FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE CONTROLES SEGÚN LA NTP-ISO/IEC 27001:2014 EN LA GESTIÓN DE ACCESOS DE LA EMPRESA SECURITAS SAC EN LIMA 2021”

Tesis para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autores:

Yonathan Damner Montenegro Martinez

Christian Augusto Conislla Ramirez

Asesor:

Mg. Ing. Jorge Alfredo Guevara Jiménez

Lima - Perú

2021

DEDICATORIA

A mis hermanos Roberto, Carolina y Karenn por su apoyo como familia, a mis padres de manera especial por su amor incondicional y enseñanzas para poder seguir adelante.

A Karol Coronado por su amor, paciencia e inmenso apoyo emocional en esta etapa de mi vida, quien me supo escuchar y dar los mejores consejos profesionales y personales.

- Christian Augusto, Conislla Ramirez

A mis padres que son el motivo de todo mi esfuerzo y por su amor infinito que me dan siempre estando conmigo apoyándome y guiándome cuando más los necesito.

- Yonathan Damner, Montenegro Martínez

AGRADECIMIENTO

Al personal de SECURITAS SAC por permitirnos investigar en beneficio y desarrollo de la organización. En especial a la Mg. Karen Rocio García Vera Tudela por permitirnos crecer profesionalmente gracias a la experiencia obtenida de esta investigación.

A nuestro asesor el Mg. Ing. Jorge Alfredo, Guevara Jiménez por tu apoyo en la investigación y desarrollo de esta tesis.

A mi compañero y gran amigo de carrera Yonathan Montenegro por su apoyo en este trabajo de enriquecedora experiencia profesional.

- Christian Augusto, Conislla Ramirez

A la empresa SECURITAS SAC que siempre me permiten tomar nuevos retos para la superación profesional, al equipo de Tecnología por su gran disposición para la investigación y también en especial a la Mg. Ing. Karen Rocío García Vera Tudela por su gran amistad aprecio y confianza para poder realizar esta investigación.

A nuestro asesor Mg. Ing. Jorge Alfredo, Guevara Jiménez por su apoyo y dedicación en el desarrollo de esta tesis.

A mi gran amigo de toda la carrera Christian Conislla por todas las horas de estudio y por la realización de este trabajo para que seamos unos mejores profesionales para la sociedad.

- Yonathan Damner, Montenegro Martínez

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La siguiente tesis "Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021" tiene como objetivo definir e implementar los controles de acceso para la empresa SECURITAS SAC, se efectuó un análisis de brechas (GAP) para conocer el estado de cumplimiento en el uso de controles de acceso y el estado deseado, asimismo se realizó un análisis de riesgo encontrando las probabilidades que existen en la materialización de un posible ataque y el impacto. Esto se realizó tomando como base la Norma NTP-ISO/IEC 27001:2014, enfocada en el Anexo A9 – Control de Accesos. Esto debido a que SECURITAS SAC ha presentado casos que han afectado a las operaciones debido al no tener implementado correctamente una buena gestión de accesos en el área de administración de TI. La tesis menciona los conceptos teóricos y su metodología para el desarrollo de la misma. Se uso el muestreo no probabilístico y por conveniencia, utilizando herramientas de observación y registro en fichas con la validación de juicio de expertos para la muestra de 10 sistemas tomadas en distintos tiempos (Pre-test, Re-Test y Post-Test) con un enfoque cuantitativo. Se pudo observar que el nivel de grado de cumplimiento inicial está por debajo de lo necesario por lo cual la implementación logra incrementar el grado de madurez de controles a un nivel aceptable por la empresa a un estado "Gestionado" que representa a más del 75% dando como valido y funcional la implementación.

Palabras clave: Controles de acceso, Gestión de accesos, Análisis de Riesgo, Seguridad de la Información, Normas ISO, Políticas de Acceso.

ABSTRACT

The following thesis "Implementation of controls according to the NTP-ISO / IEC 27001: 2014 in access management of the company SECURITAS SAC in Lima 2021" aims to define and implement access controls for the company SECURITAS SAC, a Gap analysis to know the state of compliance in the use of access controls and the desired state, a risk analysis was also carried out, finding the probabilities that exist in the materialization of a possible attack and the impact. This was done based on the NTP-ISO / IEC 27001: 2014 Standard, focused on Annex A9 - Access Control. This is due to the fact that SECURITAS SAC has presented cases that have affected operations due to not having correctly implemented good access management in the IT administration area. The thesis mentions the theoretical concepts and its methodology for its development. Non-probability and convenience sampling was used, using observation and recording tools in cards with the validation of expert judgment for the sample of 10 systems taken at different times (Pre-test, Re-Test and Post-Test) with a quantitative approach. It was observed that the initial level of compliance is below what is necessary, so the implementation manages to increase the degree of maturity of controls to an acceptable level for the company to a "Managed" state that represents more than 75% giving the implementation as valid and functional.

Keywords: Access Control, Access Management, Risk Analysis, Information Security, ISO Standards, Access Policies.

CAPÍTULO I. INTRODUCCIÓN

1.1. Bases Teóricas

1.1.1. Bases teóricas de variable para Controles de Acceso

1.1.1.1. Definición de controles de acceso

El control de acceso como definición conceptual es el proceso por el cual se necesita pasar para poder llegar a un lugar, dicho proceso se puede entender como el control. Según Antonucci (2017) afirma:

> El control de acceso se refiere a los mecanismos y técnicas que se utilizan para garantizar que el acceso a los activos estén autorizados y restringido según los requisitos de organización y seguridad (…) Los requisitos de organización para el control de acceso, los principios y actividades de control de acceso (…) deben diseñarse y formularse en función de los requisitos de seguridad de la organización y la información para el control de acceso, con el objetivo general de limitar el acceso a la información. (p.235)

Es necesario priorizar como requisito los controles de acceso, de esta manera poder asegurar la seguridad de información que están en los activos. Según Bridget (2019) afirma:

> El control de acceso es un requisito previo fundamental para asegurar la información a los servicios en los sistemas de procesamiento de información, y también es necesario para proteger las instalaciones físicas que contienen información en todas sus formas. Están en juego la confidencialidad, la integridad y la disponibilidad de la información, los servicios y los procesos comerciales de la organización, junto con otros activos comerciales. (p.69)

De los principales dominios de la norma, los controles en cuanto al acceso al sistema de información que se mencionan en esta investigación son a nivel de red informática, a nivel de sistema operativo y a nivel de aplicaciones de los usuarios basados en la NTP-ISO/IEC 27001 basados en la seguridad lógica (Figura 1).

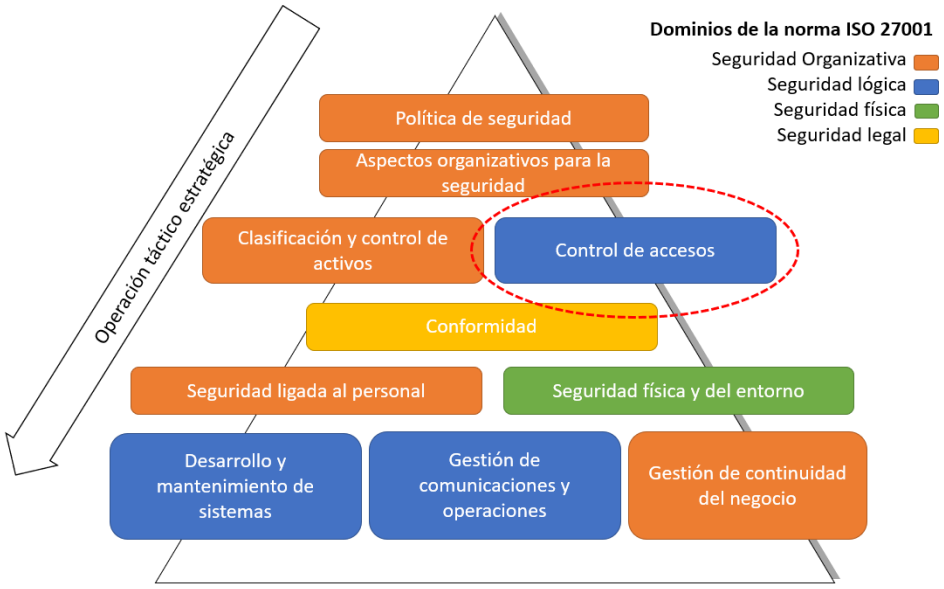


Figura 1. Dominios de la norma ISO 27001.

1.1.1.2. NTP-ISO/IEC 27001

Según la Presidencia del Consejo de ministros N° 004-2016-PCM (2016) establece:

> Los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Esta Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. "Los requisitos establecidos en esta Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza". (p.4)

Entre los controles que la norma hace referencia en el anexo A son:

Tabla 1.

Lista de controles de acceso según NTP-ISO/IEC 27001:2014

ID	Item	Objetivo/Control
A.9.1	**Requisitos de la empresa para el control de acceso**	**Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información**
A9.1.1	Política de control de acceso	*Control*: Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.
A9.1.2	Acceso a redes y a servicios en red	*Control*: Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.
A.9.2	**Gestión de acceso de usuario**	**Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.**
A.9.2.1	Registro y baja de usuarios	*Control*: Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso
A.9.2.2	Aprovisionamiento de acceso a usuario	*Control*: Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	*Control*: La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.
A.9.2.4	Gestión de información de autentificación secreta de usuarios	*Control*: La asignación de información de autentificación secreta debe ser controlada a través de un proceso de gestión formal.
A.9.2.5	Revisión de derechos de acceso de usuarios	*Control*: Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Remoción o ajuste de derechos de acceso	*Control*: Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.
A.9.3	**Responsabilidades de los usuarios**	**Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.**
A.9.3.1	Uso de información de autentificación secreta	*Control*: Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.
A.9.4	**Control de acceso a sistema y aplicación**	**Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.**

A.9.4.1	Restricción de acceso a la información	*Control*: El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.
A.9.4.2	Procedimientos de ingreso seguro	*Control*: Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control*: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control*: El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente
A.9.4.5	Control de acceso al código fuente de los programas	*Control*: El acceso al código fuente de los programas debe ser restringido.

La norma establece que se necesita un enfoque de procesos eficaz para la seguridad de la información. Calder (2017) afirma: "Uno de los enfoques más ampliamente conocido y empleado en el mundo de los sistemas de gestión es el modelo "Planificar-Hacer-Verificar-Actuar" (PDCA), que será familiar para los gerentes comerciales y de calidad en todas partes" (p, 57).

Dentro de la Norma Técnica Peruana ISO/IEC 27001:2014, se mencionan 4 fases de acuerdo al ciclo de mejora continua o también llamado Ciclo PDCA (Plan-Do-Check-Act) lo cual permite implementar de forma adecuada la gestión de seguridad de la información.

El alcance de la propuesta estará enfocado en la fase de planificación donde es necesario evaluar los riesgos y sus brechas hacia los controles de acceso según el anexo A9 de la norma.

1.1.1.3. Familia de normas ISO 27001

La norma internacional ISO 27001 está basada en la gestión de la seguridad de la información actualmente se está volviendo muy conocida y seguida durante los últimos años y forma parte de la familia ISO 27000 (Figura 2).

> Desarrolladas por un subcomité de un comité técnico mixto (ISO/IEC JTC SC27) de la Organización Internacional de Normalización (ISO) en Ginebra y la Comisión Electrotécnica Internacional (IEC), estas normas proporcionan ahora un marco reconocido mundialmente para las mejores prácticas de gestión la seguridad de la información. La designación correcta para la mayoría de estas normas incluye los prefijos ISO/IEC y todas ellas deben incluir un sufijo que es su fecha de publicación. La mayoría de estas normas, sin embargo, tienden a llamarse abreviadamente. ISO/IEC 27001:2013, por ejemplo, a menudo se le hace referencia a menudo simplemente como ISO 27001. (Calder, 2017, p.13)

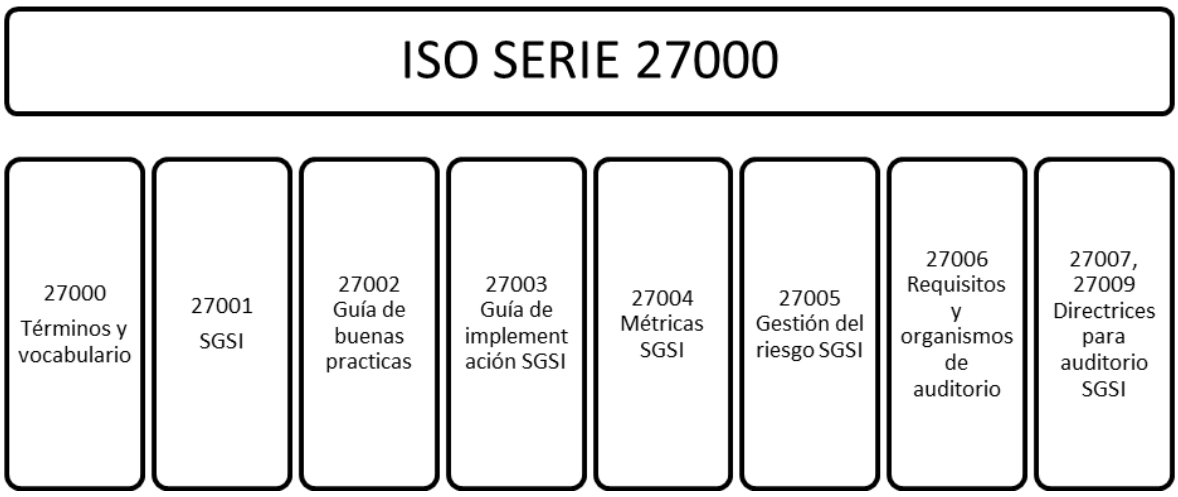


Figura 2. Familia ISO 27000.

1.1.1.4. Seguridad de la información

El activo más importante para la compañía es la información y dicha información reside en sus activos y brindad la seguridad a estos asegura la continuidad de sus operaciones por lo tanto es necesario tener en cuenta este concepto completamente definido como objetivo dentro de los análisis a elaborar. Según Delgado (2017) afirma:

> El objetivo de la seguridad informática es proteger los valiosos recursos informáticos de la organización, tales como la información, hardware o software. A través de la adopción de las medidas adecuadas, la seguridad de TI ayuda a la organización a cumplir sus objetivos, la protección de sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros activos tangibles e intangibles. Por desgracia, a veces se ve a la seguridad informática como algo que dificulta la consecución de los mismos objetivos de la organización, la imposición de reglas y procedimientos rígidos a los usuarios y administradores de sistemas. Pero debe mirar a la seguridad informática, no como un objetivo en sí mismo sino como un medio para apoyar el logro de los objetivos de la organización. (p.17)

1.1.1.5. Análisis de cumplimiento (GAP)

Es necesario establecer etapas para conocer el estado actual y deseado de un proceso en una organización por lo cual se establece las etapas necesarias para el análisis GAP (Figura 3) situación actual, situación deseada u objetivo alcanzar y análisis de deficiencias.

Un análisis de brechas GAP es un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las

aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito. GAP se refiere al espacio entre "donde estamos" (el presente) y "donde queremos estar" (el objetivo a alcanzar). Un análisis de deficiencias también puede denominarse análisis de necesidades, permitiéndonos determinar lo que nos falta y los recursos necesarios para alcanzar los objetivos. (Normaiso27001, 2017)

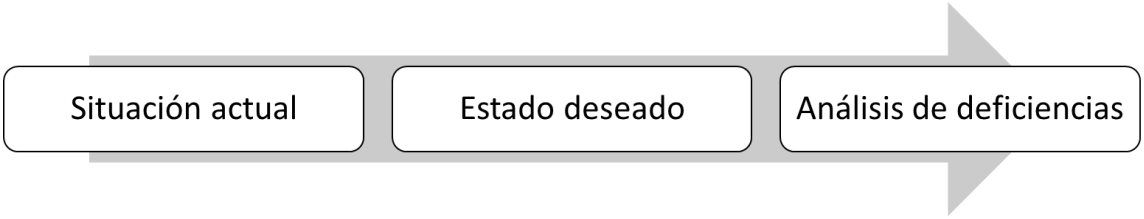


Figura 3. Etapas análisis GAP.

1.1.1.6. Modelo de madurez (COBIT)

La forma de poder tener un nivel de madurez para un proceso es aplicando un esquema con el cual se pueda evaluar los procesos en una organización.

COBIT® 2019 admite un esquema de capacidad de procesos basado en CMMI. El proceso dentro de cada objetivo de gobierno y gestión puede funcionar con distintos niveles de capacidad, que van de 0 a 5. El nivel de capacidad es una medida de lo bien que se ha implementado y funciona un proceso. (ISACA, 2019, p.40)

El modelo CORE de COBIT asigna niveles de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos y las actividades requeridas para alcanzar los distintos niveles de capacidad.

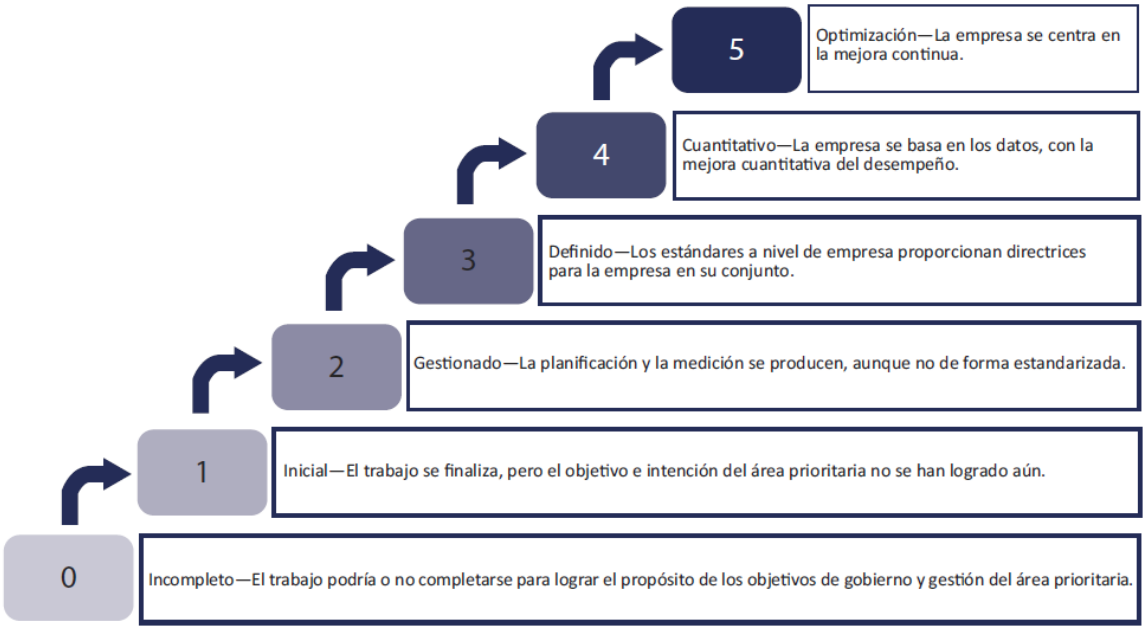


Figura 4. Niveles de capacidad para los procesos. Fuente: COBIT 2019 Introducción y Metodología.

1.1.1.7. Análisis de riesgos

Evaluar el riesgo en el marco de la norma ISO 2700 implica identificar, analizar y valorar los riesgos. Según Calder (2017) afirma:

> La identificación del riesgo es el "proceso de encontrar, reconocer y describir los riesgos", el análisis del riesgo es el "uso sistemático de información para estimar el riesgo" y la evaluación del riesgo es el "proceso de comparar el riesgo estimado frente a los criterios del riesgo dados" para determinar su importancia. En términos más simples, la evaluación del riesgo es la consideración sistemática y metódica de: a) la probabilidad realista de que ocurra un riesgo y b) el daño comercial que es probable que resulte de dichos riesgos. La evaluación del riesgo debería ser un proceso formal. En otras palabras, el proceso debería estar planificado y la introducción de datos, su análisis y los resultados todos deberían registrarse. "Formal" no significa que deben utilizarse herramientas técnicas de evaluación del riesgo, aunque en

> situaciones más complejas, es probable que mejoren el proceso y añadan valor importante. La complejidad de la evaluación del riesgo dependerá de la complejidad de la organización y de los riesgos en revisión. Las técnicas empleadas para llevarla a cabo deberían ser coherentes con esta complejidad y el nivel de garantía exigido por el consejo. (p.89)

Toda organización está expuesta a riesgos debido a que no hay un entorno u organización completamente segura. Debido a esto toda organización debe estar alerta a cualquier procedimiento extraño dentro de sus procesos que pueda considerarse negativo para sus activos, a un dominio o a toda la organización.

En este contexto de la investigación el acceso indebido a los sistemas de información es necesario realizar un análisis de riesgo para conocer el impacto que la mala gestión de accesos puede generar.

1.1.1.8. MAGERIT

> Para la definición de MAGERIT (Ferruzola, Duchimaza, Ramos y Alejandro, 2019) afirman que es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de Magerit está directamente relacionada con la generalización del uso de las TI, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios

> que se prestan gracias a ella, son valiosos, Magerit les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Ferruzola et al. (2019) (p.35)

Según (Dirección General de Modernización Administrativa, 2012) afirma:

> Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. (p.16)

Se adaptará la metodología a lo que requiere la empresa como complemento para priorizar los activos de alto valor y las amenazas con alto impacto, para esto se utilizaran los procesos necesarios (Figura 5) según su metodología.

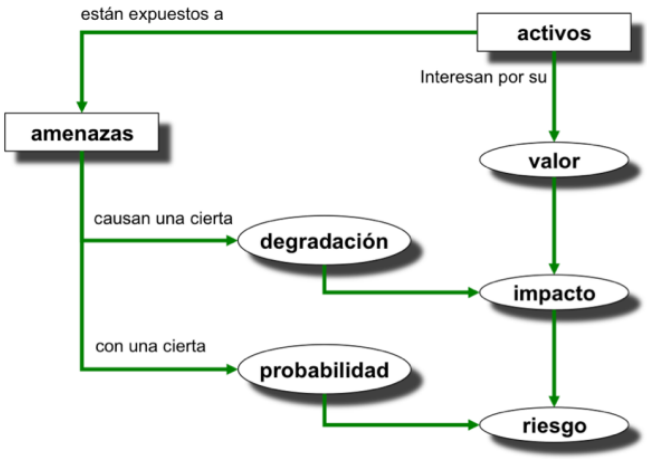


Figura 5. Elementos de análisis de riesgo potenciales.
Fuente: Metodología MAGERIT V3

1.1.1.9. Control de acceso basado en puertos

El protocolo de autenticación extensible (EAP) está diseñado para entornos de nivel de grandes empresas en los que los administradores deseen un grado de seguridad mayor que los simples nombres de usuario y contraseñas. El EAP se encuentra dentro del protocolo de autenticación de PPP y ofrece un marco generalizado para distintos métodos de autenticación. Con un EAP estandarizado, interoperabilidad y compatibilidad con métodos de autenticación, es más sencillo. IEEE 802.1X es el estándar para pasar el EAP por una LAN con cable o inalámbrica. La encapsulación del EAP sobre IEEE 802.1x se conoce como "EAP sobre LAN" o EAPOL.

1.1.1.10. Okta verify

Perumbuli, S. K. (2017) menciona, Okta Verify es un producto MFA y SSO. Funcionando como una herramienta MFA, mide estándar inicios de sesión con nombre de usuario / contraseña y variedad de servicios de servidores. Cuando funciona como una herramienta SSO, Permite a los usuarios finales iniciar sesión en un portal web que sirve como base para la autenticación de la cartera de aplicaciones de SSO de una organización. Okta verify difiere de otros productos MFA ya que tiene una característica única llamada "Aprovisionamiento justo a tiempo", que permite la autenticación con Active Cuentas de directorio sobre la marcha. Por lo tanto, cuando los usuarios comienzan a utilizar los componentes de SSO, OV puede intentar construir sus cuentas sobre la marcha.

1.1.1.11. Manejo de identidades de acceso (IAM)

Cutillas Zárate, J. (2021) afirma. El manejo de identidades de acceso o IAM en sus siglas en inglés, se considera un campo de la ciberseguridad que garantiza que la información sensible sólo puede ser accedida por usuarios seleccionados en determinados momentos. Gracias a la gestión de identidades y accesos, se reduce en gran medida la posibilidad de que se produzcan infracciones y ciberataques, además de reducir el riesgo de error humano, el cual representa la principal causa de violaciones de datos.

1.1.1.12. IDaaS (Identidad como servicio)

Según CH. RUPA, AL-TURJMAN, MOSTARDA (2020) menciona:

> Actualmente, uno de los servicios esenciales que puede permitir las organizaciones basadas en la nube es la gestión de identidades como servicio (IDaaS). Hace que se enriquezca y despliegue la seguridad, servicios como responsabilidad, autorización y control de acceso en los entornos de nube. Aunque, el paradigma del ambiente en la nube juega un papel vital en el campo de la computación en lo que respecta a para monitorear y controlar los datos. IDaaS facilita la gestión de la infraestructura a la identidad, así como los permisos para convertir hacia el modelo de entrega bajo demanda como técnicas modernas desde un enfoque tradicional al modelo de entrega de promesas. Además, IDaaS ofrece varias oportunidades para los usuarios de la nube y proveedores tales como reducción de costos, control de subcontratados datos, que están relacionados con la identidad del usuario.

1.1.2. Bases teóricas de variable para Gestión de Accesos

Torok, Day, Hartman-Baker y Snavely (2020). Aseguran que dos funciones operativas críticas e interrelacionadas de cualquier instalación informática grande son administrar los numerosos proyectos y usuarios que tienen acceso a la instalación y distribuir los recursos informáticos y de almacenamiento de manera justa entre ellos. Torok et al. (2020) refieren que el primero es relativamente común en las organizaciones de TI: la administración de usuarios, grupos y reglas de acceso se conoce como Gestión de identidades y accesos.

Vallois, Mehaoua y Amziani (2021). Mencionan que la gestión de accesos es la asociación de la gestión de identidad y el control de acceso, logrando dos objetivos principales. Vallois et al. (2021) refieren a la atribución y orquestación de la identidad digital a los usuarios (administrador, operador, desarrollador ...), dispositivo (sensor, chips RFID, maquinaria pesada ...), servicio (servicio web, aplicación, base de datos ...) o recurso (datos, potencia de cálculo ...) y autenticación y autorización de estas identidades.

Teniendo en cuenta las bases operativas en una organización en el manejo de procesos y usuarios es necesario manejar la identidad bajo la administración de accesos teniendo en cuenta elementos claves para llevar a cabo su correcta implementación como son los activos, usuarios, servicios, recursos y autenticación.

De acuerdo con ITIL®4 (2019) afirma:

El objetivo de la gestión de acceso es proteger los datos para que no accedan a ellos usuarios no autorizados. Esto es extremadamente vital para una organización, ya que los datos críticos que caen en las manos equivocadas

podrían causar daños irreversibles a la empresa y sus procesos se basan en seis etapas (Figura 6): solicitar acceso, verificar el acceso, otorgar derechos de acceso, supervisar la identidad, trazabilidad de accesos y quitar o restringir derechos.

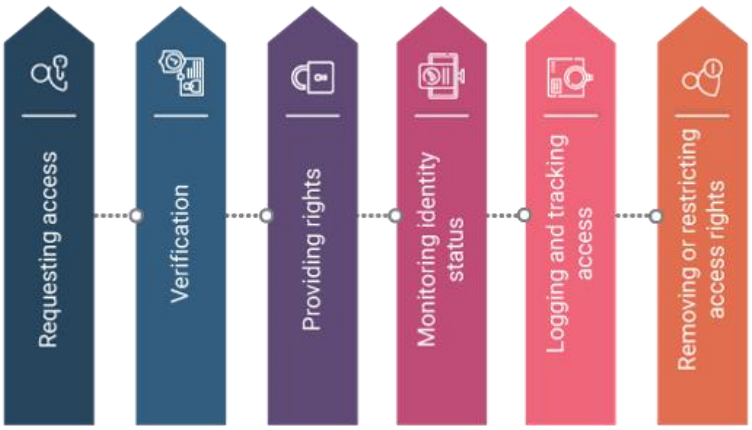


Figura 6. Proceso de gestión de accesos por ITIL.
Fuente: ITIL 2019.

1.1.2.1. Bases teóricas de dimensión políticas de accesos a usuarios

Las políticas serán los procedimientos que tiene que seguir un empleado ante una problemática o proceso, en nuestro caso el correcto uso de brindar el acceso a los sistemas. Para W. He y Zhang (2019) afirman:

> Las políticas son un conjunto de procedimientos, pautas, roles y responsabilidades formalizados que los empleados deben cumplir para salvaguardar y utilizar adecuadamente los recursos de información y tecnología de sus organizaciones.

La organización debe desarrollar, documentar e implementar una política de control de acceso que defina los derechos de acceso de los usuarios en función de las necesidades comerciales, teniendo en cuenta los requisitos de clasificación y manejo

de la información, los servicios, las redes y / o aplicaciones a las que se accede, y cualquier requisito legal o reglamentario. Según Bridget (2017) afirma:

> La organización debe desarrollar, documentar e implementar una política de control de acceso que defina los derechos de acceso de los usuarios en función de las necesidades comerciales, teniendo en cuenta los requisitos de clasificación y manejo de la información, los servicios, las redes y / o aplicaciones a las que se accede, y cualquier requisito legal o reglamentario. requisitos. Los perfiles de acceso de usuario estándar para roles específicos son una forma útil de administrar el acceso cuando hay muchos usuarios involucrados (esto se conoce como "acceso basado en roles"). Es importante revisar la política de control de acceso con regularidad y eliminar cualquier derecho de acceso que ya no sea necesario. Debe tenerse en cuenta los repositorios de información empresarial, como los sistemas de calendario. (p. 69)

1.1.2.2. Bases teóricas de dimensión administración de accesos a usuarios

La administración de los accesos a los usuarios debe seguir las condiciones mencionadas en los sistemas de información para llevar un correcto control basada en la norma. Se debe establecer los procesos necesarios basados a su vez en políticas para los sistemas de información con enfoque a los usuarios e identidades. Según Bridget (2019) menciona:

> Cada usuario debe estar registrado formal y exclusivamente por la organización, y debe mantenerse un registro de cada sistema de información, red o servicio al que tenga un requisito comercial para acceder. No controlar

> el registro puede resultar en una violación de la confidencialidad, una modificación no autorizada y / o pérdida.
>
> Cada usuario debe estar registrado formal y exclusivamente por la organización, y debe mantenerse un registro de cada sistema de información, red o servicio al que tenga un requisito comercial para acceder. No controlar el registro puede resultar en una violación de la confidencialidad, una modificación no autorizada y / o pérdida (…) Los privilegios son todas las características o instalaciones de los sistemas de procesamiento de información que permiten al usuario llevar a cabo actividades de administración del sistema o anular los controles de acceso, como el mantenimiento del sistema de seguridad o el sistema de administración de datos. Si los privilegios no están controlados, un número cada vez mayor de usuarios utilizará los privilegios, haciendo inútiles los controles de acceso cuidadosamente implementados. La asignación y el uso innecesarios de privilegios a menudo se considera un factor importante que contribuye a la vulnerabilidad de los sistemas que han sido violados. La pérdida de confidencialidad por exposición, la pérdida de integridad por modificación de datos y la falta de disponibilidad de datos son consecuencias típicas (…) La identificación y autenticación de usuarios van de la mano con el control de acceso, el registro de usuarios y la asignación de privilegios. Esto se hace muy a menudo a través de contraseñas, que siguen siendo un mecanismo común, pero no el único, para la autenticación de usuarios. (p.73)

Los derechos de acceso siempre deben basarse en las necesidades comerciales; cuando la necesidad ya no existe, el acceso debe cancelarse. Sin

embargo, con la mejor voluntad del mundo, es posible que se cometa un error y el acceso se retenga de manera inapropiada cuando un usuario abandona o cambia de rol.

1.1.2.3. Bases teóricas de responsabilidades de usuario

La información de autenticación secreta incluye cosas como contraseñas, datos biométricos y PIN, pero no ID de usuario o direcciones de correo electrónico (ya que no son secretas). También incluye las respuestas a las preguntas que se usan comúnmente para permitir que una persona realice un restablecimiento de autoservicio de su contraseña. Según Bridget (2019) menciona:

> La información de autenticación secreta expuesta (escrita), o las contraseñas obvias y fáciles de adivinar, pueden llevar al uso indebido de los sistemas por parte de personas no autorizadas, con los riesgos consiguientes de pérdida de confidencialidad, integridad y disponibilidad. Los usuarios también deben saber si pueden ser considerados responsables de las acciones llevadas a cabo por otra persona que haya utilizado su información confidencial de autenticación. (p.85)

Los usuarios deben tener asignada la responsabilidad y conocimiento por la organización sobre el correcto uso de la autentificación en la empresa. Deben entender el alcance de la responsabilidad de uso de la autentificación en la empresa y las mejores prácticas de la misma.

1.1.2.4. Bases teóricas de accesos a sistemas y aplicativos

El propietario de la información contenida en cada aplicación debe especificar los derechos de acceso y las reglas para esa aplicación, de acuerdo con los requisitos comerciales y la política de control de acceso. Según Bridget (2019) menciona:

> Algunos sistemas no tienen la capacidad de controlar o modificar el nivel de información que presentan, y la organización tiene que aceptar el sistema tal como se proporciona. En tales casos, se deben utilizar otros controles de mitigación (…) La gestión deficiente de contraseñas conlleva el riesgo de un mal uso de los sistemas por parte de personas no autorizadas, con los consiguientes riesgos de violaciones de la confidencialidad, integridad y disponibilidad de la información. Cuando se puedan usar sistemas para hacer cumplir la calidad, la vida útil y la frecuencia de cambio de las contraseñas, se deben usar. Si este no es el caso, es posible que se requieran controles de compensación y monitoreo (…) Las utilidades del sistema brindan la oportunidad de un mal uso, lo que puede dañar la integridad de los controles de seguridad de un sistema operativo o una aplicación. Dado que estos servicios pueden ser necesarios para resolver problemas de control, su uso debe controlarse estrictamente y solo debe realizarse después de una autorización y justificación suficientes. (p.87)

El código fuente del programa puede contener detalles del sistema, otras aplicaciones y controles implementados. Proporciona al atacante un punto de partida perfecto para comprender y realizar la modificación no autorizada de un sistema.

Los sistemas y aplicaciones deben tener los procedimientos y funciones adecuadas para salvaguardar la información que puedan contener los mismos.

1.2. Antecedentes

1.2.1. Antecedentes internacionales

En el trabajo de investigación "Aspectos esenciales para fomentar el control de acceso de la información" siendo un paper de la Institución de educación superior Politécnica costa atlántica del 2016. Tiene como objetivo el fomentar el control de accesos a la información como protección contra la divulgación, modificación o destrucción (accidental o maliciosa) teniendo como activo importante y valioso la información de la organización. El estudio expone los procedimientos básicos para considerar la implementación de los controles de accesos a los usuarios asegurando la seguridad de la información. En el enfoque del estudio redacta una serie de procedimientos para poder realizar un correcto control del acceso a usuarios. Como la identificación de usuarios con métodos externos de verificación de identidad, también sobre los mecanismos de autenticación que deben de ser únicos para cada usuario de la organización y para cada sistema de información como un inicio de sesión de manera única al sistema. Los identificadores son distribuidos para poder eliminar el repudio de recepción y también la protección de la confidencialidad de la información. La desactivación de cuentas es necesaria a la hora que los usuarios ya no sean necesarios y archivadas para garantizar la investigación potencial a futuro (Carmona, 2016). De modo que podemos considerar este antecedente sobre la importancia de los controles de autorización para garantizar el correcto acceso a la información referente a nuestra variable independiente.

En el trabajo de investigación "Diagnóstico de la Gestión de Acceso de Usuarios en la Superintendencia de Servicios Públicos Domiciliarios- Norma ISO/IEC 27001:2013 Numerales A.9.2.2 y A.9.3.1" de la Universidad Libre seccional Bogotá Colombia 2017. Tiene como objetivo de garantizar impedir los accesos no autorizados a los sistemas de información y servicios estableciendo procedimientos formales para gestionar y controlar los permisos de los accesos cumpliendo todo el ciclo de vida del acceso de los usuarios referente a la norma. La metodología que usaron fue cuantitativa por medio de encuestas para evaluar las pareas críticas para poder mantener la integridad, confidencialidad y disponibilidad de la información tomando como análisis el año 2016 de las 25 áreas de la organización (…) Se identifica que el apartado de la gestión de usuarios de la norma, no tiene actualmente un registro que permita identificar en cada área los accesos de la información según el rol que desempeña, ya identificado los riesgos de no tener dicho control, se debe de implantar de forma inmediata por parte del área de tecnología un procedimiento que permita gestionar dichos accesos según los perfiles identificados y requeridos por la organización. Se debe mejorar el procedimiento actualmente utilizado e implementarlo de forma detallada tomando como base los manuales que brinda el ministerio de tecnologías de la información (Parra, 2017). Por este motivo expresado en dicha investigación, consideramos como antecedente para nuestro proyecto al tratar de la importancia e implementación de una gestión de usuarios según la norma ISO 27001 relacionada a los numerales A.9.2.2 y A.9.3.1.

En el proyecto de "Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma

ISO/IEC 27001" que es un proyecto de titulación de la escuela Superior Politécnica de Litoral (EPSOL) Guayaquil-Ecuador 2012. El objetivo es la implementación es la de proporcionar a gerencia las directrices y soporte necesario para poder estar protegidos con la seguridad informática. El alcance del sistema de gestión de la seguridad informática debe de cubrir todas las operaciones de la compañía en los procesos de planeación, realización y la finalización de los servicios de las auditorias financieras, usando la metodología MAGERIT. Si bien se identificaron todos los puntos de la norma que aplican la empresa se concluye que la empresa necesita optimizar los recursos de la gestión de seguridad de la información para que se vuelva una actividad importante el cual hay que cumplirla, las políticas de seguridad de usuarios se da en el enfoque para optimizar y mejorar el proceso de políticas de seguridad, se debe de buscar compromiso y soporte gerencial para apoyar a aplicar las medidas para mantener la seguridad en la empresa y contar con personal clave dentro de la organización con las competencias exigidas para evitar contrataciones de consultorías externas. Finalmente, este proyecto aporta información sobre la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) para prevenir incidentes de seguridad y sobre la implementación de políticas de acceso para los usuarios de la compañía que deben de cumplir para la correcta gestión de Seguridad (Tola y Freire, 2015).

1.2.2. Antecedentes nacionales

En la tesis de "Modelo de seguridad informática aplicando la norma ISO/IEC 27001 para proteger los activos de información en la empresa Berendson Natación S.R.L." Que es para obtener el título de ingeniero de sistemas en la universidad de Lambayeque facultad de ciencias de ingeniería 2019.El alcance de un Sistema de

Gestión de Seguridad de la Información es uno de los puntos más importantes ya que deben ser los más precisos y que englobe a toda la organización, como objetivo es el identificar las amenazas que están afectando actualmente a la empresa para establecer políticas de seguridad con roles y responsabilidades que estén relacionadas con el Sistema de gestión de Seguridad de la información para la compañía, implementar y mantener un plan estratégico para el tratamiento de los riesgos de los activos de la organización (…) necesitan identificar las amenazas para la empresa como el robo y alteración de los datos que puedan afectar la imagen de la compañía para reducir los riesgos al mínimo e Identificar, reportar, registrar y reducir las fallas, problemas o diferentes eventos que puedan alterar la seguridad que tiene la empresa y así poder mantener una mejora en los procesos (…) los resultados que se obtuvieron permitieron determinar de forma real que, al implementar la Norma Técnica Peruana ISO/IEC 27001:2014, se obtuvo un mayor nivel de uso de documentos tales como procedimientos, política y otros, que favorecieron a la institución para descubrir las irregularidades en la seguridad de la información plasmado en varios métodos de seguridad para resguardarla. Así mismo, el Plan de Tratamiento de Riesgos, posibilitó la reducción de los niveles de riesgos de los activos de información, respecto a las amenazas y vulnerabilidades en la institución, esto plasmado en una metodología para mitigarlos a través de actividades y poder minimizar los impactos a los activos de información. (Delgado y Vásquez, 2020)

Por este motivo contamos como antecedentes el proyecto mencionado ya que, dentro de la aplicación del modelo, toman la gestión de usuarios en el plan de los riesgos implementado en la compañía.

Según el trabajo de investigación "Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la municipalidad distrital de José Crespo Y Castillo -Aucayacu", que es una tesis para optar el título de profesional de ingeniero de sistemas en Chimbote 2018. El objetivo del proyecto es la evaluación de la implementación del sistema de gestión de seguridad informática en la compañía basados en la norma, analizar las inseguridades que tiene actualmente la información, evaluar los marcos teóricos referenciales para ayudar a optimizar la seguridad de la información proponiendo la aplicación de la norma para mejorar la seguridad en el área de tecnología (…) como conclusiones se puede observar que el 85.50% de los trabajadores encuestados expresaron la necesidad de implementar un Sistema de gestión de la seguridad de la información, motivo a que no se encuentra implementado, mientras que un 14.5%, señalo que si existen procesos implementados (…) por lo descrito en la presente tesis ayudara a mejorar la gestión de los activos reduciendo las probabilidades de riesgos y mitigando los impactos que se podrían generar por una mala gestión de activos, los activos soportan los sistemas de información y estos son de vital importancia para el crecimiento empresarial. (Davila, 2018)

Por este motivo estamos tomando este proyecto como antecedente porque dentro de la norma ISO 27001 abarca los dominios aplicados a la empresa y dentro se encuentra el apartado de gestión de usuarios.

En el proyecto de un "Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la NTP ISO/IEC 27001 para la dirección de salud Virgen De Cocharcas – Chincheros" de la Universidad Nacional José María

Arguedas de la Facultad de Ingeniería para optar el título profesional de ingeniero de sistemas en APURÍMAC 2019. Como alcance de la norma solo aplicará para el proceso de gestión de la infraestructura tecnológica considerando los activos de información considerados como relevantes dentro del alcance, esto incluye el apartado A9 de la norma (…) debido al crecimiento de la entidad, la probabilidad de que la información sea interceptada, robada y/o modificada por personas inescrupulosas y sin autorización de acceso a esta, ha aumentado considerablemente. Esto resulta peligroso para la institución, ya que mucha de la información fundamental es importante para la realización de los procesos críticos del negocio puede ser vulnerada y amenazada ocasionando la interrupción de estos procesos; que conllevan, de esta manera retrasos en la ejecución de proyectos, toma de decisiones, etc. Como resultados tenemos de que se elaboró los controles de seguridad para minimizar los riesgos de los recursos activos y la información a los que se encuentra expuesta la Dirección de Salud Virgen de Cocharcas - Chincheros. Los controles de seguridad de la NTP - ISO/IEC 27001, nos permiten establecer métricas que ayudan a medir la eficacia y eficiencia del SGSI (Sistema de Gestión de Seguridad de la Información), una vez implementados se logró determinar los procesos correspondientes al alcance del SGSI. (Escalante, 2019)

De acuerdo al presente trabajo, tomamos como antecedente ya que concluyen que uno de sus problemas es el peligro de que personas no autorizadas ingresen a la información de la compañía e implementando la norma ISO 27001 se puede minimizar los riesgos, esto incluyendo la gestión de usuarios que es parte de las dimensiones de la norma

1.2.3. Antecedentes locales

En el proyecto de "Diseño Para La Automatización Del Mantenimiento De Usuarios En El Proceso De Ceses Y La Reducción Del Riesgo De Fuga De Información En El Banco Financiero Del Perú" de la universidad Tecnológica del Perú de la Facultad de Ingeniería para obtener el título de Ingeniero de Sistemas e informática en Lima del 2018. En la compañía actualmente la baja de usuarios en el sistema se realiza de forma manual toma demasiado tiempo todo el proceso de cese de aproximado de 25 minutos, la propuesta es la centralización de automatizar el mantenimiento de dichos usuarios de acuerdo a la norma técnica peruana alineado a la ISO 27001 de la gestión de acceso a usuarios. Se diseñó una automatización del mantenimiento de los usuarios para mejorar la eficiencia en tiempo de ejecución para evitar errores manuales. Como conclusiones se vio que el nuevo diseño automatizado del mantenimiento de Usuarios en el Proceso de Ceses mejora la eficiencia en la atención del servicio. Los resultados arrojan que la atención de un Cese disminuye en más del 50% del tiempo actual (…) se ha confirmado que el Nuevo Diseño automatizado del mantenimiento de Usuarios en el Proceso de Ceses reduce la carga Operativa del equipo Seguridad TI – Control de Accesos, con ello el tiempo que queda liberado puede invertirse en la atención de otros servicios que se prestan al Banco. (Acosta, 2018)

De acuerdo al presente trabajo, tomamos como antecedente ya que concluyen que un nuevo diseño para la automatización de usuarios en el proceso de Cese, mejoría la eficiencia de los servicios de la compañía relacionada a la implementación de la ISO 27001.

En el proyecto de la "Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa ESVICSAC, Callao" de la universidad César Vallejo de la escuela de posgrado para obtener el grado académico de Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la información de Lima – Perú 2020. En la implementación se actúa estableciendo acciones correctivas que permitan mejorar la implementación, ya que es necesario dar conformidad a una implementación culminada el cual debe de cumplir con el alcance debido mitigando vulnerabilidades y reduciendo los riesgos, por lo que en esta fase se da el ciclo de mejora continua, atendiendo las no conformidades. Como propuesta es las acciones que permitan implementar los controles de seguridad de la información para auditar los riesgos desarrollando políticas de controles para la compañía incluyendo el apartado 9 de gestión de usuarios de la norma ISO 27001. Se recomienda al Gerente de TI, implantará los cambios en todos los sistemas y procesos manuales que intervienen, y delegará la revisión del inventario de los activos, Se recomienda al auditor interno medir el desempeño del SGSI (Sistema de Gestión de Seguridad de la Información), para demostrar que la implementación haya sido de manera correcta y acorde a las necesidades de la institución. Como objetivo principal es la fijación de políticas que permitan establecer los lineamientos fundamentales de manera adecuada brindando continuidad de los servicios y mejorando las experiencias con los clientes y con el apoyo de los miembros de la alta dirección la implementación tendrá un peso crucial, para el uso y cumplimiento de la norma, en el trabajo expuestos. (Arias, 2020)

Tomamos como antecedente esta tesis ya que al implementar la ISO 27001 toma también el control de accesos y gestión de usuarios fijando políticas adecuadas para los lineamientos fundamentales de la institución.

1.3. Realidad problemática

1.3.1. Información de la Empresa

Securitas inició en Suecia en 1934. Desde esa fecha el Grupo Securitas ha sido un referente constante en el sector, convirtiéndose en el líder mundial en seguridad. En los años ochenta comienza su expansión internacional ganando presencia en 56 países hasta convertirse en líder mundial de la Seguridad Privada. En el año 2000 con la incorporación de APS, First Security y Burns, el Grupo pasó a liderar también el mercado norteamericano. Desde la llegada a nuestro país en el año 2007, Securitas ha brindado soluciones al mercado local, llegando así a convertirse en el referente de la industria.

Las actividades de Securitas se basan en tres valores fundamentales: Integridad, Eficacia y Servicio.

- **Integridad**: La integridad hace referencia a una conducta ética y honesta. Securitas es inflexible en sus demandas de integridad y veracidad, e insiste en el derecho de sus empleados a expresar abiertamente opiniones propias y en su deber de comunicar irregularidades u otra información relevante sin riesgo de represalias.
- **Eficacia**: La eficacia hace referencia a prestar atención de manera activa. Un empleado de Securitas debe siempre estar atento y poder observar, escuchar y hacer evaluaciones con el objetivo de proteger los locales y propiedad de nuestros clientes, y los valores y ética que Securitas representa.

- **Servicio**: El servicio hace referencia a estar preparados para prestar apoyo a nuestros clientes, compañeros y a otros que precisen asistencia.

SECURITAS utiliza como emblema de la organización: "Nosotros ayudamos a hacer de tu mundo un lugar más seguro"

Según su informe anual de sustentabilidad periodo 2020 demuestra tener un crecimiento constante entre sus competidores a nivel global de servicios se seguridad integral a nivel de ventas y personal entre sus diferentes sedes (Figura 7). El potencial de crecimiento radica en ofrecer una gama completa de seguridad servicios, incluida la tecnología, que se pueden agrupar en soluciones personalizadas para sus clientes:

Figura 7. Tamaños de mercado para servicios de seguridad 2020.
Fuente: https://annualreport.securitas.com/

La implementación de controles según la NTP-ISO/IEC 27001:2014, surge como alternativa para evitar los accesos indebidos a los sistemas de información que posee la empresa, por lo que es necesario aplicar ciertos controles respectivos para poder salvaguardar el activo más importante la organización que es la información.

Sin embargo, los controles no solamente deben de ser a nivel técnico, sino que también deben de estar acompañadas por una serie de buenas prácticas de la gestión seguridad informática cumpliendo con el estándar a modo de asegurar la información y la continuación del negocio ya que es pieza fundamental en cualquier compañía.

Es necesario un buen funcionamiento de los accesos a los diferentes sistemas de información evitando los accesos no aprobados y los no deseados por cualquier persona externa a la compañía. A nivel global la importancia hacia la seguridad de la información es cada vez más tendencia debido a los accesos indebidos y hackeos. (Figura 8)

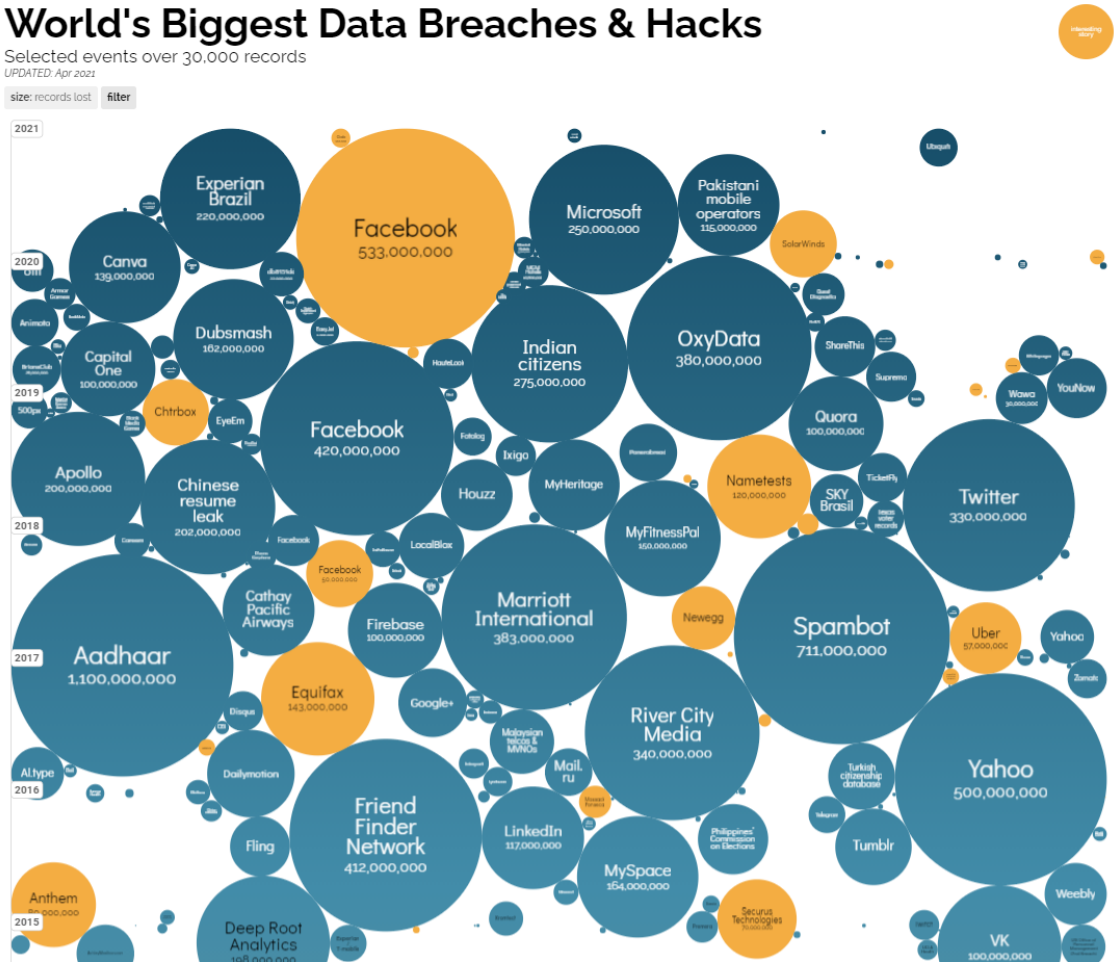


Figura 8. Infracciones de datos y hackeos de datos más grandes del mundo (2015-2021).

Fuente: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Actualmente uno de los principales problemas que tiene SECURITAS SAC es la falta de controles en la gestión de accesos que pone en riesgo a la organización en ataques informáticos por accesos indebidos, ocasionando interrupciones en sus procesos basados en los sistemas que este maneja a nivel de red, sistemas operativos y aplicaciones.

Si bien SECURITAS SAC cuenta con políticas y procesos establecidos para sus accesos estos no cuentan con el nivel de madurez suficiente para asegurar la seguridad de la información de sus sistemas y aplicaciones. Entre los sistemas de información que utiliza son:

Tabla 2.

Lista de sistemas de información considerados como activos

ID	Nombre del Sistema	Activo	Criticidad
SIS001	ERP	Información corporativa	High
SIS002	Securitas Vision	Información de Clientes	High
SIS003	SGH	Información Financiera	High
SIS004	SGM	Información Clientes	High
SIS005	Securitas Connect	Información gerencial	High
SIS006	Smart Boleta Suit	Información de Empleados	High
SIS007	Solicitud de Dinero 1.0	Información Financiera	High
SIS008	Facturación Electrónica	Información Financiera	High
SIS009	IMMIX (Securitas Pro)	Información de Seguridad	High
SIS010	Milestone	Información de Seguridad	High
SIS011	ScaleFusion	Información Tecnológica	High
SIS012	GLOBAL AVL	Información de Seguridad	High
SIS013	Mastermind Monitoring	Información de Seguridad	High
SIS014	Contratos NOE	Información Legal	High
SIS015	OKTA	Información Tecnológica	High
SIS016	VEAMS BACKUP	Información Tecnológica	High
SIS017	FORTIGATE VPN	Información Tecnológica	High
SIS018	ARUBA CONTROLLER	Información Tecnológica	High
SIS019	ACTIVE DIRECTORY	Información Tecnológica	High
SIS020	CORREO ELECTRONICO	Información Tecnológica	High
SIS021	Portal de Incidencias V0.1.10	Información tecnológica	Low
SIS022	FreshDesk	Información tecnológica	Low

SIS023	Web Vacaciones	Información Financiera	Low
SIS024	Securitas Solutions Tool (SST)	Información de riesgos	Low
SIS025	OFFISIS	Información corporativa	Low
SIS026	ONOFF	Información de Empleados	Medium
SIS027	PRTG	Información tecnológica	Medium
SIS028	Thuban	Información de Empleados	Medium
SIS029	QlikeView	Información Financiera	Medium
SIS030	PowerBi	Información Financiera	Medium
SIS031	CRM Dynamics	Información Comercial	Medium
SIS032	ServisNow	Información tecnológica	Medium
SIS033	SUTRAN	Información Vehicular	Medium
SIS034	mylearning Securitas	Información de Empleados	Medium
SIS035	HFM	Información Financiera	Medium
SIS036	GARIS	Información Legal	Medium

Entre las principales deficiencias que podemos mencionar en la gestión de accesos son las siguientes:

- Cumplimiento parcial de controles de accesos según la NTP-ISO/IEC 27001:2014.
- Los sistemas de información (sistemas y aplicaciones) no cuentan con procedimientos técnicos suficientes para el control de accesos.
- No existe una política formal basada en procesos que este correctamente documentada y normalizada por la organización para la gestión de accesos de forma general y específica para cada sistema.
- No existe una correcta capacitación al usuario sobre la gestión de accesos y sus responsabilidades con los sistemas de acceso.
- No existe una correcta asignación de roles y perfiles de usuarios por cada sistema de información.

1.4. Formulación del problema

1.4.1. Problema General

¿Cuál es el impacto en la implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021?

1.4.2. Problema especifico

- PE1: ¿De qué manera impacta la implementación de controles según la NTP-ISO/IEC 27001:2014 en las políticas de acceso a usuarios de la empresa SECURITAS SAC en Lima 2021?
- PE2: ¿De qué manera impacta la implementación de controles según la NTP-ISO/IEC 27001:2014 en la administración de acceso a usuarios de la empresa SECURITAS SAC en Lima 2021?
- PE3: ¿De qué manera impacta la implementación de controles según la NTP-ISO/IEC 27001:2014 en la responsabilidad de usuarios de la empresa SECURITAS SAC en Lima 2021?
- PE4: ¿De qué manera impacta la implementación de controles según la NTP-ISO/IEC 27001:2014 en acceso a sistemas y aplicativos de la empresa SECURITAS SAC en Lima 2021?

1.5. Objetivos

1.5.1. Objetivo general

La implementación de controles según la NTP-ISO/IEC 27001:2014 para mejorar el proceso de la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

1.5.2. Objetivo especifico

- OE1: Determinar el impacto de la implementación de controles según la NTP-ISO/IEC 27001:2014 en las políticas de acceso de la gestión de accesos de la empresa SECURITAS SAC en Lima 2021
- OE2: Determinar el impacto de la implementación de controles según la NTP-ISO/IEC 27001:2014 en la administración de acceso a usuarios de la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.
- OE3: Determinar el impacto de la implementación de controles según la NTP-ISO/IEC 27001:2014 en la responsabilidad de usuarios de la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.
- OE4: Determinar el impacto de la implementación de controles según la NTP-ISO/IEC 27001:2014 en el acceso a sistemas y aplicativos de gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

1.6. Hipótesis

1.6.1. Hipótesis general

La implementación de controles según la NTP-ISO/IEC 27001:2014 mejorará el proceso de la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

1.6.2. Hipótesis especifica

- HE1: La implementación de controles según la NTP-ISO/IEC 27001:2014 mejorará las políticas de acceso en la gestión accesos de la empresa SECURITAS SAC en Lima 2021.

- HE2: La implementación de controles según la NTP-ISO/IEC 27001:2014 mejorará la administración de usuarios en la gestión accesos de la empresa SECURITAS SAC en Lima 2021.
- HE3: La implementación de controles según la NTP-ISO/IEC 27001:2014 aumentará la responsabilidad de usuarios en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.
- HE4: La implementación de controles según la NTP-ISO/IEC 27001:2014 mejorará los accesos a sistemas y aplicativos en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

1.7. Justificación

Nuestra investigación aplica en referencia a los controles definidos en el estándar ISO/IEC 27001:2013 referidos a los controles de acceso de la sección A9 tomando en cuenta el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición" (Presidencia del Consejo de ministros, 2016), según resolución N.º 004-2016-PCM en todas las entidades integrantes del Sistema Nacional de Informática dentro de las cuales se encuentra SECURITAS SAC.

La presente investigación se justifica en que ayudará a analizar la seguridad de la Información según los controles definidos en la NTP ISO/IEC 27001:2014 con enfoque al control de accesos e implementar mejoras a la Seguridad de la Información de la gestión de accesos en SECURITAS SAC con enfoque a las políticas de acceso,

administración de usuarios, responsabilidad de los usuarios y accesos a los sistemas y aplicaciones.

1.8. Operacionalización de variables

A. Variable independiente

Controles de acceso

B. Variable dependiente

Gestión de accesos

Tabla 3.

Operacionalización de la variable dependiente

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS
Gestión de Accesos	Es el proceso responsable de permitir que los usuarios hagan uso de los servicios de TI, datos u otros activos. Gestión de acceso ayuda a proteger la confidencialidad, integridad y disponibilidad de los activos, garantizando que sólo los usuarios autorizados pueden accederlos o modificarlos. (ITIL®4, 2019)	Otorgar el derecho a un servicio a usuarios autorizados, mientras se previene el acceso de usuarios no autorizados. Los procesos de gestión del acceso ponen en práctica las políticas definidas por la gestión de seguridad de TI. La gestión del acceso también es conocida como gestión de derechos o gestión de identidad. (ITIL®4, 2019)	Políticas de Acceso a Usuario	- Porcentaje y grado de cumplimiento.	Procedimientos relacionados al control "A.9.1 Requisitos de la empresa para el control de acceso"
			Administración de Accesos a Usuarios	- Porcentaje y grado de cumplimiento.	Procedimientos relacionados al control "A.9.2 Gestión de acceso de usuario"
			Responsabilidades de Acceso a Usuarios	- Porcentaje y grado de cumplimiento.	Procedimientos relacionados al control "A.9.3 Responsabilidades de los usuarios"
			Accesos a Sistemas y Aplicativos	- Porcentaje y grado de cumplimiento.	Procedimientos relacionados al control "A.9.4 Control de acceso a sistema y aplicación"

Tabla 4.

Operacionalización de la variable independiente

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS
Controles de Acceso	El control de acceso se refiere a los mecanismos y técnicas que se utilizan para garantizar que el acceso a los activos esté autorizados y restringido según los requisitos de organización y seguridad. (Antonucci, 2013).	El control de acceso es un requisito previo fundamental para asegurar la información o los servicios en los sistemas de procesamiento de información, y también es necesario para proteger las instalaciones físicas que contienen información en todas sus formas. Están en juego la confidencialidad, integridad y disponibilidad de la información, los servicios y los procesos comerciales de la organización, junto con otros activos comerciales. (Bridget, 2019)	Protección de datos	Confidencialidad	Controles de Acceso (A9) A.9.1.1 Política de control de acceso A.9.1.2 Acceso a redes y servicios de red A.9.2.1 Registro de usuarios y anulación de registro A.9.2.2 Aprovisionamiento de acceso de usuario A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso del usuario A.9.2.6 Eliminación o ajuste de los derechos de acceso A.9.3.1 Uso de información secreta de autenticación A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimientos de inicio seguro A.9.4.3 Sistema de gestión de contraseñas A.9.4.4 Uso de programas de utilidad privilegiada A.9.4.5 Control de acceso al código fuente del programa
			Exactitud	Integridad	
			Acceso a la información	Disponibilidad	

CAPÍTULO II. MÉTODO

2.1. Métodos y análisis

2.1.1. Tipo de investigación

Según Ortega (2017) afirma:

> La investigación explicativa requiere la combinación de los métodos analítico y sintético, en conjugación con el deductivo y el inductivo, se trata de responder o dar cuenta de los porqués del objeto que se investiga. (…) Es fundamental comprender, que los resultados de una investigación pueden o no satisfacer las hipótesis de investigación; sea cual fuere la situación, los resultados deben ser publicados, para que la comunidad científica acceda y tenga una referencia sobre la investigación realizada, con el propósito de comparar y discutir sus propios resultados.

La implementación de controles busca mejorar la seguridad en los controles de accesos de los activos de información de la compañía y se enfoca en analizar y encontrar los riesgos y vulnerabilidades en el proceso de gestión de accesos revisando su situación actual en el manejo de controles y así mitigar los riesgos de seguridad de la información en la gestión de accesos y dejar la información lista para ser aprovechada por la empresa.

2.1.2. Diseño de la investigación

No experimental, según Vásquez (2020) afirma:

> Los diseños no experimentales, no tienen determinación aleatoria, manipulación de variables o grupos de comparación. El investigador observa lo que ocurre de forma natural, sin intervenir de manera alguna. Existen muchas razones para realizar este tipo de estudio. Primero, un número de

características o variables no están sujetas, o no son receptivas a manipulación experimental. Así como, por consideraciones éticas, algunas variables no pueden o no deben ser manipuladas. En algunos casos, las variables independientes aparecen y no es posible establecer un control sobre ellas.

2.1.3. Método de la investigación

Cuantitativo, según Neill y Suarez (2018) mencionan:

> El objetivo de una investigación cuantitativa es adquirir conocimientos fundamentales y la elección del modelo más adecuado que nos permita conocer la realidad de una manera más imparcial, ya que se recogen y analizan los datos a través de los conceptos y variables medibles. La investigación cuantitativa es una forma estructurada de recopilar y analizar datos obtenidos de distintas fuentes, lo que implica el uso de herramientas informáticas, estadísticas, y matemáticas para obtener resultados. Es concluyente en su propósito ya que trata de cuantificar el problema y entender qué tan generalizado está mediante la búsqueda de resultados proyectables a una población mayor. (p.69)

Se medirá los eventos (antes y después) en el proceso de gestión de accesos en base a indicadores en la investigación, utilizando datos, encuestas, entrevistas, información y otras herramientas para conocer el resultado final mediante técnicas estadísticas.

2.1.4. Población

La población según Salazar y Castillo (2018) mencionan:

> Es el colectivo que abarca a todos los elementos cuya característica o características queremos estudiar; dicho de otra manera, es el conjunto entero al que se desea describir o del que se necesita establecer conclusiones.

Según nuestra investigación la población se constituye de los sistemas de información que cuenten con información sensible para la empresa SECURITAS SAC y que se encuentren actualmente involucrados con los procesos de gestión de accesos. Nuestra población de acuerdo al significado son los siguientes:

- 36 sistemas que cuentan con información sensible para la empresa y están involucrados con el proceso de gestión de accesos
- Sistemas en producción de la empresa Securitas SAC.
- En Perú.

2.1.5. Muestra

La muestra según Salazar y Castillo (2018) mencionan:

> Es un conjunto de elementos seleccionados de una población de acuerdo a un plan de acción previamente establecido (muestreo), para obtener conclusiones que pueden ser extensivas hacia toda la población.

De acuerdo con la explicación anterior, tenemos la siguiente forma de la muestra:

- 10 aplicativos de la empresa, según su categorización de importancia, en este tipo será "alta" (High).

Tabla 5. .

Muestra de sistemas de información SECURITAS SAC.

ID	Nombre del sistema	Activo	Criticidad
SIS001	ERP	Información corporativa	High
SIS002	Securitas Vision	Información de Clientes	High
SIS003	SGH	Información Financiera	High
SIS004	SGM	Información Clientes	High

SIS005	Securitas Connect	Información gerencial	High
SIS006	Smart Boleta Suit	Información de Empleados	High
SIS007	Solicitud de Dinero 1.0	Información Financiera	High
SIS008	Facturación Electrónica	Información Financiera	High
SIS014	Contratos NOE	Información Legal	High
SIS021	Web Vacaciones	Información Financiera	High
SIS035	ACTIVE DIRECTORY	Información Tecnológica	High

2.1.5.1. Muestreo

El muestreo según Salazar y Castillo (2018) mencionan:

> Es la técnica que nos permite seleccionar muestras adecuadas de una población de estudio. El muestreo debe conducir a la obtención de una muestra representativa de la población de donde proviene, esta condición establece que cada elemento de la población tiene la misma probabilidad de ser incluida en la muestra.

2.1.5.2. Muestreo no Probabilístico

El muestreo no probabilístico según Hernández y Carpio (2019) afirman:

> En los métodos no probabilísticos se seleccionan cuidadosamente a los sujetos de la población utilizando criterios específicos, buscando hasta donde sea posible representatividad. Aun así, no se utilizan para la inferencia de resultados sobre la población. Es necesario conocer y evitar el error de muestreo. Esto es hacer conclusiones muy generales a partir de la observación de solo una parte de la población y el error de inferencia en el que se hacen conclusiones hacia una población mucho más grande de la que originalmente se tomó la muestra.

2.1.6. Técnicas de recolección de datos e instrumentos

2.1.6.1. Indicadores

- **Porcentaje y grado de cumplimiento de políticas de acceso.**

Definimos porcentaje de cumplimiento de las políticas de acceso que tienen implementadas la compañía, suma (suma (Total de valores según nivel*nivel de madurez según su nivel) /total de valores) * 100, de acuerdo a la herramienta de juicio de expertos, se valida el siguiente indicador: "Porcentaje y grado de cumplimiento de políticas de acceso", se utilizó una ficha de evaluación de expertos que valida correctamente dicha información brindada por el indicador.

- **Porcentaje y grado de cumplimiento de procedimientos de administración de accesos a usuarios.**

  Definimos porcentaje de cumplimiento de administración de accesos a usuarios que tienen implementadas la compañía suma (suma(Total de valores según nivel*nivel de madurez según su nivel)/total de valores) * 100, de acuerdo a la herramienta de juicio de expertos, se valida el siguiente indicador: "Porcentaje y grado de cumplimiento de procedimientos de administración de accesos a usuarios", se utilizó una ficha de evaluación de expertos que valida correctamente dicha información brindada por el indicador.

- **Porcentaje y grado de cumplimientos de procedimientos de responsabilidades de Usuario.**

  Definimos porcentaje de cumplimiento de responsabilidad de usuarios que tienen implementadas la compañía, (suma (Total de valores según nivel*nivel de madurez según su nivel) /total de valores) * 100, de acuerdo a la herramienta de juicio de expertos, se valida el siguiente indicador: "Porcentaje y grado de cumplimientos de procedimientos de responsabilidades de Usuario", se utilizó una ficha de evaluación de expertos que valida correctamente dicha información brindada por el indicador.

- **Porcentaje y grado de cumplimiento de Accesos a Sistemas y aplicativos.**

Definimos porcentaje de cumplimiento de accesos a sistemas y aplicaciones que tienen implementadas la compañía, (suma (Total de valores según nivel*nivel de madurez según su nivel) /total de valores) * 100, de acuerdo a la herramienta de juicio de expertos, se valida el siguiente indicador: "Porcentaje y grado de cumplimiento de Acceso a Sistemas y aplicativos", se utilizó una ficha de evaluación de expertos que valida correctamente dicha información brindada por el indicador.

2.1.6.2. Instrumentos de recolección de datos

Según lo explicado por Torres, Salazar y Paz (2019) aseguran: "Para la recolección de datos primarios en una investigación científica se procede básicamente por observación, por encuestas o entrevistas a los sujetos de estudio y por experimentación" (p.4).

Se procedió a realizar una encuesta para obtener los datos relacionados a los sistemas de información que manejan en el área de administración de TI. (Anexo 2)
Luego de la observación de los datos recolectados se procedió al registro de la información a través de las fichas de registro que se presentan a continuación:

Ficha de registro de datos de investigacion - PRE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	PRE-TEST	**Fecha de inicio**	1/6/2021	**Fecha de Final**	30/6/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Politicas de acceso a usuario	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = (Sumatoria (MA*VC) / Total)*100 MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	0	2	0	0	0	0	2	25%
SIS002	2	0	0	0	0	0	2	0%
SIS003	2	0	0	0	0	0	2	0%
SIS004	2	0	0	0	0	0	2	0%
SIS005	2	0	0	0	0	0	2	0%
SIS006	0	1	1	0	0	0	2	38%
SIS007	2	0	0	0	0	0	2	0%
SIS014	0	1	1	0	0	0	2	38%
SIS021	2	0	0	0	0	0	2	0%
SIS035	0	0	1	1	0	0	2	63%

Figura 9. Ficha de registro de datos – PRE TEST – Políticas de acceso a usuario.

Ficha de registro de datos de investigacion - PRE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	PRE-TEST	**Fecha de inicio**	1/6/2021	**Fecha de Final**	30/6/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Administracion de acceso a usuarios	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	3	0	3	1	0	0	7	32%
SIS002	5	0	2	0	0	0	7	14%
SIS003	4	3	0	0	0	0	7	11%
SIS004	4	3	0	0	0	0	7	11%
SIS005	4	1	2	0	0	0	7	18%
SIS006	1	2	2	0	0	2	7	21%
SIS007	5	1	1	0	0	0	7	11%
SIS014	1	2	2	0	0	2	7	21%
SIS021	6	1	0	0	0	0	7	4%
SIS035	3	1	1	2	0	0	7	32%

Figura 10. Ficha de registro de datos – PRE TEST – Administración de acceso a usuarios.

Ficha de registro de datos de investigacion - PRE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	PRE-TEST	**Fecha de inicio**	1/6/2021	**Fecha de Final**	30/6/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Responsabilidad de acceso de usuarios	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	2	0	0	0	0	0	2	0%
SIS002	2	0	0	0	0	0	2	0%
SIS003	2	0	0	0	0	0	2	0%
SIS004	2	0	0	0	0	0	2	0%
SIS005	1	1	0	0	0	0	2	13%
SIS006	1	0	1	0	0	0	2	25%
SIS007	2	0	0	0	0	0	2	0%
SIS014	0	1	1	0	0	0	2	38%
SIS021	2	0	0	0	0	0	2	0%
SIS035	1	1	0	0	0	0	2	13%

Figura 11. Ficha de registro de datos – PRE TEST – Responsabilidad de acceso a usuarios.

Ficha de registro de datos de investigacion - PRE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	PRE-TEST	**Fecha de inicio**	1/6/2021	**Fecha de Final**	30/6/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Acceso a sistemas y aplicaciones	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	3	1	0	0	0	1	5	5%
SIS002	2	2	0	0	0	1	5	10%
SIS003	2	2	0	0	0	1	5	10%
SIS004	2	2	0	0	0	1	5	10%
SIS005	2	1	1	0	0	1	5	15%
SIS006	1	1	2	0	0	1	5	25%
SIS007	3	0	1	0	0	1	5	10%
SIS014	1	1	2	0	0	1	5	25%
SIS021	3	0	1	0	0	1	5	10%
SIS035	0	2	1	1	0	1	5	35%

Figura 12. Ficha de registro de datos – PRE TEST – Acceso a sistemas y aplicaciones.

Ficha de registro de datos de investigacion - RE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	RE-TEST	**Fecha de inicio**	1/8/2021	**Fecha de Final**	31/8/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Politicas de acceso a usuario	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = (Sumatoria (MA*VC) / Total)*100 MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	0	2	0	0	0	0	2	25%
SIS002	2	0	0	0	0	0	2	0%
SIS003	2	0	0	0	0	0	2	0%
SIS004	2	0	0	0	0	0	2	0%
SIS005	2	0	0	0	0	0	2	0%
SIS006	0	1	1	0	0	0	2	38%
SIS007	2	0	0	0	0	0	2	0%
SIS014	0	1	1	0	0	0	2	38%
SIS021	2	0	0	0	0	0	2	0%
SIS035	0	0	1	1	0	0	2	63%

Figura 13. Ficha de registro de datos – RE TEST – Políticas de acceso a usuario.

Ficha de registro de datos de investigacion - RE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	RE-TEST	**Fecha de inicio**	1/8/2021	**Fecha de Final**	31/8/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Administracion de acceso a usuarios	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	3	0	3	1	0	0	7	32%
SIS002	5	0	2	0	0	0	7	14%
SIS003	3	4	0	0	0	0	7	14%
SIS004	4	3	0	0	0	0	7	11%
SIS005	3	2	2	0	0	0	7	21%
SIS006	1	2	2	0	0	2	7	21%
SIS007	5	1	1	0	0	0	7	11%
SIS014	2	2	2	0	0	1	7	21%
SIS021	6	1	0	0	0	0	7	4%
SIS035	2	2	1	2	0	0	7	36%

Figura 14. Ficha de registro de datos – RE TEST – Administración de acceso a usuarios

Ficha de registro de datos de investigacion - RE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	RE-TEST	**Fecha de inicio**	1/8/2021	**Fecha de Final**	31/8/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Responsabilidad de acceso de usuarios	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	2	0	0	0	0	0	2	0%
SIS002	2	0	0	0	0	0	2	0%
SIS003	2	0	0	0	0	0	2	0%
SIS004	2	0	0	0	0	0	2	0%
SIS005	1	1	0	0	0	0	2	13%
SIS006	1	0	1	0	0	0	2	25%
SIS007	2	0	0	0	0	0	2	0%
SIS014	0	1	1	0	0	0	2	38%
SIS021	2	0	0	0	0	0	2	0%
SIS035	1	1	0	0	0	0	2	13%

Figura 15. Ficha de registro de datos – RE TEST – Responsabilidad de acceso a usuarios.

Ficha de registro de datos de investigacion - RE TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	RE-TEST	**Fecha de inicio**	1/8/2021	**Fecha de Final**	31/8/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Acceso a sistemas y aplicaciones	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	3	1	0	0	0	1	5	5%
SIS002	2	2	0	0	0	1	5	10%
SIS003	2	2	0	0	0	1	5	10%
SIS004	2	2	0	0	0	1	5	10%
SIS005	2	1	1	0	0	1	5	15%
SIS006	1	1	2	0	0	1	5	25%
SIS007	3	0	1	0	0	1	5	10%
SIS014	1	1	2	0	0	1	5	25%
SIS021	3	0	1	0	0	1	5	10%
SIS035	0	2	1	1	0	1	5	35%

Figura 16. Ficha de registro de datos – RE TEST – Acceso a sistemas y aplicaciones.

Ficha de registro de datos de investigacion - POST TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	POST-TEST	**Fecha de inicio**	1/9/2021	**Fecha de Final**	30/9/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Politicas de acceso a usuario	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = (Sumatoria (MA*VC) / Total)*100 MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	0	0	0	0	2	0	2	100%
SIS002	0	0	0	2	0	0	2	75%
SIS003	0	0	0	0	2	0	2	100%
SIS004	0	0	0	0	2	0	2	100%
SIS005	0	0	0	0	2	0	2	100%
SIS006	0	0	0	0	2	0	2	100%
SIS007	0	0	0	0	2	0	2	100%
SIS014	0	0	0	0	2	0	2	100%
SIS021	0	0	0	0	2	0	2	100%
SIS035	0	0	0	0	2	0	2	100%

Figura 17. Ficha de registro de datos – POST TEST – Políticas de acceso a usuario.

Ficha de registro de datos de investigacion - POST TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	POST-TEST	**Fecha de inicio**	8/11/2021	**Fecha de Final**	12/11/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Administracion de acceso a usuarios	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	0	0	0	5	2	0	7	82%
SIS002	0	0	0	2	5	0	7	93%
SIS003	0	0	0	4	3	0	7	86%
SIS004	0	0	0	6	1	0	7	79%
SIS005	0	0	0	2	5	0	7	93%
SIS006	0	0	0	3	2	2	7	61%
SIS007	0	0	0	4	3	0	7	86%
SIS014	0	0	0	3	2	2	7	61%
SIS021	0	0	0	5	2	0	7	82%
SIS035	0	0	0	3	4	0	7	89%

Figura 18. Ficha de registro de datos – POST TEST – Administración de acceso a usuarios

Ficha de registro de datos de investigacion - POST TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	POST-TEST	**Fecha de inicio**	8/11/2021	**Fecha de Final**	12/11/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Responsabilidad de acceso de usuarios	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	0	0	0	1	1	0	2	88%
SIS002	0	0	0	0	2	0	2	100%
SIS003	0	0	0	1	1	0	2	88%
SIS004	0	0	0	1	1	0	2	88%
SIS005	0	0	0	2	0	0	2	75%
SIS006	0	0	0	2	0	0	2	75%
SIS007	0	0	0	1	1	0	2	88%
SIS014	0	0	0	1	1	0	2	88%
SIS021	0	0	0	1	1	0	2	88%
SIS035	0	0	0	1	1	0	2	88%

Figura 19. Ficha de registro de datos – POST TEST – Responsabilidad de acceso a usuarios.

Ficha de registro de datos de investigacion - POST TEST							
Encargado	Yonathan Montenegro	**Tipo de prueba**	POST-TEST	**Fecha de inicio**	8/11/2021	**Fecha de Final**	12/11/2021
Motivo de la investigacion	Toma de valores de cuestionario de procedimientos de controles de acceso.						

Variable	Dimension	Indicador	Instrumento	Formula
Gestion de acceso	Acceso a sistemas y aplicaciones	Cálculo de grado cumplimiento según procedimientos	Cuestionario	GR = Sumatoria (MA*VC) / Total MA = Grado de madurez GR = Grado de cumplimiento VC = Valor cualitativo PO = Procedimiento Optimo PG = Procedimiento Gestionado PD = Procedimiento definido PI = Procedimiento Inicial PN = Procedimiento no existe NA = No aplica

Valor cualitativo	No se realiza (PN)	Inicial (PI)	Definido (PD)	Gestionado (PG)	Optimo (PO)	No aplica (NA)	Total	Grado de cumplimiento (GR)
% Madurez	0%	25%	50%	75%	100%			
SIS001	0	0	0	1	3	1	5	75%
SIS002	0	0	0	1	3	1	5	75%
SIS003	0	0	0	1	3	1	5	75%
SIS004	0	0	0	1	3	1	5	75%
SIS005	0	0	0	2	2	1	5	70%
SIS006	0	0	0	1	3	1	5	75%
SIS007	0	0	0	1	3	1	5	75%
SIS014	0	0	0	1	3	1	5	75%
SIS021	0	0	0	1	3	1	5	75%
SIS035	0	0	0	0	4	1	5	80%

Figura 20. Ficha de registro de datos – POST TEST – Acceso a sistemas y aplicaciones.

2.1.7. Procedimiento

En la investigación se obtuvo la información mediante la recolección de datos para para lo cual utilizamos cuestionarios de tipo cuantitativo de data tipo ordinal basado en respuestas según un nivel de madurez. Lo siguiente consistió en analizar las fórmulas, tablas de frecuencia e indicadores de grados de cumplimento mediante las herramientas Excel y el software SPSS v.28.

Para el contraste de la hipótesis utilizaremos la prueba correspondiente al tipo de investigación luego de validar su normalidad y así poder evaluar la hipótesis en nuestra variable y sus dimensiones obteniendo los datos de frecuencia mediante técnicas de estadística.

2.1.8. Validez y confiabilidad del instrumento

2.1.8.1. Validez

La validez según Keever y Márquez (2018) mencionan:

> El concepto de validez en investigación se refiere a lo que es verdadero o lo que se acerca a la verdad. En general se considera que los resultados de una investigación serán válidos cuando el estudio está libre de errores. Para establecer si un determinado estudio es válido, se debe analizar la presencia de sesgos (errores sistemáticos) como mínimo en los siguientes puntos: el diseño de investigación, los criterios de selección y la forma de llevar a cabo las mediciones, es decir, la manera de registrar y evaluar las variables de estudio. De esta forma, se considera que un estudio tiene validez interna cuando está libre de sesgos.

Presentamos la validez por expertos (Anexo 3) de nuestras tablas para los indicadores de nuestras dimensiones referidas según las fichas Políticas de accesos,

Administración de acceso a usuarios, Responsabilidad de usuarios y Acceso a sistemas y aplicaciones en distintos tiempos (PRE-TEST, RE-TEST, POST TEST).

Tabla 6.

Resumen de resultados de valoración de expertos

DNI	Experto	Grado	Fichas PRE-TEST	Fichas RE-TEST	Fichas POST-TEST
40643722	Karen Rocio García Vera Tudela	Magister	75%	76%	92%
46840169	Roldan Palacios Christian Jonatan	Magister	74%	75%	92%
41297935	Dante Miguel Uechi Ota	Ingeniero	75%	76%	88%

En conclusión, tenemos la validez aprobatoria suficiente en promedio de 80.3% lo cual se ubica en la clasificación de "Muy bueno". Asimismo, no contamos con observaciones para su aplicabilidad.

2.1.8.2. Confiabilidad

La confiabilidad según León y Arancibia (2017) definen "La confiabilidad y validez son propiedades importantes de ser reportadas porque permite al lector conocer el nivel de precisión y evidencia de los instrumentos utilizados, que derivarán en conclusiones coherentes en el estudio".

- **Método RETEST**

El método RETEST según Galindo (2020) afirma:

> Respecto al test-retest, como bien dice el propio nombre, se basa en que un mismo test sea respondido en momentos diferentes por los mismos sujetos. El intervalo de tiempo que se debe dejar entre el primer momento y el segundo puede ir desde unos días hasta meses;

aunque no es muy recomendable extenderlo en exceso, debido a que puede que los sujetos cambien sus maneras de pensar. (p.56)

Tomando en cuenta el enunciado anterior del método RETEST podremos verificar la confiabilidad de nuestras muestras para el desarrollo de los indicadores relacionados a nuestras dimensiones, validadas por la correlación de PEARSON**.**

- **Correlación de PEARSON**

Según Lalinde, Castro, Rodríguez, Rangel, Sierra, Torrado y Pirela (2018) afirman:

> El coeficiente de correlación de Pearson es una medida considerablemente utilizada en diversas áreas del quehacer científico, desde estudios técnicos, econométricos o de ingeniería; hasta investigaciones relacionadas con las ciencias sociales, del comportamiento o de la salud. Es precisamente esta extensa y profusa divulgación una de las razones que explicaría el uso indebido que se le da a esta herramienta estadística, especialmente en aquellos escenarios en los que debe ser interpretada correctamente o en los que se tienen que comprobar las suposiciones matemáticas que la sustentan.

Según esto nos indican una tabla de valores para la correlación y su interpretación (Tabla *7*).

Tabla 7.

Tabla de valores de correlación de Pearson y su interpretación.

Valor	Significado
-1	Correlación negativa grande y perfecta
-0,9 a -0,99	Correlación negativa muy alta
-0,7 a -0,89	Correlación negativa alta
-0,4 a -0,69	Correlación negativa moderada
-0,2 a -0,39	Correlación negativa baja
-0,01 a -0,19	Correlación negativa muy baja
0	Correlación nula
0,01 a 0,19	Correlación positiva muy baja
0,2 a 0,39	Correlación positiva baja
0,4 a 0,69	Correlación positiva moderada
0,7 a 0,89	Correlación positiva alta
0,9 a 0,99	Correlación positiva muy alta
1	Correlación positiva grande y perfecta

Correlación de Pearson para indicador de grado de cumplimiento en dimensión Políticas de acceso (D1)

La correlación de Pearson para Pre-Test y Re-Test en el indicador grado de cumplimiento en dimensión de políticas de acceso (Tabla 8) es de r = 1,000 lo cual nos indica una correlación fuerte y nos brinda un nivel de confianza en los datos mostrados en ambas mediciones.

Tabla 8.

Correlaciones TEST/RETEST Políticas de acceso (D1)

Correlaciones			
		D1_PRE	D1_RE
D1_PRE	Correlación de Pearson	1	1.000**
	Sig. (bilateral)		.000
	N	10	10
D1_RE	Correlación de Pearson	1.000**	1

	Sig. (bilateral)	.000	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (bilateral).

Correlación de Pearson para indicador de grado de cumplimiento en dimensión Administración de acceso a usuario (D2)

La correlación de Pearson para Pre-Test y Re-Test en el indicador grado de cumplimiento en dimensión de administración de acceso a usuarios (Tabla 9) es de r = 0,798 lo cual nos da un nivel de confianza en la medición.

Tabla 9.

Correlaciones TEST/RETEST Administración de acceso a usuarios (D2)

Correlaciones			
		D2_PRE	D2_RE
D2_PRE	Correlación de Pearson	1	.798**
	Sig. (bilateral)		.006
	N	10	10
D2_RE	Correlación de Pearson	.798**	1
	Sig. (bilateral)	.006	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (bilateral).

Correlación de Pearson para indicador de grado de cumplimiento en dimensión Responsabilidad a usuarios (D3)

La correlación de Pearson para Pre-Test y Re-Test en el indicador grado de cumplimiento en dimensión de Responsabilidad a usuarios (Tabla 10) es de r = 1,000 lo cual nos da un nivel de confianza en la medición.

Tabla 10.

Correlaciones TEST/RETEST Responsabilidad a usuarios (D3)

Correlaciones			
		D3_PRE	D3_RE
D3_PRE	Correlación de Pearson	1	1.000**
	Sig. (bilateral)		.000
	N	10	10
D3_RE	Correlación de Pearson	1.000**	1
	Sig. (bilateral)	.000	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (bilateral).

Correlación de Pearson para indicador de grado de cumplimiento en dimensión Acceso a sistemas y aplicaciones (D4)

La correlación de Pearson para Pre-Test y Re-Test en el indicador grado de cumplimiento en dimensión de Acceso a sistemas y aplicaciones (Tabla 11) es de r = 1,000 lo cual nos da un nivel de confianza en la medición.

Tabla 11.

Correlaciones TEST/RETEST Acceso a sistemas y aplicaciones (D4)

Correlaciones			
		D4_PRE	D4_RE
D4_PRE	Correlación de Pearson	1	1.000**
	Sig. (bilateral)		.000
	N	10	10
D4_RE	Correlación de Pearson	1.000**	1
	Sig. (bilateral)	.000	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (bilateral).

2.2. Plan de implementación

Para nuestro plan hemos establecido los siguientes procesos según el ciclo Deming (PDCA) que conlleva la primera etapa de planificación:

- Ejecutar un análisis GAP (Análisis de brecha) para poder tener un conocimiento a nivel especifico y general de la situación actual de la organización con el uso y grado de cumplimiento interno de controles de acceso según la NTP-ISO/IEC 27001:2014 por cada sistema de información según nuestras dimensiones. A continuación, evaluar de la misma manera el grado de cumplimiento que se pretende alcanzar.
- Ejecutar un análisis de riesgo adaptado a la metodología MAGERIT para poder establecer la situación actual de los sistemas de información a nivel de valoración de activos, amenazas, riesgos y sus probabilidades e impactos. De esta manera podemos identificar a que activos y amenazas daremos prioridad de implementación en los procedimientos.
- Obteniendo los resultados del grado de cumplimiento actual y deseado, asimismo el plan de acción con los resultados del análisis GAP se complementará con los resultados del análisis de riesgo que nos indicarán a que activos debemos priorizar la implementación y también a que amenazas debemos enfocarnos. De esta manera se presentará la implementación (Figura 21).

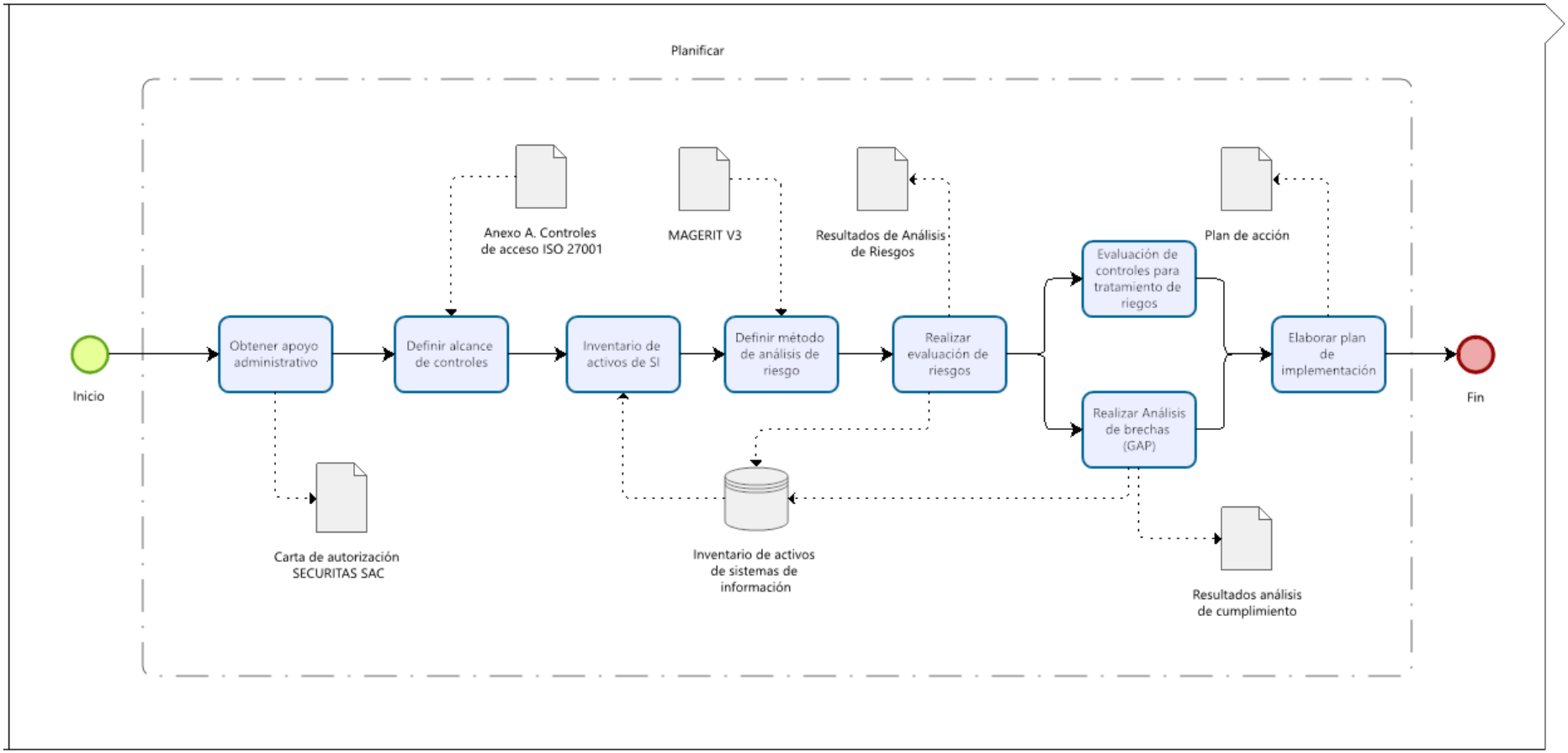


Figura 21. Diagrama de procesos de implementación.

2.2.1. Metodología de análisis de riesgos

Para establecer el análisis de riesgo en base a la metodología MAGERIT se estableció los siguientes objetivos:

- Determinar los activos de sistemas de información más críticos que cuenten con gestión de accesos como funcionalidades integras.
- Establecer las amenazas a las cuales se exponen los sistemas de información.
- Establecer las salvaguardas para estos activos.
- Estimar el impacto por la materialización de las amenazas.

Para la ejecución de esta etapa se recopilará la información por medio de encuestas, entrevistas a los usuarios, empleados responsables de los sistemas de información de SECURITAS SAC y se validará con evidencia de cada sistema (Anexo 4).

Con esta información se podrá evaluar el valor y su protección actual frente a amenazas relacionadas a la gestión de accesos.

2.2.1.1. Identificar activos

Según la Dirección General de Modernización Administrativa (2012) menciona:

> Lo esencial es siempre la información que se maneja y los servicios que se prestan. A veces nos interesa singularizar la diferente información y los diferentes servicios, mientras que otras veces podemos agrupar varias informaciones o varios servicios que son equivalentes a efectos de requisitos de seguridad. Incluso es frecuente hacer paquetes de {información + servicios} que la Dirección entiende como un uno. (p.87)

Se establecerá como activos a tomar para el contexto de la investigación que son los sistemas de información usados en SECURITAS SAC. Para poder evaluar

sus dependencias, valor, amenazas y salvaguardas (Anexo 5). Para la investigación se tomará en cuenta según el catálogo de elementos de MAGERIT los siguientes tipos de activos:

- [SW] Software - Aplicaciones informáticas
    - [prp] desarrollo propio (in house)
    - [sub] desarrollo a medida (subcontratado)

2.2.1.2. Valoración de los activos

Para esta etapa se estableció la tabla de nivel de valoración para los activos. (Anexo 6). Asimismo, de establecido las dimensiones relevantes para los activos. En este caso tomando como referencia a la variable independente referente a controles de acceso según la NTP-ISO/IEC 27001:

- [D] Disponibilidad
- [I] Integridad
- [C] Confidencialidad

2.2.1.3. Identificar amenazas

Según la Dirección General de Modernización Administrativa (2012) menciona:

> La tarea aparece como imposible: para cada activo, en cada dimensión, identificar amenazas. Se puede partir de la experiencia pasada, propia o de organizaciones similares. Lo que ha ocurrido puede repetirse y, en cualquier caso, sería impresentable no tenerlo en cuenta. Complementariamente, un catálogo de amenazas como el incluido en el "Catálogo de Elementos" ayuda a localizar lo que conviene considerar en función del tipo de activo y de las dimensiones en las que tiene un valor propio o acumulado. (p.93)

Según el catálogo de amenazas de MAGERIT utilizaremos las siguientes:

- [E] Errores y fallos no intencionados
- [A] Ataques intencionados
- [I] Desastres industriales

De las cuales vamos a relacionar las amenazas a cada activo seleccionado (Anexo 7).

2.2.1.4. Valoración del impacto

Se establece una tabla de valoración de los impactos (Tabla 12) en referencia a MAGERIT de acuerdo con la valoración de un impacto que tendría sobre el activo en la empresa SECURITAS SAC.

Tabla 12.
Estimación de impacto adaptado de MAGERIT V3

Valor cualitativo	Valor cuantitativo	Descripción
MA: casi seguro	5	La amenaza se materializa a lo sumo 1 vez a la semana
A: Muy alto	4	La amenaza se materializa a lo sumo una vez cada mes.
M: posible	3	La amenaza se materializa a lo sumo una vez cada medio año.
B: poco probable	2	La amenaza se materializa a lo sumo una vez cada año.
MB: muy raro	1	La amenaza no se ha materializado o máximo lo ha hecho una vez.

2.2.1.5. Valoración de probabilidad

Se establece una tabla de valoración de probabilidad (Tabla 13) en referencia a MAGERIT, de que se materialice una amenaza según la experiencia que haya tenido la empresa SECURITAS SAC con las amenazas relacionadas.

Tabla 13.
Estimación de probabilidad adaptado de MAGERIT V3.

Valor cualitativo	Valor cuantitativo	Descripción
MA: muy alto	5	El daño derivado de la materialización de la amenaza tiene consecuencias muy graves para la organización.

A: alto	4	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.
M: medio	3	El daño derivado de la materialización de la amenaza tiene consecuencias para la organización.
B: bajo	2	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
MB: muy bajo	1	El daño derivado de la materialización de la amenaza es totalmente inapreciable para la organización.

2.2.1.6. Valoración de riesgos

Luego de identificar los activos y a su vez asignarles un valor. Asimismo, identificar las amenazas y establecer un valor cuantitativo relacional entre probabilidad (Figura 23)e impacto de materialización se establece una tabla de valores de riesgo y sus umbrales (Figura 24). Es importante de la misma manera establecer los niveles de aceptación del riesgo (Figura 22) por parte de la empresa de esta manera saber que riesgos son los que se deberán procesar.

** Criterios de aceptacion del riesgo*

Validado por Gerente de Tecnología y procesos

Rango	Descripcion
Riesgo >=8	SECURITAS SAC considera el riesgo a consider a tratarse bajo un control.
Riesgo < 8	SECURITAS SAC considera el riesgo aceptable.

DNI: 40643722

Figura 22. Criterios de aceptación del riesgo.

Riesgo		Probabilidad				
		MB: muy raro	B: poco probable	M: posible	A: Muy alto	MA: casi seguro
Impacto	MA: muy alto	5	10	15	20	25
	A: alto	4	8	12	16	20
	M: medio	3	6	9	12	15
	B: bajo	2	4	6	8	10
	MB: muy bajo	1	2	3	4	5

Figura 23. Matriz de riesgos adaptado de MAGERIT V3.

Umbrales de riesgo		
Valor	Nivel	Descripcion
>=15	Muy alto	Riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona
>=8	Alto	Riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones
>=4	Medio	Riesgos improbables pero de muy alto impacto
>=1	Bajo	Riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno.

Figura 24. Umbrales de riesgo adaptado de MAGERIT V3.

Según los resultados de la valoración de riesgos se pudo establecer las prioridades de tratamiento a las amenazas según su nivel (Figura 25).

Tipo	Descripcion	Impacto	Probabilidad	Riesgo	Nivel prioridad	Accion
[I.5] Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	5	3	15	Muy alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[E.8] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	5	3	15	Muy alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[E.15] Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	4	3	12	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[E.1] Errores de los usuario	Equivocaciones de las personas cuando usan los servicios, datos, etc.	3	4	12	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[E.14] Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	4	2	8	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[E.21] Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	2	4	8	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[A.5] Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.	5	2	10	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[A.6] Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	4	2	8	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[A.8] Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc	5	2	10	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[A.11] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	5	2	10	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[A.15] Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio	4	2	8	Alto	Es necesario diseñar, documentar, implementar y supervisar un control de acceso.
[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	2	2	4	Medio	Es necesario diseñar un control de acceso
[E.18] Destrucción de información	Pérdida accidental de información.	3	2	6	Medio	Es necesario diseñar un control de acceso
[E.19] Fugas de información	Revelación por indiscreción.	4	1	4	Medio	Es necesario diseñar un control de acceso
[A.9] [Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.	3	2	6	Medio	Es necesario diseñar un control de acceso
[A.10] Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	4	1	4	Medio	Es necesario diseñar un control de acceso
[A.18] Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio	4	1	4	Medio	Es necesario diseñar un control de acceso
[A.19] Divulgación de información	Revelación de información.	4	1	4	Medio	Es necesario diseñar un control de acceso
[A.22] Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	4	1	4	Medio	Es necesario diseñar un control de acceso
[E.15] Alteración accidental de la información	Alteración accidental de la información	2	1	2	Bajo	Es necesario diseñar un control de acceso
[A.7] Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	3	1	3	Bajo	Es necesario diseñar un control de acceso

Figura 25. Resultados de valoración de riesgos, acciones y prioridades

2.2.2. Análisis GAP (Análisis de brecha)

Evaluar la implementación actual de controles de acceso según la NTP-ISO/IEC 27001 2014 con referencia a procedimientos específicos de la gestión de acceso en la empresa SECURITAS SAC, con el fin de determinar el grado de cumplimiento de éstos y el grado esperado. Asimismo, un plan de acción sobre las brechas. Para el análisis GAP se establecieron las siguientes etapas:

2.2.2.1. Análisis de la situación actual

Para este análisis se utilizará instrumentos de recolección de datos como cuestionarios y entrevistas hacia el personal que está a cargo de los procesos de gestión de acceso en los sistemas de información de SECURITAS SAC, así poder observar y analizar sus resultados.

Las actividades llevadas a cabo durante esta fase son las siguientes:

- Establecer las preguntas relacionadas a procedimientos específicos (Tabla *14*) de controles de acceso según sus dimensiones en políticas de acceso, administración de accesos, responsabilidad y acceso a sistemas y aplicaciones, todas relacionadas a los usuarios. Asimismo, establecer una tabla de valores para el nivel de madurez en sus procesos o procedimientos (Tabla 15) estos adaptados a los niveles de madurez de COBIT 2019.

Tabla 14.

Preguntas relacionadas a procedimientos de controles de acceso.

ID	N° procedimiento	Pregunta
Políticas de control de acceso		
PRE1	1	¿Se tiene desarrollada, documentada e implementada una política de control de acceso que defina los derechos de acceso de los usuarios en función de las necesidades comerciales, teniendo en cuenta los requisitos de clasificación y manejo de la información, servicios, redes y / o aplicaciones a las que se accede, y cualquier requisito legal o reglamentario?

PRE2	2	¿Los permisos de acceso de los usuarios están regidos por los requisitos comerciales, aprobados y revisados periódicamente por los propietarios del activo, y están claramente establecidos en la política de control de acceso?
Administración de acceso a usuarios		
PRE3	3	¿Existe algún proceso implementado para poder segmentar solo el acceso permitido del usuario a la red, equipo o aplicación a la cual se le ha dado exclusivamente permiso?
PRE4	4	¿Se cuenta con un proceso manual para rastrear quién está usando la identificación de un usuario en un momento dado, asimismo de asegurarse de que no pueda ser utilizada por más de una persona en cualquier momento y cambiar las credenciales de autenticación cada vez que la identificación se pasa a un nuevo custodio?
PRE5	5	¿Existe un formulario de registro de usuario, sobre el cual se describe el sistema de información, la red, el servicio o las aplicaciones requeridas, así como las condiciones de acceso?
PRE6	6	¿Existen usuarios que tiene acceso de nivel "superusuario" a las instalaciones o sistemas? ¿Estos cuentan con el proceso adecuado según las necesidades frente a eventos que se necesiten, supervisión e historial?
PRE7	7	¿Existe un procedimiento para garantizar que las identificaciones de usuario y las contraseñas se emitan solo para aquellos con una necesidad comercial de acceso y que estén debidamente autorizadas por el propietario del recurso al que se accede?
PRE8	8	¿Existen y se siguen procedimientos para la revisión periódica de todo tipo de derechos y privilegios de acceso de los usuarios para verificar el cumplimiento, seguida de una revisión a nivel gerencial para verificar la coherencia con los requisitos comerciales y de políticas?
PRE9	9	¿Existe algún procedimiento para quitar el acceso o modificar si se termina relaciones con un usuario (es decir, para un empleado, contratista o usuario externo)?
Responsabilidades de Usuarios		
PRE10	10	¿Existe algún material o formulario que evidencie la información brindada y compromiso de responsabilidad de los usuarios del sistema ante la confidencialidad de autenticación?
PRE11	11	¿Se comunica a los usuarios del sistema sobre la responsabilidad de autenticación de sus accesos mediante algún entrenamiento?
Acceso a Sistemas y aplicaciones		
PRE12	12	¿El propietario de la información contenida en el sistema especifica los derechos de acceso y las reglas para esa aplicación, de acuerdo con los requisitos comerciales y la política de control de acceso?
PRE13	13	¿El sistema o aplicación cuentan con procedimientos de inicio de sesión seguro? Tanto para el usuario y como para el sistema.
PRE14	14	¿El sistema o aplicación cuentan con un procedimiento basado en política para el control de contraseñas?
PRE15	15	¿Existen utilidades o programas del sistema pueden permitir el acceso a partes del sistema que las aplicaciones no permiten y también pueden permitir la invalidación de los controles del sistema?
PRE16	16	¿Existe el desarrollo del sistema o aplicación, o acceso a los códigos de fuentes de las mismas desde la organización?

Tabla 15.

Tabla de valoración de procedimientos.

Código	Valor cualitativo	Valor cuantitativo	Descripción
PO	Optimo	5	El procedimiento esta implementado, documentado y cuenta con supervisión continua.
PG	Gestionado	4	El procedimiento es aplicado y cuenta con documentación.
PD	Definido	3	El procedimiento es aplicado correctamente pero no cuenta con proceso definido.
PI	Inicial	2	El procedimiento es aplicado parcialmente.
PN	No se realiza	1	El procedimiento no existe.
NA	No aplica	0	El procedimiento no aplica al sistema.

- Entrevistar con el cuestionario al personal responsable en el área de informativa, responsable de la gestión de acceso a los sistemas. Obteniendo los valores según las opciones seleccionadas (Anexo 2).
- Obtener el grado de cumplimiento del resultado de la suma del total de productos de los puntajes y el valor de madurez (Figura 26), entre el total de la muestra.
- Según esto se observó los siguientes resultados para la situación actual (PRE) y su grado de cumplimiento (Tabla 16):

Tabla 16.

Resultados de grado de cumplimiento por dimensión.

Clausula Referencia	Dimensión	%
A.9.1	Políticas de acceso	16.3%
A.9.2	Administración de acceso a usuarios	17.5%
A.9.3	Responsabilidades de usuarios	8.8%
A.9.4	Acceso a sistemas y aplicaciones	15.5%

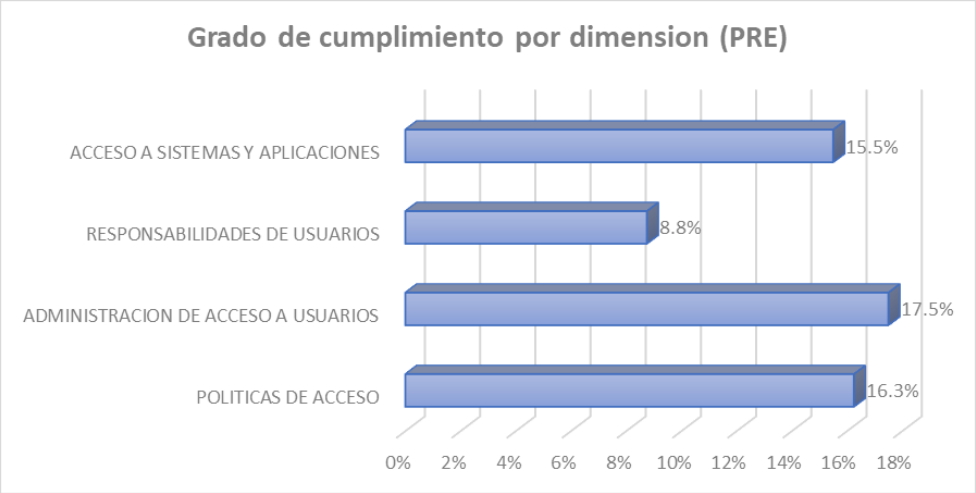


Figura 26. Grado de cumplimiento por dimensión (PRE)

- Obteniendo el resultado por cada dimensión se pudo obtener los valores generales de grado de cumplimiento (Figura 27). Asimismo, la brecha se interpreta como el porcentaje el cual es necesario cubrir en caso se desee llegar al 100% de su implementación.

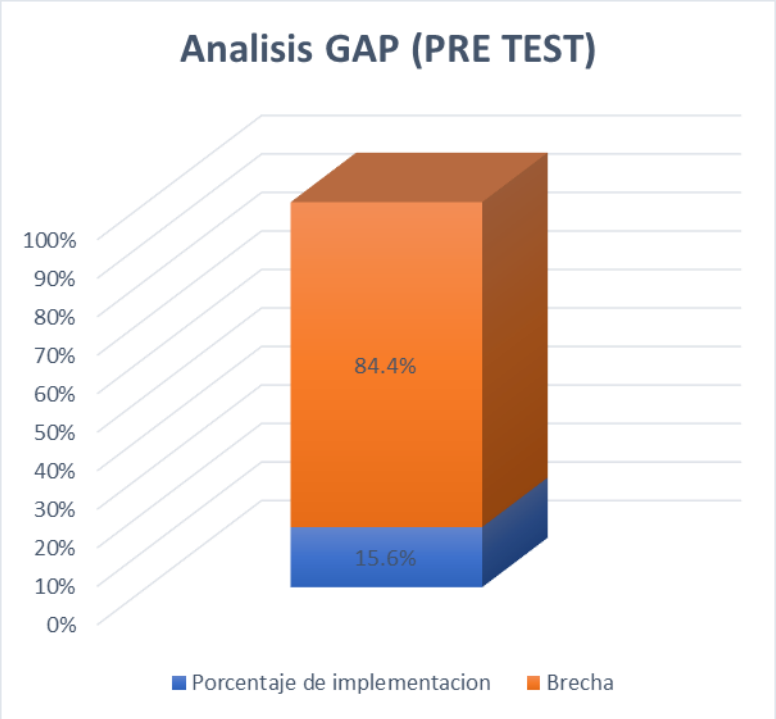


Figura 27. Resultados de análisis de brechas (PRE)

2.2.2.2. Establecer el estado deseado

Para esta etapa se establecerá un método de valoración teniendo en cuenta el nivel de madurez COBIT 2019 según los niveles establecidos en la encuesta para los procedimientos (Tabla 17), de esta manera poder obtener un porcentaje resultado con el cual compararemos con el grado establecido.

Tabla 17.

Tabla de valoración y nivel de madurez

Código	Valor cualitativo	Valor cuantitativo	% Madurez
PO	Optimo	5	100%
PG	Gestionado	4	75%
PD	Definido	3	50%
PI	Inicial	2	25%
PN	No se realiza	1	0%
NA	No aplica	0	-

Los valores obtenidos se suman y se promedian y se agrupan en cada dimensión. Asimismo, se suman y se promedian para obtener el grado general de cumplimiento.

Para fines de esta investigación de determino con SECURITAS SAC mantener el mismo nivel de valoración para los resultados generales. Teniendo en cuenta como aceptación los niveles ÓPTIMOS y GESTIONADOS que representan el 75% al 100% de procedimientos implementados.

2.2.2.3. Analizar de deficiencias

Para esta etapa evaluaremos la situación actual con el estado obtenido establecido en el paso anterior (Figura 28). Para esto mediando la implementación de controles elevar el nivel de madurez en los procedimientos ausentes o que estén en

un estado inicial. De esta manera llegar a un nivel de aceptación en estado OPTIMO o GESTIONADO.

Para poder elevar el nivel de madurez es necesario implementar los controles necesarios en los sistemas de información de manera no solo sea aplicado si no que tenga un proceso establecido, este correctamente documentado y con supervisión continua. De esta manera poder llegar a un nivel de aceptación general de Gestionado ya que optar por un nivel óptimo cuenta con limitantes según los sistemas de información en la empresa SECURITAS SAC.

Dicho esto, se aplicó en los sistemas de información los controles necesarios para poder obtener un estado deseado y obtener nuevamente un resultado de análisis de brecha (Anexo 11).

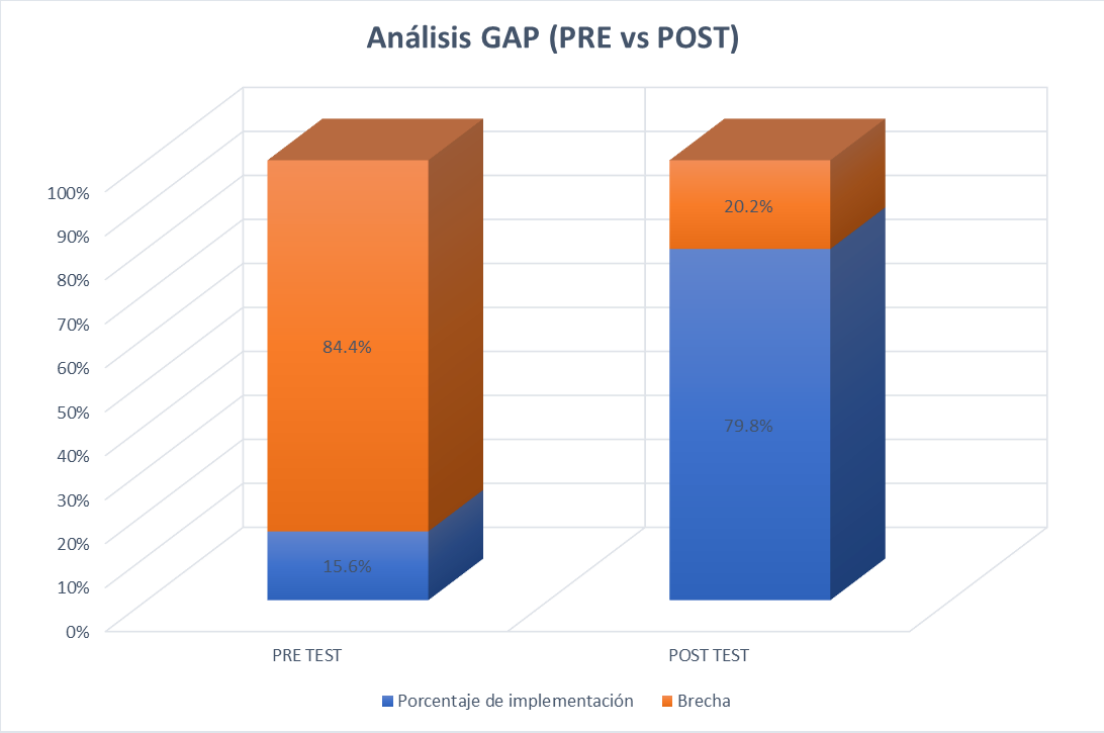


Figura 28. Análisis GAP estado actual vs obtenido.

2.2.3. Plan de trabajo de implementación

2.2.3.1. Análisis de la situación

Durante el plan de trabajo para la implementación de los controles definidos en el análisis de riesgo para mitigar los mismos según los activos críticos de sistemas de información de SECURITAS SAC se definirán una serie de actividades a continuación:

Se identificaron 21 riesgos de los cuales 2 riesgos presentan un nivel de impacto baja, 8 riesgos de impacto medio, 9 riesgos de impacto alto y 2 riesgos de impacto muy alto de los cuales nos enfocaremos en los riesgos desde alto a muy alto que representan a un total de 11 riesgos según el apetito de riesgo establecido con SECURITAS SAC, es decir se mitigaran con 9 controles definidos en procedimientos con referencia a la norma, los cuales se aplicaran de manera transversal a los riesgos; de manera que un control puede aplicarse a más de un riesgo y activos.

Se aplica los mismos riesgos a todos los sistemas y los controles se aplicarán de la misma manera con excepción de encontrarse alguna limitante especifica; es decir, algunos controles no pueden aplicarse directamente por el personal de SECURITAS SAC ya que se encuentran administrados por proveedores externos o su casa matriz. De igual manera se aplicará la estructura, arquitectura y procesos necesarios para poder comunicarlos a los mismos y de esta manera ser aplicados según su evaluación.

Según esto podemos establecer una tabla (Tabla 18) de las amenazas a tratar, su descripción, el riesgo relacionado a controles de acceso, su dimensión afectada y la referencia al control según la norma a aplicar.

Tabla 18.

Riegos y controles identificados para su mitigación.

Código de riesgo	Tipo de amenaza	Descripción	Nivel de prioridad	Descripción del riesgo	Dimensión afectada (MAGERIT, ISO 27001)	Dimensión relacionada a Gestión de Accesos	Referencia NTP Control
R001	[I.5] Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	Muy alto	Fallo por acceso indebido y manipulación de funciones CORE (fabrica) en los sistemas.	1. [D] disponibilidad	- Administración de accesos - Acceso a sistemas y aplicaciones	- A.9.2 - A.9.4
R002	[E.8] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	Muy alto	Difusión de software malintencionado por falta de eliminación de perfiles o roles por defecto en los sistemas. (No intencionado)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad	- Administración de accesos - Responsabilidad de usuarios - Acceso a sistemas y aplicaciones	- A.9.2 - A.9.3 - A.9.4
R003	[E.15] Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Alto	Falta de una política de control de acceso para establecer permisos y roles.	1. [I] integridad	- Políticas de acceso - Administración de accesos	- A.9.1 - A.9.2
R004	[E.1] Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	Alto	Permisos y roles no definidos correctamente. No hay una política definida donde se indique el perfil según sus roles para los accesos.	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad	- Políticas de accesos - Administración de accesos - Responsabilidad de usuarios	- A.9.1 - A.9.2 - A.9.3
R005	[E.14] Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	Alto	No existe un control de acceso perimetral para los sistemas sensibles, para usuarios no autorizados. (Segmentación de red para usuarios)	1. [C] confidencialidad	- Acceso a sistemas y aplicaciones	- A.9.4

R006	[E.21] Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	Alto	Falta de una política de control de acceso para establecer permisos y roles.	1. [I] integridad 2. [D] disponibilidad	- Políticas de acceso - Administración de accesos	- A.9.1 - A.9.2
R007	[A.5] Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.	Alto	No existe una responsabilidad clara del usuario sobre el manejo correcto de credenciales de acceso. Buenas prácticas sobre usuarios.	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad	- Responsabilidad de usuarios	- A.9.3
R008	[A.6] Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	Alto	Permisos y roles no definidos correctamente. No existe un historial de accesos en los sistemas.	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad	- Políticas de accesos - Administración de accesos - Responsabilidad de usuarios	- A.9.1 - A.9.2 - A.9.3
R009	[A.8] Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	Alto	Difusión de software malintencionado por falta de eliminación de perfiles o roles por defecto en los sistemas. (Intencionado)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad	- Administración de accesos - Responsabilidad de usuarios - Acceso a sistemas y aplicaciones	- A.9.2 - A.9.3 - A.9.4
R010	[A.11] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	Alto	Falta de funcionalidades de identificación y autorización en los sistemas.	1. [I] integridad 2. [C] confidencialidad	- Políticas de accesos	- A.9.1
R011	[A.15] Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio	Alto	Falta de una política de control de acceso para establecer permisos y roles.	1. [I] integridad	- Políticas de acceso - Administración de accesos	- A.9.1 - A.9.2

Asimismo, podemos especificar a continuación (Tabla 19) la lista de los 9 controles a aplicar los cuales se relacionan con los controles de la norma. Los cuales tienen se aplican a nivel de procesos, arquitectura y técnico según su alcance:

Tabla 19.

Lista de controles a implementar y su referencia a la norma y dimensión.

Dimensión	Código control	Control sugerido según anexo A. ISO 27001 (27002)	Actividad del control a implementar
Políticas de accesos	C001	✓ Los derechos y reglas de control de acceso deben estar claramente definidos en la política de control de acceso y que son consistentes con los requisitos de clasificación y manejo de la información. ✓ Debe establecerse e implementarse mecanismos adecuados para hacer cumplir esta política. ✓ Un derecho de acceso a un activo debe ser rastreable hasta una evaluación de riesgo y estar autorizado por el propietario correcto del activo. ✓ Cualquier acceso a información sensible, o a instalaciones de procesamiento de información, debe basarse en los principios de "necesidad de saber" y "necesidad de usar", es decir, justificado por los requisitos comerciales y necesario para la tarea en cuestión. ✓ El acceso en las políticas debe en lo posible ser basado en roles. ✓ Las políticas deben contar con un nivel de clasificación de información. ✓ Las políticas de acceso deben tener en cuenta procedimientos para los empleados que abandonan la organización, el cambio de funciones y requisitos laborales, etc. Estos procedimientos deben incluir que cualquier derecho de acceso que se encuentre que ya no está necesarios se eliminan inmediatamente. Deben existir registros que demuestren que este es el caso.	- Establecer un proceso a seguir según una política definida y estructurada. - Establecer una plantilla documentada la política. - Establecer la distribución y comunicación de las políticas.
Administración de acceso a usuarios	C002	✓ Se pueden usar varios controles de acceso a la red, como la seguridad basada en puertos, para limitar el acceso a los servicios de red, y estos controles deben implementarse para respaldar la política de la organización sobre el uso de servicios de red. Un buen control y gestión de cambios es esencial para mantener correctos los accesos, y se requiere un seguimiento regular para proporcionar seguridad.	- Establecer una arquitectura de red deseada desde la actual y su control de cambios con seguridad basada en puertos, segmentación y limitaciones de red.

C003	✓ El proceso para crear y eliminar las Idas de usuario debe documentarse y registrarse, y el proceso para los empleados que abandonan la organización debe incluir la eliminación inmediata de las ID de usuario. ✓ Debe haber un proceso para auditar las identificaciones de manera regular, para detectar cualquier que se haya dejado activo inadvertidamente cuando ya no se necesitan. Las ID de usuario redundantes no se deben volver a emitir a otros usuarios debido al riesgo de otorgar inadvertidamente acceso excesivo y no autorizado a los recursos. ✓ Las IDs de usuario deben ser únicas y no compartidas. ✓ Debe existir un formulario de registro de usuario y este debe estar firmado por el solicitante para documentar su aceptación de las condiciones, y por el propietario o custodio del sistema para documentar su autorización para que el solicitante se registre. Este formulario debe tener la ID de usuario agregada y luego estar archivada. ✓ El acceso de los usuarios a los recursos se debe deshabilitar rápidamente cuando alguien deja de tener una razón comercial para acceder a los recursos, por ejemplo, la terminación del empleo o el cambio de trabajo interno. Deben establecerse procedimientos para garantizar esto. Debe haber procedimientos de notificación y responsabilidades y acciones claramente definidas si los empleados dejan la organización o cambian de empleo. ✓ Los procedimientos de administración de acceso deben incluir revisiones periódicas de los derechos de acceso asignados. Estas revisiones deben estar registradas y que el acceso real se haya comparado con el acceso autorizado y que el autorizador del sistema haya verificado que el acceso autorizado es apropiado. ✓ Al terminar un usuario todos los derechos de acceso asociados con su empleo deben revisarse para su eliminación. Esto incluye derechos de acceso físico (es decir, devolución de tarjetas de control de acceso, llaves, tarjetas de identificación, etc.), así como derechos para iniciar sesión en la red de la organización, cuentas de usuario, contraseñas, direcciones de correo electrónico y cualquier otro. forma de acceso permitido. Los casos especiales deben están especificados dentro de las políticas de acceso. ✓ Se deben reconsiderar todas las formas de acceso cuando cambia los roles de usuario, y se debe eliminar cualquier acceso que no sea necesario para el nuevo rol.	- Crear un proceso general para el manejo del ciclo de vida de las identidades de usuarios y especificar cada actividad. - Scripting (Powershell) para la detección de usuarios inactivos y eliminación. - Query para verificar usuarios deshabilitados y ubicarlos en un Unidad Organizativa en el Active Directory de inactivos.
C004	✓ El acceso administrativo completo o superusuario no debe utilizarse como método predeterminado para proporcionar privilegios elevados, a menos que el sistema no pueda proporcionar ningún nivel intermedio entre el usuario estándar y el acceso completo. ✓ Para funciones críticas, como la administración del sistema, debe haber una identificación especial asignada a cada usuario únicamente para este propósito, además de su cuenta de usuario estándar en el sistema.	- Eliminar o deshabilitar usuarios predeterminados. - Creación de usuarios específicos para roles y perfiles de administración según roles y perfiles. - Crear plantilla de roles y perfiles por sistemas y usuarios de nivel administrador.

		✓ Debe guardarse un historial con las cuentas privilegiadas con datos específicos que demuestren el uso y propósito según el incidente o evento para el cual se usaron.	
	C005	✓ Los usuarios deben firmar una declaración para mantener la confidencialidad de su información secreta de autenticación. ✓ Debe existir procedimientos para garantizar que las contraseñas de proveedores temporales o predeterminadas se cambien de inmediato. ✓ Los sistemas deben contar con un proceso de restablecimiento de contraseñas para los usuarios.	- Funcionalidades activas para la recuperación de contraseñas y sus validaciones.
Responsabilidades de Usuarios	C006	✓ La política sobre información confidencial de autenticación, que incluye cuestiones como la duración, la longitud y el contenido de la contraseña, debe ser suficiente para los requisitos de seguridad de la organización y esta debe estar establecida y comunicada a los usuarios. ✓ Se debe crear conciencia a los usuarios sobre la responsabilidad de la autenticación mediante medidas preventivas y correctivas por la organización.	- Establecer y crear un planeamiento y material para la creación de conciencia en el manejo de contraseñas y accesos.
Acceso a Sistemas y aplicaciones	C007	✓ Por lo general, no se debe presentar a los usuarios listas de información o funciones de aplicaciones a las que no se les permita acceder. ✓ Las opciones de menú que no son accesibles por razones de seguridad deben eliminarse, así como la información en los manuales de usuario relacionada con funciones sensibles. Hay que prestar especial atención a las partes poco utilizadas de las aplicaciones, como las utilidades de mantenimiento.	- Establecer un mapeo de roles y perfiles de acceso según los sistemas. - Limitación de accesos a módulos según roles y perfiles de usuarios.
	C008	✓ Funciones de inicio de sesión no debe revelar información innecesaria sobre el sistema operativo, el servicio o la aplicación a la que el usuario está intentando acceder (por ejemplo, el número de versión, si existe una cuenta de usuario específica en el sistema y mensajes de error que revelen la estructura de la base de datos).	- Diseñar un proceso de inicio de sesión basado en la plataforma Okta.
	C009	✓ Se debe considerar lo siguiente: longitud y contenido de las contraseñas, frecuencia de cambio de contraseñas (límites máximos y mínimos), uso de identificaciones de usuarios individuales, uso de contraseñas comunes entre individuos y / o por el mismo individuo en diferentes aplicaciones, manejo y almacenamiento seguro de contraseñas, cambio de contraseñas predeterminadas. ✓ Debe existir un proceso de cambio de contraseñas. ¿Qué registros se guardan? ¿Se rechazan las contraseñas utilizadas anteriormente y, de ser así, cuántas contraseñas anteriores se conservan para comparar? ¿La aplicación requiere una autenticación exitosa antes de aceptar una solicitud de cambio de contraseña?	- Establecer una política de manejo de contraseñas. - Aplicar la política a todos los sistemas.

2.2.3.2. Recursos

Especificamos los recursos mínimos y generales que se necesitarán para la implementación de estos controles, algunos controles pueden estar sujetos a una inversión de software o hardware según su funcionalidad o requisito en el sistema administrado por el proveedor. Esto deberá ser evaluado por la alta gerencia tomando como sustento el análisis de riesgos, problemática e impacto.

- **Personal**: Gerente general, Gerente de TI y procesos, Gerente de proyecto (De ser necesario), personal técnico y administrador, especialista de seguridad informática (o personal dentro de la compañía que tenga este perfil).
- **Técnicos/ tecnológico**: Los controles necesarios se utilizarán bajo la misma arquitectura y recursos que cuenta la compañía.

2.2.3.3. Funciones y responsabilidades

- **Gerente general:** Apoyar el plan de trabajo, aprobar los riesgos a tratar, brindar los recursos tecnológicos físicos y de personal necesarios.
- **Gerente de TI y procesos**: Facilitar información necesaria de los sistemas y recursos aprobados por alta gerencia.
- **Gerente de proyecto:** Liderar y organizar el plan de implementación, establecer el Gantt necesario y demostrar avances según hitos e informes.
- **Personal técnico/administrador:** Ejecutar las actividades técnicas necesarias según los controles a los sistemas a nivel de hardware y software, aplicación de configuraciones y entrega de información.
- **Especialista de seguridad**: Llevar a cabo la auditoria previa y posterior de la seguridad de la información respecto a los controles.

2.2.3.4. Método de implementación

Enfoque: Se establecerá según el resultado del análisis de riesgos realizado donde la prioridad se enfocará primero desde muy alto a alto.

Reorganización: Se establecerá una matriz de contraste entre los riesgos y controles (Tabla 20). Asimismo, como se indicó en las tablas anteriores se establecerá en la tabla su abreviatura para controles "C" y riesgos "R". Para entender su relación transversal de controles a riesgos y sistemas relacionados.

Tabla 20.
Tabla de aplicación de controles según riesgos y controles

Nivel de prioridad	Riesgos / Controles	C001	C002	C003	C004	C005	C006	C007	C008	C009
Muy alto	R001			X	X					
Muy alto	R002		X	X	X					
Alto	R003			X	X			X		
Alto	R004			X	X		X	X		
Alto	R005		X	X	X		X	X		
Alto	R006				X				X	
Alto	R007		X	X	X	X	X	X		X
Alto	R008			X	X		X	X		
Alto	R009		X		X		X			
Alto	R010	X	X	X	X	X	X	X	X	
Alto	R011			X	X		X	X		

Asimismo, se establece una matriz de contraste entre los la aplicación de los controles y sistemas (Tabla 21) según se encuentre alguna limitante mencionada anteriormente como la aplicación del control dependiente del proveedor.

Tabla 21.
Tabla de aplicación de controles según el sistema de información.

Nombre Sistema	Código Sistema	C001	C002	C003	C004	C005	C006	C007	C008	C009
ERP "softland" V 3.4.0.0	SIS001	X	X	X	X	X	X	X		X
Securitas Vision	SIS002	X		X	X	X	X	X	X	X
SGH	SIS003	X	X	X	X	X	X	X	X	X
SGM	SIS004	X	X	X	X	X	X	X	X	X
Securitas Connect	SIS005	X		X	X	X	X	X	X	X
Smart Boleta Suit	SIS006	X		X	X	X	X	X	X	X
Facturación Electrónica	SIS008	X	X	X	X	X	X	X	X	X
Contratos NOE	SIS014	X		X	X	X	X	X	X	X
Web Vacaciones	SIS021	X	X	X	X	X	X	X	X	X
Active Directory	SIS035	X	X	X	X	X	X	X		X

2.2.3.5. Actividades de implementación

Si bien los controles mencionados en la NTP-ISO/IEC 27001: 2014 en referencia a la ISO 27002 no especifican la estructura o metodología a tener en cuenta al implementar los controles, se estableció los pasos necesarios siguiendo la guía de implementación de esta norma y cumpliendo el nivel de madurez deseado para el control desde su descripción inicial, su definición como proceso, su aplicación, documentación, gestión y supervisión. A continuación, se detallan los controles implementados:

- **Políticas de acceso (C001)**
  - **Descripción**: Los derechos y reglas de control de acceso deben estar claramente definidos en la política de control de acceso y que sean

consistentes con los requisitos de clasificación y manejo de la información. Asimismo, se establece un proceso general de accesos.

- **Actividad previa:** Se estableció reuniones con el personal involucrado para poder definir los parámetros a incorporar dentro de una política de accesos general a los sistemas desde el proceso anterior (Figura 29). Asimismo, se consideró en emplear un método para la distribución al personal relacionado a la administración de accesos a los sistemas.

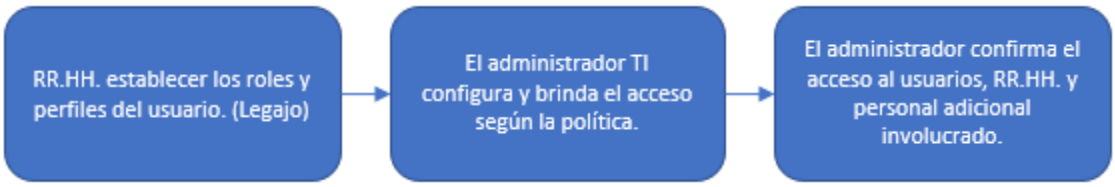


Figura 29. Proceso anterior de gestión de accesos.

- **Método**: Se estableció un proceso general (Figura 30) y se documentó las políticas a aplicar de control de accesos a cada sistema de información (Anexo 17). Asimismo, se aplicará el método a distribuirla a los usuarios.

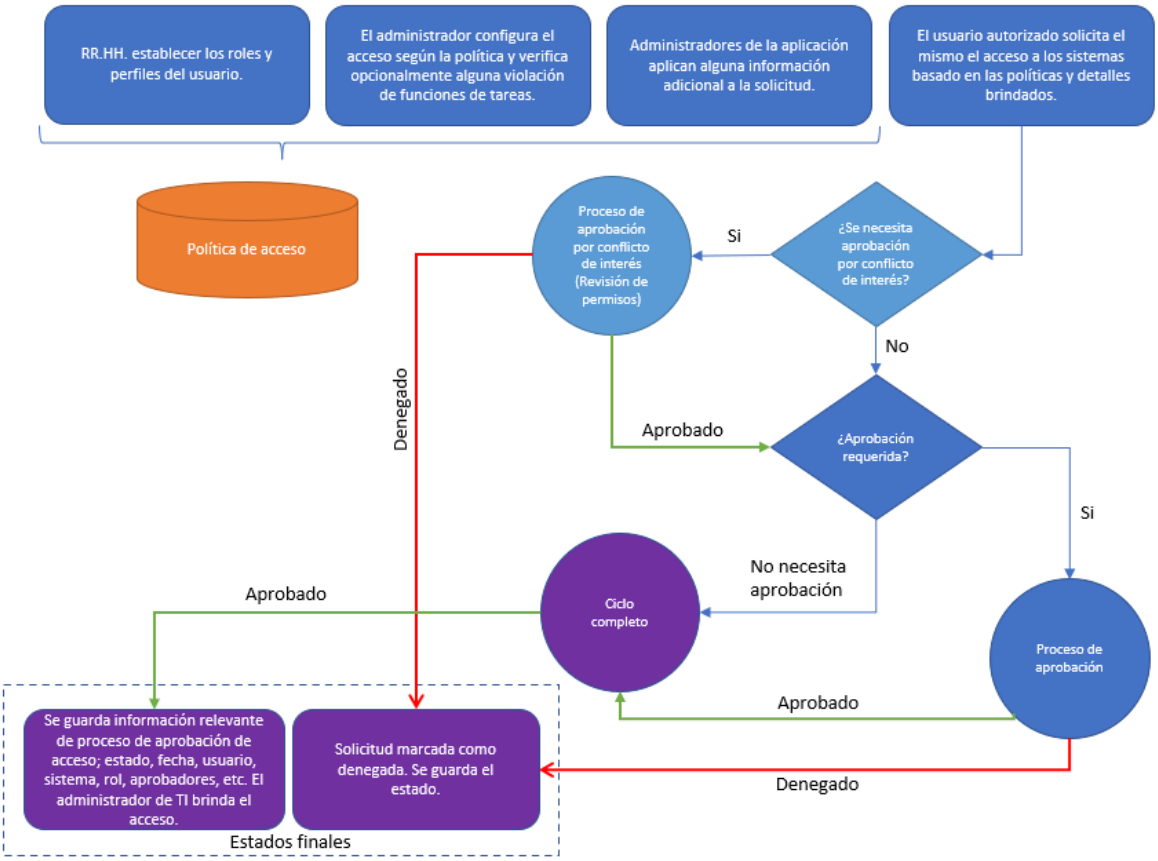


Figura 30. Proceso implementado para la gestión de accesos.

- **Actividad técnica:** La existencia de este control se aplica a nivel organizativo, no técnico, de manera documental por lo cual no hay herramienta o tecnología aplicada a esto. Sin embargo, se tiene en consideración que con la aprobación de la política por alta gerencia esta deberá ser entregada por el gerente de TI al personal técnico el cual establecerá la política dentro del sistema Smart Boleta para distribuirse al personal necesario (**Anexo 29).**

- **Administración de acceso a usuarios (C002)**

  - **Descripción:** Se pueden usar varios controles de acceso a la red, como la seguridad basada en puertos, para limitar el acceso a los servicios de red, y estos controles deben implementarse para respaldar la política de la organización sobre el uso de servicios de red.
  - **Actividad previa:** Se reviso el método a aplicar para el control de acceso a la red basado en puertos con el protocolo 802.1x en conjunto con el administrador de red y la información necesaria como diagrama y datos de la red interna actual donde se puede apreciar de color rojo los elementos implementados para este control. (Figura 31). Tanto para el switch donde se aplicó la configuración de protocolo y la activación de servicios en el servidor RADIUS.

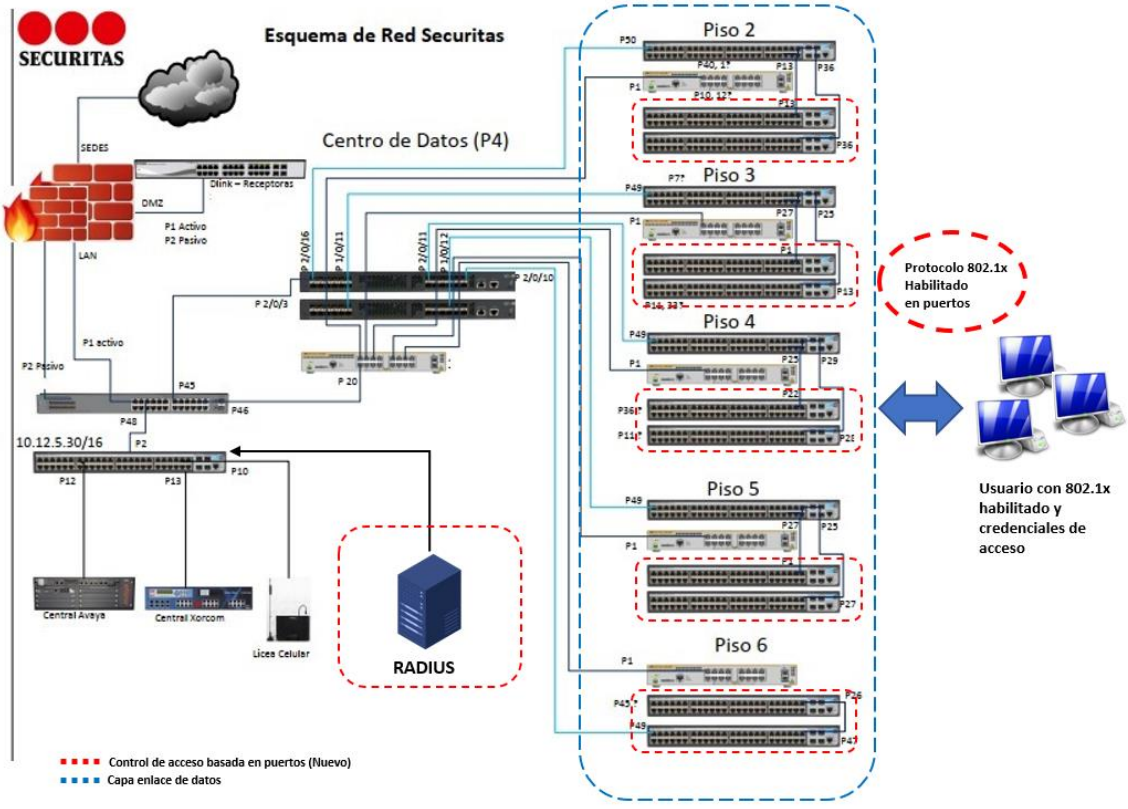


Figura 31. Esquema de red SECURITAS con protocolo 802.1x.

- **Método:** El método a aplicar según la red de SECURITAS SAC es un control de acceso a red basada en puertos en el protocolo IEEE 802.1x (Figura 32) a nivel de capa de enlace de datos. Se escogió este protocolo ya que no requiere de dispositivos adicionales ya que la compañía actualmente cuenta con el servidor RADIUS y conmutadores que aceptan dicho protocolo.
- **Actividad técnica:** Se evaluó la configuración de la red principal de SECURITAS SAC y se realizó el proceso de implementación de este control (**Anexo 18**). En donde tenemos que los switches que cuenta la compañía de marca HP (HP 1920-48G) cuentan con la funcionalidad disponible para este control. Fue necesario en adición configurar el servidor RADIUS que brinde las funciones como DHCP, DNS, AAA, EAP.

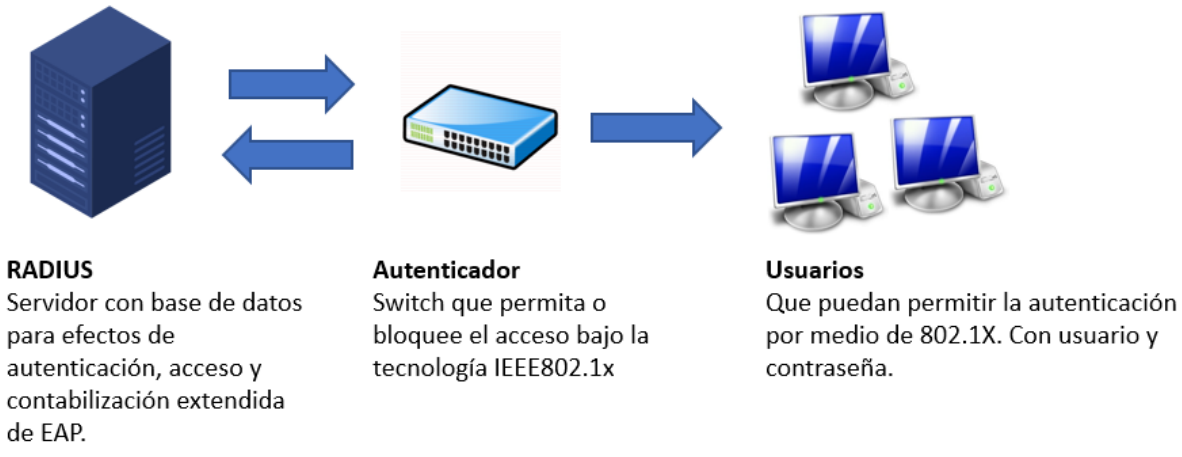


Figura 32. Modelo de red basado en protocolo IEEE 802.1x.

- **Administración de acceso a usuarios (C003)**
    - **Descripción:** El proceso para crear y eliminar las cuentas de usuario deben documentarse y registrarse. De la misma manera con el proceso para los empleados que abandonan la organización se debe incluir la eliminación inmediata de las ID de usuario. Establecer el proceso para auditar las identificaciones de manera regular, para detectar cualquier que se haya dejado activo inadvertidamente cuando ya no se necesitan. Las cuentas de usuario redundantes no se deben volver a emitir a otros usuarios debido al riesgo de otorgar inadvertidamente acceso excesivo y no autorizado a los recursos.
    - **Actividad previa:** Se reviso en conjunto con las áreas responsables como RR.HH. y administración de TI que el que el proceso actual cuenta con insuficientes pasos que puedan evidencias el correcto control del ciclo de vida de las identidades.
    - **Método:** Se estableció los procesos principales involucrados para el ciclo de vida de las cuentas de usuarios (Figura 33). La identidad para las cuentas de usuarios debe pasar por varias etapas durante su existencia, desde la creación, pasando por diversas modificaciones en respuesta a diferentes eventos, hasta la inactivación o eliminación al haberse terminado las relaciones con el trabajador o proveedor.

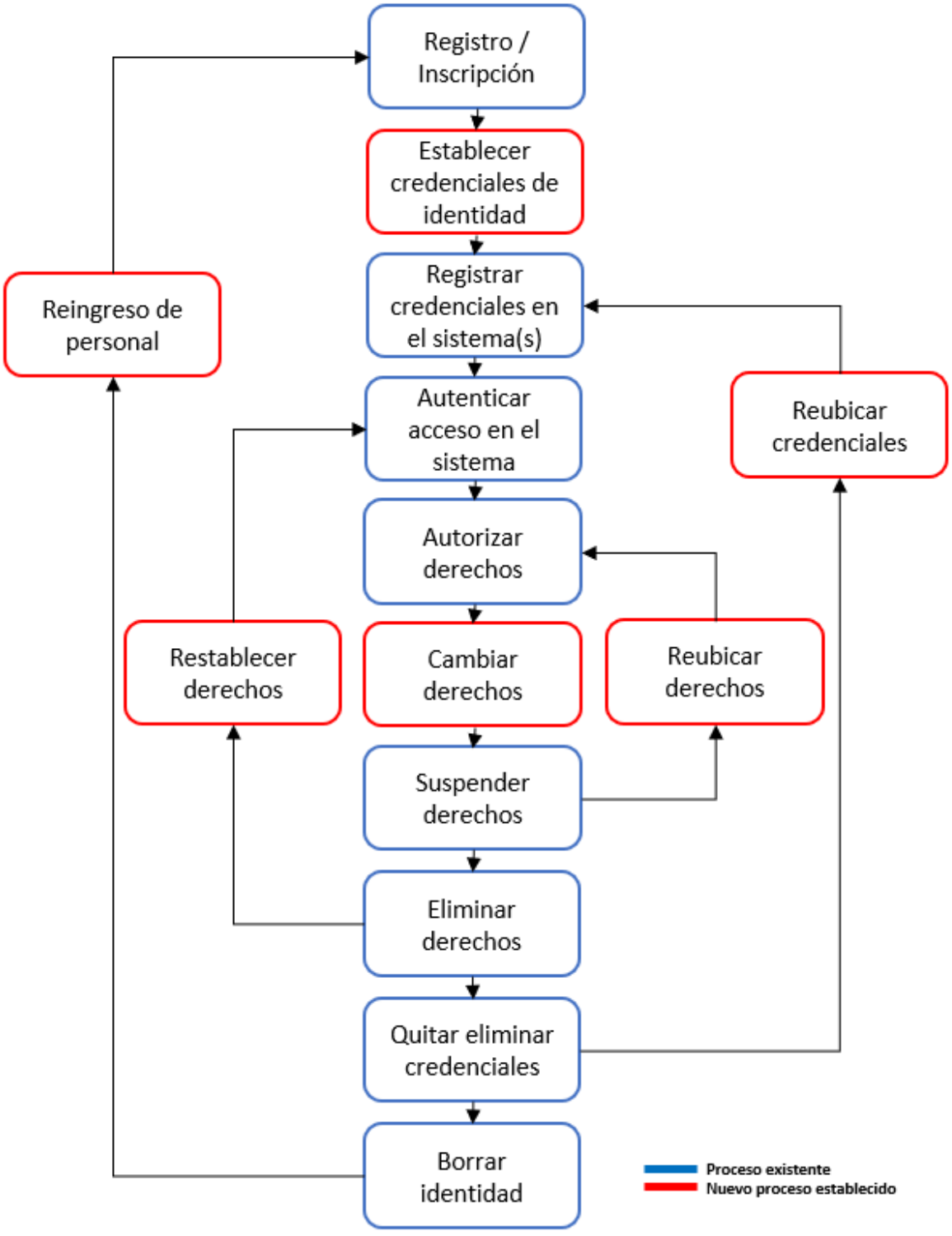


Figura 33. Proceso de ciclo de vida de identidades

Tabla 22.

Descripción de procesos para ciclo de vida de identidades.

Función	**Principal responsable**	**Responsable adicional**	**Comentarios**	**Actividad técnica**
Registro	Recursos humanos		El área de RR.HH. inicia el registro creando la identidad del usuario en el sistema ERP el cual generar un código de legajo único.	
Creación de credenciales y registro en los sistemas	Administración de TI	Administrador del área de negocio del usuario	Se toma la ficha de registro en el paso anterior para registrar datos básicos basados en nombre, ID, correo, etc., y se procede al registro en el sistema.	- Acción ejecutada por AD management plus en sistemas basado en directorio activo. Ejecución manual en los demás sistemas.
Cambio en las credenciales	Recursos humanos	Administración de TI	De ser necesario algún cambio en base al legajo inicial del ERP se envía un ticket de atención a TI con aprobación del gerente área de negocio.	
Asignación de derechos de acceso a sistemas	Administración de TI	Administrador del área de negocio del usuario	Se asignan los derechos en el sistema al usuario basado en su rol y perfil.	- Acción ejecutada por AD management plus en sistemas basado en directorio activo. Ejecución manual en los demás sistemas.
Cambio de derechos de acceso a sistemas	Administración de TI	Administrador del área de negocio del usuario	Se modifican los derechos en el sistema al usuario basado en su rol y perfil.	- Acción ejecutada por AD management plus en sistemas basado en directorio activo. Ejecución manual en los demás sistemas.
Suspensión de accesos a sistemas	Administración de TI, Recursos Humanos	Administrador del área de negocio del usuario	Se modifican los derechos en el sistema al usuario basado en su rol y perfil. Luego de recibir una notificación por parte del área de RR.HH.	- Acción ejecutada por AD management plus en sistemas basado en directorio activo. Ejecución manual en los demás sistemas.
Eliminación de derechos accesos a sistemas	Administración de TI, Recursos Humanos	Administrador del área de negocio del usuario	Se eliminan los derechos en el sistema al usuario basado en su rol y perfil luego de recibir una notificación por parte del área de RR.HH.	- Acción ejecutada por AD management plus en sistemas basado en directorio activo. Ejecución manual en los demás sistemas.
Suspensión o eliminación de credenciales	Administración de TI, Recursos Humanos	Administrador del área de negocio del usuario	Se deshabilitan o eliminan las credenciales en el sistema luego de recibir una	- Acción ejecutada por AD management plus en sistemas basado en directorio activo.

			notificación por parte del área de RR.HH.	Ejecución manual en los demás sistemas.
Eliminación de cuentas en el sistema	Administración de TI, Recursos Humanos		Se elimina completamente los accesos del sistema luego de recibir la confirmación por parte de RR.HH. de acuerdo con la política establecida de retención de la información de dicho usuario.	- Acción ejecutada por AD management plus en sistemas basado en directorio activo. Ejecución manual en los demás sistemas.
Revisión periódica de cuentas inactivas y activas.	Administración de TI		Creación de reportes granulares de cuentas inactivas, activas, bloqueadas, etc.	- Servicios de reportera con AD management plus. Y tareas de automatización para sistemas basados en directorio activo.

- **Actividad técnica:** Con la aprobación del proceso general del ciclo de vida de las identidades de cuentas de usuarios, se coordinó con el personal de TI (técnico) y RR.HH. para establecer las tareas automatizadas o manuales para la creación, eliminación y validación de cuentas en los sistemas tomando en cuenta como base las identidades creadas el sistema ERP Softland y replicando el mismo esquema a los demás sistemas que no cuenten con sincronización automatizada (**Anexo 19**). Asimismo, la ejecución de tareas automatizadas en base a software propuesto "AD management plus" para la creación, eliminación, modificación de usuarios y permisos en sistemas basados en directorio activo buscando automatizar estas mismas y ejecución de scripts basados en PowerShell para administrar las cuentas. (**Anexo 21**).

- **Administración de acceso a usuarios (C004)**
  - **Descripción:** La asignación de derechos de acceso privilegiados debe estar controlada por un proceso formal de autorización que esté alineado con las políticas de control de acceso.
  - **Actividad previa**: Se procedió a identificar las cuentas privilegiadas en los sistemas y establecer un cuadro con las cuentas estableciendo datos como ID, usuario, sistema, descripción y permisos relacionados a la misma (**Anexo *22***)más adelante
  - **Método:** Se procedió a establecer un proceso general del manejo de cuentas privilegiadas (*Figura 34*).

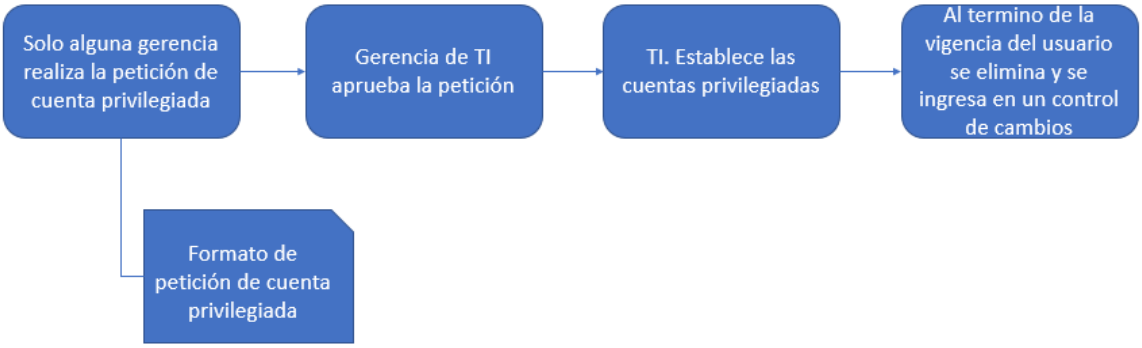


Figura 34. Proceso general de manejo de cuentas privilegiadas implementado.

Antes no existía un proceso para el manejo de cuentas privilegiadas solo era Manual ahora se implementó un proceso con un formato (**Anexo *24***) para validar rigurosamente la creación de cuentas administrativas de acuerdo con la necesidad. Asimismo, se procedió a establecer y deshabilitar las cuentas privilegiadas por defecto en los sistemas y establecer las cuentas asignadas a los administradores de

TI según el nuevo cuadro actualizado de las nuevas cuentas privilegiadas administrativas. (**Anexo *22***)

- **Actividad técnica:** La existencia de este control se aplicó a nivel organizativo, no técnico, de manera documental por lo cual no hay herramienta o tecnología aplicada a esto. Se procedió a establecer el proceso estándar de cuentas privilegiadas, se elaboró un formato para las peticiones de cuentas privilegiadas, se mapearon todas las cuentas en todos los sistemas con privilegios administrativos y se eliminaron dejando solo las cuentas necesarias para el soporte y gestión de cada sistema.

- **Administración de acceso a usuarios (C005)**
  - **Descripción:** Debe existir procedimientos para garantizar que las contraseñas de proveedores temporales o predeterminadas se cambien de inmediato. Los sistemas deben contar con un proceso de restablecimiento de contraseñas para los usuarios.
  - **Actividad previa:** Se verifico que algunos sistemas no cuentan con la funcionalidad de cambio y restablecimiento de contraseña como Securitas Vision, Web de vacaciones y Solicitud de dinero.
  - **Método:** Adicionalmente se complementa a este control en el servicio Okta como intermediario de verificación de identidades y que cuenta con la funcionalidad de cambio de contraseña ya sea inicial o por el mismo usuario.

- **Actividad técnica:** Este control cuenta con más detalles en su arquitectura e implementación en el control C008. Donde se podrá verificar que la cuenta creada una vez autenticada solicitará cambiar la contraseña inicial y también se cuenta con el proceso de restablecimiento de contraseñas.

- **Responsabilidades de Usuarios (C006)**
  - **Descripción:** La política sobre información confidencial de autenticación, que incluye cuestiones como la duración, la longitud y el contenido de la contraseña, debe ser suficiente para los requisitos de seguridad de la organización y esta debe estar establecida y comunicada a los usuarios. Se debe crear conciencia a los usuarios sobre la responsabilidad de la autenticación mediante medidas preventivas y correctivas por la organización.
  - **Actividad previa:** La aplicación de este control es trasversal con la política de acceso creada en el control C001 donde se define la política base de contraseñas para los sistemas de acuerdo a el requisito de SECURITAS SAC. Asimismo, se establece en coordinación con RR.HH. y el gerente de TI y procesos crear y aplicar una capacitación en línea a través de la plataforma "Microsoft Forms" dentro de la organización para crear consciencia en la seguridad de la información, manejo de contraseñas y accesos.
  - **Método:** Se establecerá una capacitación online en la plataforma Microsoft Forms sobre la seguridad de la información incluyendo el manejo de contraseñas y accesos **(Anexo 20)**. Asimismo, se

establecerá una serie de preguntas para que puedan ser respondidas por los usuarios.

- **Actividad técnica:** La existencia de este control se aplicó a nivel organizativo, no técnico, de manera documental por lo cual no hay herramienta o tecnología aplicada a esto. Se creo bajo la plataforma "Microsoft Forms" contenido sobre seguridad de la información y el manejo de accesos y se comunicó por correo el electrónico.

- **Acceso a Sistemas y aplicaciones (C007)**
  - **Descripción:** Por lo general, no se debe presentar a los usuarios listas de información o funciones de aplicaciones a las que no se les permita acceder. Las opciones de menú que no son accesibles por razones de seguridad deben eliminarse, así como la información en los manuales de usuario relacionada con funciones sensibles.
  - **Actividad previa**: Se procedió a revisar que los permisos y roles de usuarios sean congruentes con sus accesos solicitados. Obteniendo una lista de usuarios, roles y perfiles (***Anexo 25***) se implementó una correcta estructura de roles y perfiles de acuerdo a las necesidades de las plataformas y las personas de la operación.
  - **Método:** Se procedió a estructurar los roles y perfiles que van a tener los usuarios.
  - **Actividad técnica:** La existencia de este control se aplicó a nivel organizativo, no técnico, de manera documental por lo cual no hay herramienta o tecnología aplicada a esto.

- **Acceso a Sistemas y aplicaciones (C008)**
    - **Descripción:** Funciones de inicio de sesión no debe revelar información innecesaria sobre el sistema operativo, el servicio o la aplicación a la que el usuario está intentando acceder.
    - **Actividad previa:** Se reviso que los sistemas cuentan con las funcionalidades para este control tanto el inicio de sesión seguro y que no muestren información innecesaria del sistema al usuario y se pudo establecer el proceso actual para el acceso a los sistemas. Adicionalmente, se coordinó con el gerente de TI y procesos para implementar el acceso a sistemas a través de la plataforma Okta como intermediario para el manejo de usuarios e identificación previa para acceder a las aplicaciones que cuenta SECURITAS SAC de esta manera no revelar información importante de los sistemas al inicio de sesión.

      Se realizo una evaluación entre diferentes SaaS (Software as a service) que ofrecen esta funcionalidad identificando principales razones como Gestión de cuentas privilegiadas, políticas, usuarios, acceso, autenticación, provisión e integración. Los cuales, son principalmente lo que se busca dentro de la organización. De lo cual se obtuvo el siguiente resultado (Tabla 23).

      Permite el inicio de sesión de aplicaciones diferentes mucho más fácil. Sin tener ningún conocimiento previo poder configurar nuevas aplicaciones todavía era muy simple y directo mediante la función SWA.

La autenticación web segura (SWA) es una tecnología de Okta que proporciona la funcionalidad de inicio de sesión único (SSO) a aplicaciones web externas que no admiten protocolos federados.

Los administradores pueden configurar las credenciales para la aplicación, o el usuario final puede ingresar un nombre de usuario y contraseña específicos. Okta mantiene las credenciales de esa aplicación dentro de una tienda segura, cifrada con un cifrado AES-256 sólido. Después de configurar las credenciales, los usuarios finales solo necesitan autenticarse con Okta, y luego pueden SSO directamente en la aplicación.

Las credenciales de SWA coincidan con las credenciales de Okta del usuario configurando las opciones de inicio de sesión para esa integración de la aplicación SWA.

Posteriormente, cuando el usuario hace clic en el icono de integración de la aplicación en su panel de control, Okta completa el nombre de usuario y la contraseña y publica de forma segura las credenciales a través de SSL en la página de inicio de sesión de la aplicación. La aplicación externa registra automáticamente al usuario.

Actualmente SECURITAS cuenta con el servicio de Okta implementado para la conexión de uso de VPN al autenticarse a través del servidor RADIUS y el directorio activo. Se utilizará este mismo para extender la validación web con el AD.

Tabla 23

Comparativo en funcionalidades de IDaaS IAM

	IDaaS IAM		
Característica	**Centrify**	**Okta**	**Ping**
Gestión de cuentas privilegiadas		X	
Gestión de políticas	X	X	
Gestión de usuarios	X	X	X
Gestión de acceso	X	X	X
Autenticación multifactor		X	X
Provisión de usuarios		X	X
Integración de directorio activo	X	X	

Figura 35 Cuadrante mágico de Gartner

Por los datos anteriores, se tomó la opción del Okta por estar como líder y la variedad de funciones que cuenta el servicio que podemos observar en el ***Anexo 23***.

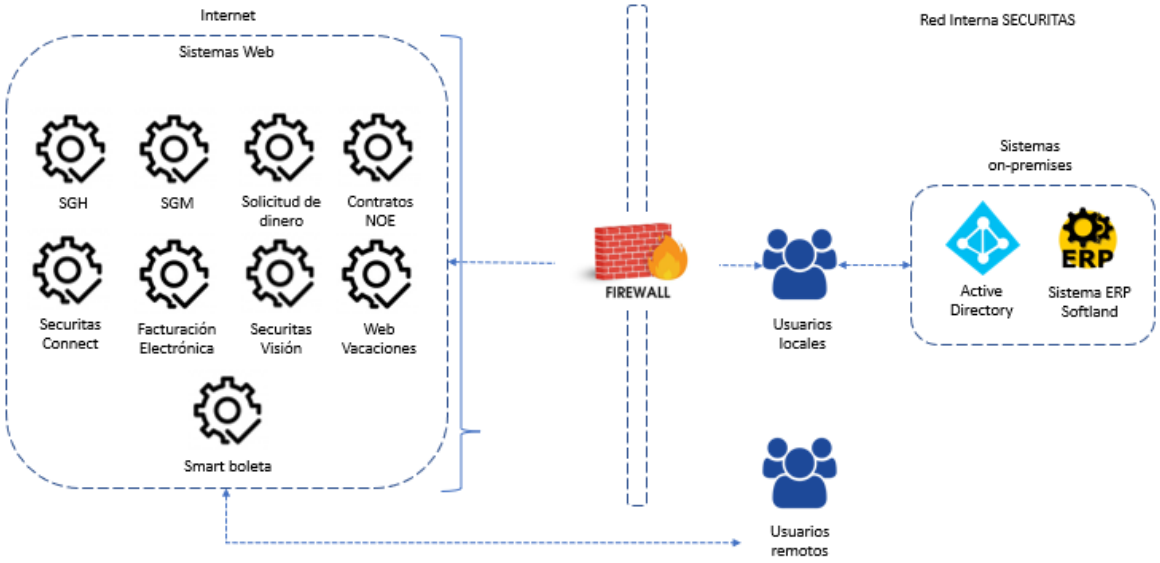


Figura 36. Arquitectura actual de acceso de los usuarios a los sistemas

- **Método:** Se procedió a establecer la arquitectura a implementar con el servicio Okta como intermediario para la autenticación y manejo de usuarios **(Figura 37).**

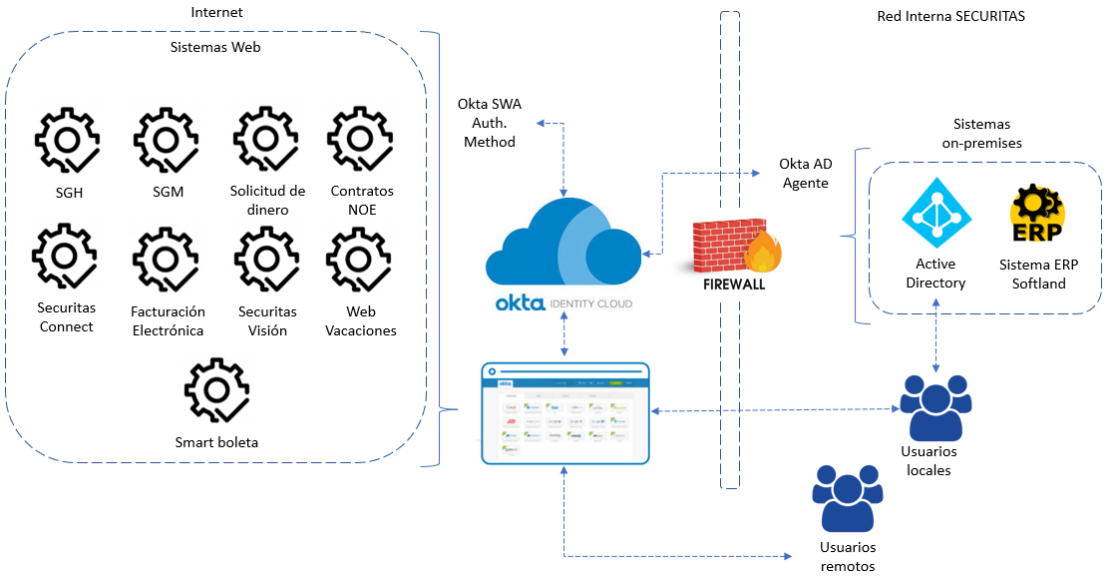


Figura 37. Arquitectura Okta SECURITAS para inicio de sesión

- **Actividad técnica:** Se procedió a configurar los agentes de Okta en los sistemas web para que puedan autenticarse por este medio para luego poder re dirigirse a las aplicaciones según los accesos que cuenten el usuario. (**Anexo 26**).

- **Acceso a Sistemas y aplicaciones (C009)**
  - **Descripción:** Se debe considerar lo siguiente: longitud y contenido de las contraseñas, frecuencia de cambio de contraseñas (límites máximos y mínimos), uso de identificaciones de usuarios individuales, uso de contraseñas comunes entre individuos y / o por el mismo individuo en diferentes aplicaciones, manejo y almacenamiento seguro de contraseñas, cambio de contraseñas predeterminadas.
  - **Actividad previa:** Este control hace referencia a el control "C001" donde se hace mención de la política de contraseñas en la política de acceso principal. Se reviso la política y se procedió aplicar la misma a todos los sistemas desde el AD y los sistemas web.
  - **Método:** Se realizo la verificación de la política GPO general en el Active directory (
  -
  - **Anexo *27*).** Los sistemas web que no cuenten con integración por AD se procedió a revisar y a llevar el control manualmente por cada sistema y a su vez se procedió a establecer la política de contraseñas en el sistema Okta (**Anexo 28**).

- **Actividad técnica:** Se realizo la configuración del GPO para la política de contraseña en el dominio SECPER.COM y se desplego a través del AD. Asimismo, se configuro la configuración Okta en el administrador.

2.2.4. Aspectos éticos

- La presente investigación cuenta con la aprobación de la organización y a su vez están informados sobre toda la información expuesta en este trabajo.
- Estamos cumpliendo con la privacidad y confidencialidad de la información de la organización.
- Seguimos los lineamientos éticos como profesionales responsables y legales al tener un documento firmado sobre la autorización de la presente investigación. (Anexo 1)
- La presente investigación no presenta conflictos de intereses (Anexo 16).
- No mostramos información sensible en ninguna parte del trabajo.
- Se obtiene acceso a la NTP-ISO/IEC 27001:2014 publicada por el diario oficial El Peruano según la resolución ministerial Nº 004-2016-PCM que es de acceso público. (Anexo 15)

CAPÍTULO III. RESULTADOS

3.1. Análisis descriptivo

3.1.1. Análisis de resultados comparativos del pre-test y post-test totales

De acuerdo con los resultados (Figura 38) se demuestra que de los procedimientos implementados, el grado de cumplimiento según su valor en gestión de accesos a los sistemas de información tomados como muestra, el 9% de estos no aplica, un 0% en estados optimo, un 3% en estados gestionado, un 16% en estados definidos, un 21% en estados inicial y un 51% en estados que no se realizan todo esto en el grupo de pre test, mientras que para el post test el 9% de estos no aplica, un 46% en estados optimo, un 46% en estados gestionado.

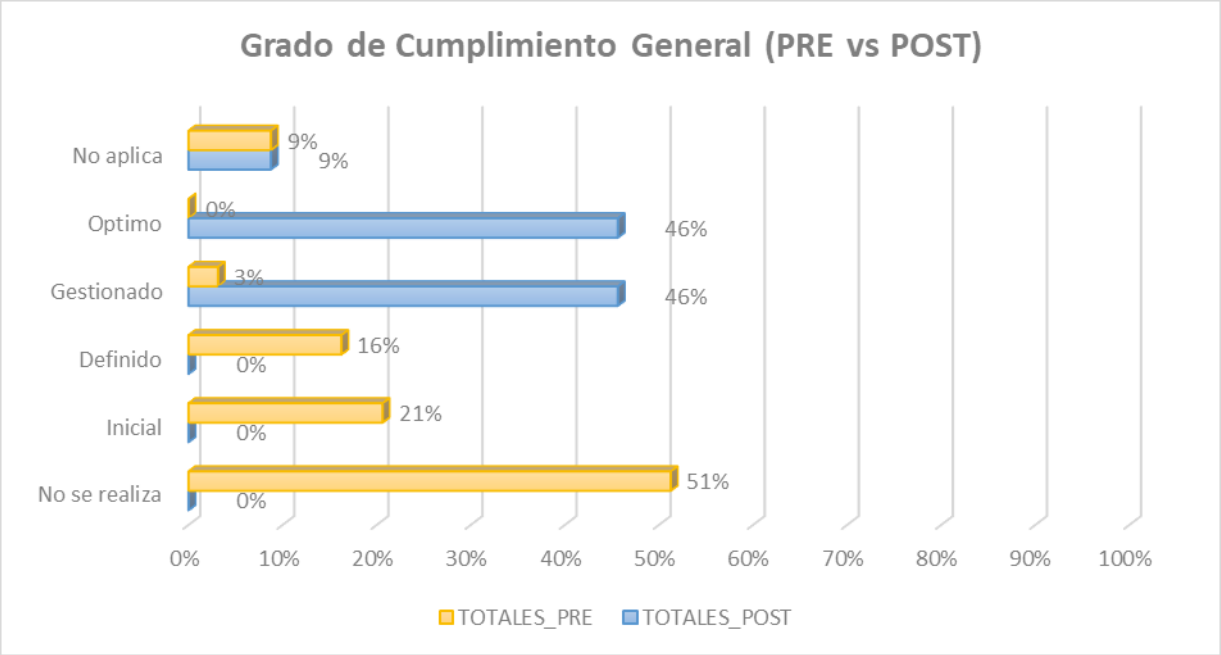


Figura 38. Grado de cumplimiento totales (PRE vs POST)

Asimismo, de acuerdo con los resultados (Figura 39) se demuestra que de los procedimientos implementados según las dimensiones de gestión de accesos a los sistemas de información tomados como muestra hay 15.5% de cumplimiento para "Acceso a sistemas y aplicaciones", un 8.8% de cumplimiento para

"Responsabilidades de acceso a usuarios", un 17.5% de cumplimiento para "Administración de acceso a usuarios" y un 16.3% para "Políticas de acceso" todo esto en el grupo de pre test, mientras que para el post test hay 68,5% de cumplimiento para "Acceso a sistemas y aplicaciones", un 86,3% de cumplimiento para "Responsabilidades de acceso a usuarios", un 81,1% de cumplimiento para "Administración de acceso a usuarios" y un 97,5% para "Políticas de acceso"

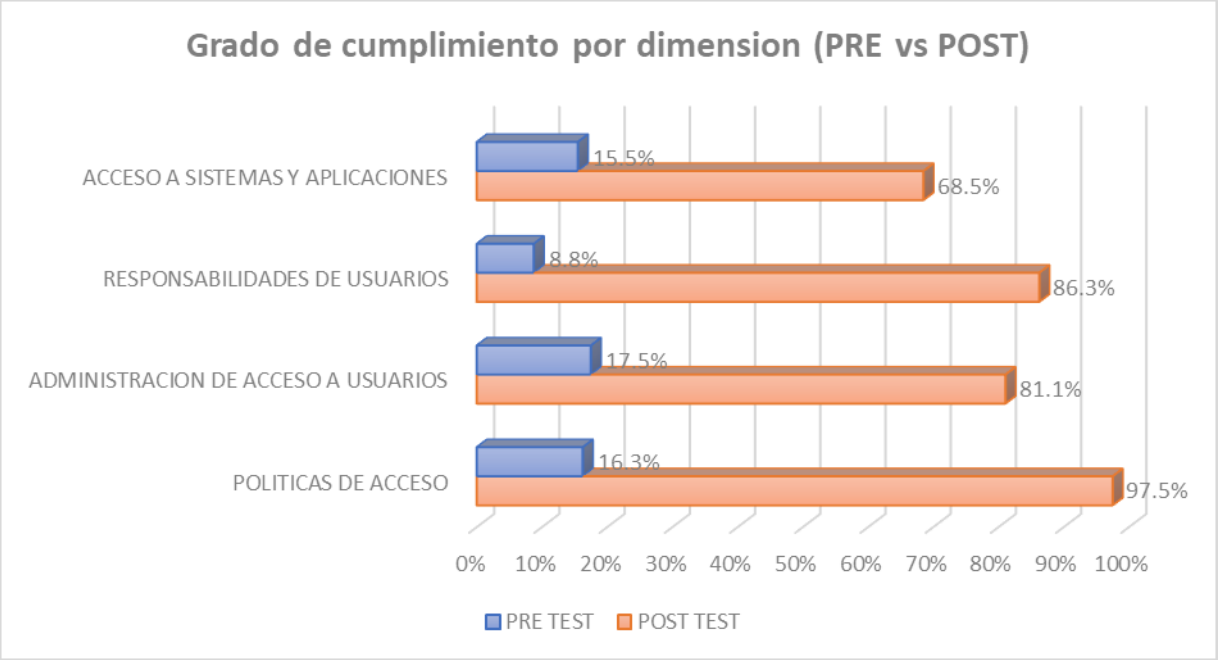


Figura 39. Grado de cumplimiento por dimensión (PRE vs POST)

3.1.2. Análisis de resultados comparativos del pre-test y post-test para la dimensión políticas de acceso a usuarios (D1)

De acuerdo con resultados (Figura 40) se demuestra que de los procedimientos implementados el grado de cumplimiento según su valor para la dimensión "Políticas de acceso a usuarios" el 60% "No se realiza", el 20% está en un estado "Inicial", el 15% esta como "Definido", el 5% se encuentra como

"Gestionado" todo esto para el grupo de pre test, mientras que para el post test el 10% se encuentra como "Gestionado" y el 90% se encuentra como "Optimo".

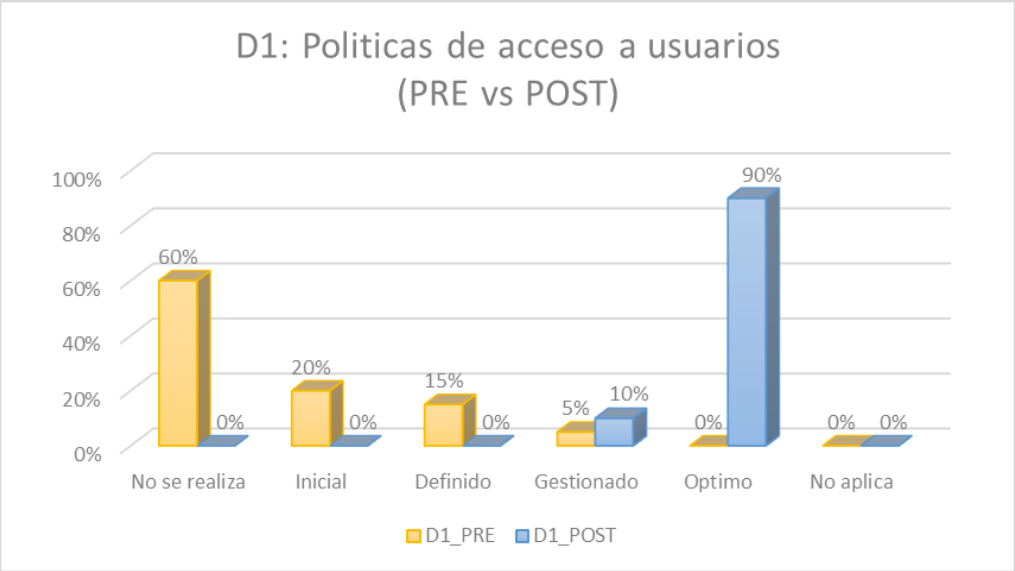


Figura 40. Grado de cumplimiento pre vs post test para la dimensión políticas de acceso a usuarios

Para el análisis descriptivo se utilizaron los datos obtenidos del pre test y post test (Tabla 24). Asimismo, se recurrió al uso del software SPSS Statistics para el análisis correcto de la información obtenida (Tabla 25).

Tabla 24.
Resultados PRE POST grado cumplimiento políticas de accesos.

Políticas de acceso a usuario (D1)		
Item	**Grado de cumplimiento (GR)**	
	D1_PRE	**D1_POST**
SIS001	0.25	1.00
SIS002	0.00	0.75
SIS003	0.00	1.00
SIS004	0.00	1.00
SIS005	0.00	1.00
SIS006	0.38	1.00
SIS007	0.00	1.00
SIS014	0.38	1.00
SIS021	0.00	1.00
SIS035	0.63	1.00
Total	0.16	0.98

Tabla 25.

Estadísticos descriptivos PRE POST de Políticas de acceso a usuario.

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desviación estándar
D1_PRE	10	.00	.63	.1640	.23076
D1_POST	10	.75	1.00	.9750	.07906
N válido (por lista)	10				

3.1.3. Análisis de resultados comparativos del pre-test y post-test para la dimensión administración de acceso a usuarios (D2)

De acuerdo con resultados (Figura 41) se demuestra que de los procedimientos implementados el grado de cumplimiento según su valor para la dimensión "Administración de acceso a usuarios" el 51% "No se realiza", el 20% está en un estado "Inicial", el 19% esta como "Definido", el 4% se encuentra como "Gestionado" todo esto para el grupo de pre test, mientras que para el post test el 52% se encuentra como "Gestionado" y el 41% se encuentra como "Optimo". Asimismo, para ambos casos hay un 6% de procedimientos que no aplican.

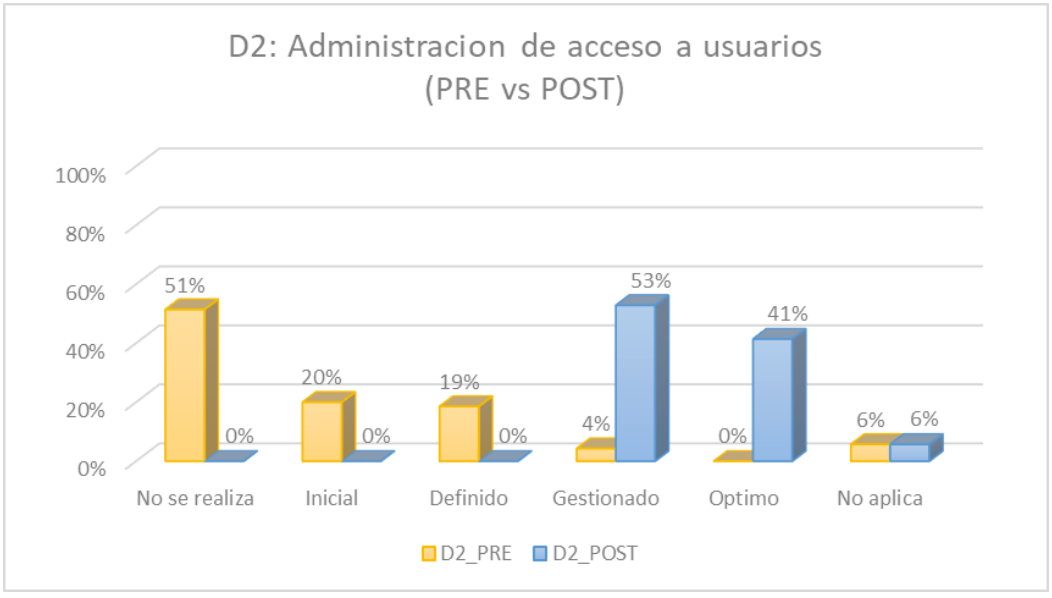


Figura 41. Grado de cumplimiento pre vs post test para la dimensión administración de acceso a usuarios.

Para el análisis descriptivo se utilizaron los datos obtenidos del pre test y post test (Tabla 26). Asimismo, se recurrió al uso del software SPSS Statistics para el análisis correcto de la información obtenida (Tabla 27).

Tabla 26.
Resultados PRE POST grado cumplimiento administración de acceso a usuarios.

Administración de acceso a usuarios		
Item	**Grado de cumplimiento (GR)**	
	PRE	**POST**
SIS001	0.25	0.82
SIS002	0.00	0.93
SIS003	0.00	0.86
SIS004	0.00	0.79
SIS005	0.00	0.93
SIS006	0.38	0.61
SIS007	0.00	0.86
SIS014	0.38	0.61
SIS021	0.00	0.82
SIS035	0.63	0.89
Total	0.16	0.81

Tabla 27.
Estadísticos descriptivos PRE POST de Administración de acceso a usuarios.

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desviación estándar
D2_PRE	10	.00	.63	.1640	.23076
D2_POST	10	.61	.93	.8120	.11584
N válido (por lista)	10				

3.1.4. Análisis de resultados comparativos del pre-test y post-test para la dimensión responsabilidad a usuarios (D3)

De acuerdo con resultados (Figura 42) se demuestra que de los procedimientos implementados el grado de cumplimiento según su valor para la dimensión "Responsabilidad de acceso a usuarios" el 75% "No se realiza", el 15% está en un estado "Inicial", el 10% esta como "Definido" todo esto para el grupo de

pre test, mientras que para el post test el 55% se encuentra como "Gestionado" y el 45% se encuentra como "Optimo".

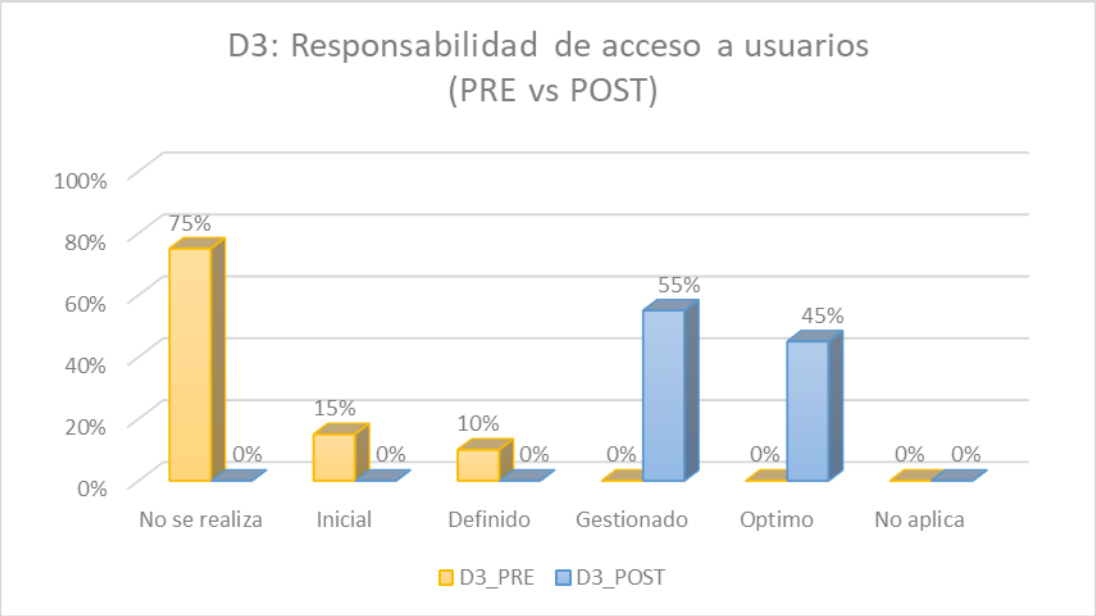


Figura 42. Grado de cumplimiento pre vs post test para la dimensión responsabilidad de acceso a usuarios.

Para el análisis descriptivo se utilizaron los datos obtenidos del pre test y post test (Tabla 28). Asimismo, se recurrió al uso del software SPSS Statistics para el análisis correcto de la información obtenida (Tabla 29).

Tabla 28.
Resultados PRE POST grado cumplimiento de responsabilidad de acceso a usuarios.

Responsabilidad de acceso de usuarios		
Item	**Grado de cumplimiento (GR)**	
	PRE	**POST**
SIS001	0.00	0.88
SIS002	0.00	1.00
SIS003	0.00	0.88
SIS004	0.00	0.88
SIS005	0.13	0.75
SIS006	0.25	0.75
SIS007	0.00	0.88
SIS014	0.38	0.88
SIS021	0.00	0.88
SIS035	0.13	0.88
Total	0.09	0.86

Tabla 29.

Estadísticos descriptivos PRE POST de responsabilidad de acceso a usuarios.

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desviación estándar
D3_PRE	10	.00	.38	.0890	.13395
D3_POST	10	.75	1.00	.8660	.07168
N válido (por lista)	10				

3.1.5. Análisis de resultados comparativos del pre-test y post-test para la dimensión acceso a sistemas y aplicaciones (D4)

De acuerdo con resultados (Figura 43) se demuestra que de los procedimientos implementados el grado de cumplimiento según su valor para la dimensión "Acceso a sistemas y aplicaciones" el 38% "No se realiza", el 24% está en un estado "Inicial", el 16% esta como "Definido", el 2% está en un estado "Gestionado" todo esto para el grupo de pre test, mientras que para el post test el 46% se encuentra como "Gestionado" y el 34% se encuentra como "Optimo". Asimismo, para ambos casos hay un 20% de procedimientos que no aplican.

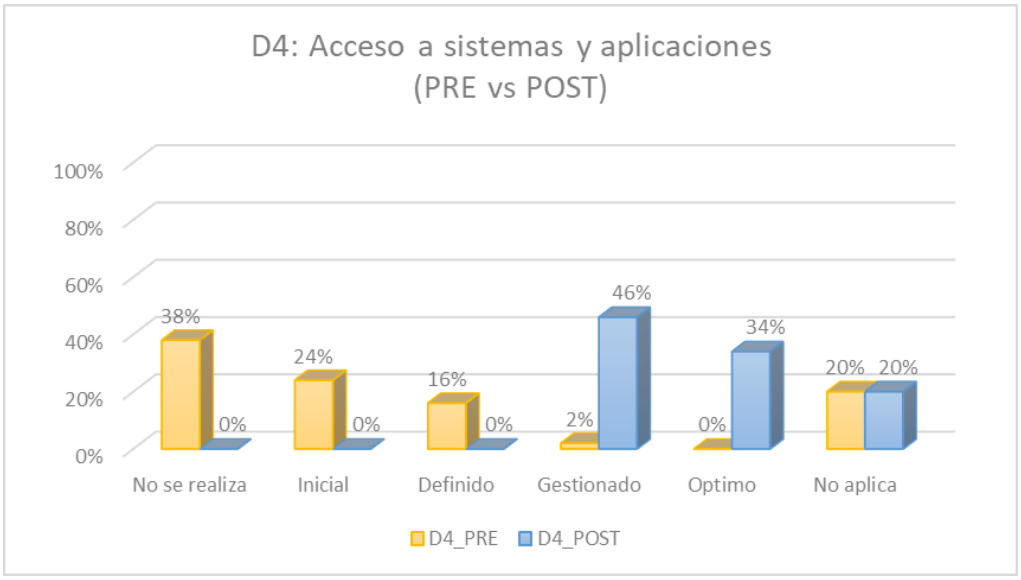


Figura 43. Grado de cumplimiento pre vs post test para la dimensión Acceso a sistemas y aplicaciones.

Para el análisis descriptivo se utilizaron los datos obtenidos del pre test y post test (Tabla 30). Asimismo, se recurrió al uso del software SPSS Statistics para el análisis correcto de la información obtenida (Tabla 31).

Tabla 30.
Resultados PRE POST grado cumplimiento de acceso a sistemas y aplicaciones.

Acceso a sistemas y aplicaciones		
Item	**Grado de cumplimiento (GR)**	
	PRE	**POST**
SIS001	0.05	0.75
SIS002	0.10	0.75
SIS003	0.10	0.75
SIS004	0.10	0.75
SIS005	0.15	0.70
SIS006	0.25	0.75
SIS007	0.10	0.75
SIS014	0.25	0.75
SIS021	0.10	0.75
SIS035	0.35	0.80
Total	0.16	0.75

Tabla 31.
Estadísticos descriptivos PRE POST de acceso a sistemas y aplicaciones.

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desviación estándar
D4_PRE	10	.05	.35	.1550	.09560
D4_POST	10	.70	.80	.7500	.02357
N válido (por lista)	10				

3.2. Análisis inferencial

3.2.1. Pruebas de normalidad

Según Flores y Cevallos (2021) mencionan que "la aplicación de las pruebas de normalidad de los datos pretende garantizar la robustez de los análisis estadísticos,

más aún cuando en las organizaciones se dedica tiempo y recursos para ello, razón por la cual es deseable llegar a conclusiones correctas".

Antes de realizar la prueba de hipótesis respectiva primero se determina si hay una distribución normal de nuestros datos (estadística paramétrica) o no, es decir una libre distribución (estadística no paramétrica). Para esto utilizaremos la prueba de normalidad de Shapiro-Wilk por ser nuestras muestras menos a mayores a 50 elementos en nuestro caso 10.

Para determinar la normalidad de los resultados, plantearemos las siguientes hipótesis a validar:

H0: Los datos no provienen de una distribución normal.

Ha: Los datos provienen de una distribución normal.

H0, sí y solo si: Sig. (p_valor) < 0,05

Ha, si y solo si: Sig. (p_valor) > 0,05

De la cual se obtuvieron los siguientes resultados (Tabla 32):

Tabla 32.

Pruebas de normalidad de dimensiones PRE y POST

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
D1_PRE	.361	10	<.001	.748	10	.003
D1_POST	.524	10	<.001	.366	10	<.001
D2_PRE	.361	10	<.001	.748	10	.003
D2_POST	.228	10	.152	.831	10	.035
D3_PRE	.347	10	.001	.733	10	.002
D3_POST	.377	10	<.001	.750	10	.004
D4_PRE	.317	10	.005	.820	10	.026
D4_POST	.400	10	<.001	.658	10	<.001

a. Corrección de significación de Lilliefors

Conclusiones de pruebas de normalidad

Sobre la prueba de normalidad en pre-test y post-test para las dimensiones se obtuvieron valores inferiores a 0,05 con esto se infiere que hay razones suficientes para rechazar la hipótesis nula, y aceptar la hipótesis alterna en todas concluyendo que los datos provienen de una distribución normal.

3.2.2. Pruebas de hipótesis

Las pruebas de hipótesis se planten como un proceso de decisión entre dos hipótesis. En él se consideran una hipótesis alternativa (Ha) que es la negación o complemento de la hipótesis nula (Ho). Se definen regiones de rechazo y no rechazo sobre la distribución muestral del estadístico de prueba.

3.2.2.1. Pruebas de hipótesis especifica HE1

Ho: La implementación de controles según la NTP-ISO/IEC 27001:2014 NO MEJORARÁ las políticas de acceso en la gestión accesos de la empresa SECURITAS SAC en Lima 2021.

Ha: La implementación de controles según la NTP-ISO/IEC 27001:2014 MEJORARÁ las políticas de acceso en la gestión accesos de la empresa SECURITAS SAC en Lima 2021.

Ho, sí y solo si: Sig. (p_valor) < 0,05

Ha, si y solo si: Sig. (p_valor) > 0,05

De la cual se obtuvieron los siguientes resultados (Tabla 33):

Tabla 33.

Prueba T-Student para políticas de acceso a usuarios.

	Diferencias emparejadas						
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia		t	gl	P de dos factores
				Inferior	Superior			

Par 1	D1_PRE - D1_POST	-.81100	.22447	.07098	-.97158	-.65042	-11.425	9	<.001

Según el resultado de la hipótesis para la dimensión se aplicó T-Student, debido a que la muestra de nuestra investigación es de distribución normal. El nivel de significación (p_valor) es 0.001 notoriamente menor que 0.05 con lo cual se RECHAZA la hipótesis nula y se ACEPTA la hipótesis alterna.

3.2.2.2. Pruebas de hipótesis especifica HE2

Ho: La implementación de controles según la NTP-ISO/IEC 27001:2014 NO MEJORARÁ la administración de acceso a usuarios en la gestión accesos de la empresa SECURITAS SAC en Lima 2021.

Ha: La implementación de controles según la NTP-ISO/IEC 27001:2014 MEJORARÁ la administración de acceso a usuarios en la gestión accesos de la empresa SECURITAS SAC en Lima 2021.

Ho, sí y solo si: Sig. (p_valor) < 0,05

Ha, si y solo si: Sig. (p_valor) > 0,05

De la cual se obtuvieron los siguientes resultados (Tabla 34):

Tabla 34.

Prueba T-Student para administración de acceso a usuarios.

		Diferencias emparejadas							
		Media	**Desviación estándar**	**Media de error estándar**	**95% de intervalo de confianza de la diferencia**		**t**	**gl**	**P de dos factores**
					Inferior	Superior			
Par 1	D2_PRE - D2_POST	-.64800	.29903	.09456	-.86191	-.43409	-6.853	9	<.001

Según el resultado de la hipótesis para la dimensión se aplicó T-Student, debido a que la muestra de nuestra investigación es de distribución normal. El nivel

de significación (p_valor) es 0.001 notoriamente menor que 0.05 con lo cual se RECHAZA la hipótesis nula y se ACEPTA la hipótesis alterna.

3.2.2.3. Pruebas de hipótesis especifica HE3

Ho: La implementación de controles según la NTP-ISO/IEC 27001:2014 NO AUMENTARÁ la responsabilidad de usuarios en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

Ha: La implementación de controles según la NTP-ISO/IEC 27001:2014 AUMENTARÁ la responsabilidad de acceso a usuarios en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

Ho, sí y solo si: Sig. (p_valor) < 0,05

Ha, si y solo si: Sig. (p_valor) > 0,05

De la cual se obtuvieron los siguientes resultados (Tabla 35):

Tabla 35. .

Prueba T-Student para responsabilidad de acceso a usuarios

		Diferencias emparejadas							
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia		t	gl	P de dos factores
					Inferior	Superior			
Par 1	D3_PRE - D3_POST	-.77700	.17689	.05594	-.90354	-.65046	-13.891	9	<.001

Según el resultado de la hipótesis para la dimensión se aplicó T-Student, debido a que la muestra de nuestra investigación es de distribución normal. El nivel de significación (p_valor) es 0.001 notoriamente menor que 0.05 con lo cual se RECHAZA la hipótesis nula y se ACEPTA la hipótesis alterna.

3.2.2.4. Pruebas de hipótesis especifica HE4

Ho: La implementación de controles según la NTP-ISO/IEC 27001:2014 NO MEJORARÁ los accesos a sistemas y aplicativos en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

Ha: La implementación de controles según la NTP-ISO/IEC 27001:2014 MEJORARÁ los accesos a sistemas y aplicativos en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021.

Ho, sí y solo si: Sig. (p_valor) < 0,05

Ha, si y solo si: Sig. (p_valor) > 0,05

De la cual se obtuvieron los siguientes resultados (Tabla 36):

Tabla 36.
Prueba T-Student para acceso a sistemas y aplicaciones.

		Diferencias emparejadas							
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia		t	gl	P de dos factores
					Inferior	Superior			
Par 1	D4_PRE - D4_POST	-.59500	.08644	.02734	-.65684	-.53316	-21.767	9	<.001

Según el resultado de la hipótesis para la dimensión se aplicó T-Student, debido a que la muestra de nuestra investigación es de distribución normal. El nivel de significación (p_valor) es 0.001 notoriamente menor que 0.05 con lo cual se RECHAZA la hipótesis nula y se ACEPTA la hipótesis alterna.

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1. Discusión

En la investigación de la "Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021", se basa en el anexo A9 de Controles de accesos que hacen referencia dentro de la norma, entre otras investigaciones como el "Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019." (Avalos, 2019); tiene como alcance este tipo de propuestas de soluciones, pero en este caso diferenciamos los siguientes puntos:

- Proponen un modelo para roles de perfiles de usuarios para los sistemas de información dándole más accesos a los usuarios según solo el cargo que desempeña en la empresa.
- La creación de una plantilla para gestionar los controles de accesos para verificar las incidencias y vulnerabilidades que puedan ocurrir y amenazar los sistemas de la información, por este motivo en nuestro caso estaremos realizando un análisis de riesgos para implementar controles de accesos para cada sistema de información.
- La creación de modelos para que el área de tecnología supervise los sistemas de información y sean automatizadas las estrategias que tienen actualmente la compañía para el control, en nuestro caso estaremos implementando controles de accesos basados en una norma para cada sistema de la información según la criticidad que esté expuesta cada una y sea a la medida de cada software que posea la compañía.

Para esta investigación tenemos estos puntos en común.

- Establecer controles de accesos.
- Mejorar la seguridad de la información.
- Gestionar los accesos a los sistemas de la información.

Nuestra investigación propone analizar el desempeño de cumplimiento de controles de accesos en los sistemas de información, para así esta manera poder identificar que políticas y controles a implementar, así reducir la brecha de seguridad que posee actualmente la empresa para evitar ataques y perdidas de información.

Entre otras investigaciones como la "Evaluación de control de accesos en correval" (Caldas, 2020); tiene como alcance similar propuestas de soluciones, pero diferenciamos los siguientes puntos que se ve a continuación:

- El acceso a la información será de manera controlada, de esta forma se pueda monitorear a las personas que están accediendo a los sistemas de la información sensibles para la empresa, en nuestro caso según la norma dentro de la implementación de controles y gestión de accesos especifica la responsabilidad de los usuarios para el impacto positivo en el manejo de la información con las políticas que implementen la compañía.
- Todos los sistemas de información deberán ser controladas mediante inicio de sesión seguros para verificar la identidad de las personas, en nuestro caso se están complementando con controles y políticas de seguridad para cada sistema y su riesgo respectivo, teniendo procedimientos y políticas para el acceso seguro a los sistemas que manejan la compañía.
- Se realizará la documentación respectiva de los procesos para que el área de gestión de accesos tenga como evidencia si en algún momento tengan un

cambio de personal, en nuestro caso las políticas y controles se implementan en toda la organización y será difundida como procedimientos estándares para todos los colaboradores que tenga acceso a algún sistema de la información de acuerdo a la responsabilidad de los usuarios que sugiere la norma.

Para esta investigación tenemos los siguientes puntos en común.

- Implementar controles de accesos en las compañías
- Mejorar la seguridad de la información.
- Gestionar el acceso correctamente a todos los usuarios de la compañía.

Como mencionamos anteriormente, nuestra investigación propone analizar el desempeño actual de los sistemas de la información para poder realizar un análisis de riesgo para cada software midiendo todos los controles de acceso y poder implementar políticas y controles eficaces para que sean ejecutadas en la compañía así reducir la brecha de seguridad que posee actualmente la compañía para evitar ataques y perdidas de información.

4.2. Limitaciones

- La implementación se limita a los controles de acceso lógicos en la organización.
- La implementación solo se enfoca en los controles de acceso según el anexo 9 de la NTP-ISO/IEC 27001:2014.
- Existen sistemas de información en la organización que no cuentan con la funcionalidad necesaria para la aplicación del control.
- El control que hace referencia al desarrollo de aplicaciones, no se aplica a la organización.

4.3. Recomendaciones

De acuerdo al análisis realizado con la investigación se recomienda los siguiente:

- El alcance de la implementación de valor se enfoca en el control de acceso lógicos por lo que se recomienda posterior a la implementación, ampliar el análisis de riegos y cumplimiento a otros controles de la norma que estén involucrados a los objetivos de la organización.
- Se recomienda la investigación de otras normas u ISO's relacionadas a el contexto de seguridad de la información de manera que se obtenga un nivel de madurez más amplia.
- Es necesario inculcar una cultura de gestión y gobierno de las tecnologías de información como COBIT a los altos directivos para obtener más apoyo organizacional de la implementación de controles u otros marcos normativos relacionados a esta.
- Se recomienda establecer un SGSI (Sistema de gestión de seguridad de la información) basado en el análisis de cumplimiento total de controles de la ISO y de la organización. Asimismo, establecer el ciclo completo Deming para obtener la mejora continua del SGSI.

4.4. Conclusiones

En la presente implementación, teniendo en cuenta todos los resultados obtenidos, podemos concluir que se cumple el objetivo general, ya que la implementación de controles según la NTP-ISO/IEC 27001:2014 mejorará según su grado de cumplimiento establecido hasta 79.8% de forma general, un 97.5% para su dimensión en políticas de accesos, un 81.1% para su dimensión de administración de

acceso a usuarios, un 86.3% en la responsabilidad de usuarios y un 68.5% en la dimensión de acceso a sistemas y aplicaciones todos logrando la madurez deseada dentro de lo "Definido", "Optimo" y "Gestionado" todos dentro del proceso de la gestión de accesos de la empresa SECURITAS SAC generando un impacto positivo en la organización con su implementación.

1. Realizando el método aplicado los cuales son identificación de los activos, realizando un análisis de cumplimiento (GAP), realizando el análisis de riesgo y proponiendo un plan, logramos concluir que fortaleceremos la confidencialidad, integridad y disponibilidad de la información de la empresa SECURITAS SAC.
2. Logramos concluir que la implementación de controles en los activos de información de la empresa SECURITAS SAC, mejorará la gestión de accesos permitiendo un óptimo uso en la seguridad en los accesos a las plataformas informáticas.
3. Con la implementación de controles, concluimos que es importante las buenas prácticas en la gestión de accesos de los softwares para proteger la información de la empresa SECURITAS SAC dando un seguro acceso a la información, protegiendo los datos para una buena exactitud.
4. Pudimos determinar que las políticas de accesos de la gestión de accesos en la empresa SECURITAS SAC, causa un impacto positivo alcanzando hasta un 97.5% de cumplimiento y madurez basado en controles para aumentar la seguridad de la información de acuerdo a la NTP-ISO/IEC 27001:2014.
5. Pudimos determinar el impacto positivo en la empresa SECURITAS SAC al tener controles que ayuden a la administración de accesos de usuarios en la gestión de accesos de acuerdo a la norma alcanzando hasta un 81.1% de su cumplimiento y madurez.

6. Se pudo determinar el impacto positivo en la responsabilidad de los usuarios para los controles de acceso a los sistemas de información para la gestión de accesos de la compañía SECURITAS SAC alcanzando hasta un 86.3% de su cumplimiento y madurez.
7. Se determinó el impacto positivo en el mejor control de accesos a los sistemas y aplicativos de la empresa SECURITAS SAC para la gestión de accesos de acuerdo a la NTP-ISO/IEC 27001:2014 alcanzando hasta un 68.5% de cumplimiento y madurez.

REFERENCIAS

Antonucci, D. (2017). The cyber risk handbook: Creating and measuring effective cybersecurity capabilities. New Jersey: Wiley.

Acosta, J. J. (2018). Diseño para la automatización del mantenimiento de usuarios en el proceso de ceses y la reducción del riesgo de fufa de información en el Banco Financiero del Perú. Universidad Tecnológica del Perú Lima, Perú.

Arias, E. S. (2020). Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao. Universidad Cesar Vallejo Lima, Perú.

Avalos, C. V. (2019). Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Universidad Norbert Wiener Lima, Perú.

Avenía, C. (2017). Fundamentos de seguridad informática. Colombia, Bogotá: Fondo editorial Areandino.

Bridget, K. (2019). ISO 27001 Controls - a Guide to Implementing and Auditing. United Kingdom: IT Governance Ltd.

Caldas, J. C. (2020). Evaluación de control de accesos en correval. Universidad Piloto de Colombia, Bogotá, Colombia.

Calder, A. (2017). Nueve Pasos para El éxito: Una Visión de Conjunto para la Aplicación de la ISO 27001:2013. Reino Unido: IT Governance Ltd.

C. Rupa, R. Patan, F. Al-Turjman and L. Mostarda, "Enhancing the Access Privacy of IDaaS System Using SAML Protocol in Fog Computing," in *IEEE Access,* vol. 8, pp. 168793-168801, 2020, doi: 10.1109/ACCESS.2020.3022957.

Carmona, D. H. (23 de diciembre de 2016). Aspectos esenciales para fomentar el control de acceso de la información. Gestión Competitividad e Innovación. P.54-59.

Cutillas Zárate, J. (2021). Mejora al sistema de seguridad de una empresa mediante gestión de identidades (Doctoral dissertation, Universitat Politècnica de València).

Davila, M. A. (2018). Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la municipalidad distrital de JOSÉ CRESPO Y CASTILLO -AUCAYACU. Universidad católica los ángeles de Chimbote, Perú.

Delgado, M. M. & Vásquez, J. L. (2020). MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN SRL. Universidad de Lambayeque Chiclayo, Perú.

Dirección General de Modernización Administrativa, P. e. (2012). MAGERIT - versión 3.0. Madrid, España: Ministerio de Hacienda y Administraciones Públicas de España.

Escalante, D. M. (2019). Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ntp iso/iec 27001 para la Dirección de Salud Virgen de Cocharcas–Chincheros. Universidad nacional José maría Arguedas Apurímac, Perú.

Ferruzola,E., Duchimaza, J., Ramos, J. y Alejandro, M.(2019).Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. Revista Científica y Tecnológica UPSE, 6(1), 34-41. DOI: 10.26423/rctu.v6i1.429

Flores, K. L. & Flores, C. E (diciembre de 2021) Pruebas para comprobar la normalidad de datos en procesos productivos. Revista de ciencias sociales y humanísticas. Vol. 23, No. 2, pp 83-106

Gabriel-Ortega, J. (2017). Cómo se genera una investigación científica que luego sea motivo de publicación. Journal of the Selva Andina Research Society, 8(2), 155-156.

Gabriel-Ortega, J. (2017). Cómo se genera una investigación científica que luego sea motivo de publicación. Journal of the Selva Andina Research Society, 8(2), 155-156.

Galindo, H. (2020). ESTADÍSTICA PARA NO ESTADÍSTICOS UNA GUÍA BÁSICA SOBRE LA METODOLOGÍA CUANTITATIVA DE TRABAJOS ACADÉMICOS. España, Alicante: Editorial Área de Innovación y Desarrollo S.L

Graus, E. G. (Enero de 2018). Estadística aplicada a la investigación educativa. Dilemas Contemporáneos. Recuperado de www.dilemascontemporaneoseducacionpoliticayvalores.com

He, W & Zhang, Z (2019). Enterprise cybersecurity training and awareness programs: recommendations for success, Journal of Organizational Computing and Electronic Commerce, 249-257, 2019.

Hernández, C. E. & Carpio, N. (15 de febrero de 2019) Metodología de la investigación. Revista científica de instituto nacional de Salud. Recuperado de www.alerta.salud.gob.sv

ISACA. (2019). Marco de referencia COBIT® 2019: Introducción y Metodología, 2019. Schaumburg, IL 60173, USA. ISBN 978-1-60420-788-0.

ITIL®4 Foundation (2019). Guía de fundamentos en castellano. United States, Seattle: Axelos

Lalinde, J. D. H., Castro, F. E., Rodríguez, J. E., Rangel, J. G. C., Sierra, C. A. T., Torrado, M. K. A., & Pirela, V. J. B. (2018). Sobre el uso adecuado del coeficiente de correlación de Pearson: definición, propiedades y suposiciones. Archivos venezolanos de Farmacología y Terapéutica, 37(5), 587-595.

Neil, D. A. & Suarez, L. C. (2018). Procesos y fundamentos de la investigación científica. Machala, Ecuador: Editorial UTMACH.

Normaiso27001. (2019). Guía para implementar ISO 27001 paso a paso. Recuperado de https://normaiso27001.es

Parra, A. M. (2017). Diagnóstico de la gestión de acceso de usuarios en la Superintendencia de Servicios públicos domiciliarios-norma ISO/IEC 27001: 2013 numerales a. 9.2. 2 y a. 9.3. 1. Universidad Libre seccional Bogotá, Colombia.

Presidencia del Consejo de Ministros (2016). Resolución Ministerial N° 004-2016-PCM. Recuperado de https://www.gob.pe

Perumbuli, S. K. (2017). An Authentication Security and Governance Frame Work for Near Field Communication in Sri Lankan Context (Doctoral dissertation).

Salazar, C. P. & Castillo, S. G. (2018) Fundamentos básicos de estadística. ISBN: 978-9942-30-616-6

Tola, D. F & Freire, L. C. (2015). Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoria, aplicando la norma ISO/IEC 27001. Escuela Superior Politécnica del Litoral (ESPOL) Guayaquil, Ecuador.

Torok, G., Day, MR, Hartman-Baker, RJ y Snavely, C. (noviembre de 2020). Iris: banca de asignación y gestión de identidades y accesos para la era de la exaescala. En SC20: Conferencia internacional de informática de alto rendimiento, redes, almacenamiento y análisis (págs. 1-11). IEEE.

Torres, M.& Salazar, F. G. & Paz, K. (2019). Métodos de recolección de datos para una investigación. Universidad Rafael Landivar Guatemala.

Vallois, V., Mehaoua, A. y Amziani, M. (mayo de 2021). Gestión de acceso e identidad basada en blockchain en sistemas industriales de IoT. En 2021, Simposio

Internacional IFIP / IEEE sobre Gestión Integrada de Redes (IM) (págs. 623-627). IEEE.

Vásquez, W. A. (2020). Metodología de la investigación. Recuperado de www.usmp.edu.pe

Ventura-León, J. L., Arancibia, M., & Madrid, E. (2017). La importancia de reportar la validez y confiabilidad en los instrumentos de medición: Comentarios a Arancibia et al. Revista médica de Chile, 145(7), 955-956.

Villasís-Keever, M. Á., Márquez-González, H., Zurita-Cruz, J. N., Miranda-Novales, G., & Escamilla-Núñez, A. (2018). El protocolo de investigación VII. Validez y confiabilidad de las mediciones. Revista Alergia México, 65(4), 414-421.

ANEXOS

Anexo 1. Carta de autorización de uso de información de empresa

CARTA DE AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

UNIVERSIDAD PRIVADA DEL NORTE

Yo.....MIGUEL ALEJANDRO LUJAN BULLON... ..... ,
Identificado con DNI...42716398... en mi calidad de.....DIRECTOR.....
..... del área de .....RECURSOS HUMANOS.....
..... de la empresa/institución.....SECURITAS SAC.....
con R.U.C N° .....20117920144....., ubicada en la ciudad de .....LIMA.....

OTORGO LA AUTORIZACIÓN,

Al señor.....YONATHAN DAMNER MONTENEGRO MARTINEZ..... ,
identificado con DNI N°.....45208321....., egresado de la (X)Carrera profesional o ( )Programa de Postgrado de .....INGENIERIA DE SISTEMAS COMPUTACIONALES.....para
(Nombre de la carrera o programa)

que utilice la siguiente información de la empresa:

Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesosde la empresa SECURITAS SAC en Lima 2021;

con la finalidad de que pueda desarrollar su ( )Trabajo de Investigación, (X)Tesis o ( )Trabajo de suficiencia profesional para optar al grado de ( )Bachiller, ( )Maestro, ( )Doctor o (X)Título Profesional.

Recuerda que para el trámite deberás adjuntar también, el siguiente requisito según tipo de empresa:

- Vigencia de Poder. *(para el caso de empresas privadas).*
- ROF / MOF / Resolución de designación, u otro documento que evidencie que el firmante está facultado para autorizar el uso de la información de la organización. *(para el caso de empresas públicas)*
- Copia del DNI del Representante Legal o Representante del área para validar su firma en el formato.

Indicar si el Representante que autoriza la información de la empresa, solicita mantener el nombre o cualquier distintivo de la empresa en reserva, marcando con una "X" la opción seleccionada.
( ) Mantener en Reserva el nombre o cualquier distintivo de la empresa; o
(X) Mencionar el nombre de la empresa.

SECURITAS S.A.C.
MIGUEL A. LUJAN BULLON
Representante Legal

Firma y sello del Representante Legal o Representante del área
DNI: 42716398
CONTACTO: 936368021

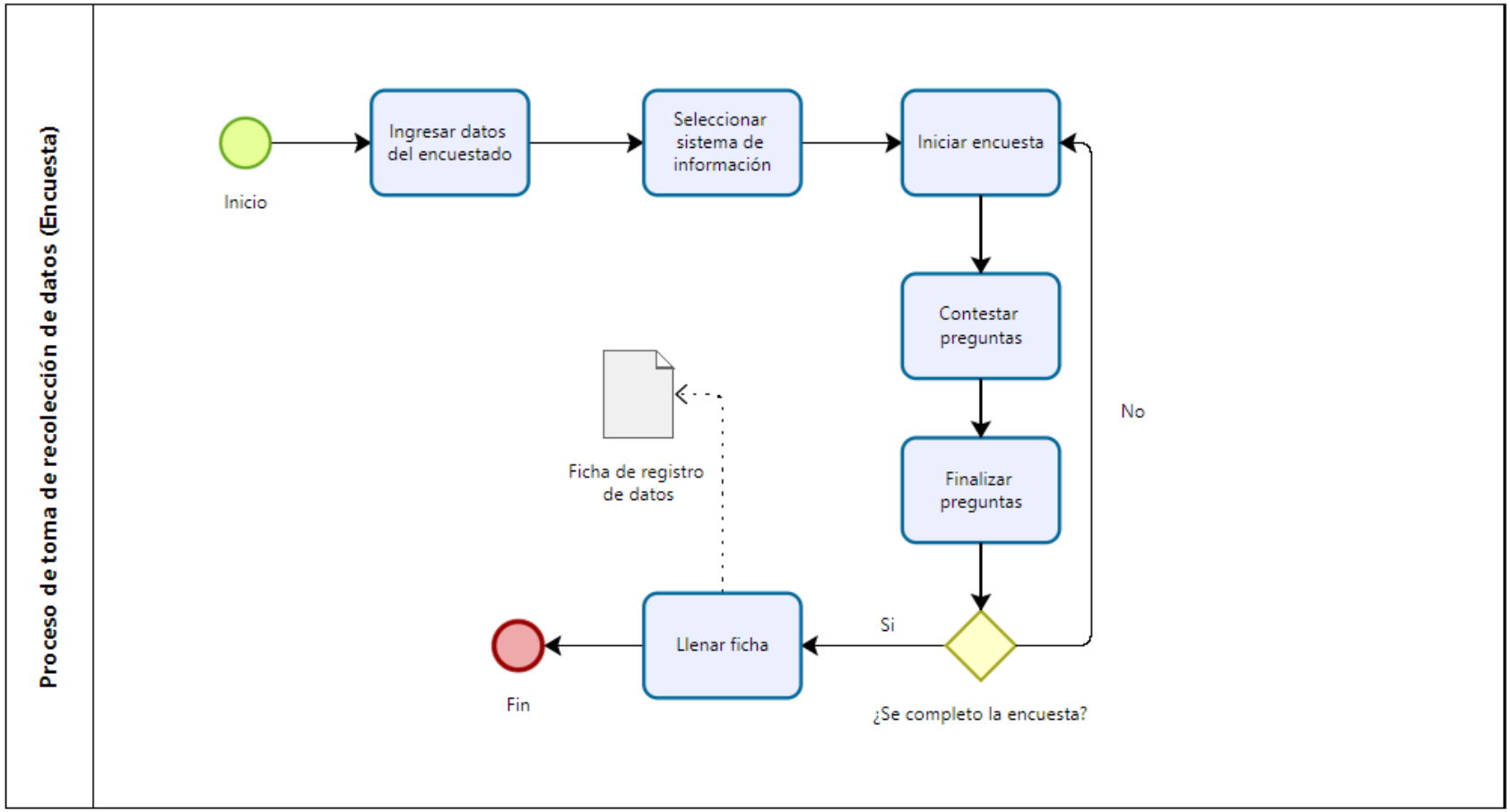
El Egresado/Bachiller declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos. En caso de comprobarse la falsedad de datos, el Egresado será sometido al inicio del procedimiento disciplinario correspondiente; asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.

Firma del Egresado
CHRISTIAN AUGUSTO CONISLLA RAMIREZ
DNI: 45193295

Firma del Egresado
YONATHAN DAMNER MONTENEGRO MARTINEZ
DNI: 45208321

CÓDIGO DE DOCUMENTO	COR-F-REC-VAC-05.04	NÚMERO VERSIÓN	07	PÁGINA	Página 1 de 1
FECHA DE VIGENCIA	21/09/2020				

Anexo 2. Datos obtenidos de las encuestas.



Muestra de datos obtenidos de las encuestas. RE TEST. Periodo Agosto. Sistema "ERP Softland V.3.4.0.0."

Cuestionario en base a la Gestión de accesos y su relación con los controles de la NTP-ISO/IEC 27001:2014						Sistema	ERP "softland" V 3.4.0.0
Fecha:	26-08-2021	Tipo	RE TEST	Periodo	Agosto	Encuestado	Giovanni Ramirez Romero

* Marque con un "x" el nivel escogido.

		Nivel de cumplimiento *						Control de Referencia		
ID	Nº Disposición/procedimiento	Optimo (5)	Gestionado (4)	Definido (3)	Inicial (2)	No se realiza (1)	No aplica (0)	Control NTP	Sub Control	Recomendaciones / Procedimientos
Políticas de control de acceso										
PRE1	1 ¿Se tiene desarrollada, documentada e implementada una política de control de acceso que defina los derechos de acceso de los usuarios en función de las necesidades comerciales, teniendo en cuenta los requisitos de clasificación y manejo de la información, servicios, redes y / o aplicaciones a las que se accede, y cualquier requisito legal o reglamentario?				X			A9.1	A.9.1.1	- Los derechos y reglas de control de acceso deben estar claramente definidos en la política de control de acceso y que son consistentes con los requisitos de clasificación y manejo de la información. - Debe establecerse e implementarse mecanismos adecuados para hacer cumplir esta política. - Un derecho de acceso a un activo debe ser rastreable hasta una evaluación de riesgo y estar autorizado por el propietario correcto del activo. - Cualquier acceso a información sensible, o a instalaciones de procesamiento de información, debe basarse en los principios de "necesidad de saber" y "necesidad de usar", es decir, justificado por los requisitos comerciales y necesario para la tarea en cuestión. - El acceso en las políticas debe en lo posible ser basado en roles. - Las políticas deben contar con un nivel de clasificación de información. - Las políticas de acceso deben tener en cuenta procedimientos para los empleados que abandonan la organización, el cambio de funciones y requisitos laborales, etc. Estos
PRE2	2 ¿Los permisos de acceso de los usuarios están regidos por los requisitos comerciales, aprobados y revisados periódicamente por los propietarios del activo, y están claramente establecidos en la política de control de acceso?				X			A9.1	A.9.1.1	
Administración de acceso a usuarios										
PRE3	3 ¿Existe algún proceso implementada para poder segmentar solo el acceso permitido del usuario a la red, equipo o aplicación a la cual se le ah dado exclusivamente permiso?			X				A9.1	A.9.1.2	- Se pueden usar varios controles de acceso a la red, como la seguridad basada en puertos, para limitar el acceso a los servicios de red, y estos controles deben implementarse para respaldar la política de la organización sobre el uso de servicios de red. Un buen control y gestión de cambios es esencial para mantener correctos los accesos, y se requiere un seguimiento regular para proporcionar seguridad.
PRE4	4 ¿Se cuenta con un proceso manual para rastrear quién está usando la identificación de un usuario en un momento dado, asimismo de asegurarse de que no pueda ser utilizada por más de una persona en cualquier momento y cambiar las credenciales de autenticación cada vez que la identificación se pasa a un nuevo custodio.?					X		A9.2	A.9.2.1	- El proceso para crear y eliminar las Id de usuario debe documentarse y registrarse, y el proceso para los empleados que abandonan la organización debe incluir la eliminación inmediata de las ID de usuario. - Debe haber un proceso para auditar las identificaciones de manera regular, para detectar cualquier que se haya dejado activo inadvertidamente cuando ya no se necesitan. Las ID de usuario redundantes no se deben volver a emitir a otros usuarios debido al riesgo de otorgar inadvertidamente acceso excesivo y no autorizado a los recursos. - Las Id de usuario deben ser únicas y no compartidas.
PRE5	5 ¿Existe un formulario de registro de usuario, sobre el cual se describe el sistema de información, la red, el servicio o las aplicaciones requeridas, así como las condiciones de acceso?		X					A9.2	A.9.2.2	- Debe existir un formulario de registro de usuario y este debe estar firmado por el solicitante para documentar su aceptación de las condiciones, y por el propietario o custodio del sistema para documentar su autorización para que el solicitante se registre. Este formulario debe tener la ID de usuario agregada y luego estar archivada. - El acceso de los usuarios a los recursos se deben deshabilitar rápidamente cuando alguien deja de tener una razón comercial para acceder a los recursos, por ejemplo, la terminación del empleo o el cambio de trabajo interno. Deben establecerse procedimientos para garantizar esto. Debe haber procedimientos de notificación y responsabilidades y acciones claramente definidas si los empleados dejan la organización o cambian de empleo.
PRE6	6 ¿Existen usuarios que tiene acceso de nivel "superusuario" a las instalaciones o sistemas?¿Estos cuentan con el proceso adecuado según las necesidades frente a eventos que se necesiten, supervisión e historial?					X		A9.2	A.9.2.3	- El acceso administrativo completo o superusuario no debe utilizarse como método predeterminado para proporcionar privilegios elevados, a menos que el sistema no pueda proporcionar ningún nivel intermedio entre el usuario estándar y el acceso completo. - Para funciones críticas, como la administración del sistema, debe haber una identificación especial asignada a cada usuario únicamente para este propósito, además de su cuenta de usuario estándar en el sistema. - Debe guardarse un historial con las cuentas privilegiadas con datos específicos que demuestren el uso y propósito según el incidente o evento para el cual se usaron.
PRE7	7 ¿Existe un procedimiento para garantizar que las identificaciones de usuario y las contraseñas se emitan solo para aquellos con una necesidad comercial de acceso y que estén debidamente autorizadas por el propietario del recurso al que se accede?			X				A9.2	A.9.2.4	- Los usuarios deben firmar una declaración para mantener la confidencialidad de su información secreta de autenticación. - Debe existir procedimientos para garantizar que las contraseñas de proveedores temporales o predeterminadas se cambien de inmediato. - Los sistemas deben contar con un proceso de restablecimiento de contraseñas para los usuarios.

Muestra de datos obtenidos de las encuestas. PRE TEST. Periodo Junio. Sistema "SGH"

Cuestionario en base a la Gestión de accesos y su relación con los controles de la NTP-ISO/IEC 27001:2014						Sistema	SGH
Fecha:	26-07-2021	Tipo	PRE TEST	Periodo	Junio	Encuestado	Giovanni Ramirez Romero

* Marque con un "x" el nivel escogido.

			Nivel de cumplimiento *						Control de Referencia		
ID		Nº Disposición/procedimiento	Optimo (5)	Gestionado (4)	Definido (3)	Inicial (2)	No se realiza (1)	No aplica (0)	Control NTP	Sub Control	Recomendaciones / Procedimientos
Políticas de control de acceso											
PRE1	1	¿Se tiene desarrollada, documentada e implementada una política de control de acceso que defina los derechos de acceso de los usuarios en función de las necesidades comerciales, teniendo en cuenta los requisitos de clasificación y manejo de la información, servicios, redes y / o aplicaciones a las que se accede, y cualquier requisito legal o reglamentario?					X		A9.1	A.9.1.1	- Los derechos y reglas de control de acceso deben estar claramente definidos en la política de control de acceso y que son consistentes con los requisitos de clasificación y manejo de la información. - Debe establecerse e implementarse mecanismos adecuados para hacer cumplir esta política. - Un derecho de acceso a un activo debe ser rastreable hasta una evaluación de riesgo y estar autorizado por el propietario correcto del activo. - Cualquier acceso a información sensible, o a instalaciones de procesamiento de información, debe basarse en los principios de "necesidad de saber" y "necesidad de usar", es decir, justificado por los requisitos comerciales y necesario para la tarea en cuestión. - El acceso en las políticas debe en lo posible ser basado en roles. - Las políticas deben contar con un nivel de clasificación de información. - Las políticas de acceso deben tener en cuenta procedimientos para los empleados que abandonan la organización, el cambio de funciones y requisitos laborales, etc. Estos
PRE2	2	¿Los permisos de acceso de los usuarios están regidos por los requisitos comerciales, aprobados y revisados periódicamente por los propietarios del activo, y están claramente establecidos en la política de control de acceso?					X		A9.1	A.9.1.1	
Administración de acceso a usuarios											
PRE3	3	¿Existe algún proceso implementada para poder segmentar solo el acceso permitido del usuario a la red, equipo o aplicación a la cual se le ah dado exclusivamente permiso?				X			A9.1	A.9.1.2	- Se pueden usar varios controles de acceso a la red, como la seguridad basada en puertos, para limitar el acceso a los servicios de red, y estos controles deben implementarse para respaldar la política de la organización sobre el uso de servicios de red. Un buen control y gestión de cambios es esencial para mantener correctos los accesos, y se requiere un seguimiento regular para proporcionar seguridad.
PRE4	4	¿Se cuenta con un proceso manual para rastrear quién está usando la identificación de un usuario en un momento dado, asimismo de asegurarse de que no pueda ser utilizada por más de una persona en cualquier momento y cambiar las credenciales de autenticación cada vez que la identificación se pasa a un nuevo custodio.?					X		A9.2	A.9.2.1	- El proceso para crear y eliminar las Id de usuario debe documentarse y registrarse, y el proceso para los empleados que abandonan la organización debe incluir la eliminación inmediata de las ID de usuario. - Debe haber un proceso para auditar las identificaciones de manera regular, para detectar cualquier que se haya dejado activo inadvertidamente cuando ya no se necesitan. Las ID de usuario redundantes no se deben volver a emitir a otros usuarios debido al riesgo de otorgar inadvertidamente acceso excesivo y no autorizado a los recursos. - Las Id de usuario deben ser únicas y no compartidas.
PRE5	5	¿Existe un formulario de registro de usuario, sobre el cual se describe el sistema de información, la red, el servicio o las aplicaciones requeridas, así como las condiciones de acceso?					X		A9.2	A.9.2.2	- Debe existir un formulario de registro de usuario y este debe estar firmado por el solicitante para documentar su aceptación de las condiciones, y por el propietario o custodio del sistema para documentar su autorización para que el solicitante se registre. Este formulario debe tener la ID de usuario agregada y luego estar archivada. - El acceso de los usuarios a los recursos se deben deshabilitar rápidamente cuando alguien deja de tener una razón comercial para acceder a los recursos, por ejemplo, la terminación del empleo o el cambio de trabajo interno. Deben establecerse procedimientos para garantizar esto. Debe haber procedimientos de notificación y responsabilidades y acciones claramente definidas si los empleados dejan la organización o cambian de empleo.
PRE6	6	¿Existen usuarios que tiene acceso de nivel "superusuario" a las instalaciones o sistemas?¿Estos cuentan con el proceso adecuado según las necesidades frente a eventos que se necesiten, supervisión e historial?				X			A9.2	A.9.2.3	- El acceso administrativo completo o superusuario no debe utilizarse como método predeterminado para proporcionar privilegios elevados, a menos que el sistema no pueda proporcionar ningún nivel intermedio entre el usuario estándar y el acceso completo. - Para funciones críticas, como la administración del sistema, debe haber una identificación especial asignada a cada usuario únicamente para este propósito, además de su cuenta de usuario estándar en el sistema. - Debe guardarse un historial con las cuentas privilegiadas con datos específicos que demuestren el uso y propósito según el incidente o evento para el cual se usaron.
PRE7	7	¿Existe un procedimiento para garantizar que las identificaciones de usuario y las contraseñas se emitan solo para aquellos con una necesidad comercial de acceso y que estén debidamente autorizadas por el propietario del recurso al que se accede?					X		A9.2	A.9.2.4	- Los usuarios deben firmar una declaración para mantener la confidencialidad de su información secreta de autenticación. - Debe existir procedimientos para garantizar que las contraseñas de proveedores temporales o predeterminadas se cambien de inmediato. - Los sistemas deben contar con un proceso de restablecimiento de contraseñas para los usuarios.

Muestra de datos obtenidos de las encuestas. POST TEST. Periodo Noviembre. Sistema "Web Vacaciones"

Cuestionario en base a la Gestión de accesos y su relación con los controles de la NTP-ISO/IEC 27001:2014						Sistema	Web Vacaciones
Fecha:	26-09-2021	Tipo	POST TEST	Periodo	Septiembre	Encuestado	Giovanni Ramirez Romero

* Marque con un "x" el nivel escogido.

			Nivel de cumplimiento *						Control de Referencia		
ID		N° Disposición/procedimiento	Optimo (5)	Gestionado (4)	Definido (3)	Inicial (2)	No se realiza (1)	No aplica (0)	Control NTP	Sub Control	Recomendaciones / Procedimientos
Políticas de control de acceso											
PRE1	1	¿Se tiene desarrollada, documentada e implementada una política de control de acceso que defina los derechos de acceso de los usuarios en función de las necesidades comerciales, teniendo en cuenta los requisitos de clasificación y manejo de la información, servicios, redes y / o aplicaciones a las que se accede, y cualquier requisito legal o reglamentario?	X						A9.1	A.9.1.1	- Los derechos y reglas de control de acceso deben estar claramente definidos en la política de control de acceso y que son consistentes con los requisitos de clasificación y manejo de la información. - Debe establecerse e implementarse mecanismos adecuados para hacer cumplir esta política. - Un derecho de acceso a un activo debe ser rastreable hasta una evaluación de riesgo y estar autorizado por el propietario correcto del activo. - Cualquier acceso a información sensible, o a instalaciones de procesamiento de información, debe basarse en los principios de "necesidad de saber" y "necesidad de usar", es decir, justificado por los requisitos comerciales y necesario para la tarea en cuestión.
PRE2	2	¿Los permisos de acceso de los usuarios están regidos por los requisitos comerciales, aprobados y revisados periódicamente por los propietarios del activo, y están claramente establecidos en la política de control de acceso?	X						A9.1	A.9.1.1	- El acceso en las políticas debe en lo posible ser basado en roles. - Las políticas deben contar con un nivel de clasificación de información. - Las políticas de acceso deben tener en cuenta procedimientos para los empleados que abandonan la organización, el cambio de funciones y requisitos laborales, etc. Estos
Administración de acceso a usuarios											
PRE3	3	¿Existe algún proceso implementada para poder segmentar solo el acceso permitido del usuario a la red, equipo o aplicación a la cual se le ah dado exclusivamente permiso?	X						A9.1	A.9.1.2	- Se pueden usar varios controles de acceso a la red, como la seguridad basada en puertos, para limitar el acceso a los servicios de red, y estos controles deben implementarse para respaldar la política de la organización sobre el uso de servicios de red. Un buen control y gestión de cambios es esencial para mantener correctos los accesos, y se requiere un seguimiento regular para proporcionar seguridad.
PRE4	4	¿Se cuenta con un proceso manual para rastrear quién está usando la identificación de un usuario en un momento dado, asimismo de asegurarse de que no pueda ser utilizada por más de una persona en cualquier momento y cambiar las credenciales de autenticación cada vez que la identificación se pasa a un nuevo custodio.?	X						A9.2	A.9.2.1	- El proceso para crear y eliminar las Id de usuario debe documentarse y registrarse, y el proceso para los empleados que abandonan la organización debe incluir la eliminación inmediata de las ID de usuario. - Debe haber un proceso para auditar las identificaciones de manera regular, para detectar cualquier que se haya dejado activo inadvertidamente cuando ya no se necesitan. Las ID de usuario redundantes no se deben volver a emitir a otros usuarios debido al riesgo de otorgar inadvertidamente acceso excesivo y no autorizado a los recursos. - Las Id de usuario deben ser únicas y no compartidas.
PRE5	5	¿Existe un formulario de registro de usuario, sobre el cual se describe el sistema de información, la red, el servicio o las aplicaciones requeridas, así como las condiciones de acceso?		X					A9.2	A.9.2.2	- Debe existir un formulario de registro de usuario y este debe estar firmado por el solicitante para documentar su aceptación de las condiciones, y por el propietario o custodio del sistema para documentar su autorización para que el solicitante se registre. Este formulario debe tener la ID de usuario agregada y luego estar archivada. - El acceso de los usuarios a los recursos se deben deshabilitar rápidamente cuando alguien deja de tener una razón comercial para acceder a los recursos, por ejemplo, la terminación del empleo o el cambio de trabajo interno. Deben establecerse procedimientos para garantizar esto. Debe haber procedimientos de notificación y responsabilidades y acciones claramente definidas si los empleados dejan la organización o cambian de empleo.
PRE6	6	¿Existen usuarios que tiene acceso de nivel "superusuario" a las instalaciones o sistemas?¿Estos cuentan con el proceso adecuado según las necesidades frente a eventos que se necesiten, supervisión e historial?		X					A9.2	A.9.2.3	- El acceso administrativo completo o superusuario no debe utilizarse como método predeterminado para proporcionar privilegios elevados, a menos que el sistema no pueda proporcionar ningún nivel intermedio entre el usuario estándar y el acceso completo. - Para funciones críticas, como la administración del sistema, debe haber una identificación especial asignada a cada usuario únicamente para este propósito, además de su cuenta de usuario estándar en el sistema. - Debe guardarse un historial con las cuentas privilegiadas con datos específicos que demuestren el uso y propósito según el incidente o evento para el cual se usaron.
PRE7	7	¿Existe un procedimiento para garantizar que las identificaciones de usuario y las contraseñas se emitan solo para aquellos con una necesidad comercial de acceso y que estén debidamente autorizadas por el propietario del recurso al que se accede?		X					A9.2	A.9.2.4	- Los usuarios deben firmar una declaración para mantener la confidencialidad de su información secreta de autenticación. - Debe existir procedimientos para garantizar que las contraseñas de proveedores temporales o predeterminadas se cambien de inmediato. - Los sistemas deben contar con un proceso de restablecimiento de contraseñas para los usuarios.

Anexo 3. Fichas de expertos

Ficha de registro de datos de investigacion - PRE TEST

I. Datos Generales

Apellidos y nombres	Karen Rocio García Vera Tudela
Grado académico	Ing, Magister
Fecha	20-Nov-21

Datos a evaluar	Fichas de registro **PRE TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investig	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumen	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

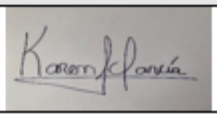
INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.			70%		
Objetividad	Esta expresado en conductas observables.				73%	
Pertinencia	Adecuado para el tipo de investigación.				72%	
Organización	Muestra los datos ordenados.					80%
Suficiencia	Comprende los aspectos de cantidad y calidad.				75%	
Adecuación	Adecuado para valorar el constructo o variable a medir.			70%		
Consistencia	Basado en aspectos teóricos científicos.				79%	
Coherencia	Presenta coherencia en la información presentada.				78%	
Metodología	Responde al propósito de la investigación.			70%		
Significatividad	Es útil y adecuado para la medición.					82%

III. Promedio	75%	**Muy Bueno**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 24/09/2021	40643722	

Ficha de registro de datos de investigacion - RE TEST

I. Datos Generales

Apellidos y nombres	Karen Rocio García Vera Tudela
Grado académico	Ing, Magister
Fecha	20-Nov-21

Datos a evaluar	Fichas de registro **RE TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investig	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumen	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

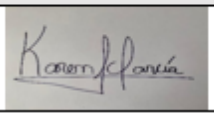
INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.				72%	
Objetividad	Esta expresado en conductas observables.				75%	
Pertinencia	Adecuado para el tipo de investigación.				75%	
Organización	Muestra los datos ordenados.					80%
Suficiencia	Comprende los aspectos de cantidad y calidad.				75%	
Adecuación	Adecuado para valorar el constructo o variable a medir.			70%		
Consistencia	Basado en aspectos teóricos científicos.				80%	
Coherencia	Presenta coherencia en la información presentada.				78%	
Metodología	Responde al propósito de la investigación.			70%		
Significatividad	Es útil y adecuado para la medición.					82%

III. Promedio	76%	**Muy Bueno**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 24/09/2021	40643722	

Ficha de registro de datos de investigacion - POST TEST

I. Datos Generales

Apellidos y nombres	Karen Rocio García Vera Tudela
Grado académico	Ing, Magister
Fecha	20-Nov-21

Datos a evaluar	Fichas de registro **POST TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investig	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumen	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

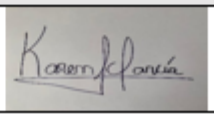
INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.					95%
Objetividad	Esta expresado en conductas observables.					90%
Pertinencia	Adecuado para el tipo de investigación.					90%
Organización	Muestra los datos ordenados.					95%
Suficiencia	Comprende los aspectos de cantidad y calidad.					92%
Adecuación	Adecuado para valorar el constructo o variable a medir.					90%
Consistencia	Basado en aspectos teóricos científicos.					95%
Coherencia	Presenta coherencia en la información presentada.					95%
Metodología	Responde al propósito de la investigación.					90%
Significatividad	Es útil y adecuado para la medición.					91%

III. Promedio	92%	**Excelente**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 24/09/2021	40643722	

Ficha de registro de datos de investigacion - PRE TEST

I. Datos Generales

Apellidos y nombres	Roldan Palacios Christian Jonatan
Grado académico	Ing, Magister
Fecha	20/11/2021

Datos a evaluar	Fichas de registro **PRE TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investigació	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumento	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.				72%	
Objetividad	Esta expresado en conductas observables.				71%	
Pertinencia	Adecuado para el tipo de investigación.			70%		
Organización	Muestra los datos ordenados.				78%	
Suficiencia	Comprende los aspectos de cantidad y calidad.				73%	
Adecuación	Adecuado para valorar el constructo o variable a medir.			69%		
Consistencia	Basado en aspectos teóricos científicos.				75%	
Coherencia	Presenta coherencia en la información presentada.				80%	
Metodología	Responde al propósito de la investigación.			70%		
Significatividad	Es útil y adecuado para la medición.					80%

III. Promedio	74%	**Muy Bueno**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 24/09/2021	46840169	

Ficha de registro de datos de investigacion - RE TEST

I. Datos Generales

Apellidos y nombres	Roldan Palacios Christian Jonatan
Grado académico	Ing, Magister
Fecha	20/11/2021

Datos a evaluar	Fichas de registro **RE TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investigac	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumento	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.				75%	
Objetividad	Esta expresado en conductas observables.				71%	
Pertinencia	Adecuado para el tipo de investigación.			70%		
Organización	Muestra los datos ordenados.				80%	
Suficiencia	Comprende los aspectos de cantidad y calidad.				73%	
Adecuación	Adecuado para valorar el constructo o variable a medir.			70%		
Consistencia	Basado en aspectos teóricos científicos.				78%	
Coherencia	Presenta coherencia en la información presentada.				80%	
Metodología	Responde al propósito de la investigación.			70%		
Significatividad	Es útil y adecuado para la medición.					80%

III. Promedio	75%	**Muy Bueno**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 24/09/2021	46840169	

Ficha de registro de datos de investigacion - POST TEST

I. Datos Generales

Apellidos y nombres	Roldan Palacios Christian Jonatan
Grado académico	Ing, Magister
Fecha	20/11/2021

Datos a evaluar	Fichas de registro **POST TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investigaci	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumento	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.					85%
Objetividad	Esta expresado en conductas observables.					90%
Pertinencia	Adecuado para el tipo de investigación.					89%
Organización	Muestra los datos ordenados.					95%
Suficiencia	Comprende los aspectos de cantidad y calidad.					93%
Adecuación	Adecuado para valorar el constructo o variable a medir.					89%
Consistencia	Basado en aspectos teóricos científicos.					94%
Coherencia	Presenta coherencia en la información presentada.					95%
Metodología	Responde al propósito de la investigación.					95%
Significatividad	Es útil y adecuado para la medición.					90%

III. Promedio	92%	**Excelente**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 24/09/2021	46840169	

Ficha de registro de datos de investigacion - PRE TEST

I. Datos Generales

Apellidos y nombres	Luz Elizabeth Mejia Ulffe
Grado académico	Ing
Fecha	20/11/2021

Datos a evaluar	Fichas de registro **PRE TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investigaci	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumento	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

INDICADORES	CRITERIOS	DEFICIENTE 0 - 20%	REGULAR 21 - 50 %	BUENO 51 - 70%	MUY BUENO 71 - 80%	EXCELENTE 81 - 100%
Claridad	Esta formulado con lenguaje apropiado.				75%	
Objetividad	Esta expresado en conductas observables.			70%		
Pertinencia	Adecuado para el tipo de investigación.			65%		
Organización	Muestra los datos ordenados.				80%	
Suficiencia	Comprende los aspectos de cantidad y calidad.				75%	
Adecuación	Adecuado para valorar el constructo o variable a medir.			70%		
Consistencia	Basado en aspectos teóricos científicos.				80%	
Coherencia	Presenta coherencia en la información presentada.				79%	
Metodología	Responde al propósito de la investigación.			70%		
Significatividad	Es útil y adecuado para la medición.					84%

III. Promedio	75%	**Muy Bueno**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 30/09/2021	41297935	

Ficha de registro de datos de investigacion - RE TEST

I. Datos Generales

Apellidos y nombres	Luz Elizabeth Mejia Ulffe
Grado académico	Ing
Fecha	20/11/2021

Datos a evaluar	Fichas de registro **RE TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investig	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumen	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.				78%	
Objetividad	Esta expresado en conductas observables.			70%		
Pertinencia	Adecuado para el tipo de investigación.			70%		
Organización	Muestra los datos ordenados.				80%	
Suficiencia	Comprende los aspectos de cantidad y calidad.				78%	
Adecuación	Adecuado para valorar el constructo o variable a medir.			70%		
Consistencia	Basado en aspectos teóricos científicos.					82%
Coherencia	Presenta coherencia en la información presentada.				79%	
Metodología	Responde al propósito de la investigación.			70%		
Significatividad	Es útil y adecuado para la medición.					85%

III. Promedio	76%	**Muy Bueno**

IV. Aplicabilidad

*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

Lugar y fecha	DNI	Firma
Lima, 30/09/2021	41297935	

Ficha de registro de datos de investigacion - POST TEST

I. Datos Generales

Apellidos y nombres	Luz Elizabeth Mejia Ulffe
Grado académico	Ing
Fecha	20/11/2021

Datos a evaluar	Fichas de registro POST **TEST** - Políticas de acceso, Administración de acceso, Responsabilidad de usuarios y Acceso a Sistemas y aplicaciones
Titulo de la investigaci	"Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021"
Autor del instrumento	Montenegro Martínez, Yonathan Damner - Conislla Ramirez, Christian Augusto

II. Aspecto de evaluación

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50 %	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
Claridad	Esta formulado con lenguaje apropiado.					90%
Objetividad	Esta expresado en conductas observables.					92%
Pertinencia	Adecuado para el tipo de investigación.					89%
Organización	Muestra los datos ordenados.					95%
Suficiencia	Comprende los aspectos de cantidad y calidad.					95%
Adecuación	Adecuado para valorar el constructo o variable a medir.					90%
Consistencia	Basado en aspectos teóricos científicos.					94%
Coherencia	Presenta coherencia en la información presentada.					93%
Metodología	Responde al propósito de la investigación.					94%
Significatividad	Es útil y adecuado para la medición.					92%

III. Promedio	92%	**Excelente**

IV. Aplicabilidad

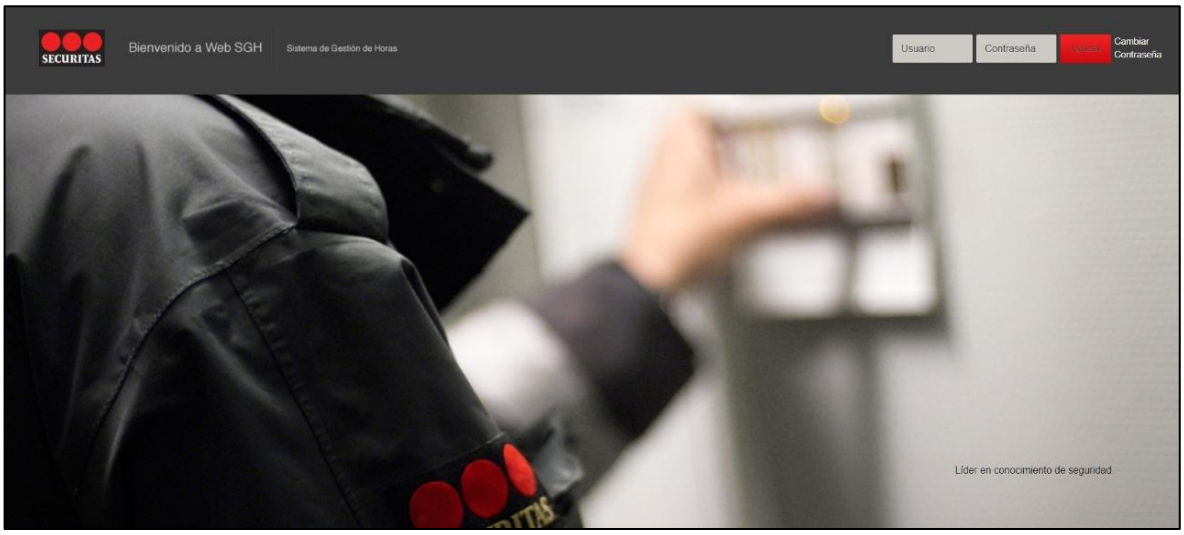
*** Marque con una "X"**

Voto de aplicabilidad	Procede su aplicación	X
	Procede su aplicación previo levantamiento de las observaciones	
	No procede su aplicación	

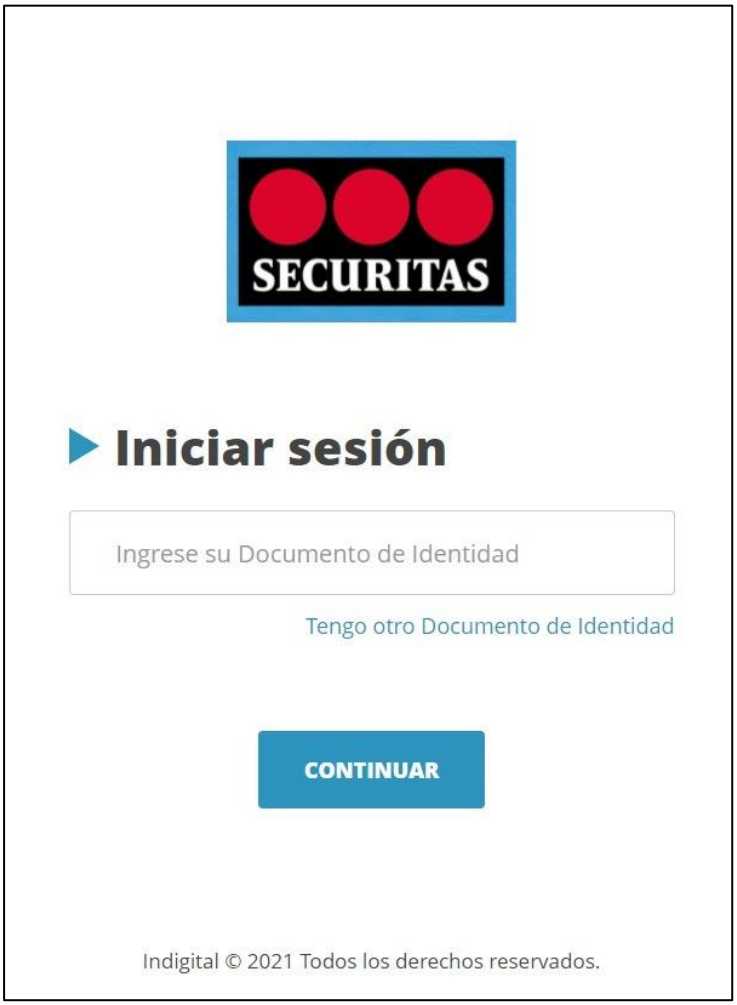
Lugar y fecha	DNI	Firma
Lima, 30/09/2021	41297935	

Anexo 4. Sistemas de información Securitas SAC

Sistema SGH



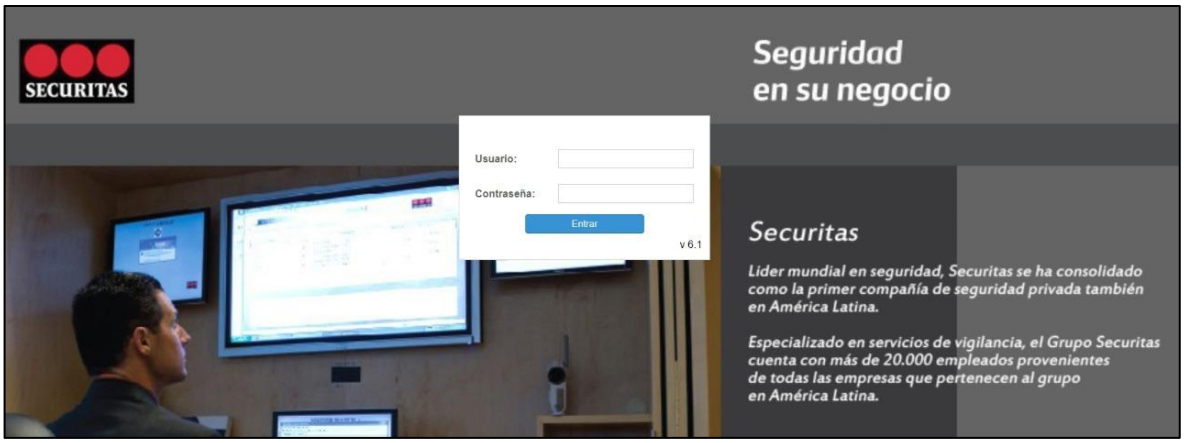
Sistema Smart Boletas



Sistema web de vacaciones

Sistema Contratos NOE

Sistema Securitas Visión



Anexo 5. Tabla de activos de sistemas de información

Tipo	Tipo de activo	ID	Nombre	Supported Business Service	Description del software	Clasificación
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS001	ERP "softland" V 3.4.0.0	Enterprise Resource Planner	Planificador de Recursos Empresariales de la empresa.	On premise
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS002	Securitas Vision	Customer Relationship Management	Gestión operativa para las rondas controladas en Clientes	Cloud
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS003	SGH	Human Capital Management	Gestión operativa para tareo de Colaboradores	On premise
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS004	SGM	Customer Relationship Management	Gestión operativa para las rondas Mobiles de clientes	On premise
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS005	Securitas Connect	Reporting Serv	Gestión de información en reportes a clientes y gerencia	Cloud
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS006	Smart Boleta Suit	Human Capital Management	Gestión de documentos laborales para colaboradores, boletas contratos	Cloud
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS008	Facturación Electronica	Expense Management System	Gestor de documentos digitales de índole fiscal Perú	On premise
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS014	Contratos NOE	Customer Relationship Management	Portal para gestionar contratos comerciales y proveedores	Cloud
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS021	Web Vacaciones	Human Capital Management	Gestión de vacaciones para colaboradores de securitas	On premise
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS035	Active Directory	Usuarios de dominio	Creaciòn de usuarios y licencias windows	On premise

Anexo 6. Tablas de valoración de activos

							Valor de los activos					
Tipo	**Tipo de activo**	**ID**	**Nombre**	**Supported Business Service**	**Description del software**	**Clasificación**	**D**	**I**	**C**	**Total**	**Valor**	**Descripción de impactos al negocio**
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS001	ERP "softland" V 3.4.0.0	Enterprise Resource Planner	Planificador de Recursos Empresariales de la empresa.	On premise	10	10	10	10	Extremo	Los daños son extremos ya que los datos del ERP son muy sensibles a todas las áreas de la compañía y esta son de carácter fiscal.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS002	Securitas Vision	Customer Relationship Management	Gestión operativa para las rondas controladas en Clientes	Cloud	8	6	7	7	Medio	El impacto es importante ya que el aplicativo cuenta con inforamción operativa y maneja personal para la seguridad de los clientes todos los días.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS003	SGH	Human Capital Management	Gestión operativa para tareo de Colaboradores	On premise	9	8	7	24	Alto	El impacto es alto ya que se maneja información sensible de los tareos de todos los colaboradores operativo de la compañía que prestan el servicio de seguridad en los clientes.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS004	SGM	Customer Relationship Management	Gestión operativa para las rondas Mobiles de clientes	On premise	8	8	7	23	Alto	El impacto es importante ya que el aplicativo cuenta con información operativa que maneja personal y vehículos para la seguridad de los clientes todos los días.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS005	Securitas Connect	Reporting Serv	Gestión de información en reportes a clientes y gerencia	Cloud	6	9	10	25	Alto	El impacto es alto porque en este aplicativo se gestionan todos los reportes tanto por parte de gerencia como para los clientes, es información muy sensible para la compañía.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS006	Smart Boleta Suit	Human Capital Management	Gestión de documentos laborales para colaboradores, boletas contratos	Cloud	8	6	10	24	Alto	El impato es alto porque maneja todo los documentos laborales de los trabajadores de la compañía como boletas de pago, gratificaciones, firam de contratos, etc.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS008	Facturación Electronica	Expense Management System	Gestor de documentos digitales de índole fiscal Perú	On premise	9	10	9	28	Alto	El impacto es alto ya que maneja documentos de índole fiscal para la facturación de los clientes.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS014	Contratos NOE	Customer Relationship Management	Portal para gestionar contratos comerciales y proveedores	Cloud	9	10	10	29	Alto	El impacto es alto ya que maneja información de los acuerdos entre los clientes y la compañía de manera Legal y fiscal.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS021	Web Vacaciones	Human Capital Management	Gestión de vacaciones para colaboradores de securitas	On premise	7	8	7	22	Alto	El impacto es alto ya que se maneja información relacionada a la gestión de todas las vacaciones de los colaboradores, es muy importante ya que se relaciona con muchas áreas de la compañía.
[SW] Software - Aplicaciones informáticas	[sub] desarrollo a medida (subcontratado)	SIS035	Active Directory	Usuarios de dominio	Creaciòn de usuarios y licencias windows	On premise	10	6	6	22	Alto	El impacto es alto porque se maneja todos los usuarios de los colaboradores de la compañía y se gestiona todas las licencias de windows como Office 365, powerBi entre otros.

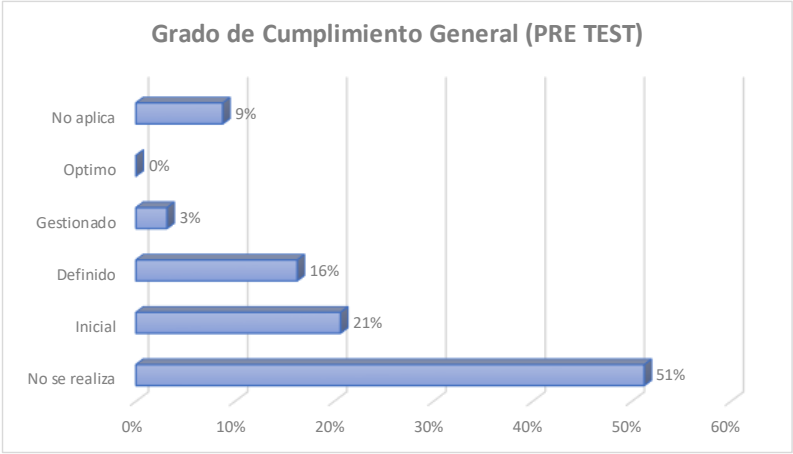
Anexo 7. Análisis de amenazas por cada sistema de información

Análisis de amenazas					
Tipo	**Descripcion**	**Impacto**	**Probabilidad**	**Riesgo**	**Nivel**
[E.15] Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	4	3	12	Alto
[I.5] Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	5	3	15	Muy alto
[E.1] Errores de los usuario	Equivocaciones de las personas cuando usan los servicios, datos, etc.	3	4	12	Alto
[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	2	2	4	Medio
[E.8] Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	5	3	15	Muy alto
[E.14] Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	4	2	8	Alto
[E.15] Alteración accidental de la información	Alteración accidental de la información	2	1	2	Bajo
[E.18] Destrucción de información	Pérdida accidental de información.	3	2	6	Medio
[E.19] Fugas de información	Revelación por indiscreción.	4	1	4	Medio
[E.21] Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	2	4	8	Alto
[A.5] Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.	5	2	10	Alto
[A.6] Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	4	2	8	Alto
[A.7] Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	3	1	3	Bajo
[A.8] Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc	5	2	10	Alto
[A.9] [Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.	3	2	6	Medio
[A.10] Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	4	1	4	Medio
[A.11] Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	5	2	10	Alto
[A.15] Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio	4	2	8	Alto
[A.18] Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio	4	1	4	Medio
[A.19] Divulgación de información	Revelación de información.	4	1	4	Medio
[A.22] Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	4	1	4	Medio

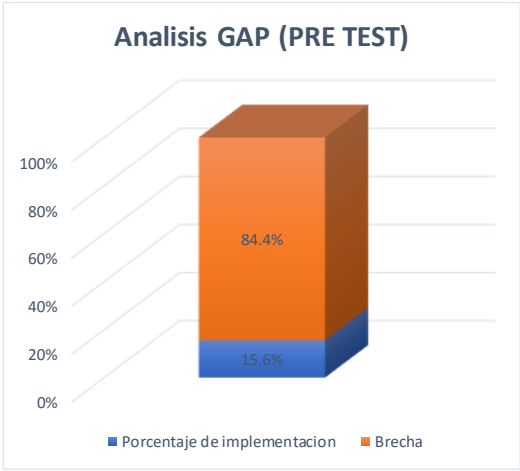
Anexo 8. Análisis de cumplimiento PRE TEST – Resultado de procedimientos

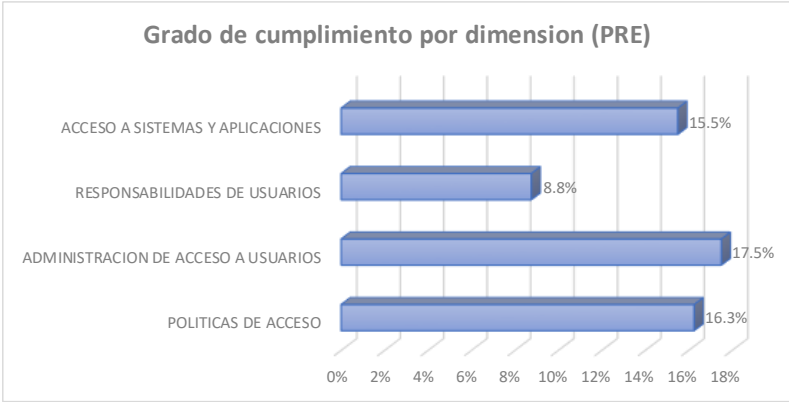
Análisis de cumplimiento PRE TEST - Procedimientos

GESTION DE ACCESOS							
	No se realiza	Inicial	Definido	Gestionado	Optimo	No aplica	
Items	0%	25%	50%	75%	100%	N/A	TOTALES
D1	12	4	3	1	0	0	20
D2	36	14	13	3	0	4	70
D3	15	3	2	0	0	0	20
D4	19	12	8	1	0	10	50
TOTALES	82	33	26	5	0	14	160
%	51%	21%	16%	3%	0%	9%	
	0	8.25	13	3.75	0		
PORCENTAJE DE IMPLEMENTACION							
15.6%							



% CUMPLIMIENTO POR DIMENSION	
POLITICAS DE ACCESO	16.3%
ADMINISTRACION DE ACCESO A USUARIOS	17.5%
RESPONSABILIDADES DE USUARIOS	8.8%
ACCESO A SISTEMAS Y APLICACIONES	15.5%
Porcentaje de implementacion	**15.6%**
Brecha	**84.4%**

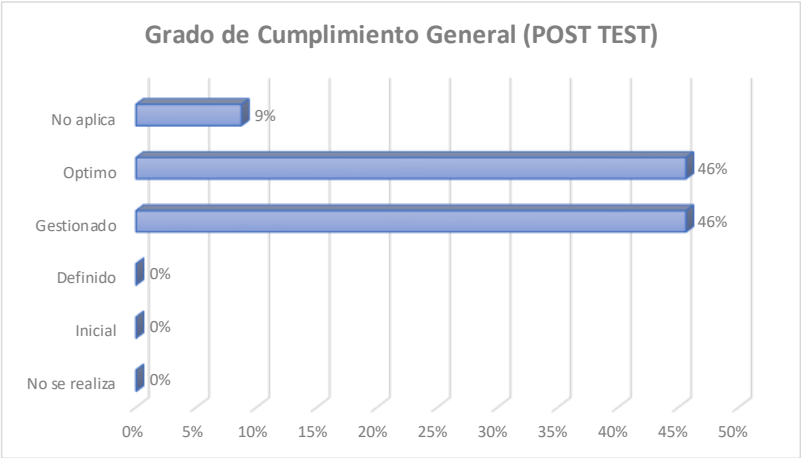




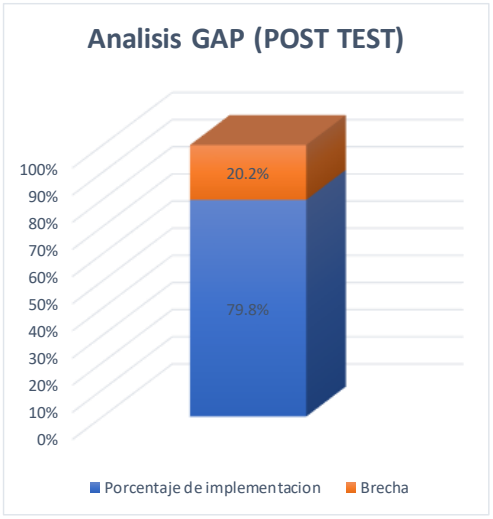
Anexo 9. Análisis de cumplimiento POST TEST – Resultado de procedimientos

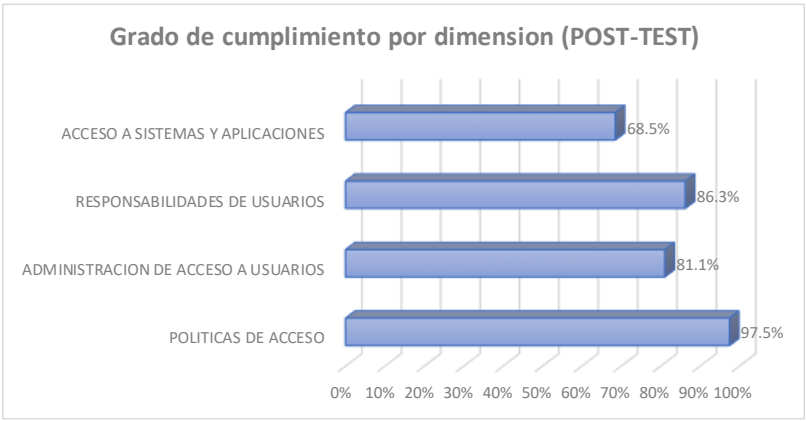
Análisis de cumplimiento POST TEST - Procedimientos

GESTION DE ACCESOS							
	No se realiza	Inicial	Definido	Gestionado	Optimo	No aplica	
Items	0%	25%	50%	75%	100%	N/A	TOTALES
D1	0	0	0	2	18	0	20
D2	0	0	0	37	29	4	70
D3	0	0	0	11	9	0	20
D4	0	0	0	23	17	10	50
TOTALES	0	0	0	73	73	14	160
%	0%	0%	0%	46%	46%	9%	
	0	0	0	54.75	73		
PORCENTAJE DE IMPLEMENTACION							
79.84%							



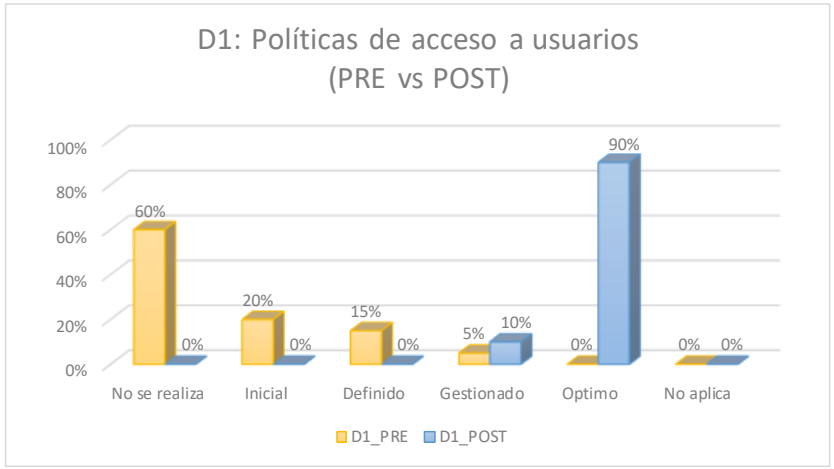
% CUMPLIMIENTO POR DIMENSION	
POLITICAS DE ACCESO	97.5%
ADMINISTRACION DE ACCESO A USUARIOS	81.1%
RESPONSABILIDADES DE USUARIOS	86.3%
ACCESO A SISTEMAS Y APLICACIONES	68.5%
Porcentaje de implementacion	**79.8%**
Brecha	**20.2%**

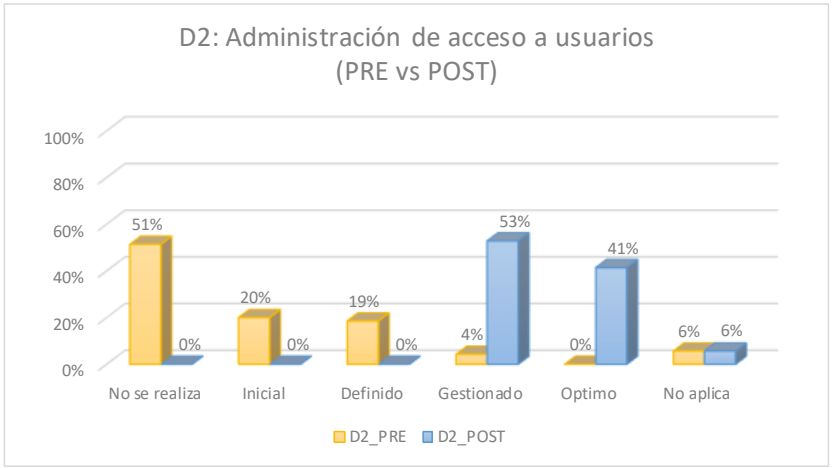


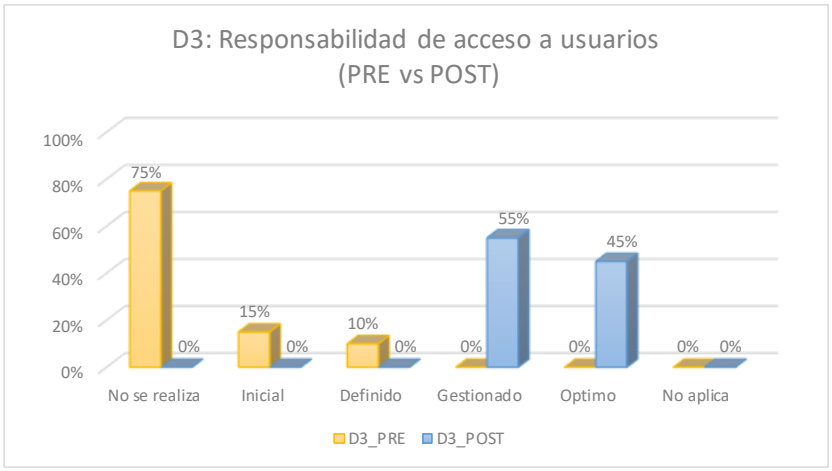


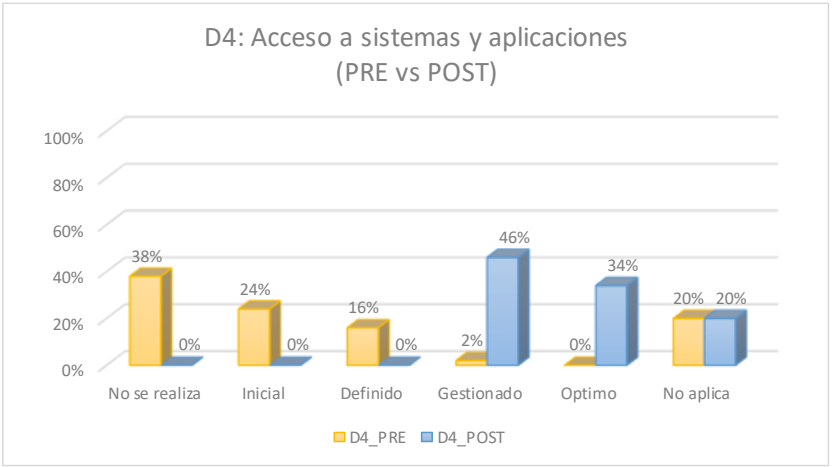
Anexo 10. Grados de cumplimiento según sus valores PRE vs POST

Grados de cumplimiento por dimensiones (PRE vs POST)



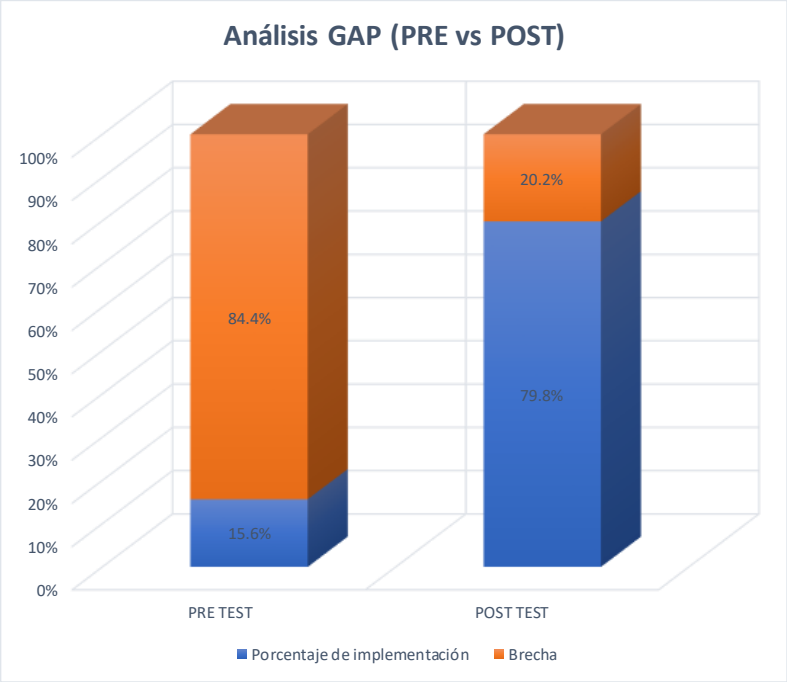


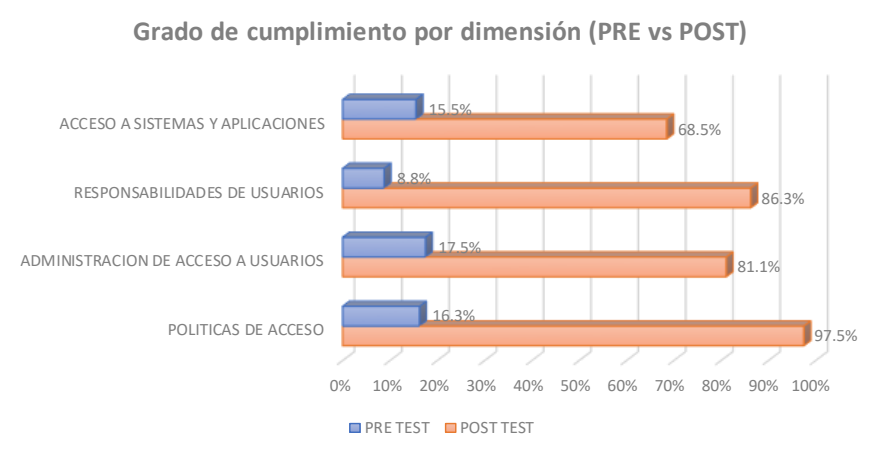


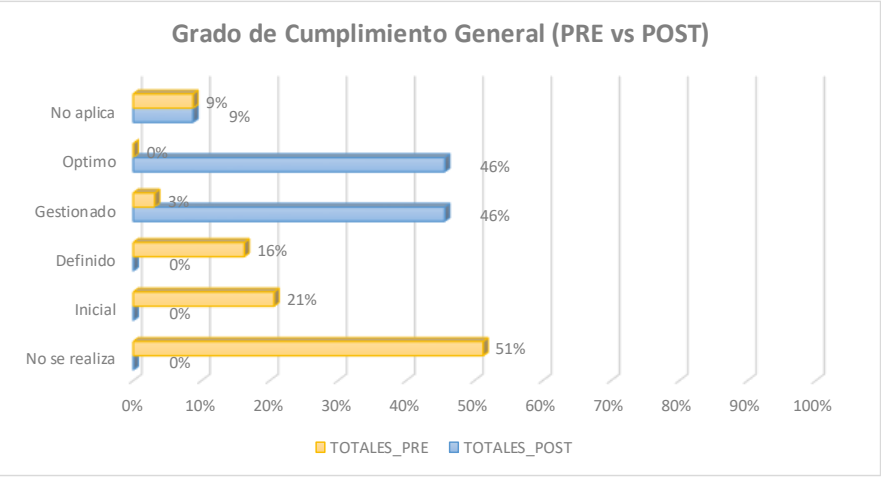


Anexo 11. Resultados generales para valores PRE vs POST. Análisis GAP.

% CUMPLIMIENTO POR DIMENSION		
Dimensión	**PRE TEST**	**POST TEST**
POLITICAS DE ACCESO	16.3%	97.5%
ADMINISTRACION DE ACCESO A USUARIOS	17.5%	81.1%
RESPONSABILIDADES DE USUARIOS	8.8%	86.3%
ACCESO A SISTEMAS Y APLICACIONES	15.5%	68.5%
Porcentaje de implementación	**15.6%**	**79.8%**
Brecha	**84.4%**	**20.2%**







}

Anexo 12. Base de datos obtenida para PRE, RE y POST TEST que se usaran a través de la herramienta SPSS.

Políticas de acceso a usuario		
Item	Grado de cumplimiento	
	PRE	POST
SIS001	0.25	1.00
SIS002	0.00	0.75
SIS003	0.00	1.00
SIS004	0.00	1.00
SIS005	0.00	1.00
SIS006	0.38	1.00
SIS007	0.00	1.00
SIS014	0.38	1.00
SIS021	0.00	1.00
SIS035	0.63	1.00
Total	0.16	0.98

Administración de acceso a usuarios		
Item	Grado de cumplimiento	
	PRE	POST
SIS001	0.25	0.82
SIS002	0.00	0.93
SIS003	0.00	0.86
SIS004	0.00	0.79
SIS005	0.00	0.93
SIS006	0.38	0.61
SIS007	0.00	0.86
SIS014	0.38	0.61
SIS021	0.00	0.82
SIS035	0.63	0.89
Total	0.16	0.81

Responsabilidad de acceso de usuarios		
Item	Grado de cumplimiento	
	PRE	POST
SIS001	0.00	0.88
SIS002	0.00	1.00
SIS003	0.00	0.88
SIS004	0.00	0.88
SIS005	0.13	0.75
SIS006	0.25	0.75
SIS007	0.00	0.88
SIS014	0.38	0.88
SIS021	0.00	0.88
SIS035	0.13	0.88
Total	0.09	0.86

Acceso a sistemas y aplicaciones		
Item	Grado de cumplimiento	
	PRE	POST
SIS001	0.05	0.75
SIS002	0.10	0.75
SIS003	0.10	0.75
SIS004	0.10	0.75
SIS005	0.15	0.70
SIS006	0.25	0.75
SIS007	0.10	0.75
SIS014	0.25	0.75
SIS021	0.10	0.75
SIS035	0.35	0.80
Total	0.16	0.75

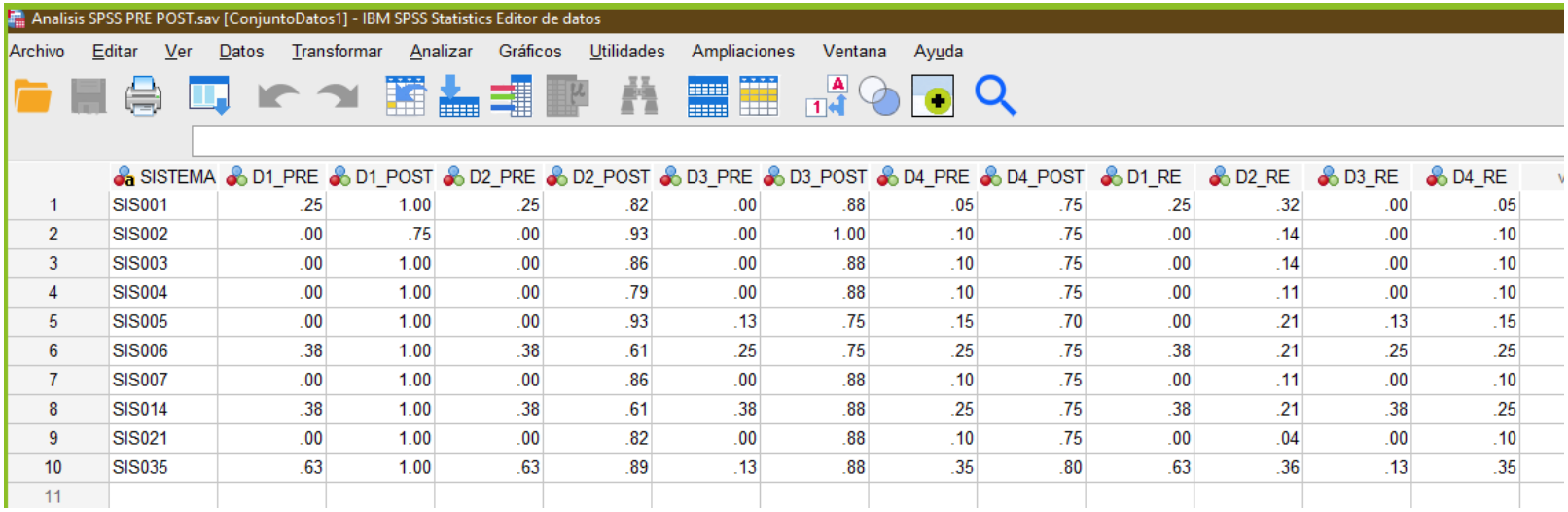
Políticas de acceso a usuario		
Item	Grado de cumplimiento	
	PRE	RE
SIS001	0.25	0.25
SIS002	0.00	0.00
SIS003	0.00	0.00
SIS004	0.00	0.00
SIS005	0.00	0.00
SIS006	0.38	0.38
SIS007	0.00	0.00
SIS014	0.38	0.38
SIS021	0.00	0.00
SIS035	0.63	0.63

Administración de acceso a usuarios		
Item	Grado de cumplimiento	
	PRE	RE
SIS001	0.25	0.32
SIS002	0.00	0.14
SIS003	0.00	0.14
SIS004	0.00	0.11
SIS005	0.00	0.21
SIS006	0.38	0.21
SIS007	0.00	0.11
SIS014	0.38	0.21
SIS021	0.00	0.04
SIS035	0.63	0.36

Responsabilidad de acceso de		
Item	Grado de cumplimiento	
	PRE	RE
SIS001	0.00	0.00
SIS002	0.00	0.00
SIS003	0.00	0.00
SIS004	0.00	0.00
SIS005	0.13	0.13
SIS006	0.25	0.25
SIS007	0.00	0.00
SIS014	0.38	0.38
SIS021	0.00	0.00
SIS035	0.13	0.13

Acceso a sistemas y aplicaciones		
Item	Grado de cumplimiento	
	PRE	RE
SIS001	0.05	0.05
SIS002	0.10	0.10
SIS003	0.10	0.10
SIS004	0.10	0.10
SIS005	0.15	0.15
SIS006	0.25	0.25
SIS007	0.10	0.10
SIS014	0.25	0.25
SIS021	0.10	0.10
SIS035	0.35	0.35

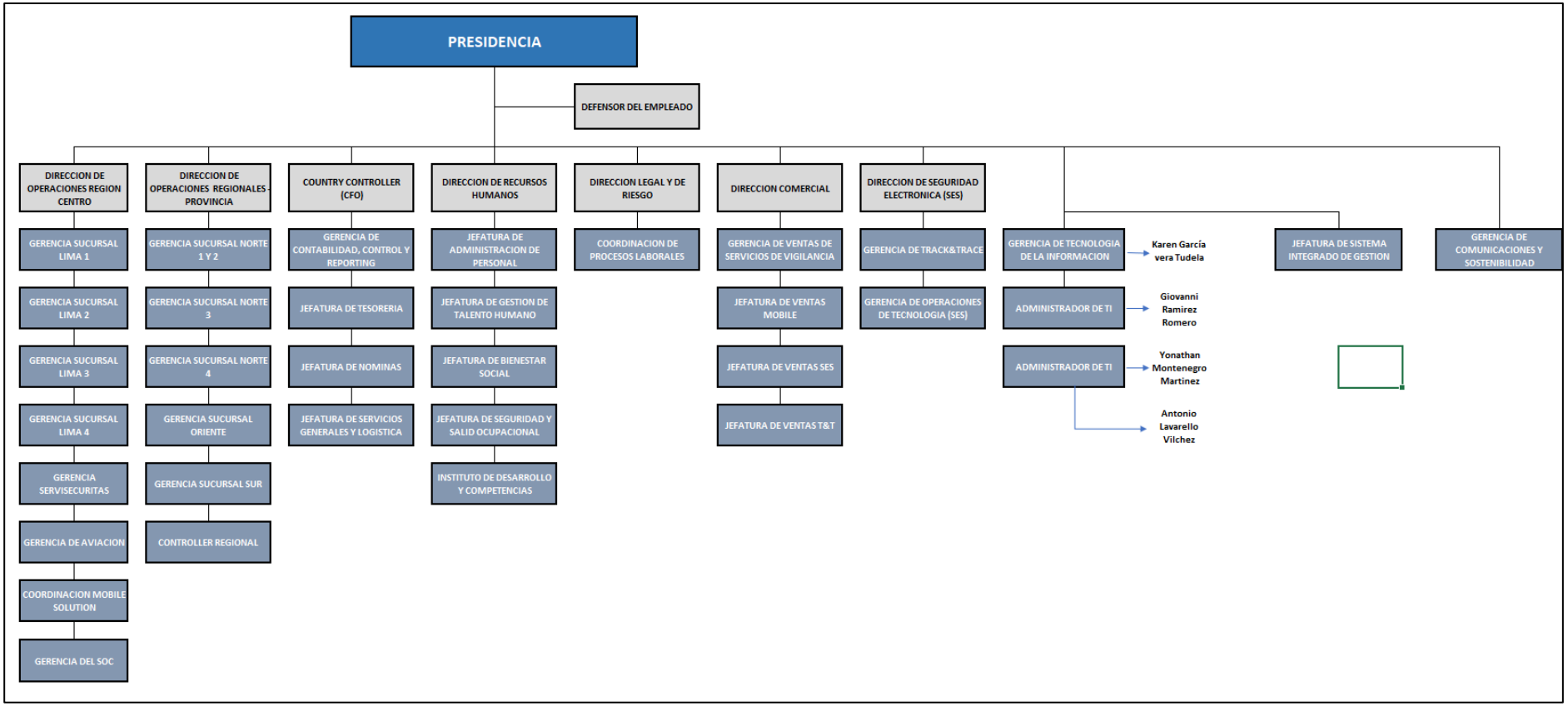
Anexo 13. Base de datos SPSS.



	SISTEMA	D1_PRE	D1_POST	D2_PRE	D2_POST	D3_PRE	D3_POST	D4_PRE	D4_POST	D1_RE	D2_RE	D3_RE	D4_RE
1	SIS001	.25	1.00	.25	.82	.00	.88	.05	.75	.25	.32	.00	.05
2	SIS002	.00	.75	.00	.93	.00	1.00	.10	.75	.00	.14	.00	.10
3	SIS003	.00	1.00	.00	.86	.00	.88	.10	.75	.00	.14	.00	.10
4	SIS004	.00	1.00	.00	.79	.00	.88	.10	.75	.00	.11	.00	.10
5	SIS005	.00	1.00	.00	.93	.13	.75	.15	.70	.00	.21	.13	.15
6	SIS006	.38	1.00	.38	.61	.25	.75	.25	.75	.38	.21	.25	.25
7	SIS007	.00	1.00	.00	.86	.00	.88	.10	.75	.00	.11	.00	.10
8	SIS014	.38	1.00	.38	.61	.38	.88	.25	.75	.38	.21	.38	.25
9	SIS021	.00	1.00	.00	.82	.00	.88	.10	.75	.00	.04	.00	.10
10	SIS035	.63	1.00	.63	.89	.13	.88	.35	.80	.63	.36	.13	.35
11													

	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
1	SISTEMA	Cadena	8	0		Ninguna	Ninguna	8	Izquierda	Nominal	Entrada
2	D1_PRE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
3	D1_POST	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
4	D2_PRE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
5	D2_POST	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
6	D3_PRE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
7	D3_POST	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
8	D4_PRE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
9	D4_POST	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
10	D1_RE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
11	D2_RE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
12	D3_RE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
13	D4_RE	Numérico	8	2		Ninguna	Ninguna	8	Derecha	Nominal	Entrada
14											

Anexo 14. Organigrama Funcional SECURITAS SAC



Anexo 15. Publicación El Peruano resolución ministerial N° 004-2016-PCM

ANEXO 2

RELACIÓN DE REPRESENTANTES DEL GOBIERNO NACIONAL ANTE COMISIÓN INTERGUBERNAMENTAL DEL SECTOR AGRICULTURA Y RIEGO, CONFORMADA EN EL MARCO DEL DECRETO SUPREMO Nº 047-2009-PCM

	CARGO	DEPENDENCIA / INSTITUCIÓN	CARGO
1	Viceministro (a) de Política Agrarias	Despacho Viceministerial	Presidente Comisión Intergubernamental
2	Director (a) de la Oficina General de Planeamiento	Oficina General de Planeamiento y Presupuesto	Miembro
3	Profesional		Miembro Alterno
4	Profesional	Oficina General de Asesoría Jurídica	Miembro
5	Profesional	Oficina General de Administración	Miembro
6	Profesional	Oficina General de Gestión de Recursos Humanos	Miembro
7	Director (a) General de Articulación Intergubernamental	Dirección General de Articulación Intergubernamental	Miembro
8	Director (a) de Gestión Descentralizada		Miembro
9	Director de Seguimiento y Evaluación de Políticas (a)	Dirección General de Seguimiento y Evaluación de Políticas	Miembro
10	Director (a) de Estadística Agraria		Miembro Alterno
11	Director (a) General de Políticas Agrarias	Dirección General de Políticas Agrarias	Miembro
12	Director (a) de Políticas y Normatividad Agraria		Miembro
13	Profesional	Dirección General de Negocios Agrarios	Miembro
14	Profesional		Miembro Alterno
15	Profesional	Dirección General de Asuntos Ambientales Agrarios	Miembro
16	Profesional	Dirección General de Infraestructura Agraria y Riego	Miembro
17	Profesional	Servicio Nacional Forestal y de Fauna Silvestre	Miembro
18	Profesional		Miembro
19	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRORURAL	Miembro
20	Profesional		Miembro Alterno
21	Jefe (a) del Programa	Programa de Compensaciones para la Competitividad - AGROIDEAS	Miembro
22	Jefe (a) de la Unidad de Planificación, Seguimiento y Evaluación		Miembro
23	Director (a) de Gestión del Riego	Programa Sub Sectorial de Irrigaciones (PSI)	Miembro
24	Profesional		Miembro Alterno
25	Director (a) de la Unidad de Estudios y Cooperación de la Oficina de Planificación y Desarrollo Institucional	Servicio Nacional de Sanidad Agraria (SENASA)	Miembro
26	Profesional		Miembro
27	Director (a) General de la Oficina de Planeamiento y Presupuesto	Instituto Nacional de Innovación Agraria (INIA)	Miembro
28	Profesional		Miembro Alterno
29	Director (a) de Conservación y Planeamiento de Recursos Hídricos	Autoridad Nacional del Agua (ANA)	Miembro

1332846-1

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL
Nº 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo Nº 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia Nº 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo Nº 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema

Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerandos precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando Nº 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo Nº 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación

Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación

La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 3.- De la implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.

Artículo 4.- De la certificación de la norma

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

- El/la titular de la entidad;
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1° de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial Nº 129-2012-PCM.

Regístrese, comuníquese y publíquese.

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1333015-1

AGRICULTURA Y RIEGO

Delegan facultades a diversos funcionarios del Ministerio durante el Ejercicio 2016

RESOLUCIÓN MINISTERIAL
Nº 0006-2016-MINAGRI

Lima, 12 de enero de 2016

CONSIDERANDO:

Que, mediante la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, se definen las funciones generales y la estructura orgánica de los Ministerios, precisando en el último párrafo de su artículo 25, que los Ministros de Estado pueden delegar, en los funcionarios de su cartera ministerial, las facultades y atribuciones que no sean privativas a su función, siempre que la normatividad lo autorice;

Que, de acuerdo a lo dispuesto en el último párrafo del artículo 9 del Decreto Legislativo N° 997, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de Agricultura, modificado por la Ley N° 30048, en adelante la LOF del MINAGRI, el Ministro puede delegar las facultades y atribuciones que no sean privativas a su función;

Que, el tercer párrafo del literal c) del artículo 8 de la Ley N° 30225, Ley de Contrataciones del Estado, señala que el Titular de la Entidad podrá delegar, mediante resolución, la autoridad que dicha Ley le otorga, salvo los casos expresamente previstos en el referido literal;

Que, según el numeral 7.1 del artículo 7 del Texto Único Ordenado de la Ley Nº 28411, Ley General del Sistema Nacional de Presupuesto, aprobado mediante Decreto Supremo Nº 304-2012-EF, el Titular de una Entidad es la más alta Autoridad Ejecutiva y puede delegar sus funciones en materia presupuestal cuando lo establezca expresamente, entre otras, la citada Ley General;

Que, asimismo, el numeral 40.2 del artículo 40 del referido Texto Único Ordenado de la Ley Nº 28411, establece que las modificaciones presupuestarias en el nivel Funcional Programático son aprobadas mediante Resolución del Titular, a propuesta de la Oficina de Presupuesto o de la que haga sus veces en la Entidad, y que el Titular puede delegar dicha facultad de aprobación, a través de disposición expresa, la misma que debe ser publicada en el Diario Oficial El Peruano;

Resolución Ministerial

N° 004-2016-PCM

Lima, - 8 ENE. 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo Nº 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia Nº 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos

Anexo 16. Declaración jurada de no tener conflicto de intereses

Securitas

DECLARACIÓN JURADA DE NO TENER CONFLICTO DE INTERES

Yo, Yonathan Damner Montenegro Martinez, investigador Principal de la investigación: "Propuesta de implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021", declaro bajo juramento y en honor a la verdad que no me encuentro en una situación de conflicto de intereses de índole económica, política, familiar, sentimental o de otra naturaleza que puedan afectar la ejecución del presente protocolo de investigación.

En caso de tener situación de conflicto de interés, este es: Ninguno

Como constancia de lo expresado en la presente declaración firmo a continuación.

Magdalena, 05 de Setiembre de 2021

Yonathan Damner Montenegro Martinez

45208321

SECURITAS S.A.C.
RECIBIDO
05 SEP. 2021
RECEPCIÓN
HORA..... FIRMA.....

Anexo 17. Política general de control de accesos

SECURITAS

1. CONTROL DE ACCESO

1.1. Antecedentes

Para la empresa Securitas SAC es importante controlar quienes tienen acceso a la información. Es esencial de que el área de TI pueda decidir quien tiene permiso para acceder a la información de la compañía el saber el cómo, cuándo y con que finalidad. A la hora de gestionar el control de acceso a nuestros datos debemos tener en cuenta que la información, los servicios y las aplicaciones utilizadas no tienen por qué ubicarse de manera centralizada en nuestras instalaciones, sino que pueden estar **diseminadas** en equipos y redes remotas propias o de terceros. También tenemos que considerar que cada vez es más habitual el uso de **dispositivos móviles** en los centros de trabajo. En ocasiones estos dispositivos son propiedad del propio empleado lo que dificulta esta tarea. Por otra parte, el registro de los accesos en *logs* de los sistemas va a ser determinante para analizar los incidentes de seguridad.

1.2. Objetivos

Establecer **quien**, **como** y **cuando** puede acceder a los activos de información de la empresa SECURITAS SAC y registrar convenientemente dichos accesos.

1.3. Lista de verificación

Para el cumplimiento de la política de seguridad en lo relativo al control de acceso incluimos a continuación una serie de controles.

Por su nivel de complejidad se clasifican en dos niveles:
-Básico (**B**):
Son asumibles los esfuerzos y recursos necesarios. Para las aplicaciones más comunes se pueden aplicar funcionalidades sencillas ya incorporadas. Para prevenir los ataques se pueden instalar herramientas de seguridad elementales.

-Avanzado (**A**):
Son considerables los esfuerzos y recursos necesarios para implementarlos.
Se pueden precisar mecanismos de recuperación ante fallos al requerir configuraciones complejas de los sistemas.

Los controles podrán tener el siguiente **alcance**:
Procesos (**PRO**): aplica a la dirección o al personal de gestión.
Tecnología (**TEC**): aplica al personal técnico especializado.
Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Política de usuarios y grupos** Defines los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.	☐
B	PRO	**Asignación de permisos** Asignas los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.	☐
B	TEC	**Creación/modificación/borrado de cuentas de usuario con permisos** Defines y aplicas un **procedimiento** para dar de alta/baja o modificar las cuentas de usuario.	☐
B	TEC	**Cuentas de administración** Gestionas las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.	☐

A	TEC	**Mecanismos de autenticación** Determinas e implantas las técnicas de autenticación más apropiados para permitir el acceso a la información de tu empresa.	☐
A	TEC	**Registro de eventos** Estableces los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de tu empresa.	☐
B	TEC	**Revisión de permisos** Revisas cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.	☐
B	TEC	**Revocación de permisos y eliminación de cuentas** Desactivas los permisos de acceso y eliminas las cuentas de usuario una vez finalizada la relación contractual.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

Política de usuarios y grupos.

Definiremos una serie de grupos que tendrán determinados accesos para cada tipo de información establecido. Esta clasificación se puede hacer teniendo en cuenta los siguientes aspectos:

- ✓ En función del área o departamento al que pertenezca el empleado.
- ✓ En función del tipo de información a la qué accederá.
- ✓ En función de las operaciones permitidas sobre la información a la que se tiene acceso.
- ✓ En función de los criterios anteriores podemos establecer diversos perfiles de usuarios.

Asignación de permisos. Una vez establecidos los tipos de información, los perfiles de usuarios y los grupos existentes, podremos concretar los tipos de acceso a la información a los que tienen derecho. Los permisos concretarán que acciones pueden realizar sobre la información (escritura, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el **mínimo privilegio** en el establecimiento de los permisos.

Creación/modificación/borrado de cuentas de usuario. Para permitir el acceso real a los sistemas de información de la empresa debemos tener un **procedimiento** que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios (por ejemplo: cuenta de correo, acceso al ERP, etc.) indicando quién debe autorizarlo. Detallaremos los datos identificativos de las mismas, las acciones que se permiten y las dotaremos de las credenciales de accesos correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales, así como de la Política de contraseñas.

SECURITAS

Cuentas de administración: Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Tendremos en cuenta los siguientes aspectos:

- ✓ Utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración.
- ✓ Implantar un control de acceso basado en un doble factor de autenticación.
- ✓ Registrar convenientemente todas sus acciones (registro de *logs*).
- ✓ El acceso como administrador debería ser notificado convenientemente.
- ✓ Evitar que los privilegios de las cuentas de administrador puedan ser heredados.
- ✓ Las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia.
- ✓ Pueden ser sometidas a auditorías periódicas.

Mecanismos de autenticación: Se debe definir e implantaremos los mecanismos de autenticación más adecuados para permitir el acceso a la información de la empresa SECURITAS SAC. Tendremos en cuenta aspectos tales como:

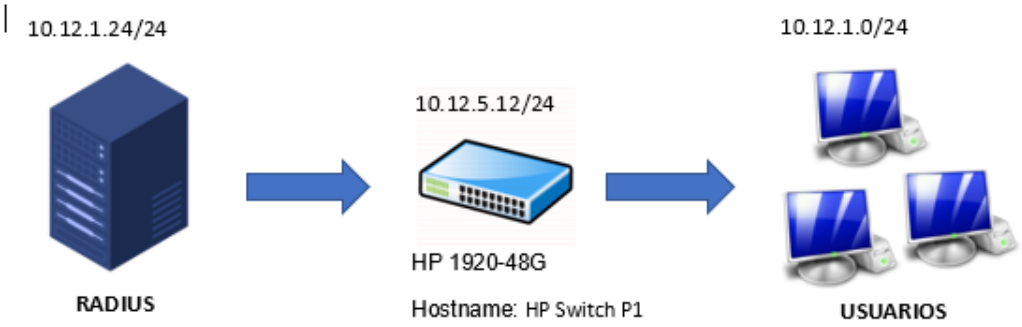
- ✓ utilizar mecanismos de autenticación internos o basados en servicios de autenticación aprobados por la empresa (como autenticación con Microsoft Azure*)* las tecnologías que utilizaremos:
  - Autenticación vía web
  - Servicios de directorio activo
  - Factores de los mecanismos de autenticación (uno o varios):
  - Algo que sabemos (a través de contraseñas)
  - Algo que tenemos (a través de dispositivos personales, *tokens*)

Registro de eventos: Se debe de establecer los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa. Registraremos convenientemente quién accede a nuestra información, cuando, cómo y con qué finalidad.

Revisión de permisos: Se debe revisar periódicamente que los permisos concedidos a los usuarios son los adecuados.

Revocación de permisos y eliminación de cuentas: Al finalizar la relación contractual con el empleado, es necesario revocar sus permisos de accesos a los sistemas e instalaciones. Eliminaremos cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, exigiremos la devolución de cualquier activo de información que se le hubiese asignado (laptos, tokens o celulares).

Anexo 18. Procedimiento de implementación de control de accesos en capa de red de datos con protocolo 802.1X y servidor RADIUS.



CONFIGURACIÓN DE SWITCH HP

A continuación, se muestras los principales pasos para poder habilitar este método en el switch de capa 2 enlace de datos en la red de SECURITAS SAC. Es necesario tener en cuenta que esto se aplicó a dos puertos de prueba que se contaban en dicho switch. Asimismo, la configuración adicional en el servidor RADIUS como AAA, EAP necesarias son posible habilitarlas:

1. Configurando puertos de switch como autenticación 802.1X.

Usuario -→ HP Switch P1(config)# aaa port-access authenticator 10-12

HP Switch P1(config)# aaa port-access authenticator 10-12 client-limit 4

2. Configurar el método de autenticación a 802.1X

HP Switch P1(config)# aaa authentication port-access eap-radius

HP Switch P1(config)# show authentication

3. Asignar la dirección IP del servidor RADIUS

HP Switch P1(config)# radius host 10.12.1.24

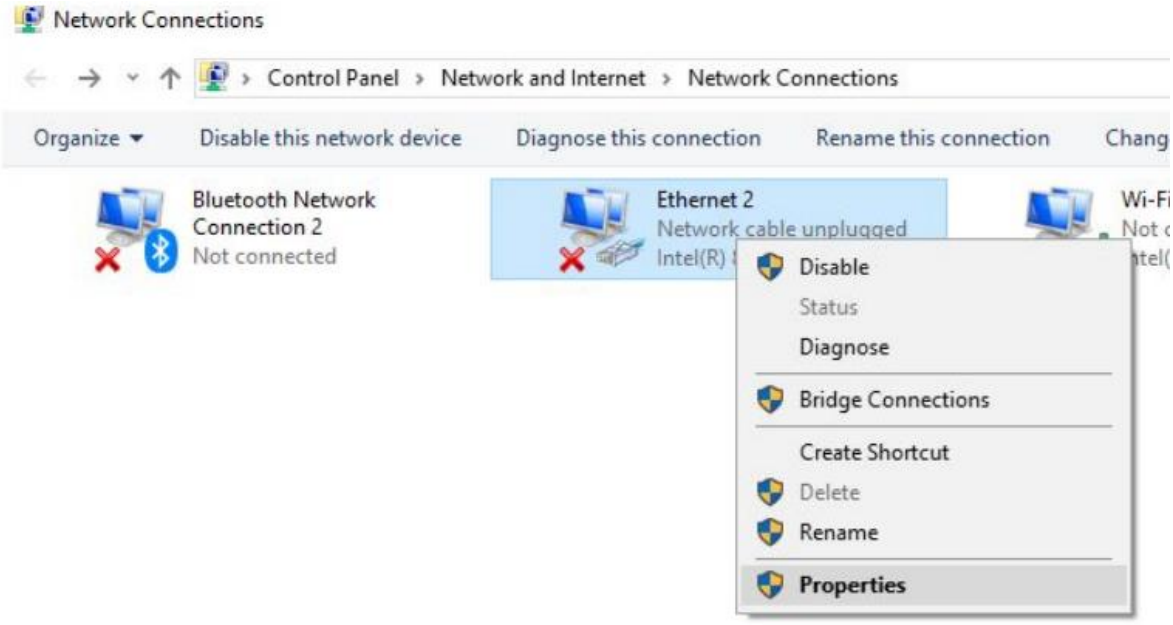
4. Habilitar el método de autenticación a 802.1X

HP Switch P1(config)# aaa port-access authenticator active

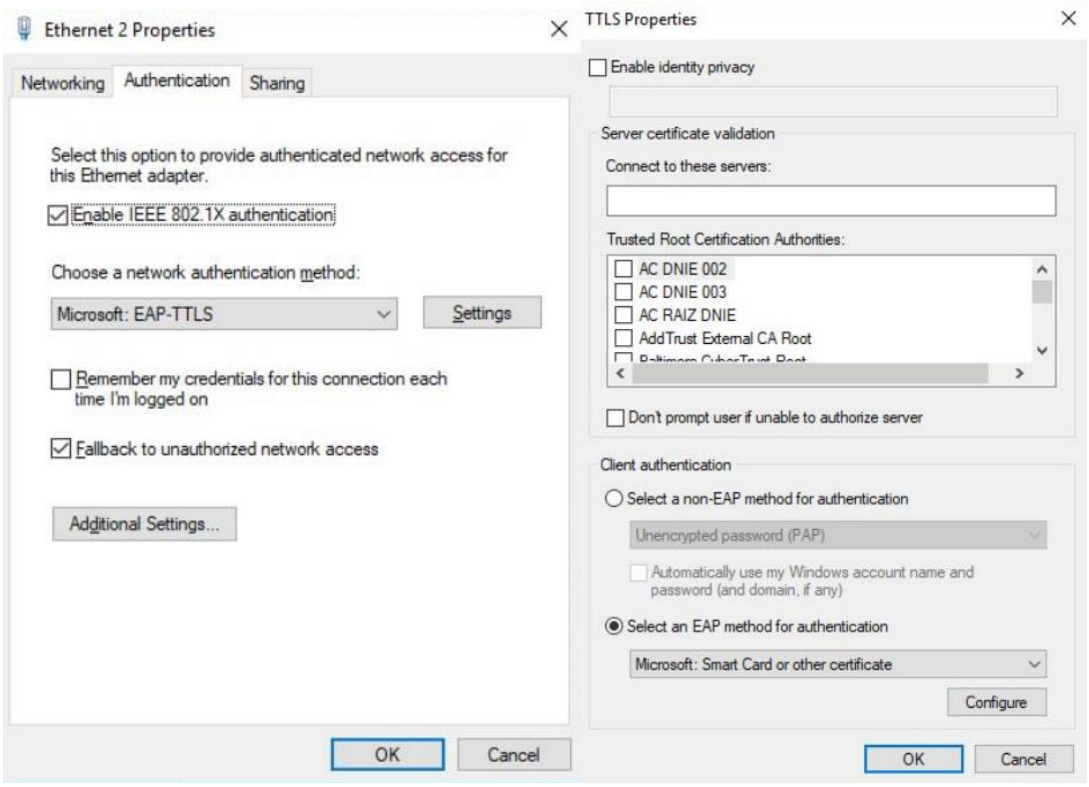
CONFIGURACIÓN DE SERVICIOS EN SERVIDOR RADIUS

1. Instalamos el rol de Servicios de dominio Active Directory (AD DS), DHCP y DNS2.
2. Instalar Direct Access y VPN (RAS)
3. Configuración de servidor Radius desde Directivas de red (nps.msc).
4. Registrar servidor en Active Directory desde MMC
5. Autorizar Servidor NPS para usar active Directory en la autenticación de usuarios y grupos.
6. Agregar cliente RADIUS creando nombre de cliente y dirección IP valida
7. Agregar método de autenticación MS-CHAP V2
8. Agregar grupos del dominio.
9. Ajustar filtrado IP
10. Ajustamos Cifrado para tráfico entre los clientes y servidores.
11. Asignar nombre Kerberos.

Se configura por PC conectada a la red la configuración adicional en los adaptadores para que permitan la autenticación por 801.1x solicitando el usuarios y contraseña.

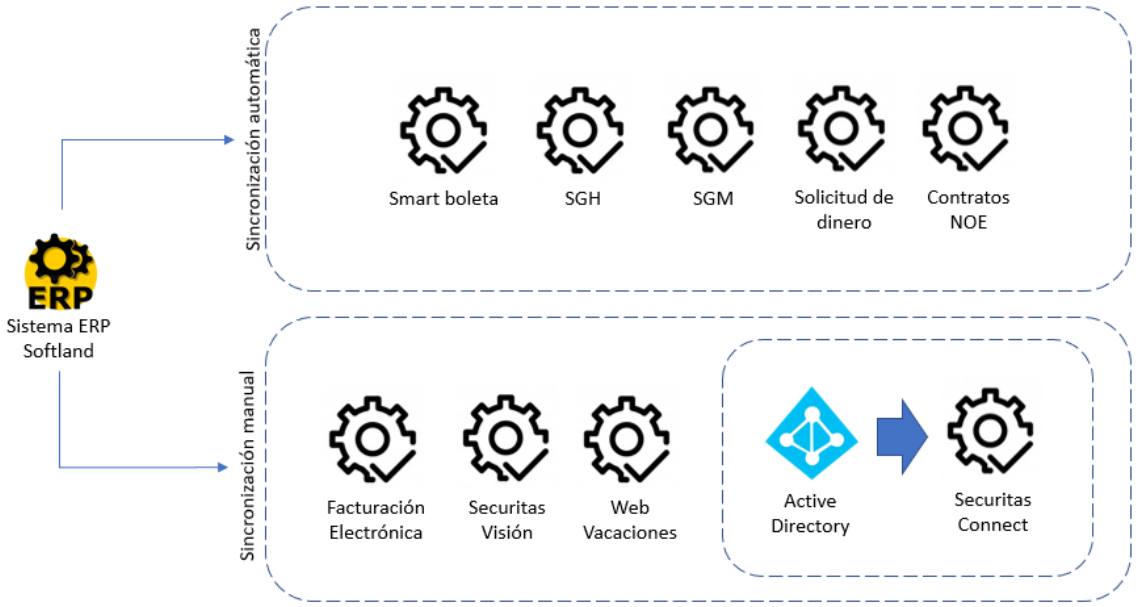


Se habilita la opción IEEE 802.1X y luego en las propiedades de EAP TTLS se configura el método de authentication por EAP.



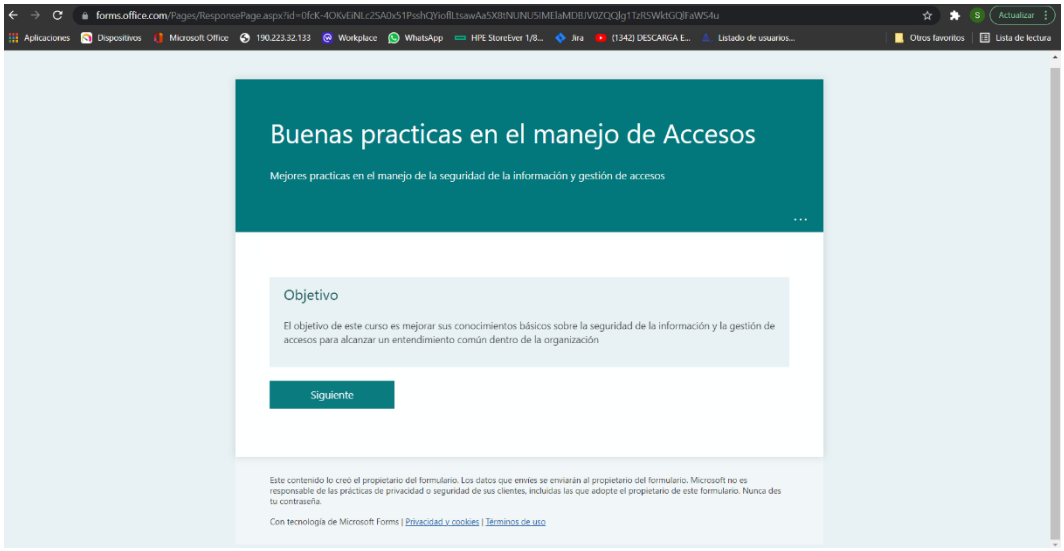
Anexo 19. Esquema de sistemas críticos y su relación automatizada en la creación de usuarios basados en sistema ERP Softland.

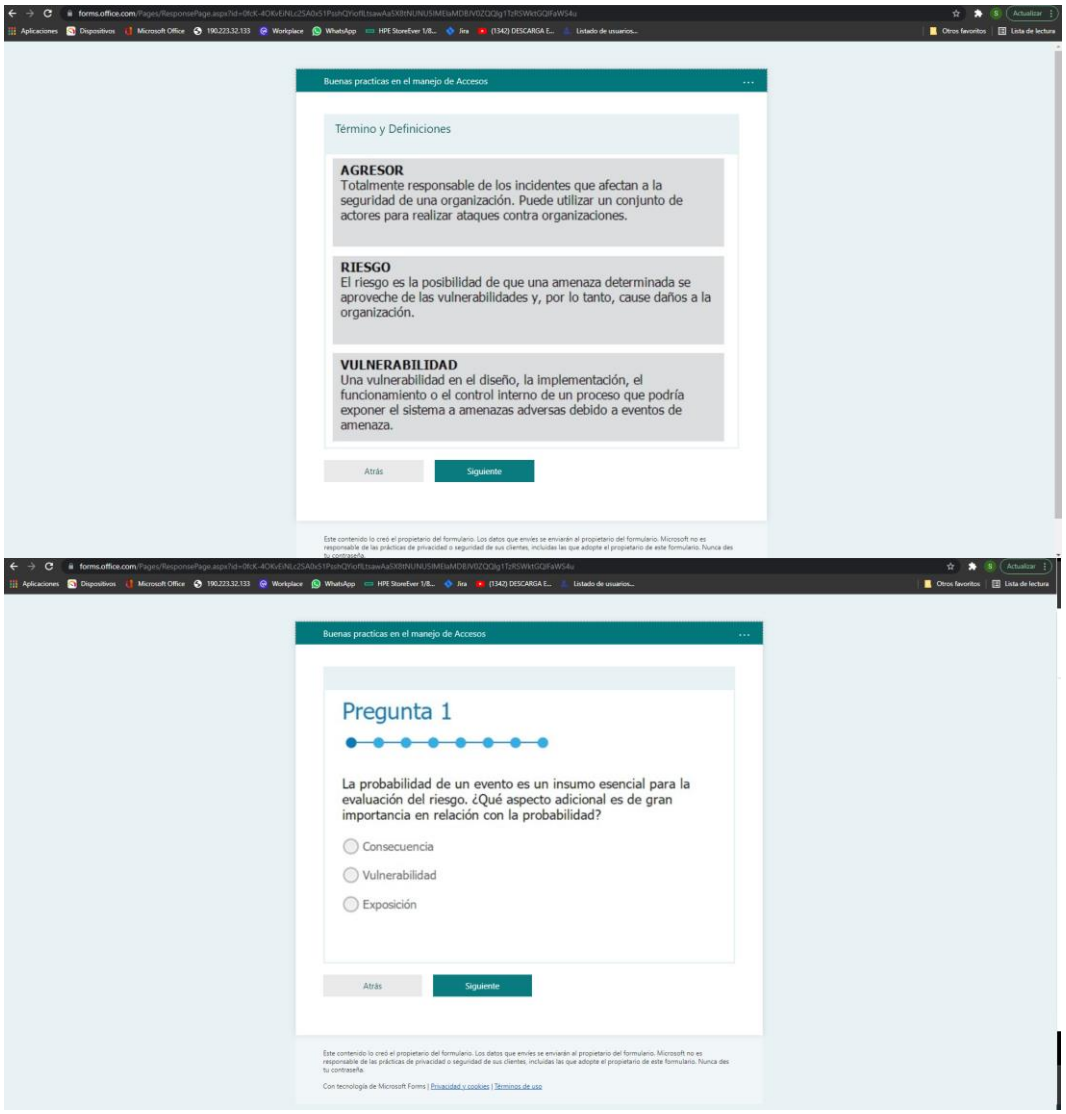
Se observa que las sincronizaciones automáticas son relacionadas al ERP el cual crea las identidades principales de los usuarios cuando empiezan a trabajar en la compañía y otra serie de aplicaciones que no son sincronizadas con el mismo método.

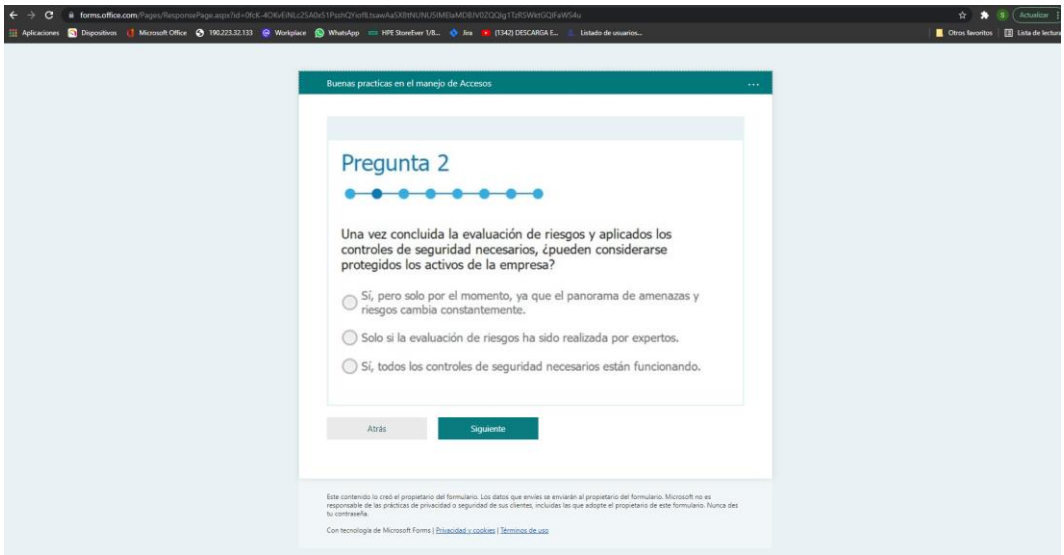


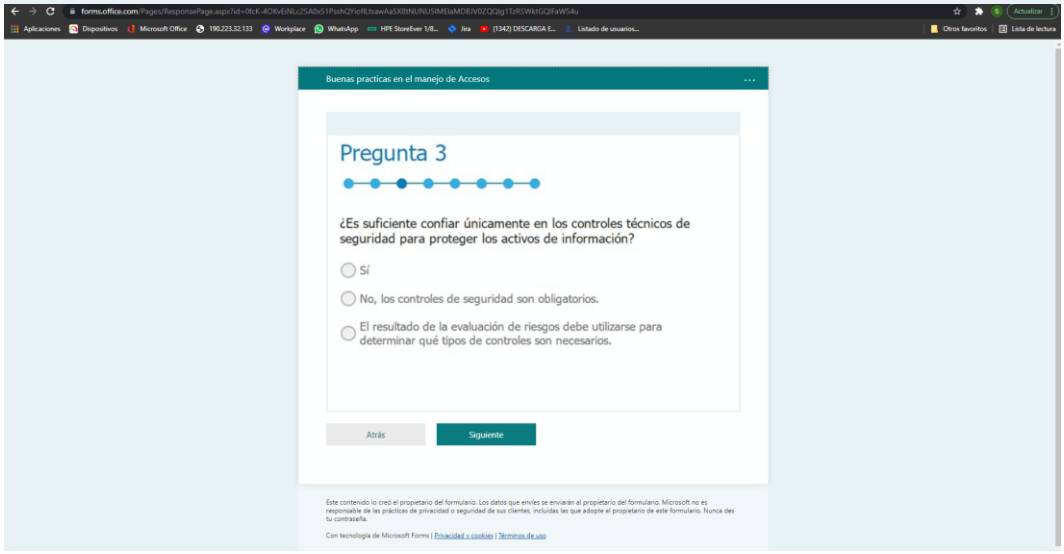
Anexo 20. Capacitación online en la plataforma Microsoft Forms.

Se creó una capacitación sobre las buenas practicas de Accesos a las plataformas por medio de forms de Microsoft como parte de la responsabilidad de usuarios.



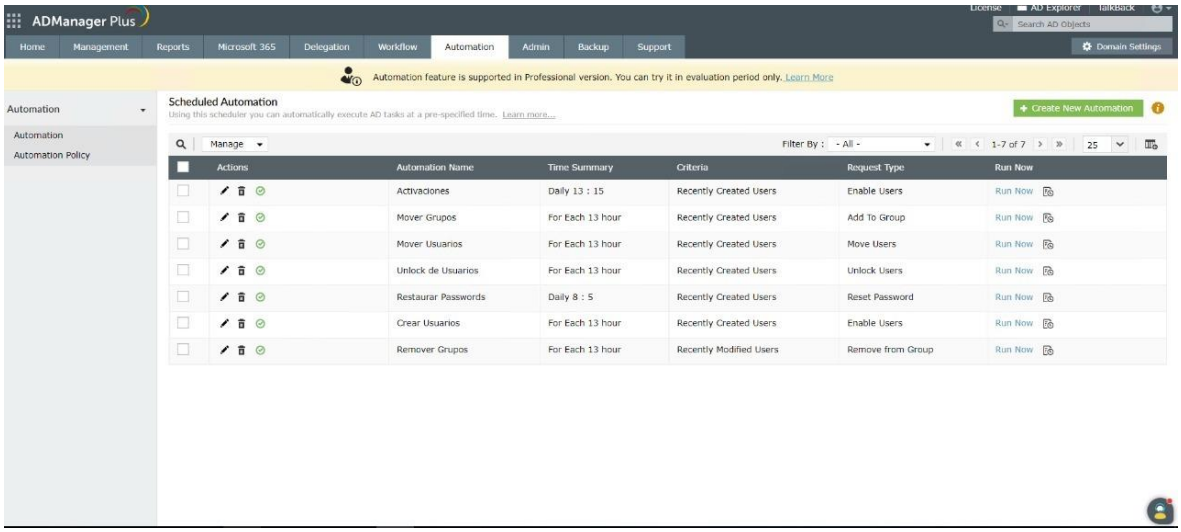

Buenas practicas en el manejo de Accesos
Término y Definiciones
AGRESOR
Totalmente responsable de los incidentes que afectan a la seguridad de una organización. Puede utilizar un conjunto de actores para realizar ataques contra organizaciones.
RIESGO
El riesgo es la posibilidad de que una amenaza determinada se aproveche de las vulnerabilidades y, por lo tanto, cause daños a la organización.
VULNERABILIDAD
Una vulnerabilidad en el diseño, la implementación, el funcionamiento o el control interno de un proceso que podría exponer el sistema a amenazas adversas debido a eventos de amenaza.
Atrás
Siguiente
Buenas practicas en el manejo de Accesos
Pregunta 1
La probabilidad de un evento es un insumo esencial para la evaluación del riesgo. ¿Qué aspecto adicional es de gran importancia en relación con la probabilidad?
Consecuencia
Vulnerabilidad
Exposición
Atrás
Siguiente


Buenas practicas en el manejo de Accesos
Pregunta 2
Una vez concluida la evaluación de riesgos y aplicados los controles de seguridad necesarios, ¿pueden considerarse protegidos los activos de la empresa?
Sí, pero solo por el momento, ya que el panorama de amenazas y riesgos cambia constantemente.
Solo si la evaluación de riesgos ha sido realizada por expertos.
Sí, todos los controles de seguridad necesarios están funcionando.
Atrás
Siguiente


Buenas practicas en el manejo de Accesos
Pregunta 3
¿Es suficiente confiar únicamente en los controles técnicos de seguridad para proteger los activos de información?
Sí
No, los controles de seguridad son obligatorios.
El resultado de la evaluación de riesgos debe utilizarse para determinar qué tipos de controles son necesarios.
Atrás
Siguiente

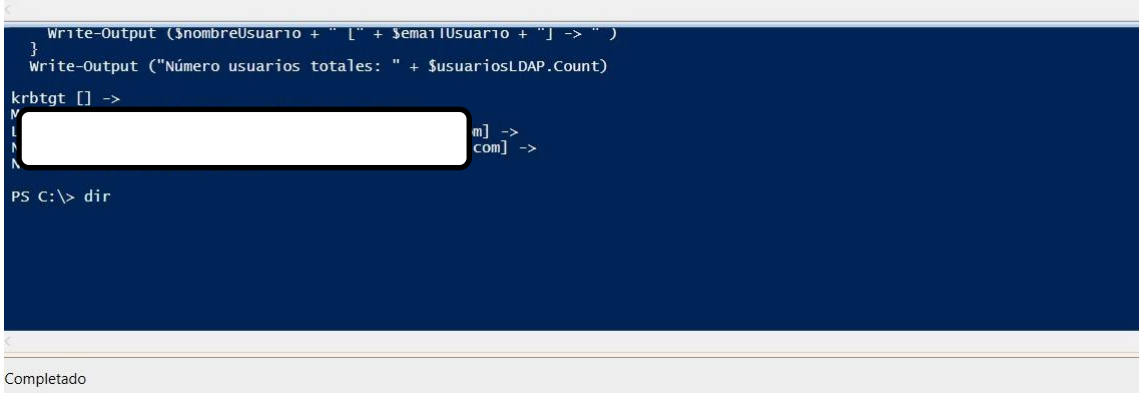
Anexo 21. Implementación de tareas automatizadas para manejo de usuarios en "AD management plus"

Se realiza la instalación y configuración de la aplicación Ad Management Plus para mantener automatizadas varios procesos del AD como son las activaciones de usuarios, Movimientos de grupos de usuarios, Mover usuarios de OU, Inactivar usuarios, restauración de contraseñas, creación de usuarios y eliminación de grupos de acuerdo a las necesidades del trabajo.

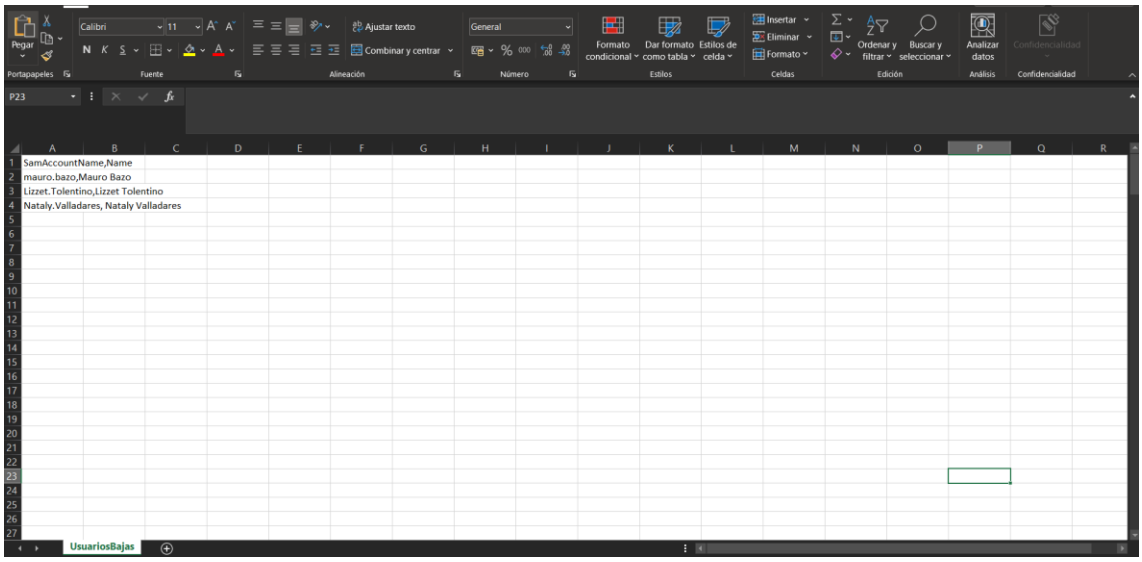


Para poder encontrar todos los usuarios inactivos para una correcta verificación y evidencias, se creó este Query para ejecutarlo por PowerShell de Microsoft.

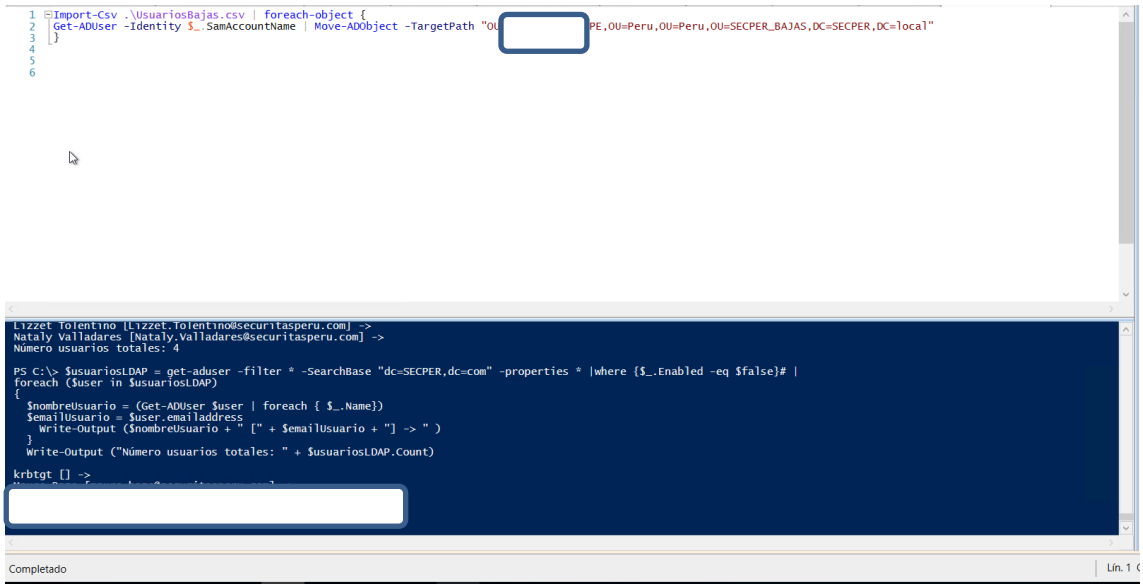
```
#Con este procedimiento se obtiene el número total de usuarios deshabilitados y sus detalles como nombres y correo
#Los cuales se contrastarán con la lista de RRHH de usuarios desvinculados a la empresa hasta la fecha de la consulta.


$usuariosLDAP = get-aduser -filter * -SearchBase "dc=SECPER,dc=com" -properties * |where {$_.Enabled -eq $false}# |
foreach ($user in $usuariosLDAP)
{
  $nombreUsuario = (Get-ADUser $user | foreach { $_.Name})
  $emailUsuario = $user.emailaddress
    Write-Output ($nombreUsuario + " [" + $emailUsuario + "] -> " )
  }
  Write-Output ("Número usuarios totales: " + $usuariosLDAP.Count)

```



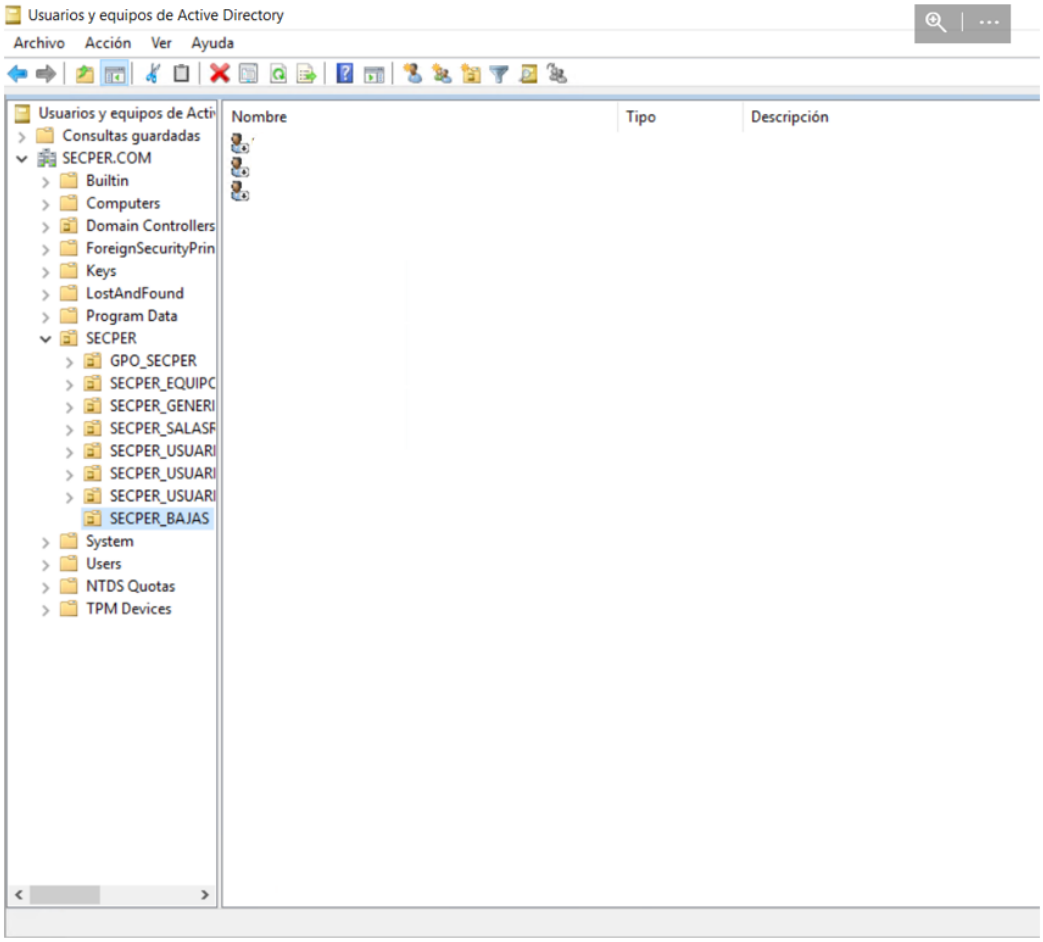
Para bajas en específicos RRHH ingresa los datos de acuerdo a una plantilla en Excel exportarlos en un archivo .SCV



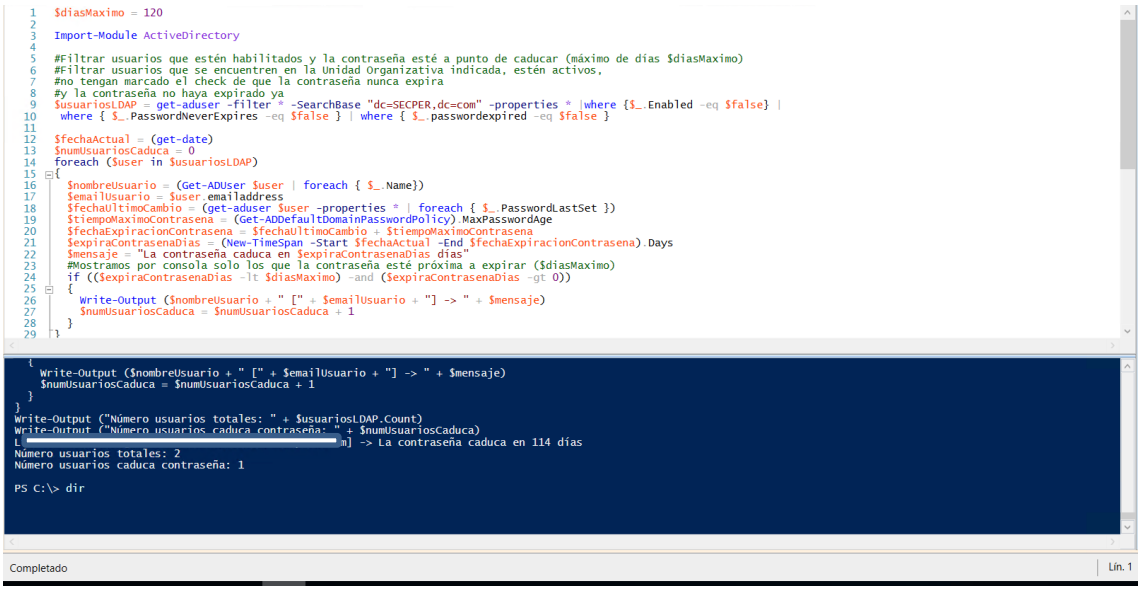
Se creó el siguiente Query que realiza la tarea de enviar los usuarios inactivos a otra unidad organizativa específicamente para bajas



Se muestra los usuarios en la OU especificada en el paso anterior

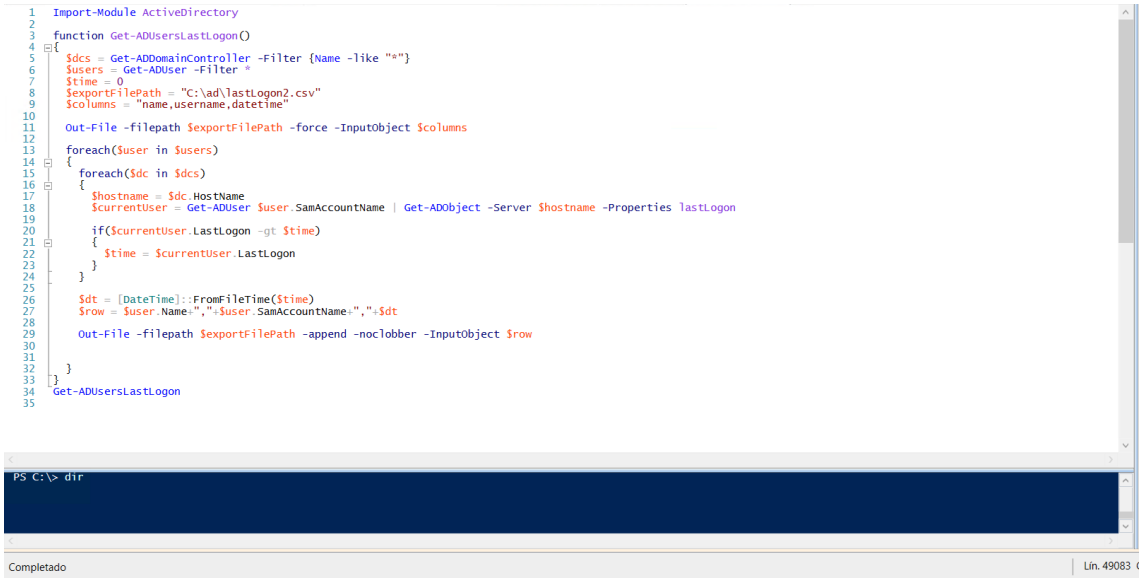


Para la verificación de contraseñas expiradas, se creó el siguiente Query para su ejecución periódica por el área de tecnología.



```
$diasMaximo = 120

Import-Module ActiveDirectory

#Filtrar usuarios que estén habilitados y la contraseña esté a punto de caducar (máximo de días $diasMaximo)
#Filtrar usuarios que se encuentren en la Unidad Organizativa indicada, estén activos,
#no tengan marcado el check de que la contraseña nunca expira
#y la contraseña no haya expirado ya
$usuariosLDAP = get-aduser -filter * -SearchBase "dc=SECPER,dc=com" -properties * |where {$_.Enabled -eq $false} |
 where { $_.PasswordNeverExpires -eq $false } | where { $_.passwordexpired -eq $false }

$fechaActual = (get-date)
$numUsuariosCaduca = 0
foreach ($user in $usuariosLDAP)
{
    $nombreUsuario = (Get-ADUser $user | foreach { $_.Name})
    $emailUsuario = $user.emailaddress
    $fechaUltimoCambio = (get-aduser $user -properties * | foreach { $_.PasswordLastSet })
    $tiempoMaximoContrasena = (Get-ADDefaultDomainPasswordPolicy).MaxPasswordAge
    $fechaExpiracionContrasena = $fechaUltimoCambio + $tiempoMaximoContrasena
    $expiraContrasenaDias = (New-TimeSpan -Start $fechaActual -End $fechaExpiracionContrasena).Days
    $mensaje = "La contraseña caduca en $expiraContrasenaDias dias"
    #Mostramos por consola solo los que la contraseña esté próxima a expirar ($diasMaximo)
    if (($expiraContrasenaDias -lt $diasMaximo) -and ($expiraContrasenaDias -gt 0))
    {
      Write-Output ($nombreUsuario + " [" + $emailUsuario + "] -> " + $mensaje)
      $numUsuariosCaduca = $numUsuariosCaduca + 1
    }
}
Write-Output ("Número usuarios totales: " + $usuariosLDAP.Count)
Write-Output ("Número usuarios caduca contraseña: " + $numUsuariosCaduca)
L[redacted]m] -> La contraseña caduca en 114 días
Número usuarios totales: 2
Número usuarios caduca contraseña: 1

PS C:\> dir
```

Para verificar y evidenciar los últimos inicios de sesión por usurarios, se implementó el siguiente Query para su ejecución.



```
Import-Module ActiveDirectory

function Get-ADUsersLastLogon()
{
  $dcs = Get-ADDomainController -Filter {Name -like "*"}
  $users = Get-ADUser -Filter *
  $time = 0
  $exportFilePath = "C:\ad\lastLogon2.csv"
  $columns = "name,username,datetime"

  Out-File -filepath $exportFilePath -force -InputObject $columns

  foreach($user in $users)
  {
    foreach($dc in $dcs)
    {
      $hostname = $dc.HostName
      $currentUser = Get-ADUser $user.SamAccountName | Get-ADObject -Server $hostname -Properties lastLogon

      if($currentUser.LastLogon -gt $time)
      {
        $time = $currentUser.LastLogon
      }
    }

    $dt = [DateTime]::FromFileTime($time)
    $row = $user.Name+","+$user.SamAccountName+","+$dt

    Out-File -filepath $exportFilePath -append -noclobber -InputObject $row


  }
}
Get-ADUsersLastLogon
```

```
PS C:\> dir
```

Completado | Lín. 49083

Anexo 22. Lista de usuarios con privilegios de administrador

Se realizó un análisis y mapeo de todos los usuarios con cuentas administrativas en cada uno de los sistemas.

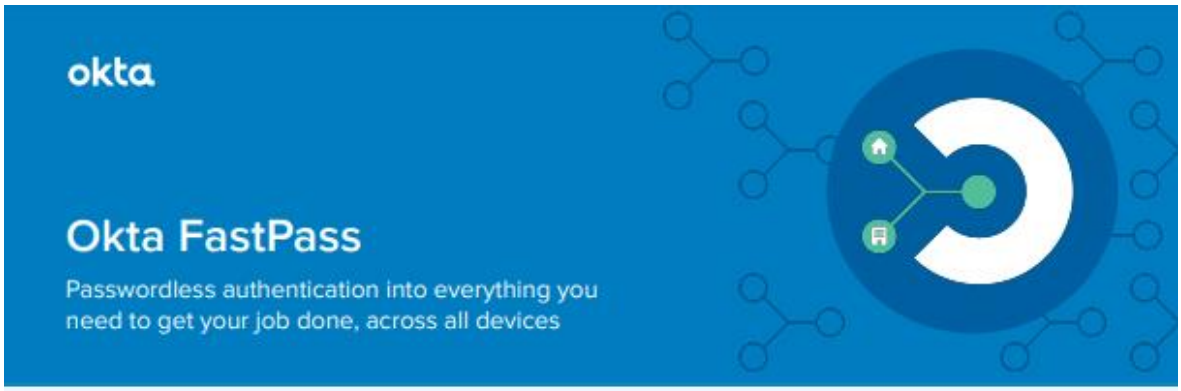
SISTEMAS	ADMINISTRADOR	DESCRIPCIÓN
ERP	3	Se encontraron 3 cuentas administradores usadas para proveedores de soporte.
Securitas visión	1	se encontró 1 usuario administrador para el sistema.
SGH	5	Se encontraron 5 usuarios administradores el cual realizan funcionalidades no necesarias
SGM	4	Se encontraron 4 usuarios administradores el cual realizan funcionalidades no necesarias
Securitas connect	2	Se encontrarn 2 usuarios administradores para creación de usuarios y publicacion de reportes
Smart Boleta Suit	4	Se encontraron 4 usuarios administradores para funcionalidades no necesarias
Solicitud de dinero 1.0	2	Se encontraron 2 usuarios administradores para creación de usuarios y perfiles
Facturación electronica	3	se encontraron 3 usuarios administradores para funcionalidades no necesarias
Contratos NOE	3	Se encontraron 3 usuarios administradores para aprobaciones de documentos
web vacaciones	2	Se encontraron 2 usuarios administradores para creación de usuarios y flujo de trabajo
Active directory	5	Se encontraron 5 administradores totales de dominio.

Al finalizar se consideraron todos estos usuarios necesarios para el trabajo y soporte de las aplicaciones de la empresa

SISTEMAS	ADMINISTRADOR	DESCRIPCIÓN
ERP	1	Se propuso solo un administrador para soporte otro tipo de perfiles para el resto de labores
Securitas visión	1	Se mantiene una sola cuenta administrativa para creación y soprote de aplicacion
SGH	1	Se propuso solo un administrador y perfiles especificos para las demas funcionalidades
SGM	1	Se propuso solo un administrador y perfiles especificos para las demas funcionalidades
Secuitas connect	1	Se propuso solo un adminitrador para administrador de credenciales y publicación a traves de power BI
Smart Boleta Suit	2	Se propuso solo dos adminsitradores uno para lima y otra para provincia
Solicitud de dinero 1.0	1	Se propuso solo un administrador para creacion de usuarios y perfiles opr medio de autorizaciones
Facturación electronica	1	Se propuso solo un administrador para creacion de usuarios y perfiles especificos para el resto.
Contratos NOE	2	Se propuso solo 2 administradores para gestión de documentos y creación de usuarios
web vacaciones	1	Se propuso solo 1 usuario creador de usuaios y soporte.
Active directory	5	Se mantiene las cuentas administradores solo para el personal de tI

Anexo 23. Funcionalidades y características de Okta verify

Servicio que explica en la página web del proveedor



Okta FastPass enables passwordless authentication into anything you need to get your work done, on any device, from any location. Utilize Okta FastPass to minimize end user friction when accessing corporate resources, while still enforcing Okta's adaptive policy checks.

Why use Okta FastPass?

Enabling secure, device-based access is a challenge for many organizations, especially with the influx of new device types across mobile and desktop platforms. With Okta FastPass, you benefit from:

Always On Passwordless. As long as the device is registered to Okta, users get passwordless authentication to any app, from any location.

Using any directory or enterprise mobility management tool (EMM). Although not required, Okta FastPass can be combined with your existing user/device directory or EMM. Still using AD? Not a problem. Using an EMM to manage mobile devices or laptops? We can work with that. Check if devices are managed before users get the passwordless experience delivered by Okta FastPass.

End to end passwordless. When users are on devices which support biometrics for login (Windows Hello, Touch ID on Mac), they log into the device with no password, register the device to Okta with no password, and access all apps with no password.

Supported use cases

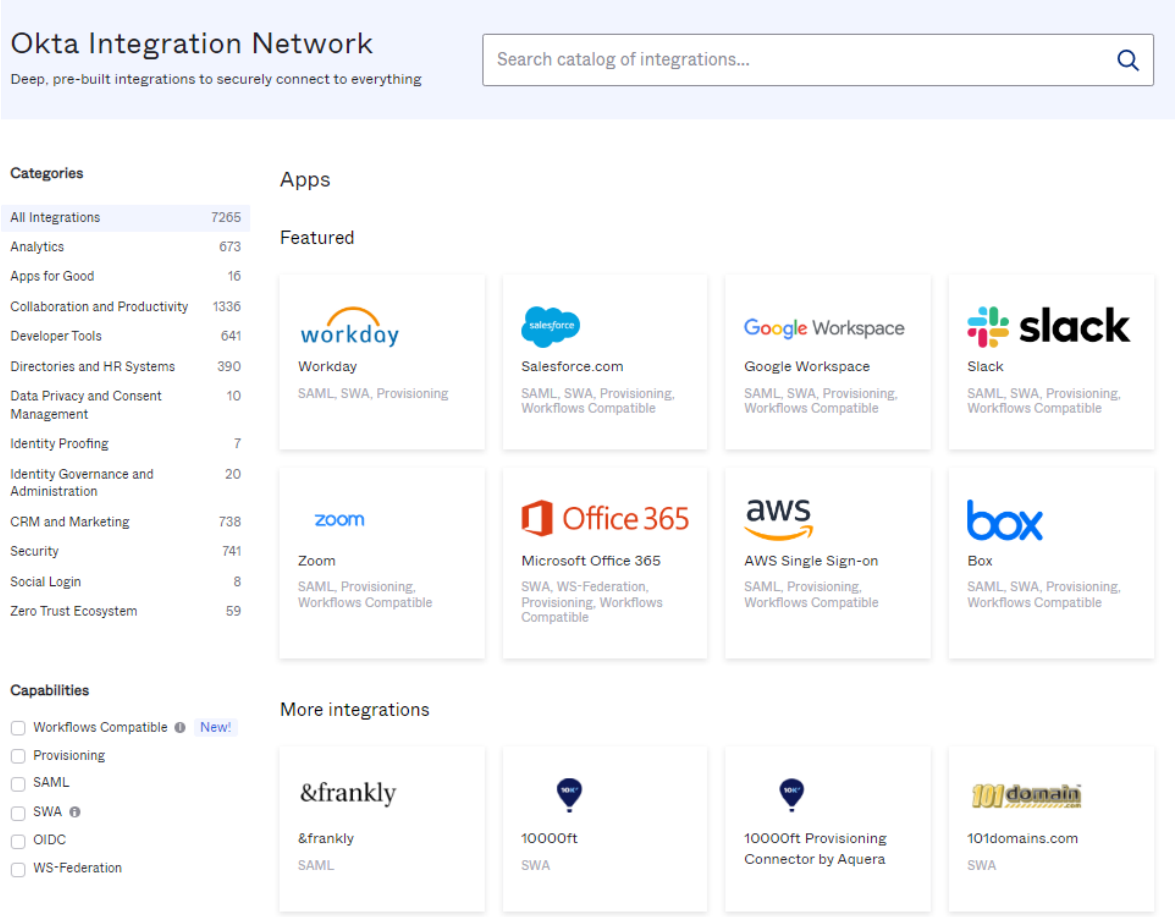
Many organizations use a combination of different tools for device management, but the good news is that Okta FastPass can work alongside a wide range of use cases. Okta FastPass can be combined with the following deployments to check if a device is managed before delivering passwordless auth:

- ✓ Windows devices that are Azure Active Directory joined/Hybrid AAD joined + EMM/MDM managed (VmWare Workspace ONE, Msft Intune, System Center Configuration Manager, MobileIron etc)
- ✓ MacOS devices managed by Jamf Pro
- ✓ Mobile devices (iOS, Android) managed by an EMM/MDM (Intune, VmWare Workspace ONE, MobileIron etc.)

...and many more!

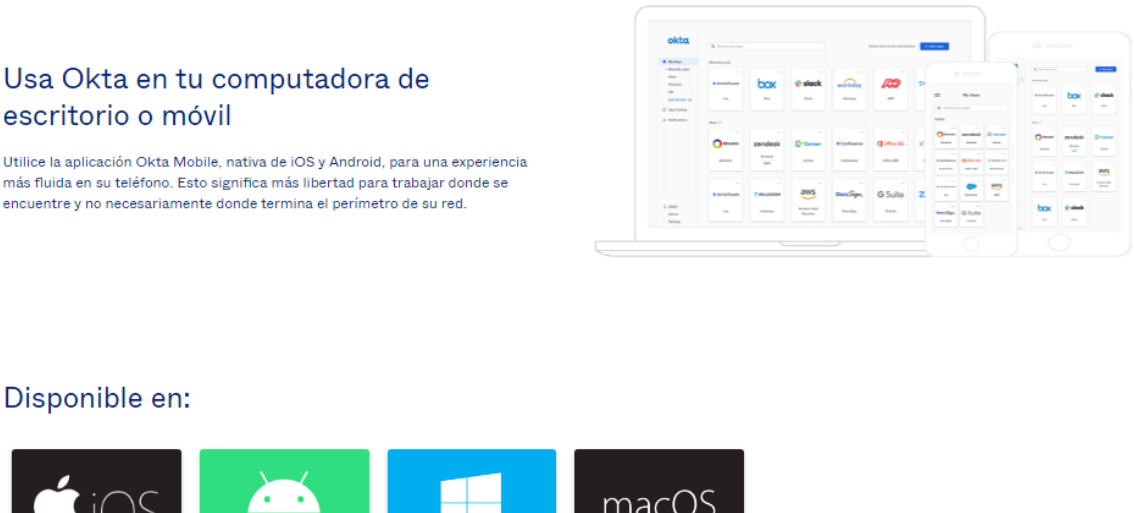
Learn more at www.okta.com/platform/devices.

Gran catálogo de integraciones con aplicativos y servicios.



Servicio de autenticación de doble factor

Compatibilidad con la mayoría de SO



Casos de uso del servicio

Anexo 24. *Formato para petición de cuentas privilegiadas*

Se implementó un formato para tener controlar y registrar los accesos privilegiados que sean necesario para la compañía.

Securitas

FORMATO DE PETICIÓN DE CUENTAS PRIVILEGIADAS

Objetivo: Formalizar las peticiones de usuarios privilegiados.

Alcance: De aplicación aprobada solo por gerencia requerida.

Por medio del presente documento yo _____ asumo lo siguiente:

1 El acceso es uso necesario para actividades de implementación o de soporte a alguna aplicación que sea necesario.

2 El acceso será uso exclusivo de la persona asignada, esta no debe de ser publicada ni difundida a ninguna persona.

3 El acceso solo será habilitado en los rangos de fechas establecidos en el presente documento.

4 Se tendrá un log de transacciones y cambios que realice esta cuenta administrativa.

Por lo anteriormente descrito doy fe de mi conformidad y acepto los puntos descritos en el presente documento

FECHA DE INICIO	FECHA DE TERMINO	ÁREA	SISTEMA	SERVIDOR	BASE DE DATOS

Lima de del 202

_____ Usuario

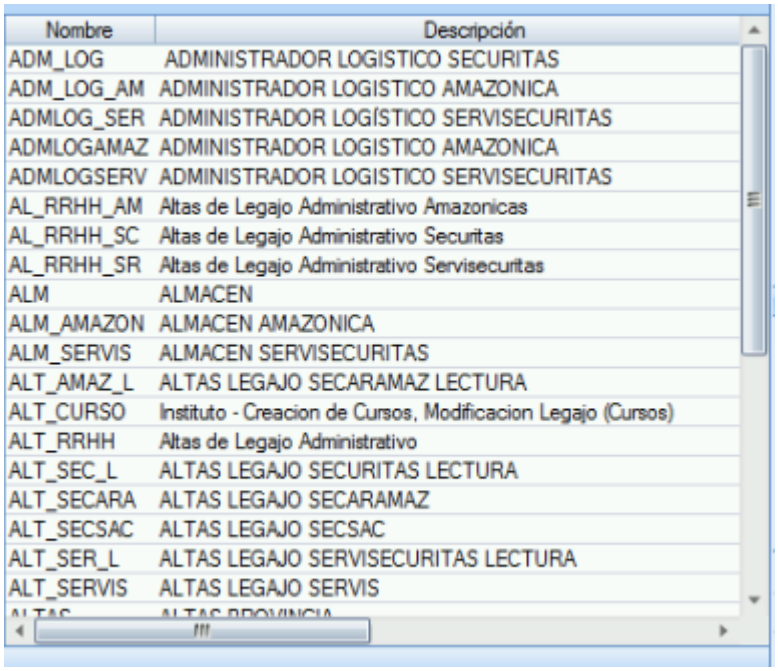
_____ Gerencia

_____ TI

Anexo 25. Listado de roles y perfiles.

Antes no se contaba con un orden adecuado de los perfiles y roles de los accesos en los sistemas de la compañía.

Sistema ERP



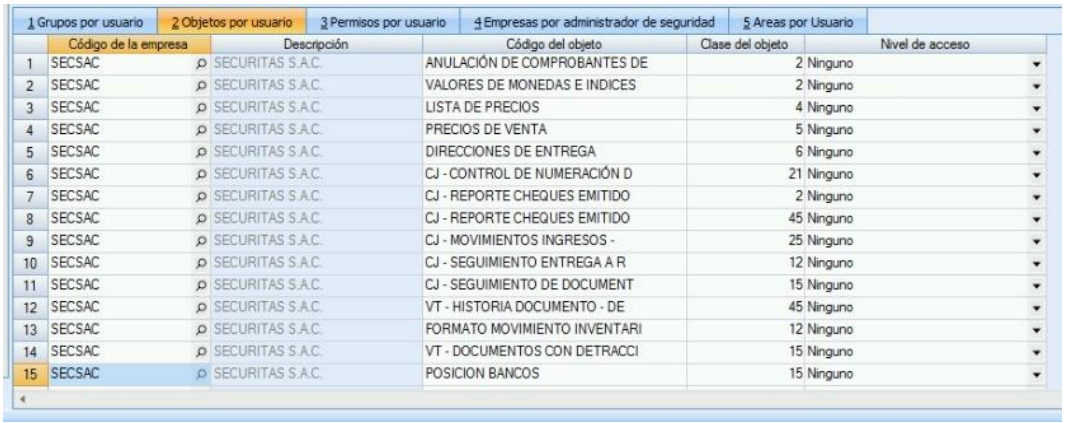
Nombre	Descripción
ADM_LOG	ADMINISTRADOR LOGISTICO SECURITAS
ADM_LOG_AM	ADMINISTRADOR LOGISTICO AMAZONICA
ADMLOG_SER	ADMINISTRADOR LOGÍSTICO SERVISECURITAS
ADMLOGAMAZ	ADMINISTRADOR LOGISTICO AMAZONICA
ADMLOGSERV	ADMINISTRADOR LOGISTICO SERVISECURITAS
AL_RRHH_AM	Altas de Legajo Administrativo Amazonicas
AL_RRHH_SC	Altas de Legajo Administrativo Securitas
AL_RRHH_SR	Altas de Legajo Administrativo Servisecuritas
ALM	ALMACEN
ALM_AMAZON	ALMACEN AMAZONICA
ALM_SERVIS	ALMACEN SERVISECURITAS
ALT_AMAZ_L	ALTAS LEGAJO SECARAMAZ LECTURA
ALT_CURSO	Instituto - Creacion de Cursos, Modificacion Legajo (Cursos)
ALT_RRHH	Altas de Legajo Administrativo
ALT_SEC_L	ALTAS LEGAJO SECURITAS LECTURA
ALT_SECARA	ALTAS LEGAJO SECARAMAZ
ALT_SECSAC	ALTAS LEGAJO SECSAC
ALT_SER_L	ALTAS LEGAJO SERVISECURITAS LECTURA
ALT_SERVIS	ALTAS LEGAJO SERVIS

Se realizó un análisis para ordenar y crear perfiles y roles necesarios para los trabajos en específicos de cada usuario para los sistemas de la empresa.

PERFILES	ROLES	CODIGOS	TRAZABILIDAD	STATUS USUARIO
ADMINISTRADORES	Anulación de comprobantes de cobranza	CGTDSH	Alta	Vigente
ANALISTA CONTABLE	Valores de monedas e indices	CVMCTH01	Modificar	De baja
COORDINADOR CONTABLE	Lista de precios	CVMCTH01	Borrado	
JEFE CONTABLE	Precios de venta	SJACLH	Abrir	
GERENCIA CONTABILIDAD	Direcciones de entrega	SJCCBH		
AUXILIAR CONTABLE	CJ - Control de numeración de Cheques	SJCCOH		
ASISTENTE CONTABLE	CJ - Reporte Cheques Emitidos - Detallado	SJCECH		
SUPERVISOR CONTABILIDAD	CJ - Reporte Cheques Emitidos - Resumido	SJTACU		
PLANIFICADOR CONTABILIDAD	CJ - Movimientos Ingresos - Egresos (Template)	SJTARE		
GERENCIA FINANZAS	CJ - Seguimiento Entrega a Rendir	SJTATH		
ANALISTA FINANCIERO	CJ - Seguimiento de Documento	SJSATH		
COORDINADOR FINANCIERO	VT - Historia documento - Deposito Detracción	SJTDTH		
JEFE FINANCIERO	Formato Movimiento Inventario - EQELECT	AJTATH		
AUXILIAR FINANCIERO	VT - Documentos con Detracción	SJFBIL		
ASISTENTE FINANCIERO	Posicion Bancos	SJTHDAT		
SUPERVISOR FINANCIERO	PV - Kardex de Proveedor (Template)	SJTCLC		
PLANIFICADOR FINANCIERO	Seguimiento de Requerimientos de Compras - Detallado	SJTCLE		
GERENCIA LOGISTICO	CJ - Voucher Tesoreria	SJTCTH		
ANALISTA LOGISTICO	Voucher Pago Masivo	SJTDSEH		
COORDINADOR LOGISTICO	Operaciones Varias	SJTDGH		
JEFE LOGISTICO	Aprobación Detallada - Requerimiento	SJTENH		
AUXILIAR LOGISTICO	Atención Orden de Servicio	SJTESC		
ASISTENTE LOGISTICO	Requerimiento de Compra	SJTESH		
SUPERVISOR LOGISTICO	Cobranza Documentos por Cobrar (Con o Sin detracción)	SJTEST		
PLANIFICADOR LOGISTICO	Aplicación Documentos a Nota Credito Cliente	SJTFOH		
COMPRADOR LOGISTICO	PV - Provision / Rendicion - Gastos	SJTLIQ		
ADMINISTRADORES OPERATIVO	Aprobación de Requerimientos	SJTMOD		
ANALISTA OPERATIVO	Distribuciones por dimensión	SJTMOV		

Con la lista de los perfiles y roles, se implementaron en los sistemas para su uso correcto de la aplicación y control de usuarios.

	Nombre de la empresa	Descripción	NombreDelObjeto	Clase del objeto	Nivel de acceso
2	SECSAC	SECURITAS S.A.C.	ANALISTA CONTABLE	2	Alta y modificación
3	SECSAC	SECURITAS S.A.C.	COORDINADOR CONTABLE	2	Modificado y borrado
4	SECSAC	SECURITAS S.A.C.	JEFE CONTABLE	3	Modificado y borrado
5	SECSAC	SECURITAS S.A.C.	GERENCIA CONTABILIDAD	4	Alta, modificado y borrado
6	SECSAC	SECURITAS S.A.C.	AUXILIAR CONTABLE	2	Alta y modificación
7	SECSAC	SECURITAS S.A.C.	ASISTENTE CONTABLE	2	Alta y borrado
8	SECSAC	SECURITAS S.A.C.	SUPERVISOR CONTABILIDAD	2	Modificado y borrado
9	SECSAC	SECURITAS S.A.C.	PLANIFICADOR CONTABILIDAD	4	Alta y borrado
10	SECSAC	SECURITAS S.A.C.	GERENCIA FINANZAS	4	Alta, modificado y borrado
11	SECSAC	SECURITAS S.A.C.	ANALISTA FINANCIERO	2	Alta y borrado
12	SECSAC	SECURITAS S.A.C.	COORDINADOR FINANCIERO	3	Alta y borrado
13	SECSAC	SECURITAS S.A.C.	JEFE FINANCIERO	3	Modificado y borrado
14	SECSAC	SECURITAS S.A.C.	AUXILIAR FINANCIERO	2	Alta y modificación
15	SECSAC	SECURITAS S.A.C.	ASISTENTE FINANCIERO	2	Modificar
16	SECSAC	SECURITAS S.A.C.	SUPERVISOR FINANCIERO	2	Alta y modificación
17	SECSAC	SECURITAS S.A.C.	PLANIFICADOR FINANCIERO	2	Alta y borrado
18	SECSAC	SECURITAS S.A.C.	GERENCIA LOGISTICO	4	Modificado y borrado
19	SECSAC	SECURITAS S.A.C.	ANALISTA LOGISTICO	2	Alta, modificado y borrado
20	SECSAC	SECURITAS S.A.C.	COORDINADOR LOGISTICO	2	Alta y borrado
21	SECSAC	SECURITAS S.A.C.	JEFE LOGISTICO	3	Modificado y borrado
22	SECSAC	SECURITAS S.A.C.	AUXILIAR LOGISTICO	2	Modificado y borrado
23	SECSAC	SECURITAS S.A.C.	ASISTENTE LOGISTICO	2	Alta y borrado
24	SECSAC	SECURITAS S.A.C.	SUPERVISOR LOGISTICO	2	Alta y modificación
25	SECSAC	SECURITAS S.A.C.	PLANIFICADOR LOGISTICO	2	Alta y borrado
26	SECSAC	SECURITAS S.A.C.	COMPRADOR LOGISTICO	3	Modificado y borrado
27	SECSAC	SECURITAS S.A.C.	ADMINISTRADORES OPERATIVO	2	Modificado y borrado
28	SECSAC	SECURITAS S.A.C.	ANALISTA OPERATIVO	2	Modificado y borrado
29	SECSAC	SECURITAS S.A.C.	COORDINADOR OPERATIVO	3	Alta, modificado y borrado
30	SECSAC	SECURITAS S.A.C.	JEFE OPERATIVO	3	Alta y borrado
31	SECSAC	SECURITAS S.A.C.	GERENCIA OPERATIVO	4	Alta, modificado y borrado
32	SECSAC	SECURITAS S.A.C.	AUXILIAR OPERATIVO	2	Alta y modificación
33	SECSAC	SECURITAS S.A.C.	ASISTENTE OPERATIVO	2	Alta y borrado
34	SECSAC	SECURITAS S.A.C.	SUPERVISOR OPERATIVO	2	Alta y borrado
35	SECSAC	SECURITAS S.A.C.	PLANNER OPERATIVO	2	Alta y borrado
36	SECSAC	SECURITAS S.A.C.	BRANCH OPERATIVO	3	Ninguno



	Código de la empresa	Descripción	Código del objeto	Clase del objeto	Nivel de acceso
1	SECSAC	SECURITAS S.A.C.	ANULACIÓN DE COMPROBANTES DE	2	Ninguno
2	SECSAC	SECURITAS S.A.C.	VALORES DE MONEDAS E INDICES	2	Ninguno
3	SECSAC	SECURITAS S.A.C.	LISTA DE PRECIOS	4	Ninguno
4	SECSAC	SECURITAS S.A.C.	PRECIOS DE VENTA	5	Ninguno
5	SECSAC	SECURITAS S.A.C.	DIRECCIONES DE ENTREGA	6	Ninguno
6	SECSAC	SECURITAS S.A.C.	CJ - CONTROL DE NUMERACIÓN D	21	Ninguno
7	SECSAC	SECURITAS S.A.C.	CJ - REPORTE CHEQUES EMITIDO	2	Ninguno
8	SECSAC	SECURITAS S.A.C.	CJ - REPORTE CHEQUES EMITIDO	45	Ninguno
9	SECSAC	SECURITAS S.A.C.	CJ - MOVIMIENTOS INGRESOS -	25	Ninguno
10	SECSAC	SECURITAS S.A.C.	CJ - SEGUIMIENTO ENTREGA A R	12	Ninguno
11	SECSAC	SECURITAS S.A.C.	CJ - SEGUIMIENTO DE DOCUMENT	15	Ninguno
12	SECSAC	SECURITAS S.A.C.	VT - HISTORIA DOCUMENTO - DE	45	Ninguno
13	SECSAC	SECURITAS S.A.C.	FORMATO MOVIMIENTO INVENTARI	12	Ninguno
14	SECSAC	SECURITAS S.A.C.	VT - DOCUMENTOS CON DETRACCI	15	Ninguno
15	SECSAC	SECURITAS S.A.C.	POSICION BANCOS	15	Ninguno

Antes no se contaba con un orden adecuado de los perfiles y roles de los accesos en los sistemas de la compañía

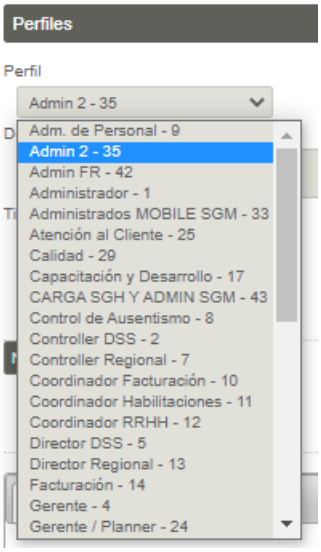
Sistema SGH

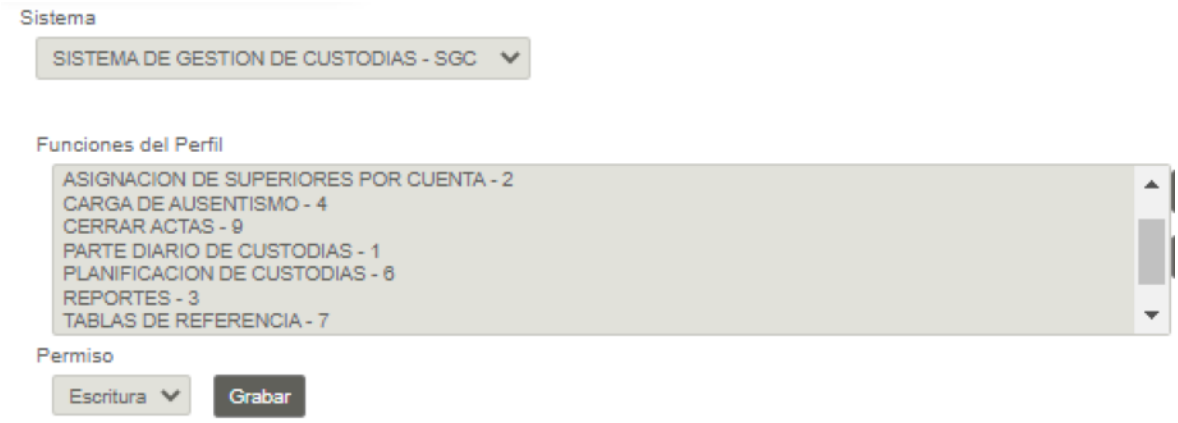
Se realizó un análisis para ordenar y crear perfiles y roles necesarios para los trabajos en específicos de cada usuario para los sistemas de la empresa.

PERFIL
ADMINISTRADOR
PLANIFICADOR MOBILE
PLANIFICADOR HORAS
PLANIFICADOR DE CARGA
PLANIFICADOR DE AUSENCIAS
PLANIFICADOR REGIONAL
PLANIFICADOR FACTURACION
PLANIFICADOR DE ALTAS
PLANIFICADOR DE RRHH
PLANIFICADOR DE DSS
PLANIFICADOR DE PERSONAL
PLANIFICADOR DE LIQUIDACIONES
PLANIFICADOR DE LOGISTICA
PLANIFICADOR DE ONOFF
PLANIFICADOR OPERATIVO
PLANIFICADOR DE CLIENTES
ADMINISTRADOR MOBILE
ADMINISTRADOR HORAS
ADMINISTRADOR DE CARGA
ADMINISTRADOR DE AUSENCIAS
ADMINISTRADOR REGIONAL
ADMINISTRADOR FACTURACION
ADMINISTRADOR DE ALTAS
ADMINISTRADOR DE RRHH
ADMINISTRADOR DE DSS
ADMINISTRADOR DE PERSONAL
ADMINISTRADOR DE LIQUIDACIONES
ADMINISTRADOR DE LOGISTICA
ADMINISTRADOR DE ONOFF
ADMINISTRADOR OPERATIVO
ADMINISTRADOR DE CLIENTES
CARGA MOBILE
CARGA HORAS
CARGA DE CARGA
CARGA DE AUSENCIAS

ROL
Anulaciones
Atributos
Prestamos
Liquidaciones
Reportes
Comprobantes
Ingreso Faltas
Modificar faltas
Carga de horas
Porcesar horas
Ingreso datos personales
Ingresar clientes
Modificar Cleinte
Ingresar proveedores
Ingresar factura
Ingresar liquidacion
Procesar liquidaciones
Ingresar DSS
Procesar DSS
Ingresar Regiones
Cargar Rondas
Moficiar Rondas
Gestionar servidores
Centros de costos
Ingresar guardias
Modificar Guardias
Anular Guardias
Ingresar Rondas
Modificar Rondas
Eliminar Rondas
Gestionar Empresas
Gestionar proceedores
Gestionar usuarios
Gestionar contraseñas

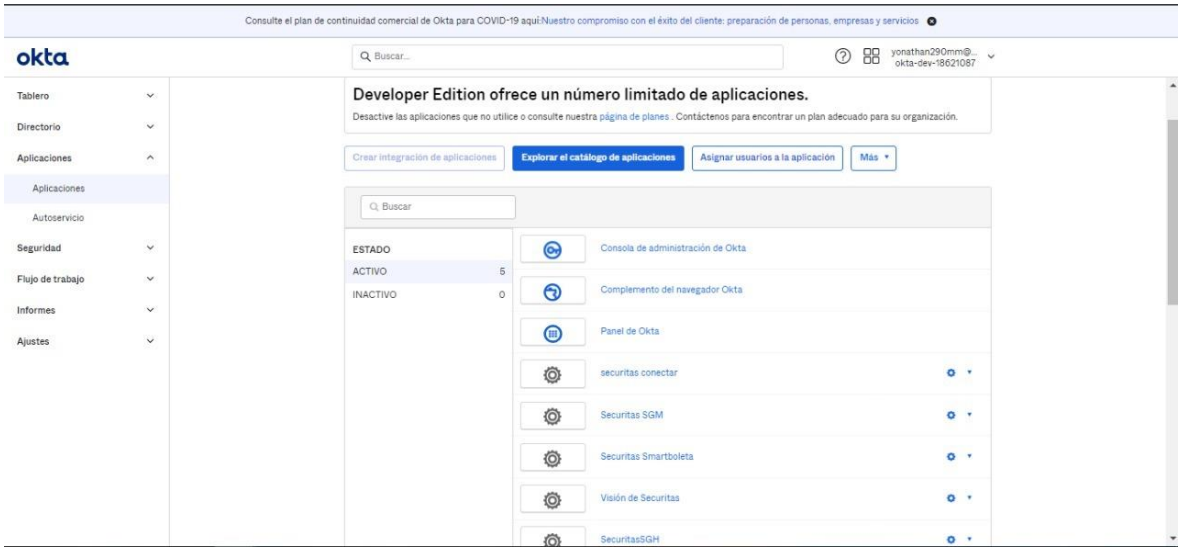
Con la lista de los perfiles y roles, se implementaron en los sistemas para su uso correcto de la aplicación y control de usuarios.

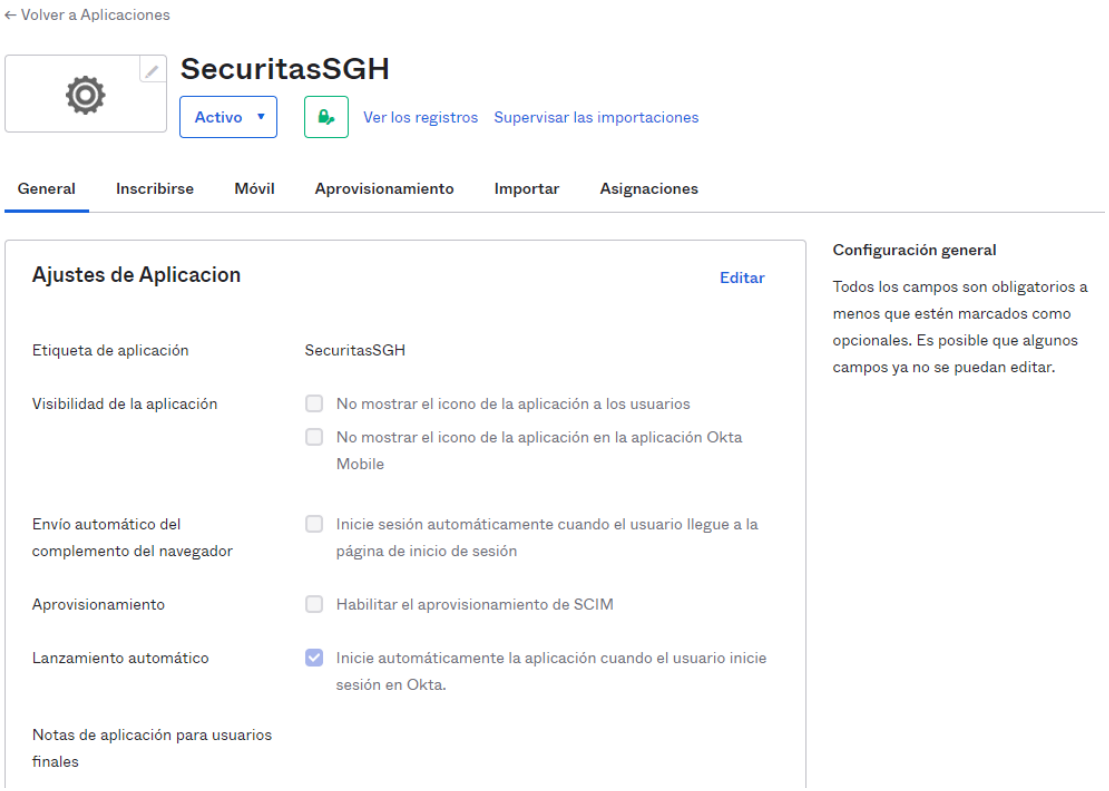




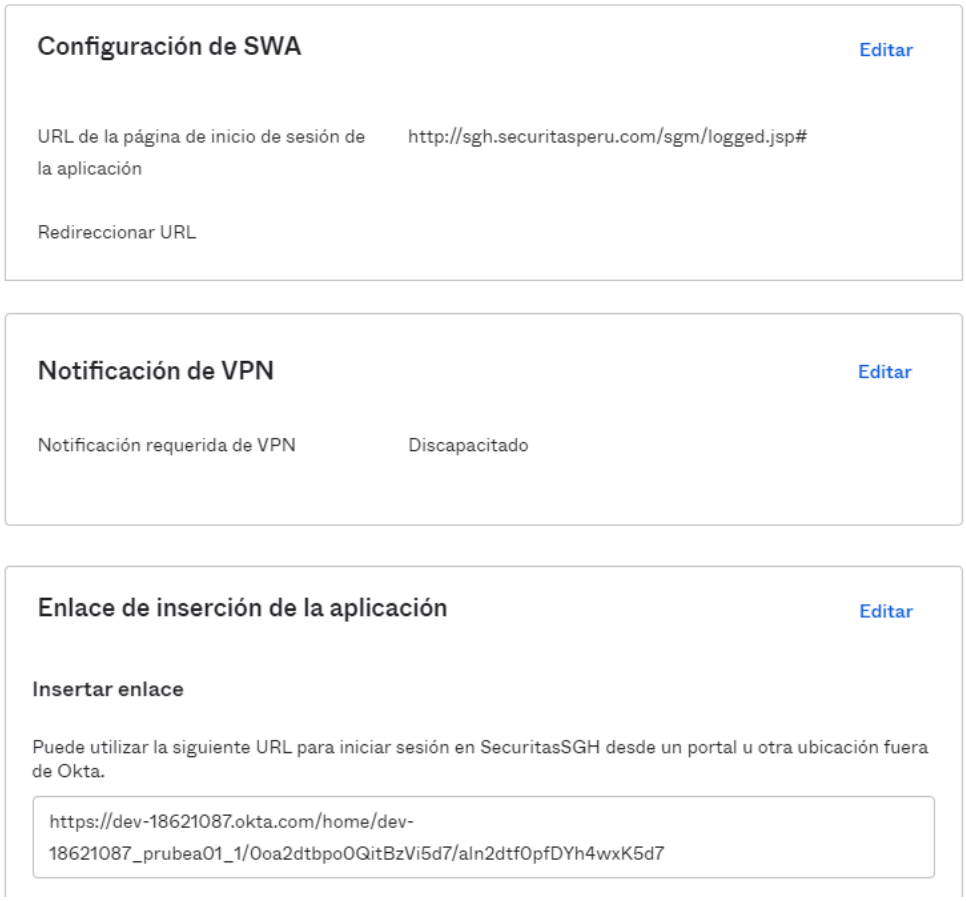
Anexo 26. Implementación de Okta para sistemas web SECURITAS SAC.

Se configuro las referencias del sistema web al cual se redireccionará luego de haber iniciado sesión en Okta.

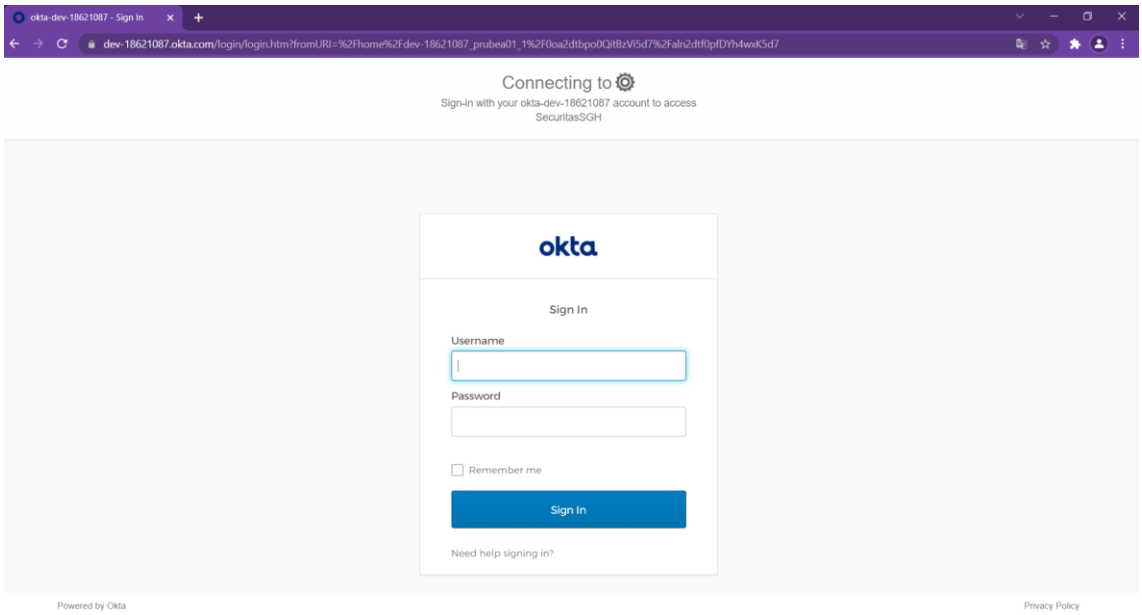




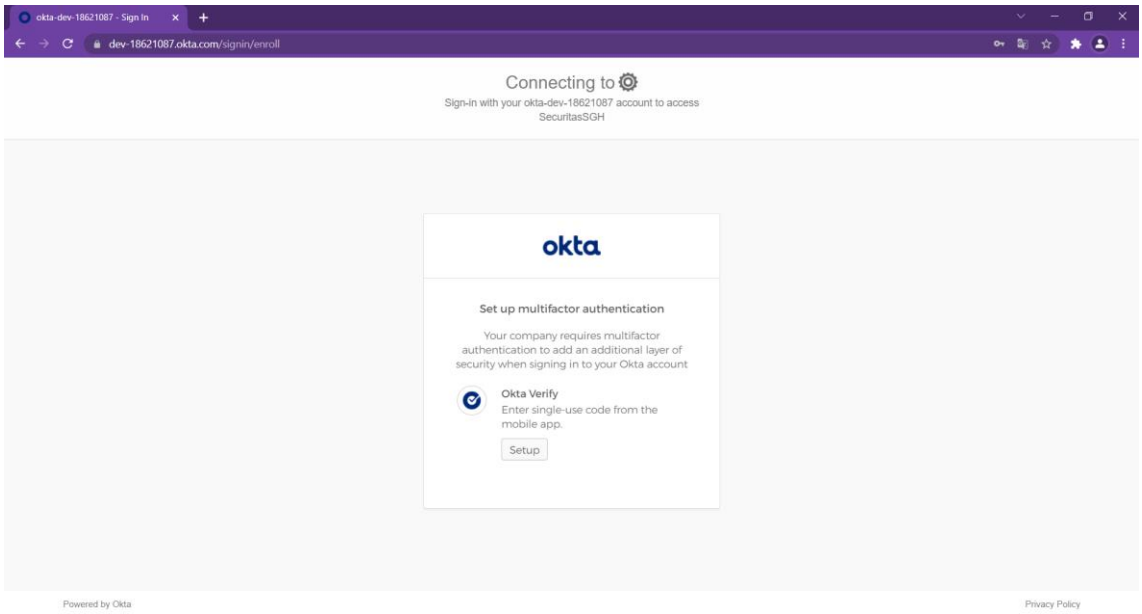
Se muestra la configuración SWA (Security Web Authenticator) donde se muestra las URL que se administrarán dentro del servicio Okta.



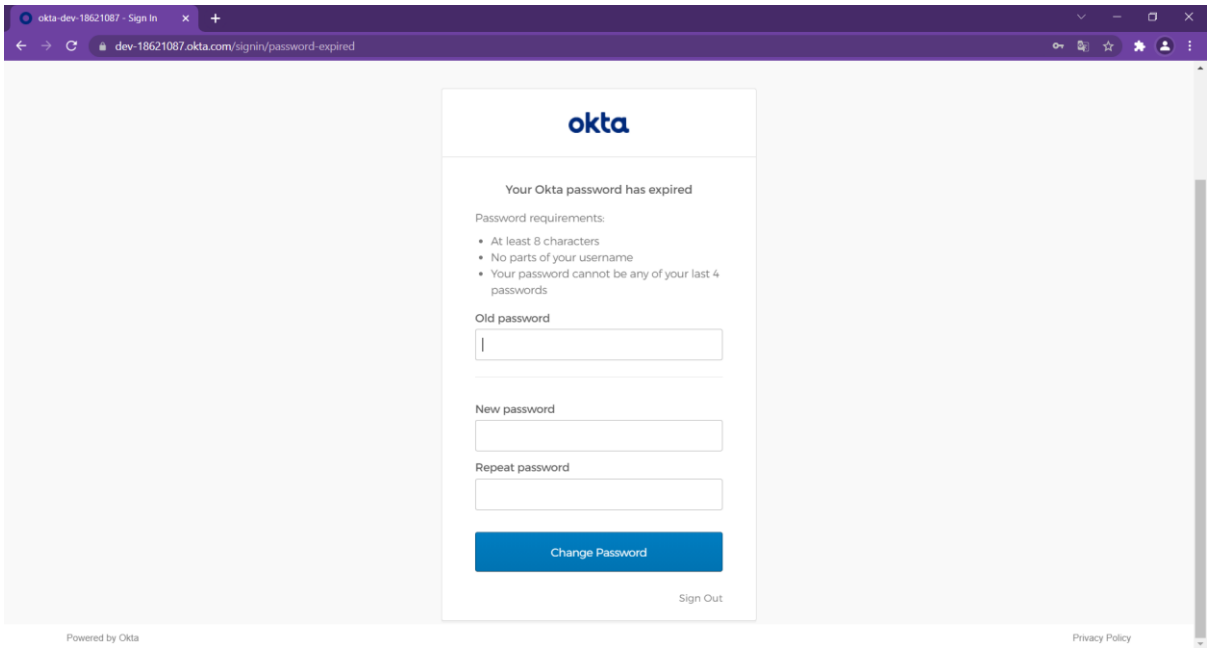
Inicio de sesión en Okta



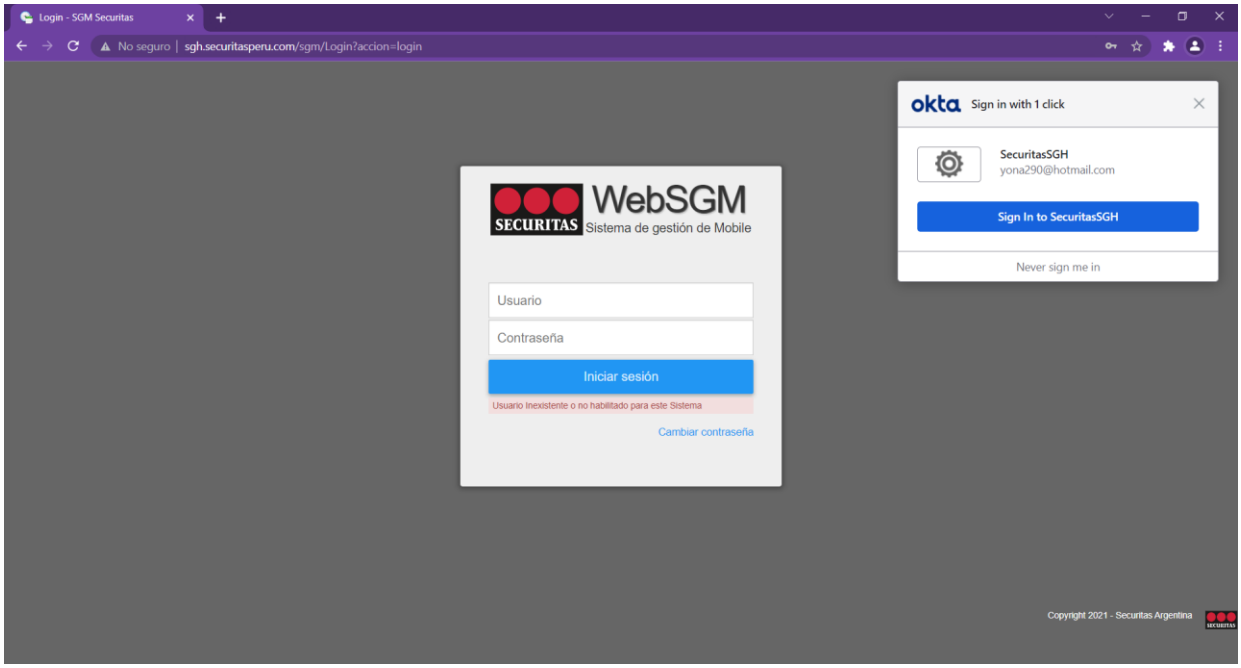
Validación de usuario.



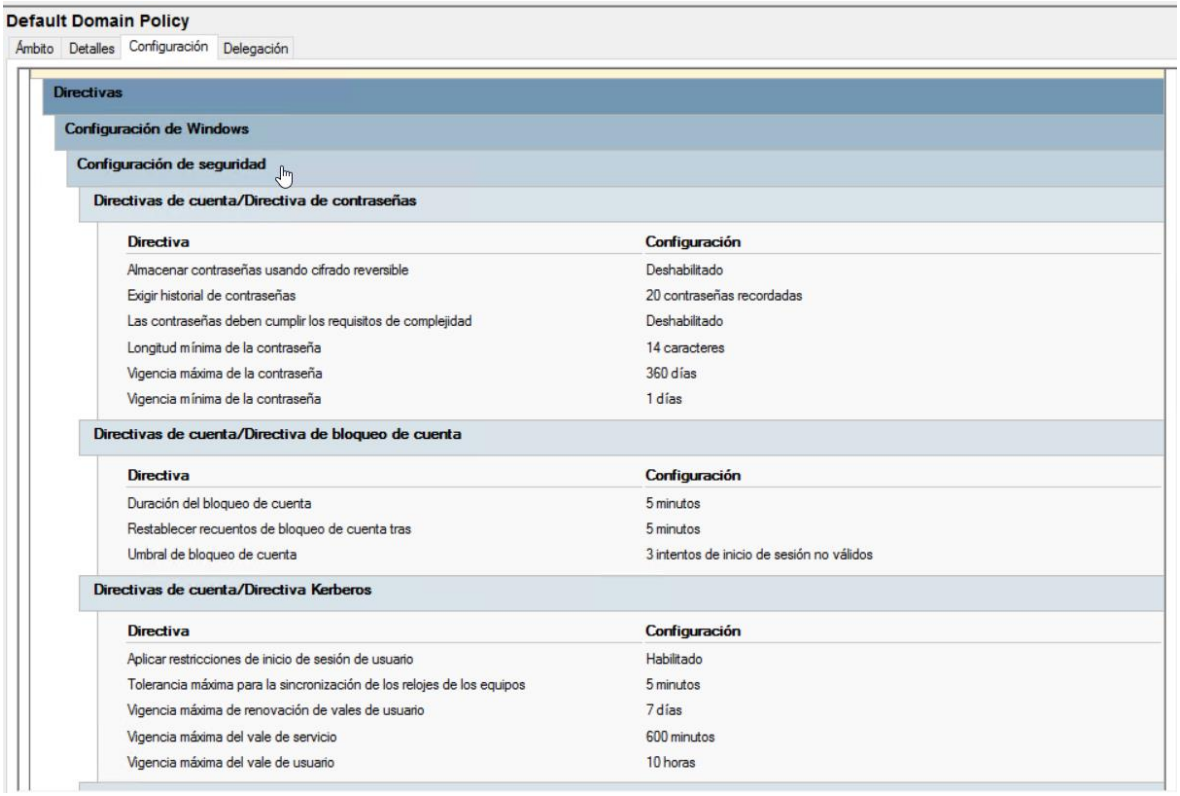
El sistema Okta solicitara el cambio de clave inicial brindado al usuario.



Luego de validar el acceso permitirá redireccionar desde el menú al sistema el cual tiene acceso y también validara las credenciales del mismo en base a los tags del sistema web para usuario y contraseña con SWA.



Anexo 27. Políticas Registradas en el Active Directory (SECPER.COM)



Default Domain Policy

Ámbito | Detalles | Configuración | Delegación

Directivas

Configuración de Windows

Configuración de seguridad

Directivas de cuenta/Directiva de contraseñas

Directiva	Configuración
Almacenar contraseñas usando cifrado reversible	Deshabilitado
Exigir historial de contraseñas	20 contraseñas recordadas
Las contraseñas deben cumplir los requisitos de complejidad	Deshabilitado
Longitud mínima de la contraseña	14 caracteres
Vigencia máxima de la contraseña	360 días
Vigencia mínima de la contraseña	1 días

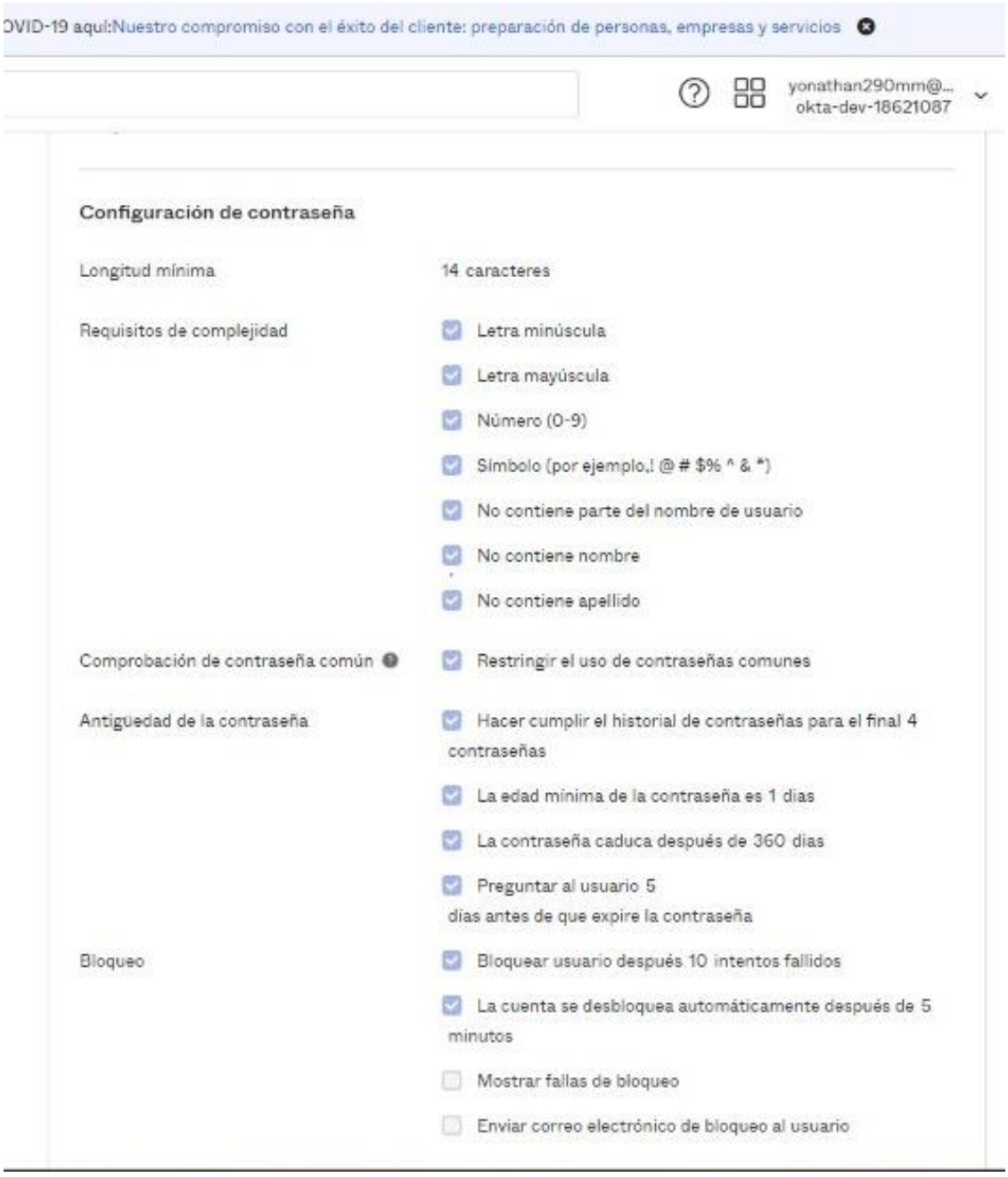
Directivas de cuenta/Directiva de bloqueo de cuenta

Directiva	Configuración
Duración del bloqueo de cuenta	5 minutos
Restablecer recuentos de bloqueo de cuenta tras	5 minutos
Umbral de bloqueo de cuenta	3 intentos de inicio de sesión no válidos

Directivas de cuenta/Directiva Kerberos

Directiva	Configuración
Aplicar restricciones de inicio de sesión de usuario	Habilitado
Tolerancia máxima para la sincronización de los relojes de los equipos	5 minutos
Vigencia máxima de renovación de vales de usuario	7 días
Vigencia máxima del vale de servicio	600 minutos
Vigencia máxima del vale de usuario	10 horas

Anexo 28. Configuración de política de contraseña en Okta.



Anexo 29. Distribución de política de acceso a través del sistema Smart Boleta.