España).

- Mediante la implementación del software de autenticación como sistema centralizado de autenticación en la organización se ha mejorado significativamente en los tiempos. En términos de seguridad, ha demostrado ser una solución confiable, ya que implementa protocolos de seguridad SAML, entre otros, lo que crea sólidos mecanismos de autenticación y autorización de usuarios. Además, la autenticación multifactor y la gestión centralizada permiten aumentar la seguridad del acceso al sistema (Gutiérrez, 2023).

Según el estudio realizado por Andrade (2019), titulado "Diseño de un Sistema de Triple Factor de Autenticación basado en Reconocimiento de Similitud de Imágenes".

- El propósito del estudio fue diseñar e implementar un sistema de autenticación avanzado, integrando tres factores: conocimiento (contraseña), posesión (dispositivo) y biometría (reconocimiento de similitud de imágenes). El objetivo era mejorar la seguridad de la autenticación, proporcionando una capa adicional de protección mediante el uso de múltiples factores. La metodología fundamentó su enfoque en el diseño e implementación de un sistema que permitiera la autenticación a través de tres factores. Utilizó el reconocimiento de similitud de imágenes como enfoque biométrico, complementando la autenticación basada en conocimiento y posesión. Con las pruebas exhaustivas realizadas para evaluar la efectividad y la usabilidad del sistema, los resultados del estudio demostraron la viabilidad y eficacia del sistema de triple factor de autenticación. La combinación de conocimiento, posesión y biometría contribuyó significativamente a la robustez del proceso de autenticación, mejorando la seguridad del acceso a sistemas sensibles. La conclusión del estudio resalta la importancia de implementar sistemas de autenticación avanzados que utilicen múltiples factores, especialmente el reconocimiento de similitud de imágenes como una forma segura y conveniente de autenticación biométrica. Este enfoque ofrece una mayor protección contra accesos no

autorizados y fortalece la seguridad en entornos que requieren un alto nivel de protección (Andrade, 2019).

2.2. Bases teóricas

2.2.1 Control de Identidades

Con el propósito de resguardar la seguridad y privacidad de individuos, se emplea al limitar el acceso a información y recursos delicados, permitiendo únicamente a aquellos autorizados acceder. Este enfoque requiere la identificación y diferenciación entre individuos, estableciendo una distinción clara entre aquellos que cuentan con los derechos de acceso y aquellos que no los poseen (González, 2023).

Se basa en negar el acceso a personas no autorizadas y permitir el acceso a personas autorizadas. Saber a quién permitir significa: identificación, autenticación y autorización. Constantemente nos identificamos, reconocemos y autorizamos en diferentes sistemas. Sin embargo, mucha gente confunde el significado de estas palabras consiste en:

- Identificación implica verificar la identidad de una persona.
- Autentificación consiste en confirmar la identidad de un usuario en un sistema informático al comparar la contraseña ingresada con la almacenada en la base de datos.
- Autorización se refiere a la función que establece los privilegios de acceso a los recursos (Drozhzhin, 2020).

2.2.2. Autenticación Multifactor

La autenticación multifactor constituye un enfoque que demanda la utilización de más de un mecanismo de autenticación, proporcionando así un nivel adicional de seguridad para los usuarios. Su operatividad se basa en la solicitud de dos o más formas de autenticación, tales como información conocida por el usuario, posesión de objetos específicos, y características físicas particulares que posea el usuario (Sevilla, 2018).

Requiere que el usuario tenga una combinación de al menos dos de los siguientes tres tipos de credenciales:

- algo que sabe (contraseña, PIN).
- algo que tienes (token de hardware, contraseña de un solo uso).
- algo que eres (datos biométricos como la huella dactilar) (Kennedy & Millard, 2016).

2.2.3. Métodos de autenticación Multifactor

Es posible utilizar varios métodos en conjunto con una contraseña para llevar a cabo la autenticación multifactor. Entre estos métodos se encuentran:

- Biometría: Se fundamenta en que un dispositivo reconozca datos biométricos, como la huella dactilar o los rasgos faciales de un individuo.
- Pulsar para aprobar (PUSH): Implica enviar una notificación al dispositivo del usuario, solicitándole que apruebe una solicitud de acceso mediante la acción de tocar la pantalla de su dispositivo.
- Contraseña de un solo uso (OTP): Consiste en un conjunto de caracteres generado automáticamente que autentica a un usuario únicamente para una sesión o transacción específica.
- Texto SMS: Utiliza mensajes de texto para enviar una contraseña de un solo uso al teléfono inteligente u otro dispositivo del usuario.
- Token de hardware o token físico: Se refiere a un dispositivo portátil que genera contraseñas de un solo uso, a veces conocido como llavero.
- Token de software: Es un token que se presenta como una aplicación de software en un dispositivo, como un teléfono inteligente, en lugar de utilizar un token físico.

Estos métodos adicionales fortalecen la seguridad al requerir múltiples formas de autenticación, reduciendo los riesgos asociados con el uso exclusivo de contraseñas (RSA Blog, 2021).

2.2.4. Inicio de sesión único SSO

El inicio de sesión único es un procedimiento de autenticación que habilita a los usuarios para acceder a diversos sistemas de software distintos mediante el uso de múltiples credenciales. Mediante esta funcionalidad, los usuarios evitan la necesidad de iniciar sesión por separado en cada aplicación que emplean. Con el

inicio de sesión único, los usuarios tienen la capacidad de utilizar todas las aplicaciones necesarias sin requerir autenticación adicional.

La selección de un método de inicio de sesión único está determinada por la configuración específica de autenticación de la aplicación. Las aplicaciones alojadas en la nube tienen la capacidad de emplear alternativas basadas en federación, como OpenID Connect, OAuth y SAML. Asimismo, el sistema puede optar por el inicio de sesión único mediante contraseña, el inicio de sesión único basado en emparejamiento, o la opción de desactivar la función de inicio de sesión único (Microsoft Learn, 2023a).

2.2.5. SAML

SAML (Security Assertion Markup Language) representa un protocolo estandarizado de código abierto diseñado para facilitar la federación de identidades y la implementación de Single Sign-On (SSO). Su estructura se basa en la transmisión de documentos XML para el intercambio seguro de datos relacionados con la autenticación y la autorización. Dentro del marco de SAML, un usuario inicia sesión inicialmente con un proveedor de identidad, lo que le permite posteriormente acceder a diversos servidores de recursos mediante esa única sesión iniciada (Campbell et al., 2015). Este protocolo define tres roles fundamentales: Usuario (Principal), Proveedor de Identidades (IdP) y Proveedor de Servicios (SP).

2.2.6. Metadatos SAML

El archivo de metadatos SAML alberga datos acerca de las diversas autorizaciones SAML aplicables en los intercambios de mensajes del protocolo SAML 2.0. Estos metadatos identifican los puntos finales del proveedor de identidades y los certificados para proteger los intercambios de mensajes de SAML 2.0.

El archivo debe ajustarse al esquema de metadatos de SAML 2.0 (xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"). El archivo debe tener un elemento de nivel superior <md:EntitiesDescriptor> con un elemento hijo <EntityDescriptor> para cada proveedor de identidades (IBM, 2022).

2.2.7. Flujo de trabajo de autenticación

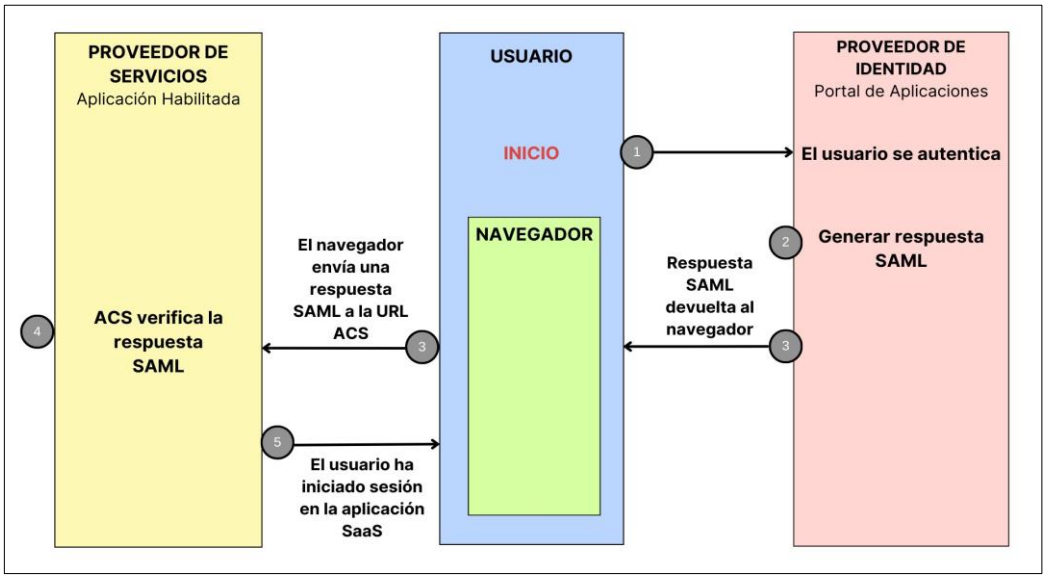
Cuando un usuario intenta acceder al Proveedor de Servicios a través de un enlace directo o un portal de aplicaciones, el enrutador de identidad autentica al usuario si es necesario y envía una respuesta SAML a la aplicación. La respuesta contiene una aserción SAML que contiene credenciales codificadas en XML para el usuario autenticado.

a) Perfil de SSO iniciado por IdP (Proveedor de Identidad):

El flujo de trabajo de autenticación entre un SP habilitado para SAML y el IdP se denomina perfil SSO cuando es iniciado por el proveedor de identidad tal como se muestra en la figura 1.

Figura 1.

Flujo de trabajo para un perfil SSO iniciado por IdP en SecurID.



Nota. Elaboración propia con base en la muestra de RSA.

Las etapas del flujo de trabajo para la autenticación son:

- Iniciar sesión en el portal de la aplicación, mediante el ingreso de contraseña, e intenta acceder a la aplicación protegida habilitada para SAML.
- El enrutador de identidad genera una respuesta que contiene la aserción SAML.
- El enrutador de identidad redirige el navegador del usuario a la

URL del Servicio de consumidor de aserción (ACS) de la aplicación junto con la respuesta SAML.

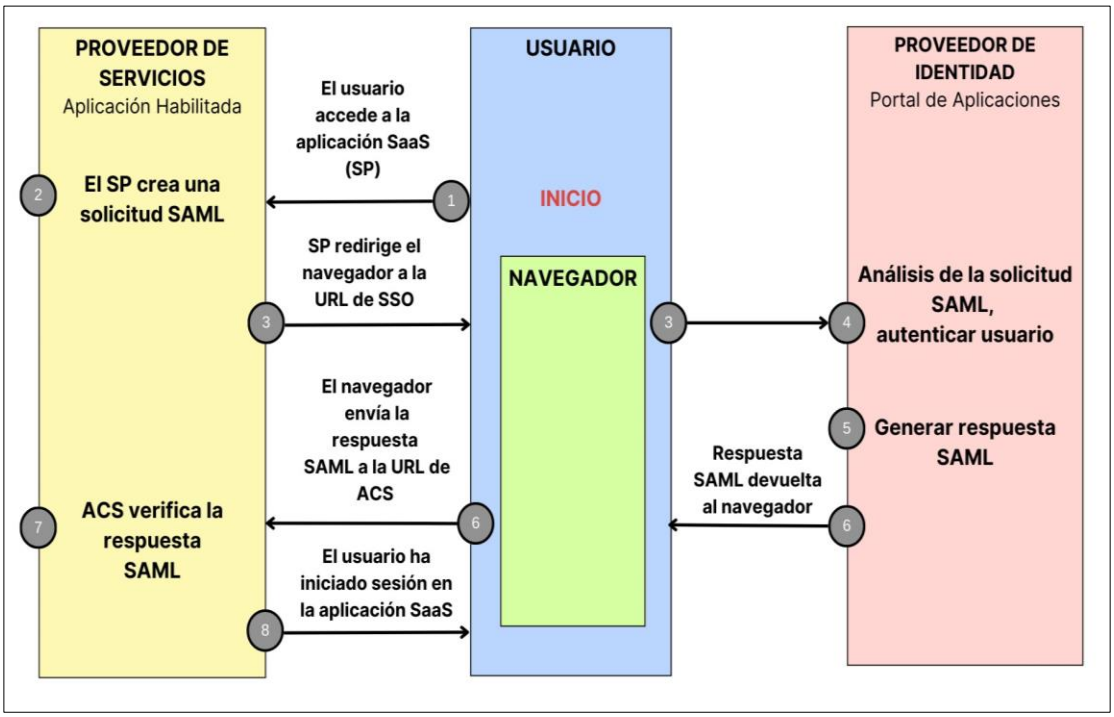
- El ACS valida la afirmación en la respuesta SAML.
- El usuario puede acceder a la aplicación.

b) Perfil SSO iniciado por SP:

El flujo de trabajo de autenticación entre un SP habilitado para SAML denominado perfil SSO iniciado por el SP se muestra en la figura 2.

Figura 2.

Flujo de trabajo para un perfil SSO iniciado por SP en SecurID.



Nota. Elaboración propia con base en la muestra de RSA.

El procedimiento del flujo de trabajo para la autenticación es:

- Un usuario que puede o no haber iniciado sesión en el portal de la aplicación abre un navegador intenta acceder a la aplicación protegida habilitada para SAML.
- La aplicación genera una solicitud SAML.
- Envía la solicitud SAML a través del navegador, al enrutador de identidad.

- El enrutador de identidad recibe la solicitud SAML y, si es necesario, autentica al usuario mediante sus credenciales. El usuario ahora ha iniciado sesión en el enrutador de identidad.
- El enrutador de identidad genera una respuesta que contiene la aserción SAML.
- El enrutador de identidad redirige el navegador del usuario a la URL ACS de la aplicación junto con la respuesta SAML.
- El ACS valida la afirmación en la respuesta SAML.
- El usuario puede acceder a la aplicación.

2.3 Definición de términos básicos.

Las definiciones más importantes que se utilizaron en el trabajo son las siguientes: **MFA:** La autenticación de múltiples factores es un componente de gestión de acceso que implica que los usuarios confirmen su identidad mediante la utilización dos factores de verificación diferentes antes de poder acceder a cualquier recurso (OneSpan, n.d.).

OTP: El código de token o código de acceso es una contraseña válida para un único uso, es decir, una única sesión o transacción, en un sistema u otro dispositivo digital (Guerrero, 2019).

SSO: El inicio de sesión único se da cuando un usuario se autentica en el portal de aplicaciones, y este puede acceder a todas las aplicaciones asignadas (Microsoft Learn, 2023a).

SAML: El Lenguaje de Marcado para Confirmaciones de Seguridad es un estándar de federación abierta que permite a un proveedor de identidad (IdP) autenticar usuarios a otra aplicación conocida como proveedor de servicios (SP) (Cortez, 2023).

IdP: Un proveedor de identidad es un servicio encargado de almacenar y verificar la identidad de un usuario. Generalmente, estos proveedores, alojados en la nube, colaboran con servicio de inicio de sesión único para autenticar usuarios (Cloudfire, n.d.) .

SP: Un proveedor de servicios confía en el IdP y autoriza a un usuario específico a utilizar el recurso solicitado. Un SP requiere la autenticación de IdP autorizar al usuario y, dado que ambos sistemas usan el mismo lenguaje, el usuario solo necesita iniciar sesión una vez (Oracle Perú, n.d.).

ACS: Servicio al consumidor de aserciones es el extremo (URL) del proveedor de servicios que es responsable de recibir y analizar una aserción SAML (Netscaler, 2023).

IDR: Un enrutador de identidad es un software que impone la autenticación y el acceso a los usuarios de recursos protegidos, es una máquina virtual que se tiene que desplegar en la infraestructura del cliente (RSA Community, n.d.-a).

AD: Active Directory almacena información sobre objetos en la red y facilita los usuarios y administradores encontrarlos y acceder a ellos. Active Directory utiliza un almacén de datos organizado como base para una organización jerárquica lógica de la información del directorio (Microsoft Learn, 2023b).

SaaS: El Software como servicio posibilita a los usuarios conectarse a aplicaciones alojadas en la nube mediante de Internet y utilizarlas (Legadmi, n.d.).

CAPÍTULO III: DESARROLLO DEL TRABAJO PROFESIONAL

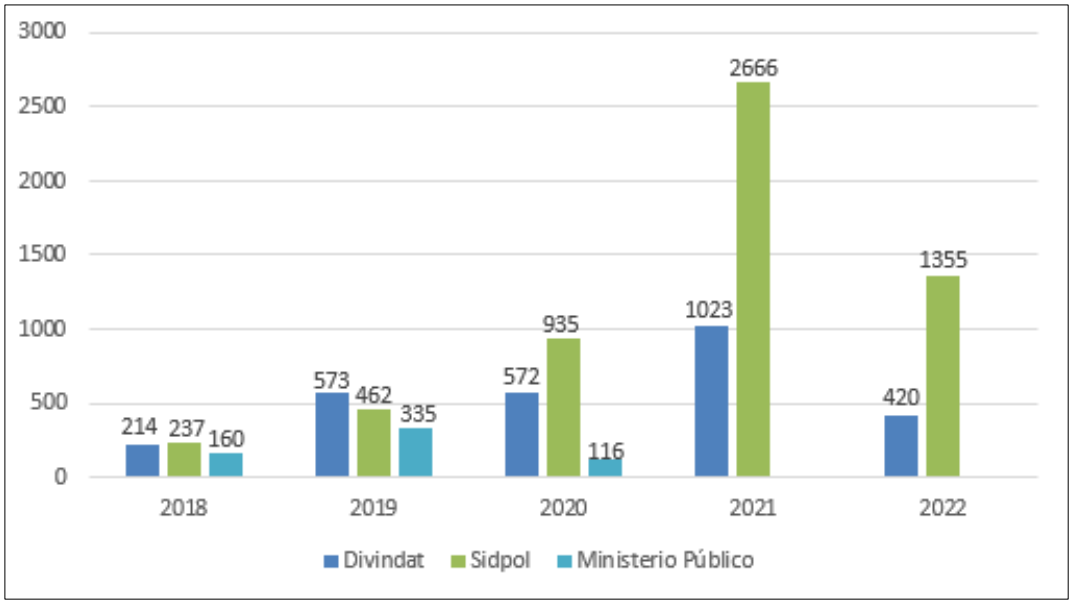
3.1. Determinación y análisis del problema

Perú se encuentra ante múltiples retos relacionados con la protección de sus sistemas de inicio de sesión. Los métodos de autenticación con contraseñas han demostrado ser inseguros frente a diversas amenazas, como los ataques de fuerza bruta, el robo de identidad y las filtraciones de contraseñas. Esta situación presenta un riesgo importante para la seguridad de los datos sensibles y confidenciales que la entidad maneja.

La suplantación de identidad es uno de los ciberdelitos más frecuentes en el Estado Peruano, que va en aumento desde el inicio de la pandemia. El Ministerio Público (MP), la Dirección de Alta Tecnología (Divindat) y el Sistema de Denuncias de la PNP (Sidpol) según sus últimos registros, demuestra que, en el periodo desde el año 2018 a mayo del 2022, la modalidad de este ciberdelito ha incrementado tal como se muestra en la figura 3.

Figura 3.

Denuncias por Suplantación de Identidad (2018 -2022).



Nota. Elaboración propia con base en el número de denuncias del Divindat, Sidpol y Ministerio Público.

Para abordar el impacto de la suplantación de identidad en las entidades públicas, se hace indispensable la adopción de medidas de seguridad sólidas. Algunas de estas acciones clave incluyen la implementación de sistemas de verificación de identidad, la protección eficiente de los datos y la creación de conciencia sobre este grave problema.

El equipo de Respuestas ante Incidentes de Seguridad Digital de la institución del estado consideró garantizar un acceso seguro a su amplia variedad de aplicaciones corporativas, por intermedio del inicio de sesión único agregando una autenticación robusta a través de la segunda autenticación ofreciendo de esta manera comodidad y seguridad a todos los colaboradores.

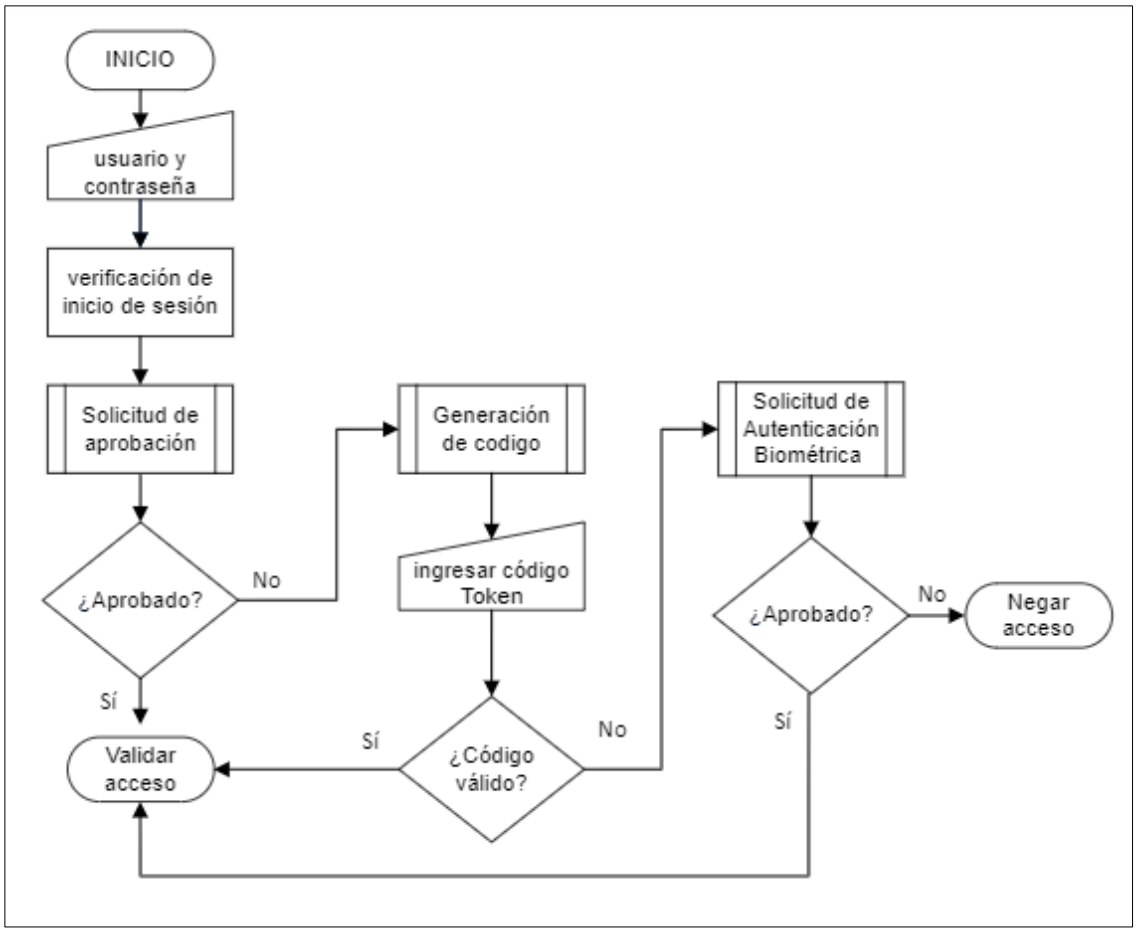
3.2. Modelo de solución propuesto

El modelo de solución propuesto para el presente trabajo combina SAML y MFA para mejorar la seguridad de autenticación y el acceso a los sistemas y servicios gubernamentales, garantizando que solo los usuarios autorizados puedan acceder a los recursos y datos sensibles. Además, simplifica la experiencia de inicio de sesión único de los colaboradores y reduce el riesgo de acceso no autorizado y la suplantación de identidad. La entidad gubernamental ya había adquirido servicios de seguridad informática para administrar las identidades en la cual adquirieron el software de autenticación multifactor SecurID Access que ofrece la integración por SAML para el inicio de sesión único.

Para la integración mediante SAML se necesita de un proveedor de Identidad (SecurID Access) que ya se encuentre implementado, y un proveedor de servicios que pueden ser aplicaciones web o SaaS, por ese motivo, luego de la evaluación de los requisitos, Tableau fue la aplicación que cumplió con la compatibilidad, debido a que ofrece múltiples opciones para la autenticación entre ellas mediante la autenticación SAML. Luego de definir que aplicación se necesita integrar con SSO mediante SAML, que nivel de seguridad y autenticación se necesita con MFA, se desarrolló el diagrama del despliegue de autenticación Multifactor que muestra la secuencia de fases en el proceso de autenticación MFA, que implica desde la solicitud de acceso por parte del usuario hasta la concesión de acceso por parte del proveedor de servicios como se muestra en la figura 4.

Figura 4.

Diagrama de autenticación multifactor desplegado en la entidad.



Nota. Elaboración propia.

Las etapas para la autenticación desplegada en la Entidad pública que se logra apreciar en el diagrama de autenticación son los siguientes:

- Inicio: el proceso comienza cuando el usuario intenta acceder a un sistema o servicio protegido.
- Solicitud de aprobación: El sistema envía una solicitud de acceso, el usuario aprueba la solicitud a través de un dispositivo autorizado mediante una aplicación de autenticación.
- Generación de Código token: Si el usuario no acepta la solicitud de aprobación, el sistema genera un código token a través de la aplicación de autenticación.

- Verificación Biométrica: Si el código token no es válido, el sistema inicia el proceso de verificación biométrica.
- Fin del proceso: Si la verificación es correcta, el usuario tiene acceso al sistema.

Para cumplir con los objetivos específicos planteados al inicio de este trabajo, es necesario desarrollar los siguientes puntos.

- Etapa de planificación en donde se definió las políticas de acceso para la autenticación multifactor, además de asegurar la compatibilidad con los sistemas existentes en la entidad.
- Etapa de implementación en donde se realizó la configuración SAML y la implementación del portal web seguro basado en la nube para acceder a las aplicaciones mediante el inicio de sesión único.
- Validar la funcionalidad del sistema de autenticación Multifactor RSA SecurID mediante la integración por SAML para la verificación de su efectividad.

3.2.1. Etapa de Planificación

La implementación de la autenticación multifactor (MFA) mediante el lenguaje marcado de afirmación de seguridad (SAML) para el inicio de sesión único (SSO) de usuarios en una entidad del estado requiere la configuración adecuada de sistemas y políticas de seguridad y asegurar la compatibilidad con los sistemas existentes a través de las condiciones de integración SAML. Llevar a cabo esta implementación dentro de la etapa de planificación es necesario tener en cuenta lo siguiente:

Figura 5.

Etapa de Planificación.

Nota. Elaboración propia.

a) **Evaluación de Requisitos y políticas:**

Es imprescindible tener en cuenta los requisitos de seguridad y las políticas de la entidad estatal antes de proceder a implementar cualquier solución de autenticación multifactor. Es necesario identificar qué tipos de factores de autenticación son necesarios y determinar cómo deben aplicarse para lograr el inicio de sesión único.

b) **Selección de Factores MFA:**

La elección de los factores de autenticación multifactor (MFA) adecuados para la entidad estatal puede incluir elementos como la contraseña que el usuario conoce, el código token que el usuario posee y la identificación biométrica del usuario, como la huella dactilar o el reconocimiento facial, así como la aprobación de una solicitud de acceso.

c) **Condiciones de la integración SAML:**

La integración SAML se procedió con el programa Tableau, dicho programa ya se encontraba en funcionamiento en la entidad estatal.

El acceso del usuario a la aplicación fluye a través de una relación de confianza entre el enrutador de identidad y una aplicación web por lo que es necesario poseer los siguientes lineamientos:

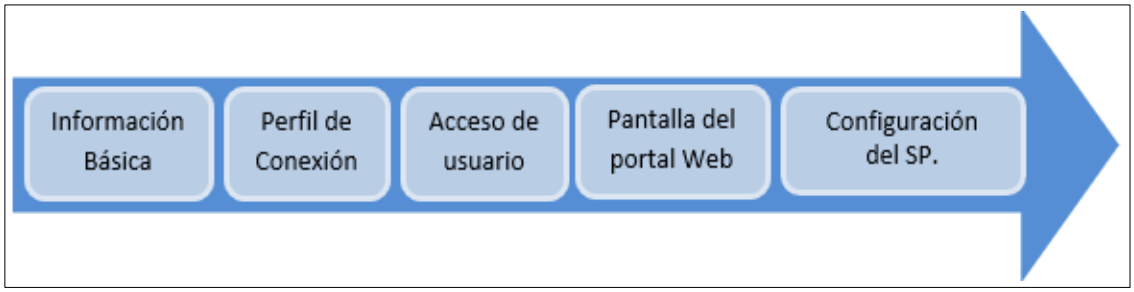
- Verificar y conocer por parte del proveedor de aplicaciones SaaS (Tableau), sus políticas SAML y tener en cuenta el tiempo que se necesita para habilitar la configuración.
- Configurar al menos un enrutador de identidad y una fuente de identidad en la consola de administración de RSA SecurID.
- Recopilar los ajustes de configuración de SSO para la aplicación web a la que está configurando la conexión.
- Identificación de los sistemas y usuarios que necesitan acceso a Tableau.
- Asegurarse de que Tableau Server esté correctamente instalado y configurado.
- Procedimiento para la importación de metadatos del SP.

3.2.2. Etapa de Implementación

La etapa de implementación comprende desde la configuración en el proveedor de identidad (SecurID Access) hasta del proveedor de servicios (Tableau). En la figura 6 se muestra el procedimiento de la etapa de implementación.

Figura 6.

Etapa de Implementación.



Nota. Elaboración propia.

Las etapas de implementación de RSA SecurID con Tableau:

a) **Información Básica:**

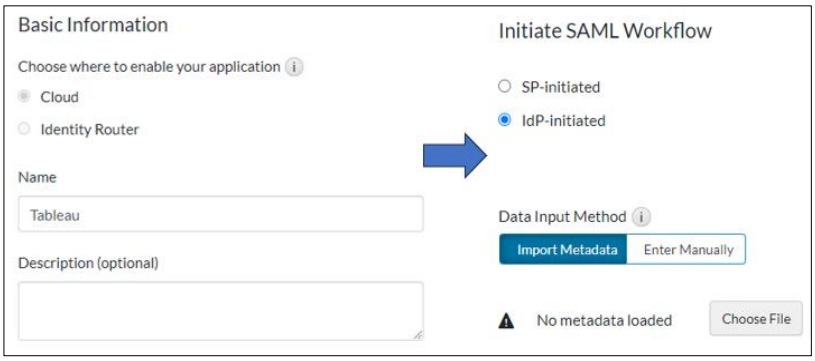
   En la consola de administración de la nube de SecurID Access se requiere crear una plantilla de conector eligiendo SAML. En la sección de información básica, Es factible activar la aplicación para el inicio de sesión único mediante un portal alojado en la nube o a través del enrutador de identidad.

b) **Perfil de conexión:**

   En la consola de administración de la nube de SecurID Access se procede con la configuración de la relación entre el servicio de autenticación en la nube que actúa como proveedor de identidad (IdP) SAML y la aplicación que actúa como proveedor de servicios (SP) SAML. Puede cargar un archivo de metadatos SAML para configurar automáticamente el SP o agregar manualmente la información como se muestra en la figura 7.

Figura 7.

Configuración en la consola de RSA.

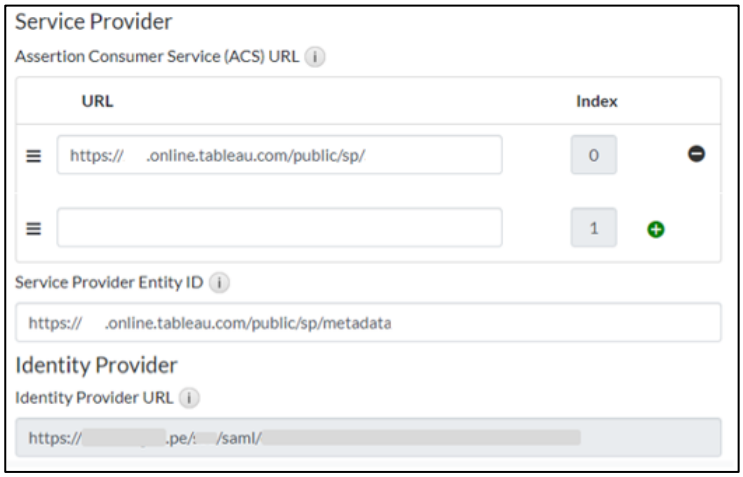


Nota. Elaboración propia.

Esta opción depende de la aplicación a usar, algunos sistemas no te proporcionan su exportación de metadatos, por lo tanto, es necesario ingresar manualmente la información solicitada, en este caso, Tableau., si nos proporciona la opción de exportarlos, por lo que seleccionar importar metadatos y cargar el archivo de metadatos que se obtuvo de Tableau, la URL del Assertion Consumer Service (ACS), la ID de entidad del proveedor de identidad y la audiencia para la respuesta SAML se completará automáticamente, se observa dentro de la figura 8 que se completa la URL del proveedor de servicios y el proveedor de identidad.

Figura 8.

Proveedor de Servicios y Proveedor de Identidad.



Nota. Elaboración propia.

Mediante la importación del metadato brindado por Tableau, se carga automáticamente la protección de mensajes la solicitud y respuesta SAML, SecurID valida la firma de la solicitud utilizando el certificado cargado que proporciona el SP como se observa en la figura 9.

Figura 9.

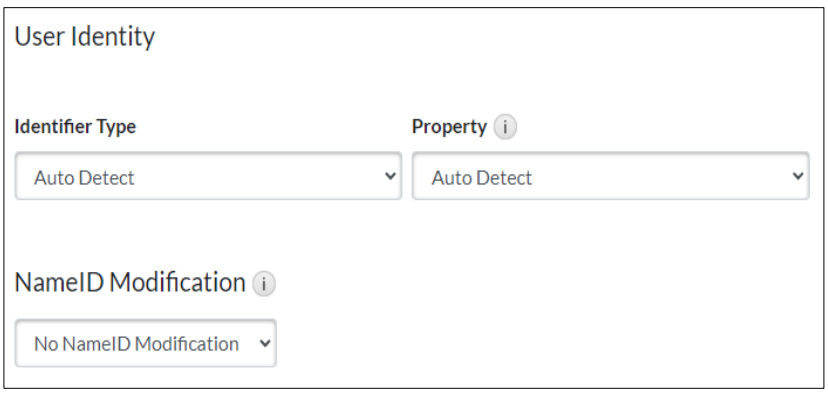
Protección de solicitud y respuesta SAML.

Nota. Elaboración propia.

En la configuración de la identidad de usuario tener en consideración siempre tomar el tipo de identificador y propiedad como Detección automática. La modificación de ID de preferencia colocar sin modificación para no cambiar el ID de nombre viendo en la figura 10 la selección de estos.

Figura 10.

Identidad del usuario.



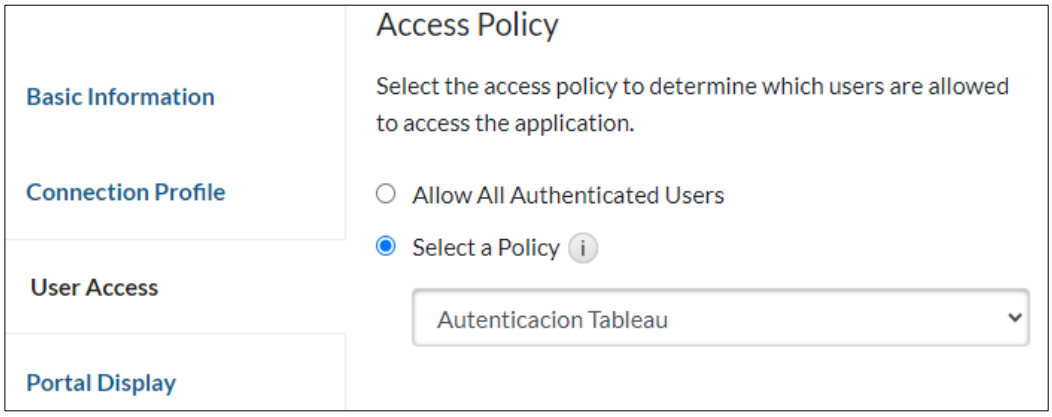
Nota. Elaboración propia.

c) Acceso de usuario:

La política de acceso determina que usuarios pueden acceder a la aplicación y los métodos de autenticación habilitados. En la figura 11 se muestra que se aplicará la política MFA.

Figura 11.

Política de acceso.



Nota. Elaboración propia.

Para la creación de una política de seguridad se tienen los siguientes aspectos en consideración:

- Fuente de Identidad: Una fuente de identidad contiene los usuarios de una organización. Cada fuente puede ser una instancia LDAP/AD local, un directorio local en CAS o una fuente externa administrada por la API SCIM dependiendo que Directorio Activo utiliza su entidad. Seleccionar una fuente de identidad es necesario para identificar la población de usuarios objetivo de esta política.
- Conjunto de reglas: El conjunto de reglas define la población objetivo, las condiciones de acceso y los requisitos de autenticación para esta política. En la figura 12 se muestra que la creación de política MFA, cuenta con los métodos de autenticación aprobación, autenticación OTP, y el biométrico.

Figura 12.

Conjunto de reglas de la política de seguridad.

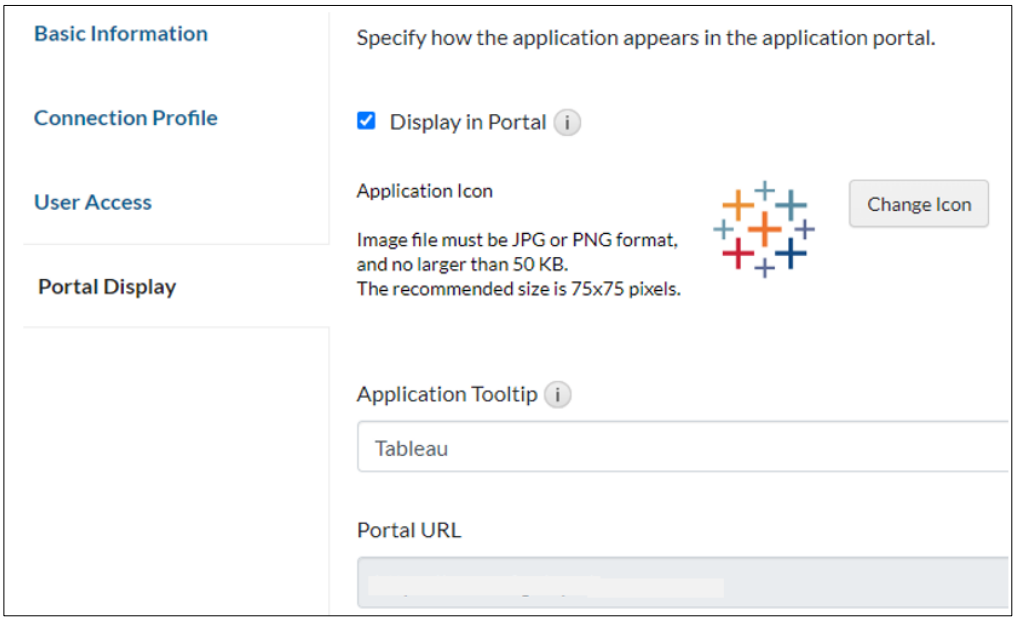
Nota. Elaboración propia.

d) Pantalla del portal:

Este campo especifica cómo aparece la aplicación en el portal de aplicaciones. Seleccionar la opción mostrar en el portal para que el ícono cargado aparezca dentro del portal de aplicaciones como se muestra en la figura 13.

Figura 13.

Pantalla del Portal



Nota. Elaboración propia.

En esta sección se detallan los siguientes procedimientos:

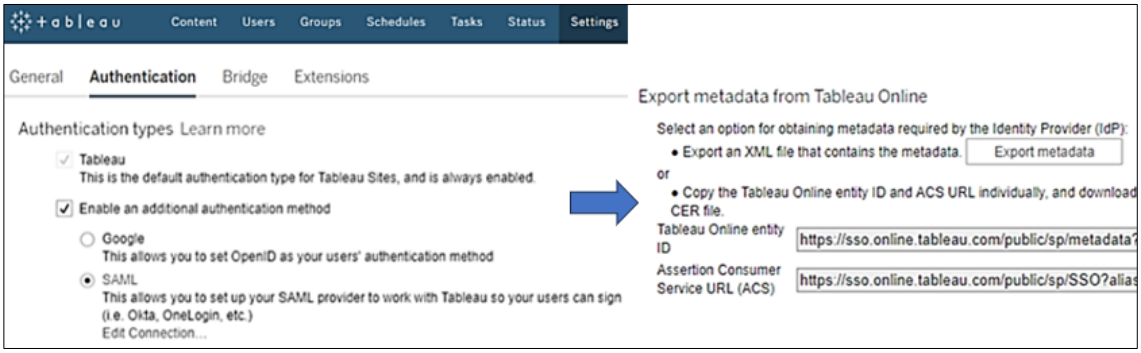
- El archivo de imagen del icono de la aplicación debe tener formato JPG o PNG y no debe superar los 50 KB. El tamaño recomendado es 75x75 píxeles.
- La información sobre la herramienta de la aplicación colocar el título que aparece dentro del ícono.
- El portal URL se configura automáticamente.

e) Configuración de Tableau como un SP SAML del agente SSO para el servicio de autenticación en la nube RSA.

- Acceder al sistema como administrador.
- Dirigirse a la ventana de configuración y seleccionar la pestaña de autenticación. En esta sección, optar por activar un método de autenticación adicional, eligiendo la opción SAML.
- seleccionar en exportar metadatos para descargar el proveedor de servicios que se utilizará para configurar la aplicación Tableau de RSA como se muestra en la figura 14.

Figura 14.

Configuración Tableau.



Nota. Tableau.

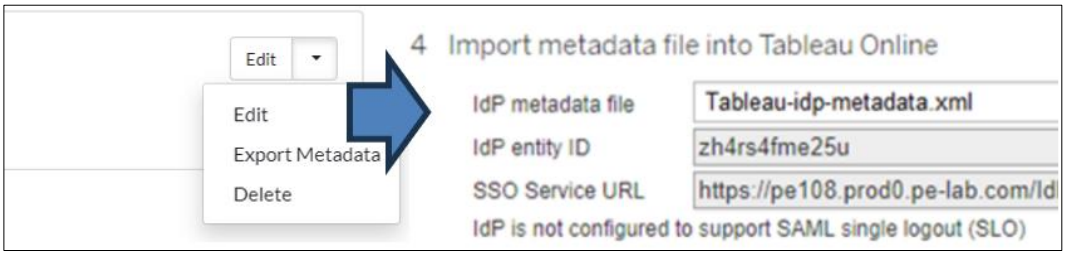
- Importar el archivo de metadatos desde el proveedor de identidad (SecurID Access), luego de ya tener la plantilla realizada, buscar la aplicación Tableau ya configurada, para desplegar la opción de exportar

metadatos Este archivo se debe cargar en la configuración del proveedor de servicios (Tableau).

- En la página de administración de Tableau, importar el archivo de metadatos IDP de RSA se debe seleccionar en Examinar y elegir el archivo de metadatos que se exporto desde SecurID, el ID de la entidad IDP y la URL del servicio SSO se completarán automáticamente y la configuración está completa, como se presenta en la figura 15.

Figura 15.

Exportar metadatos Tableau desde SecurID.



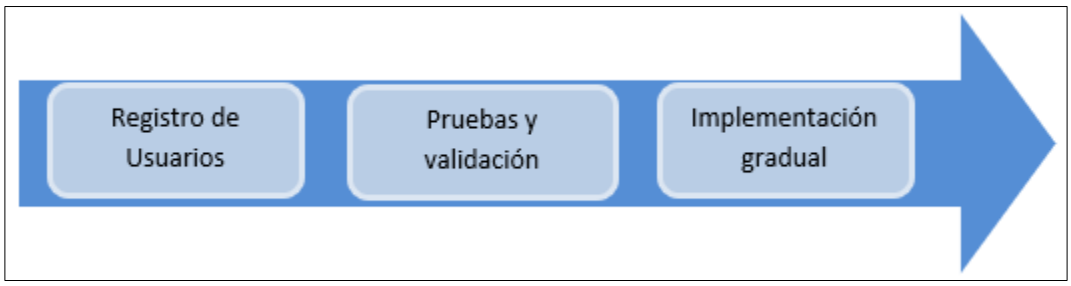
Nota. Elaboración propia.

3.2.3. Etapa de Validación del Pedido

En la etapa de validación del pedido comprende varios puntos de las cuales se describe a continuación, como se muestra en la figura 16:

Figura 16.

Etapa de validación del Pedido.



Nota. Elaboración propia.

a) **Registro de Usuarios:**

Educar a los usuarios sobre el uso de MFA y guiarlos mediante el proceso de registro, cada usuario debe configurar sus factores de autenticación MFA.

- Procedimiento para el registro de dispositivo autenticador en PC:
    1. Descarga la aplicación SecurID desde la tienda de aplicaciones de tu dispositivo.
    2. Después de completar la descarga y aceptar los términos y condiciones, hacer clic en el símbolo "+".
    3. Ingresar los siguientes datos: Código de registro, Dirección de correo electrónico y el ID de la organización.
    4. Al finalizar, seleccionar "Enviar". El procedimiento para el registro del dispositivo en la PC se ilustra en la figura 17.

Figura 17.

Descarga del aplicativo SecurID en PC.

Nota. Elaboración Propia.

- Procedimiento para el registro de dispositivo autenticador en celular:
    1. Descarga la aplicación SecurID desde la tienda de aplicaciones de tu dispositivo.
    2. Después de completar la descarga y aceptar los términos y condiciones, hacer clic en "comenzar".
    3. Ingresar los siguientes datos: Código de registro, Dirección de correo electrónico y el ID de la organización.
    4. Al finalizar, seleccionar "Enviar". El procedimiento para el registro del dispositivo en el celular se ilustra en la figura 18.

Figura 18.

Descarga del aplicativo SecurID en celular.

Nota. Elaboración Propia.

.

b) Pruebas y validación:

Antes de implementar completamente MFA y SSO, se llevaron a cabo pruebas exhaustivas para garantizar su correcto funcionamiento, siendo esencial para prevenir interrupciones no deseadas. Durante estas pruebas, se examinaron detalladamente los aspectos técnicos de MFA y SSO, asegurándose de su operación fluida y segura, así como de que el inicio de sesión único ofreciera la experiencia de usuario esperada.

c) Implementación Gradual:

En lugar de un cambio abrupto hacia la implementación completa de la autenticación multifactor (MFA) para todos los usuarios, se adoptó una estrategia gradual. Se inició con un grupo piloto compuesto por usuarios representativos de diversas áreas y niveles en la organización, permitiendo pruebas en un entorno controlado y recopilando retroalimentación valiosa. Con los aprendizajes de la fase piloto, se amplió progresivamente la implementación de MFA, garantizando ajustes ágiles y una gestión eficiente del impacto en la operatividad diaria. Además, se proporcionaron sesiones de capacitación e información a los usuarios para asegurar su comprensión y adaptación a las nuevas medidas de seguridad.

3.3 Resultados

En esta sección se presentan detalladamente los resultados obtenidos tras concluir la implementación de una solución de autenticación multifactor RSA SecurID Access mediante el lenguaje marcado de afirmación de seguridad SAML para el inicio de sesión único (SSO) en una entidad del estado peruano.

Se identificaron las políticas de autenticación necesarias para mitigar el riesgo de acceso no autorizado, logrando la creación de tres métodos de autenticación disponibles: aprobación, código Token y sensor biométrico.

El protocolo SAML se configuró de manera que admitiera la autenticación multifactor, asegurando su compatibilidad con el sistema existente Tableau de la entidad gubernamental.

La implementación del inicio de sesión único se llevó a cabo a través de un portal web seguro basado en la nube para acceder a la aplicación Tableau, demostrando su funcionalidad y estableciendo las bases para futuras integraciones con otros servicios.

Se procedió a validar la funcionalidad del sistema de autenticación multifactor, asegurando la verificación efectiva de los usuarios y fortaleciendo así la seguridad del acceso al sistema implementado.

3.3.1 Ingreso al Portal web seguro de inicio de sesión único.

Se constata la presencia del portal web de inicio de sesión único tras la exitosa implementación de la configuración SAML. Tras ingresar a la URL específica de Tableau, la plataforma dirige automáticamente al usuario hacia el portal de aplicaciones. Este proceso centralizado se visualiza detalladamente en la figura 19, que ilustra el inicio de sesión.

En esta etapa inicial de autenticación, el usuario se encuentra con una interfaz que solicita el ingreso de su correo institucional y la contraseña asociada a su cuenta de Active Directory (AD), tal como se muestra en la figura 19.

Figura 19.

Portal web del SSO.

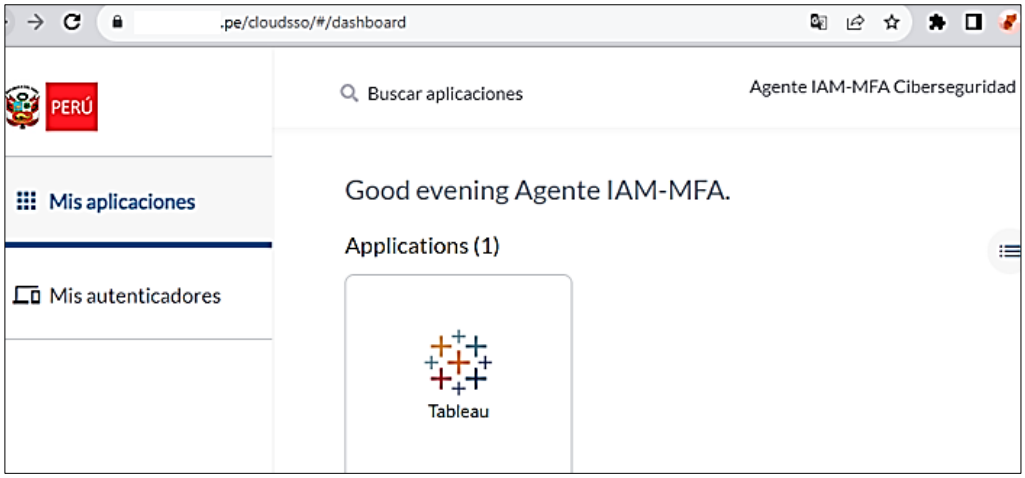
Nota. Elaboración Propia.

3.2.2. Autenticación Multifactor.

Tras ingresar las credenciales necesarias, se destaca la aparición de la aplicación Tableau en el Portal de Aplicaciones del Inicio de Sesión Único. Para acceder a la plataforma, el siguiente paso implica seleccionarla, acción que se ilustra detalladamente en la figura 20.

Figura 20.

Aplicación Tableau en el portal de SSO.



Nota. Elaboración Propia.

Dentro del portal web habilitado, se pudo verificar la capa adicional de autenticación. En este contexto, se han habilitado tres métodos distintos para fortalecer la seguridad: la solicitud de aprobación, la Autenticación OTP (código token) y el uso de la Biometría. Estos métodos adicionales se presentan visualmente en detalle en la figura 21.

Figura 21.

MFA en el portal SSO.

Nota. Elaboración propia.

La incorporación de estos métodos de autenticación no solo responde a la necesidad de seguridad, sino que también ofrece a los usuarios la flexibilidad de elegir el método que mejor se adapte a sus preferencias o requisitos de seguridad.

Los métodos de autenticación para el acceso al portal de aplicaciones son:

- Método de Aprobación: luego del ingreso de credenciales como su usuario y contraseña, le llegará a su dispositivo autenticador la solicitud de inicio de sesión, al seleccionar aprobar se valida el MFA, y logra acceder a la página de Tableau tal como se muestra en la figura 22.

Figura 22.

Método de aprobación.

Nota. Elaboración propia.

- Método del Código token: luego del ingreso de credenciales como su usuario y contraseña, si elige la opción Autenticación OTP, le indicará abrir el dispositivo autenticador, y colocar el número de 8 cifras que aparece. En la figura 23 se muestra el número del código token.

Figura 23.

Método código token.

Nota. Elaboración propia.

Posteriormente, se procede a ingresar el número del código token que aparece en el dispositivo autenticador en el campo correspondiente del portal de aplicaciones para acceder a la página, tal como se muestra en la figura 24.

Figura 24.

Autenticación código token

Nota. Elaboración propia.

- Método de Biometría: después de ingresar las credenciales que incluyen usuario y contraseña, se presenta la opción de utilizar el Sensor Biométrico. Cuando eligen esta alternativa, el proceso se inicia con la recepción de una solicitud en el dispositivo autenticador del usuario, instándolo a colocar su huella en el sensor biométrico, según se muestra en la figura 25.

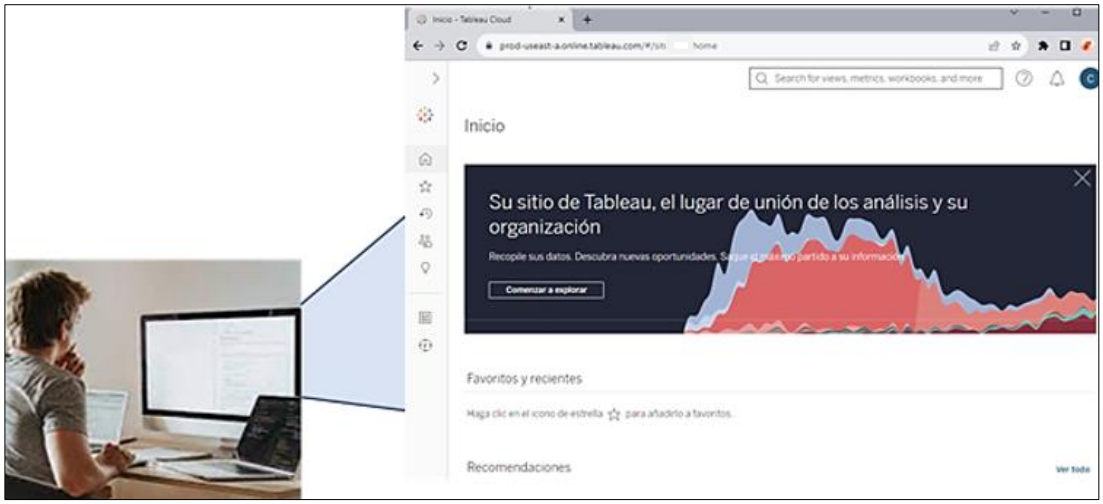
Figura 25.
Método Biometría.

Nota. Elaboración propia.

3.3.3 Acceso a la aplicación.

Después de completar con el MFA, según cualquiera de los tres métodos de autenticación habilitados, se logra tener acceso a la aplicación, tal como se ilustra en la figura 26.

Figura 26.
Aplicación Tableau.

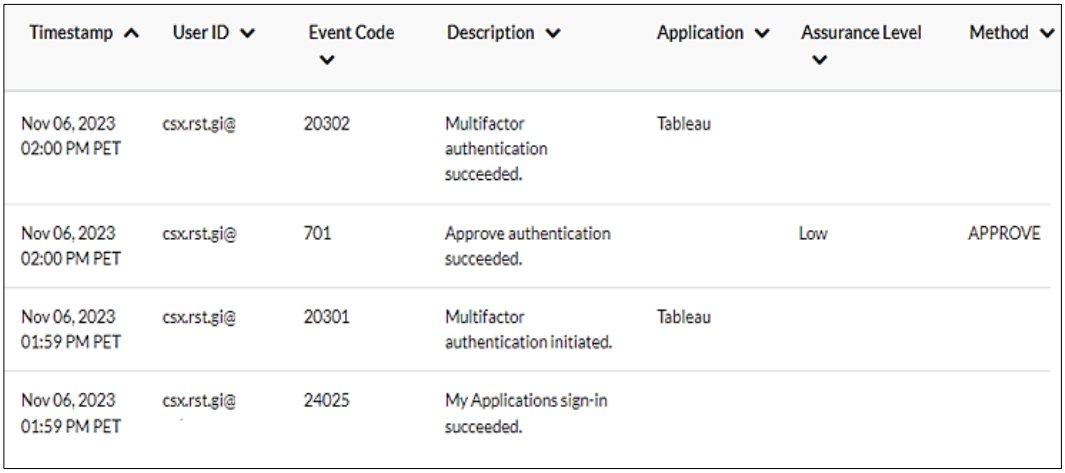


Nota. Elaboración propia.

A continuación, se valida el correcto acceso dentro de la consola de administración de la nube de RSA SecurID, en el monitor de eventos del usuario. En la figura 27 se aprecia que el usuario logra acceder exitosamente a Tableau mediante el portal web seguro SSO de aplicaciones luego de completar el MFA de aprobación.

Figura 27.

Acceso exitoso mediante la aprobación.



Timestamp	User ID	Event Code	Description	Application	Assurance Level	Method
Nov 06, 2023 02:00 PM PET	csx.rst.gi@	20302	Multifactor authentication succeeded.	Tableau		
Nov 06, 2023 02:00 PM PET	csx.rst.gi@	701	Approve authentication succeeded.		Low	APPROVE
Nov 06, 2023 01:59 PM PET	csx.rst.gi@	20301	Multifactor authentication initiated.	Tableau		
Nov 06, 2023 01:59 PM PET	csx.rst.gi@	24025	My Applications sign-in succeeded.			

Nota. Elaboración propia.

El acceso a través del método de aprobación inicia con la introducción de las credenciales de usuario y contraseña, marcando la primera fase del proceso. Posteriormente, el usuario experimenta una integración fluida y eficiente al sistema de autenticación mediante un dispositivo autenticador asociado. En este punto, de manera automática, se envía una solicitud de inicio de sesión al dispositivo autenticador del usuario.

Una vez recibida la solicitud en el dispositivo, el usuario tiene la capacidad de revisar y gestionar el acceso directamente desde su dispositivo. La opción de aprobar se presenta, ofreciendo al usuario la posibilidad de validar la Autenticación Multifactor (MFA). Al seleccionar la opción de aprobar, se completa exitosamente el proceso de verificación y se asegura un acceso seguro a la plataforma.

Se evidencia de manera clara y precisa que el usuario ha alcanzado un acceso exitoso a la plataforma Tableau a través del portal web seguro de Single Sign-On (SSO) para aplicaciones. Este logro se materializa después de haber completado

con éxito el proceso de Autenticación Multifactor (MFA) utilizando el código token (OTP), tal como se muestra en la figura 28.

Figura 28.

Acceso exitoso mediante código token.

Timestamp	User ID	Event Code	Description	Application	Assurance Level	Method
Nov 06, 2023 02:01 PM PET	csx.rst.gi@	20302	Multifactor authentication succeeded.	Tableau		
Nov 06, 2023 02:01 PM PET	csx.rst.gi@	103	Authenticate OTP authentication succeeded.		Low	OTP
Nov 06, 2023 02:01 PM PET	csx.rst.gi@	20301	Multifactor authentication initiated.	Tableau		
Nov 06, 2023 02:01 PM PET	csx.rst.gi@	24025	My Applications sign-in succeeded.			

Nota. Elaboración propia.

El proceso de acceso mediante código token se inicia con la introducción de las credenciales de usuario y contraseña. Una vez completada esta primera etapa, se procede a seleccionar la opción de Autenticación OTP. En este punto, el usuario recibe una indicación para abrir el dispositivo autenticador asociado y colocar el número de 8 cifras que se muestra en el aplicativo. La interfaz del dispositivo autenticador facilita la generación del código OTP, asegurando un factor de autenticación temporal y único.

Posteriormente, el usuario introduce este código de 8 dígitos en la casilla correspondiente del portal de aplicaciones. Este proceso garantiza la sincronización exitosa entre el dispositivo autenticador y la plataforma, fortaleciendo así la seguridad del acceso.

Al ingresar el código proporcionado en la casilla designada, se completa la autenticación por código token y se accede de manera efectiva a la página de Tableau.

En la figura 29, se evidencia de manera explícita y convincente que el usuario ha logrado acceder de manera exitosa a la plataforma Tableau mediante el portal web seguro de Single Sign-On (SSO) para aplicaciones, tras haber completado con éxito el proceso de Autenticación Multifactor (MFA) a través del sensor biométrico. Por ende, ilustra de manera elocuente la culminación exitosa de un proceso de autenticación robusto y la entrada segura del usuario al entorno de Tableau.

Figura 29.

Acceso exitoso mediante sensor biométrico.

Timestamp	User ID	Event Code	Description	Application	Assurance Level	Method
Nov 06, 2023 02:03 PM PET	csx.rst.gi@	20302	Multifactor authentication succeeded.	Tableau		
Nov 06, 2023 02:03 PM PET	csx.rst.gi@	801	Biometric authentication succeeded.		Low	BIOMETRICS
Nov 06, 2023 02:02 PM PET	csx.rst.gi@	20301	Multifactor authentication initiated.	Tableau		
Nov 06, 2023 02:02 PM PET	csx.rst.gi@	24025	My Applications sign-in succeeded.			

Nota. Elaboración propia.

Para acceder mediante el sensor biométrico, el usuario debe ingresar las credenciales correspondientes de usuario y contraseña. Posteriormente, elige la opción Biometría, y con ello, el dispositivo recibe automáticamente una solicitud para utilizar el sensor de biometría. A continuación, se registra la huella del usuario, y finalmente, se presenta el número del código token necesario para ingresar a la página Tableau.

En el estudio llevado a cabo, se implementó con éxito un sistema de autenticación multifactor basado en el protocolo SAML en una entidad estatal. El objetivo principal era mejorar la seguridad del acceso a los sistemas internos, garantizando un entorno de inicio de sesión único (SSO) para los usuarios.

Se observó una notable mejora en la seguridad del acceso a sistemas sensibles mediante la autenticación multifactor. La combinación de factores proporcionó una barrera adicional contra accesos no autorizados.

- Experiencia del Usuario: A pesar de la implementación de medidas de seguridad más rigurosas, se consiguió mantener una experiencia de usuario fluida y eficiente, gracias a la simplificación del proceso mediante el inicio de sesión único (SSO). La introducción de SSO ha permitido que los usuarios accedan de manera rápida y segura a la aplicación, eliminando la necesidad de múltiples credenciales y facilitando la interacción con el sistema.
- Reducción de Incidentes de Seguridad: Un análisis retrospectivo detallado ha evidenciado una disminución significativa en los incidentes de seguridad relacionados con accesos no autorizados. Esto subraya la efectividad del nuevo sistema de autenticación multifactor con SAML implementado. La adopción de esta solución ha fortalecido la seguridad, mitigando las vulnerabilidades previas y mejorando la resistencia contra posibles amenazas cibernéticas.
- Beneficios para el Centro Laboral: La entidad estatal experimentó un nivel sustancial de beneficio gracias a la implementación de la autenticación multifactor con SAML. Se logró reducir riesgos de seguridad al garantizar la identificación sólida de usuarios, cumplir con estándares de seguridad y regulaciones gubernamentales. Y minimizar el riesgo de accesos no autorizados a información clasificada.

La implementación exitosa de la autenticación multifactor con SAML en la entidad estatal ha demostrado ser una medida efectiva para fortalecer la seguridad informática y salvaguardar la integridad de los datos sensibles. Estos resultados respaldan la contribución positiva del estudio a la solución de las problemáticas de seguridad identificadas.

CONCLUSIONES

1. La implementación de políticas de seguridad con autenticación multifactor ha logrado un sólido equilibrio del 88.44% entre la robustez de la seguridad y la comodidad del usuario, asegurando una experiencia eficaz y sin complicaciones para la mayoría de los usuarios.
2. La configuración del protocolo SAML para la autenticación multifactor es variable según las aplicaciones integradas, implicando una adaptación personalizada en la implementación.
3. La implementación de un portal web seguro en la nube para acceder a aplicaciones gubernamentales es un proceso altamente personalizado, ajustándose meticulosamente a las necesidades específicas de la entidad.
4. La validación del sistema de autenticación multifactor RSA SecurID mediante la integración con SAML confirma la funcionalidad y confiabilidad del sistema.

RECOMENDACIONES

- Impartir capacitaciones y proporcionar recursos claros para garantizar que los usuarios comprendan la importancia de la seguridad y sepan utilizar las soluciones MFA de manera efectiva.
- Realizar una evaluación exhaustiva de las aplicaciones que se integrarán al configurar el protocolo SAML para la autenticación multifactor, entendiendo los requisitos específicos de cada aplicación y anticipando posibles adaptaciones necesarias, garantizará una configuración adecuada y eficiente.
- Comprender las necesidades en conjunto con todos los equipos de seguridad de la entidad asegurará una integración efectiva a través de los requisitos de seguridad y una protección adecuada de los datos confidenciales en el proceso de implementación del portal web seguro.
- Ejecutar actualizaciones regulares y pruebas de seguridad es esencial. Aunque la validación exitosa del sistema de autenticación multifactor mediante la integración por SAML demuestre su funcionalidad y confiabilidad, realizar actualizaciones y pruebas continuas garantizará que el sistema siga siendo robusto frente a futuras amenazas.

REFERENCIAS BIBLIOGRÁFICAS

Andrade, J. (2019). *Diseño de un sistema de triple factor de autenticación basado en reconocimiento de similitud de imágenes*.

Bernal, W., & Echevarría, N. (2019). Modelo de niveles de seguridad para pruebas de intrusión en aplicaciones web para PYMES en el Perú. *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://bit.ly/3bU1mIq

Cloudfire. (n.d.). *¿Qué es un proveedor de identidad (IdP)?* Retrieved December 1, 2023, from https://www.cloudflare.com/es-es/learning/access-management/what-is-an-identity-provider/

Cortez, T. (2023). *Diseño e implementación de sistema de autenticación de usuarios conectando bases de datos preexistentes*. 1–60. https://repositorio.uchile.cl/bitstream/handle/2250/192777/Diseno-e-implementacion-de-sistema-de-autenticacion-de-usuarios-conectando-bases-de-datos-preexistentes.pdf?sequence=1&isAllowed=y

Dasu, L., Dhamija, M., Dishitha, G., Vivekanandan, A., & Sarasvathi, V. (2023). Defending Against Identity Threats using Adaptive Authentication. *2023 IEEE 8th International Conference for Convergence in Technology, I2CT 2023*. https://doi.org/10.1109/I2CT57861.2023.10126295

Drozhzhin, A. (2020). *En qué se diferencian la identificación, la autentificación y la autorización*. Blog Oficial de Kaspersky. https://www.kaspersky.es/blog/identification-authentication-authorization-difference/23914/

González, F. (2023). *Servicio de firmado digital de facturas electrónicas con control de acceso basado en MFA*. https://openaccess.uoc.edu/handle/10609/148120

Guerrero, J. (2019). *Autenticación de doble factor mediante OTPs*. https://openaccess.uoc.edu/handle/10609/99946

Gutiérrez, J. (2023). *Implantación de un SSO en un entorno empresarial Seguridad empresarial Jesús Gutiérrez de la Vega*.

SEON. Retrieved December 1, 2023, from https://seon.io/es/recursos/autenticacion-basada-en-el-riesgo/

Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States.

Computer Law & Security Review, *32*(1), 91–110. https://doi.org/10.1016/J.CLSR.2015.12.004

Legadmi. (n.d.). *¿Qué es SaaS?* Retrieved December 1, 2023, from https://legadmi.com/que-es-saas/

Microsoft Learn. (2023a). *¿Qué es el inicio de sesión único?* | *Microsoft Learn*. Microsoft. https://learn.microsoft.com/es-es/entra/identity/enterprise-apps/what-is-single-sign-on

Microsoft Learn. (2023b). *Introducción a Active Directory Domain Services*. https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Netscaler. (2023). *Funciones adicionales compatibles con SAML* | *Autenticación, autorización y auditoría del tráfico de aplicaciones*. https://docs.netscaler.com/es-es/citrix-adc/current-release/aaa-tm/saml-additional-features-supported.html

Ñique, V. (2016). Implementación de solución de autenticación segura basada en doble factor en una entidad del Estado. *Universidad San Ignacio de Loyola*. http://repositorio.usil.edu.pe/handle/USIL/2481

OneSpan. (n.d.). *What is Multi-Factor Authentication (MFA)?* Retrieved December 1, 2023, from https://www.onespan.com/topics/multi-factor-authentication

Oracle Perú. (n.d.). *¿Qué es lenguaje de marcado para confirmaciones de seguridad (SAML)?* Retrieved December 1, 2023, from https://www.oracle.com/pe/security/cloud-security/what-is-saml/#who

RSA Blog. (2021). *What is Multi-Factor Authentication (MFA) and How does it Work?* RSA. https://www.rsa.com/multi-factor-authentication/what-is-mfa/

RSA Community. (n.d.-a). *Identity Router*. Retrieved December 1, 2023, from https://community.rsa.com/t5/securid-cloud-authentication/identity-router/ta-p/572354

Securesoft. (2023). *Secure Soft*. https://www.securesoftcorp.com/

Sepúlveda, J. (2022). *Análisis de la efectividad de los modelos de autenticación 2FA y MFA de acuerdo a los algoritmos y protocolos aplicados en la seguridad de cuentas de servicios y plataformas online en Colombia*. https://repository.unad.edu.co/handle/10596/53822

Sevilla, B. (2018). *Análisis de factibilidad de procedimiento de autenticación única para acceder a los servicios informáticos de Pontificia Universidad Católica*

del Ecuador-Sede Esmeraldas.

Vásquez, D. (2019). Implantación de EMS (Enterprise Mobility+ Security) contra amenazas avanzadas en infraestructura hibrida. *Universidad Tecnológica Del Perú*, undefined-undefined. https://www.mendeley.com/catalogue/30586e0b-ccbd-33a9-9b1e-dcfe02c1a896/?utm_source=desktop

ANEXOS

Anexo I.- Correo de coordinación para la implementación del sistema de seguridad.

Integración RSA SecurID Access con Tableau mediante un agente SAML SSO

Ciberseguridad

Responder a todos

vie 02/06/2023 11:57

Para:

Cc:

Marcado para seguimiento. Completado a las jueves, 09 de noviembre de 2023.

Estimados,

Buen día, se agenda la sesión en conjunto el día de hoy a las 02:30 pm para revisar y detallar el acceso mediante SAML para el inicio de sesión a la plataforma Tableau mediante el SecurID según lo coordinado por llamada.

A si mismo se envía el link de la reunión:
link de la sesión: https://meet.google.com/

Quedamos atentos a cualquier duda y/o comentario.

Atentamente,

Equipo de Ciberseguridad - HI

Nota. Elaboración Propia

Anexo II.- Correo de confirmación del cambio realizado.

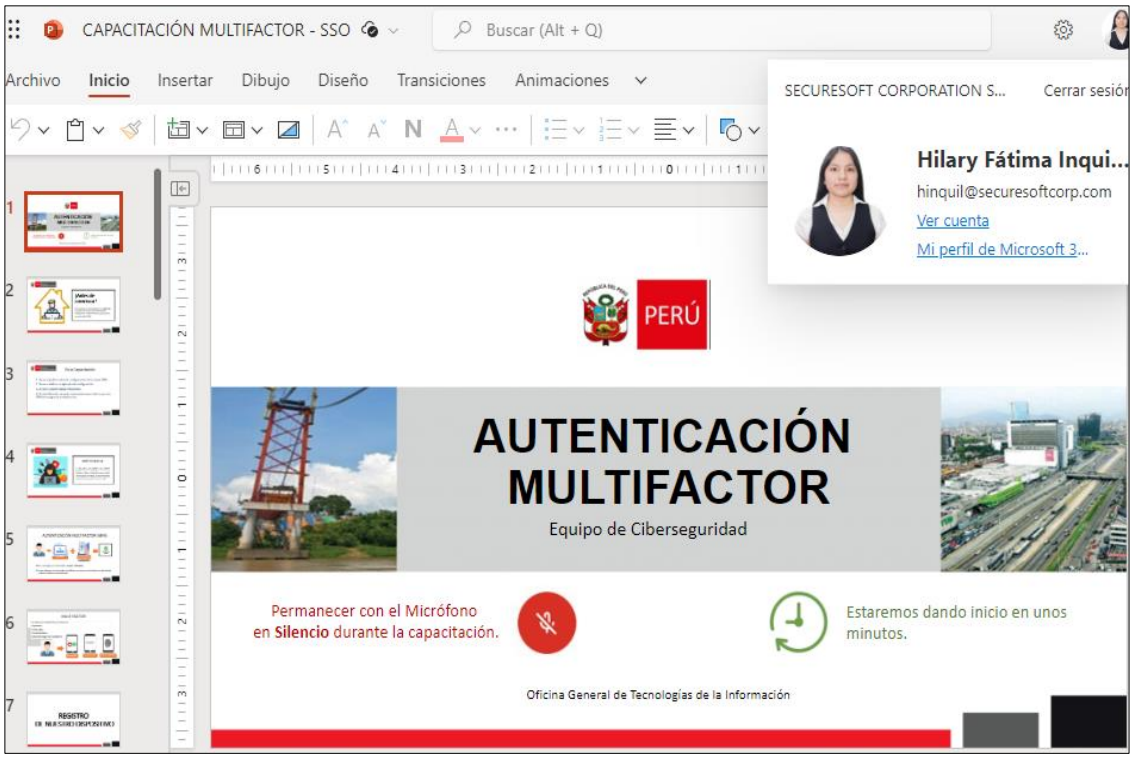
Nota. Elaboración Propia.

Anexo III.- Plan de Migración de la integración del Inicio de Sesión Único con Autenticación Multifactor.

Plan de Migración de la Integración del Inicio de Sesión Único con autenticación Multifactor						
Actividades Previas, durante y finales						
Actividad	**Servicio**	**Fecha Inicio**	**Fecha Fin**	**Responsable**	**Observaciones**	**Estado**
Etapa de Planificación	Si	26/04/2023	3/05/2023	Ciberseguridad / Hilary Inquil	Evaluación de requisitos y políticas: Identificar que tipos de factores son necesarios.	Terminado
	Si	4/05/2023	11/05/2023	Ciberseguridad / Hilary Inquil	Selección de factor de autenticación multifactor: Elección de los factores de autenticación multifactor.	Terminado
	Si	12/05/2023	19/05/2023	Ciberseguridad / Hilary Inquil	Condiciones de la integración SAML: conocer los requerimientos para el correcto funcionamiento.	Terminado
Etapa de Implementación	Si	29/05/2023	2/06/2023	Ciberseguridad / Hilary Inquil	Configuración del proveedor de identidad (SecurID Access): Información básica, perfil de conexión, acceso del usuario	Terminado
	Si	29/05/2023	2/06/2023	Ciberseguridad / Hilary Inquil	Configuración del portal de aplicaciones (SecurID Access): Pantalla del portal Web	Terminado
	Si	29/05/2023	2/06/2023	Ciberseguridad / Hilary Inquil	Configuración del proveedor de servicios (Tableau): Habilitar SAML, importar y exportar metadatos	Terminado
Etapa de Confirmación	Si	12/06/2023	16/06/2023	Ciberseguridad / Hilary Inquil	Registro de usuarios: proceder con el registro de dispositivos autenticadores.	Terminado
	Si	19/06/2023	23/06/2023	Ciberseguridad / Hilary Inquil	Pruebas y Validación: realizar pruebas exhaustivas para asegurar la correcta funcionalidad.	Terminado
	Si	26/06/2023	30/06/2023	Ciberseguridad / Hilary Inquil	Capacitación: Elaborar diapositivas, manuales de usuario y realizar la capacitación por áreas programadas.	Terminado
	Si	3/07/2023	7/07/2023	Ciberseguridad / Hilary Inquil	Implementación gradual: Proceder con la implementación gradual mediante grupos Pilotos en distintas áreas.	Terminado
	Si	10/07/2023	Todos los días	Ciberseguridad / Hilary Inquil	Despliegue: Se procede con el despliegue total de los usuarios y la atención de incidencias obtenidas.	Terminado

Nota. Elaboración Propia.

Anexo IV.- Capacitaciones brindadas a los usuarios de la entidad mediante diapositivas.

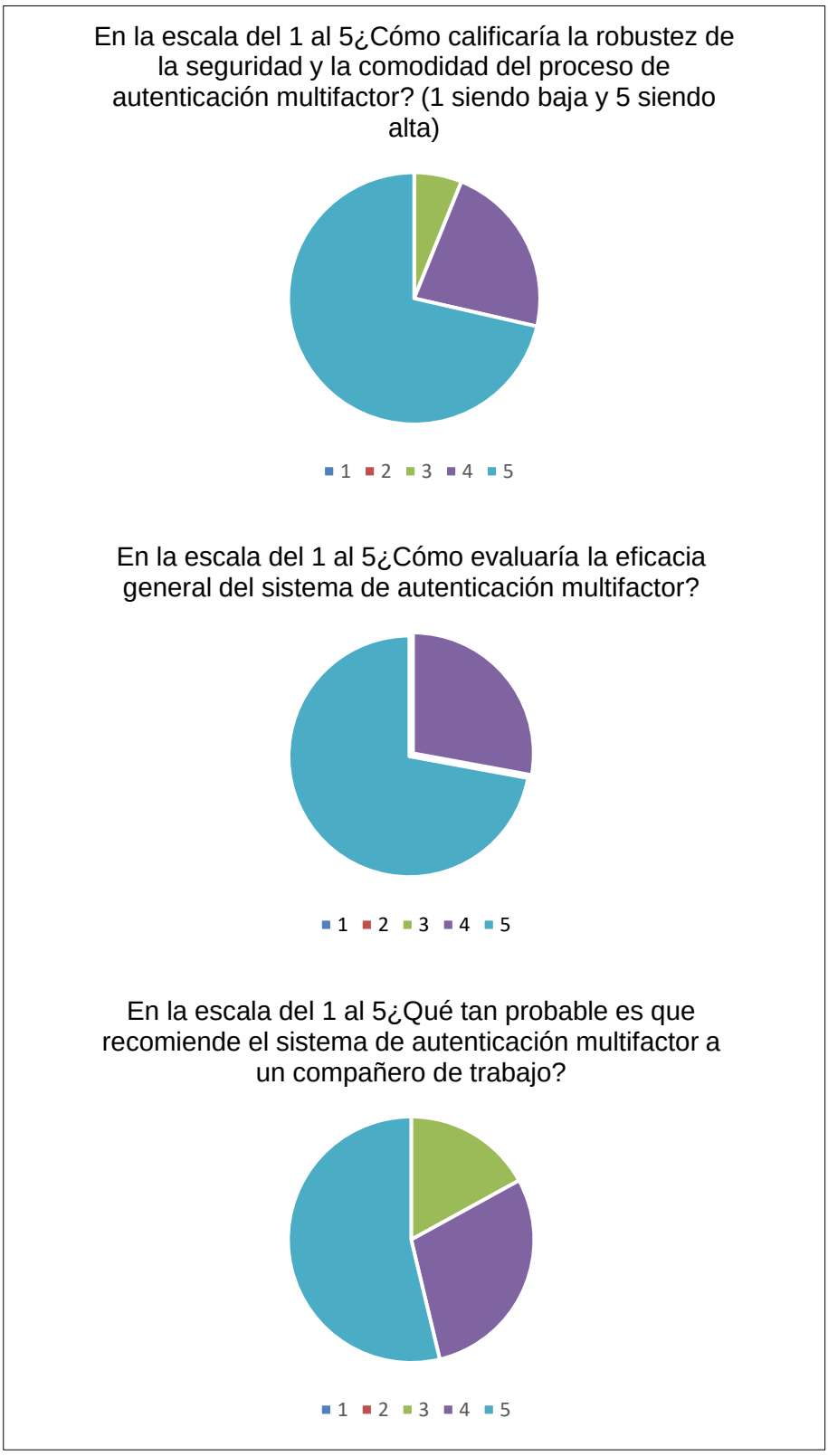


Nota. Elaboración Propia

Anexo V.- Capacitaciones brindadas a los usuarios de la entidad mediante manuales de implementación.

Nota. Elaboración Propia.

Anexo VI. – Gráfico de la encuesta sobre la percepción de los usuarios sobre la implementación de autenticación multifactor con una muestra de 147 usuarios.



Nota. Elaboración Propia.