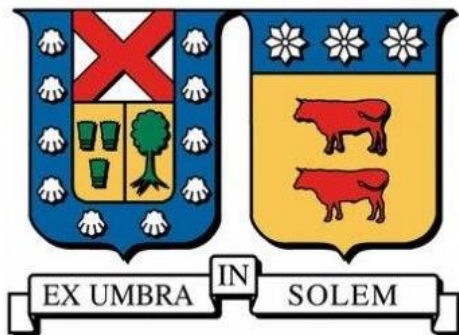




**UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INDUSTRIAS**

**PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE
GESTIÓN DE IDENTIDAD Y ACCESO EN JIRA PARA WHEREX**

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERÍA CIVIL

INDUSTRIAL

AUTOR

FELIPE IGNACIO GARCÍA MORALES

PROFESOR GUÍA

OSCAR JULIO

SAAVEDRA RODRÍGUEZ

PROFESOR

CORREFERENTE

GONZALO DAVID

AMÉSTICA HERNÁNDEZ

SANTIAGO DE CHILE, 19 DE MARZO DE 2024

Dedicatoria

Quisiera dedicar este trabajo a mi familia, especialmente a mis padres, Jimena Morales y Ronald García, quienes siempre me brindaron el apoyo necesario para llegar hasta donde estoy hoy. Ellos han sido mis guías, mentores, maestros y un constante apoyo en cada paso que he dado. Gracias a sus enseñanzas, sabiduría y amor, me han inculcado los valores más importantes de la vida: ser una buena persona y, sobre todo, un buen hijo.

A mi hermana, Simone García, le agradezco por inspirarme a alcanzar mis metas y por darme la fuerza de ser un ejemplo por seguir. Ella me motiva a ser mejor cada día y a superarme constantemente.

Por último, a mi pareja, Karen Bustamante, quiero agradecerle por estar a mi lado durante mi trayectoria universitaria, apoyándome en los momentos difíciles y celebrando mis éxitos.

Su amor y apoyo incondicional me han hecho crecer como persona y me inspiran a seguir adelante. A todos ustedes, les dedico este trabajo y les agradezco por ser mi pilar fundamental en la vida.

Agradecimientos

Quiero expresar mi profundo agradecimiento a mi familia, incluyendo abuelos, tíos, primos y padres de mi pareja, por su constante apoyo y aliento en la búsqueda de mis metas y objetivos. Cada abrazo, cada palabra de aliento y cada enseñanza han sido cruciales para alcanzar mis logros.

También quiero agradecer a WherEX por brindarme la oportunidad de poner a prueba mis habilidades y conocimientos. Agradezco a mis colegas de otras áreas por los buenos momentos compartidos tanto en el trabajo como fuera de él, y especialmente a mi equipo en Finance, cuya colaboración hizo mi experiencia laboral en la empresa sumamente gratificante.

Un agradecimiento especial a mi equipo principal, Process & Compliance y parte de Engineering, incluyendo a Cristy Barría, Eddie Baeza, Hildriana Henríquez, Idalia Ochoa y Nacira Brizuela, por proporcionarme las herramientas necesarias para llevar a cabo mi proyecto y por enseñarme tanto durante este proceso.

También agradezco a mi profesor guía, Oscar Saavedra, por su disposición y ayuda durante mi etapa universitaria.

Por último, a mis amigos, quienes siempre están ahí para sacarme una sonrisa y levantar mi ánimo en los momentos difíciles, agradezco su constante preocupación por mi bienestar y su ánimo siempre alentador.

Todo este proceso ha sido posible gracias a ustedes y su inquebrantable apoyo, enseñanzas y afecto.

Resumen

El contexto empresarial actual está marcado por la creciente importancia de salvaguardar la información y los sistemas tecnológicos ante posibles vulnerabilidades y ataques. En este sentido, WherEX se enfrenta a la necesidad de implementar un sistema de gestión de identidad y acceso (IAM) para controlar y monitorear a los usuarios y sistemas, reconociendo el riesgo existente y la necesidad de proteger sus activos. Este informe detalla el proceso completo de implementación del IAM, desde la selección de la plataforma Jira, hasta el rediseño de los procesos relacionados con los colaboradores. A través de cinco etapas definidas en el proyecto, se llevó a cabo un análisis exhaustivo, identificando brechas, desarrollando flujos de entrada y salida mejorados, e integrando el sistema con el equipo de Sysadmin. Los resultados obtenidos reflejan una solución efectiva a las brechas identificadas, optimizando los procesos de on boarding y off boarding, así como mejorando el monitoreo y registro de las plataformas de la empresa. Esta implementación ha tenido un impacto económico positivo al reducir costos asociados a cuentas inactivas y mejorar la eficiencia operativa. Además, sienta las bases para futuras mejoras y optimizaciones en la gestión de identidad y acceso.

Palabras clave: gestión de identidad y acceso (IAM), monitoreo y registro, brechas, optimización de procesos, eficiencia.

Abstract

The current business context is marked by the growing importance of safeguarding information and technological systems against potential vulnerabilities and attacks. In this regard, WherEX is faced with the need to implement an Identity and Access Management (IAM) system to control and monitor user and system access, acknowledging the existing vulnerability and the need to protect its assets. This report details the complete process of IAM implementation, from selecting the Jira platform to redesigning processes related to employees. Through five stages defined in the project, a comprehensive analysis was conducted, identifying gaps, developing enhanced onboarding and offboarding flows, and integrating the system with the Sysadmin team. The results reflect an effective solution to the identified gaps, optimizing onboarding and offboarding processes, as well as enhancing monitoring and logging of the company's platforms. This implementation has had a positive economic impact by reducing costs associated with inactive accounts and improving operational efficiency. Additionally, it lays the groundwork for future improvements and optimizations in identity and access management.

Keywords: identity and access management (IAM), monitoring and logging, gaps, process optimization, efficiency.

Índice General

Dedicatoria	2
Agradecimientos.....	3
Resumen	4
Abstract	5
Índice General	6
Índice de Gráficos	9
Índice de Tablas	9
Índice de Figuras	9
1. Capítulo I: Introducción.....	12
1.1. Contexto	12
1.2. Origen o Justificación del problema.....	15
1.3. Objetivos	17
1.3.1. Objetivo General	17
1.3.2. Objetivos Específicos.....	17
2. Capítulo II: Estado del Arte y Alcance	18
2.1. Estado actual del Conocimiento.....	18
2.2. Antecedentes de la organización	19
2.2.1. Sobre la organización	19
2.2.2. Origen.....	19
2.2.3. Desarrollo	20
2.2.4. Misión.....	22
2.2.5. Visión	22
2.2.6. Modelos de negocio	22
2.3. Propuesta de Valor del tema.....	24
2.4. Alcance de la memoria/proyecto.....	24
3. Capítulo III: Marco Teórico.....	26
3.1. Marco de referencia a utilizar.....	26
3.1.1. Sistema	26
3.1.2. Riesgos para los sistemas: Ataques informáticos.....	27
3.1.3. Sistema de gestión de seguridad de la información	27

3.1.4.	Control de accesos.....	29
3.1.5.	Gestión de identidad y Accesos (IAM)	29
3.1.6.	Encargado de gestión de accesos: Sysadmin.....	32
3.1.7.	Plataforma de integración: Jira Atlassian.....	33
3.2.	Teorías y Metodologías de apoyo al tema.....	38
3.2.1.	Metodología de investigación	38
3.2.2.	Metodología KANBAN	40
3.2.3.	Metodología PDCA.....	41
4.	Capítulo IV: Propuesta de Metodología a Utilizar	44
4.1.	Propuesta o Método teórico a utilizar	44
4.1.1.	Etapas I: Planificación y estudio de plataforma a utilizar.	44
4.1.2.	Etapas II: Análisis de los procesos de On Boarding, gestión de cuentas y Off Boarding de la empresa WherEX.	46
4.1.3.	Etapas III: Levantamiento de sistemas de la organización.	53
4.1.4.	Etapas IV: Integración del sistema de gestión e identidad y acceso.....	54
4.2.	Métodos y procedimientos por utilizar.....	92
4.2.1.	Métodos de aplicación de Kanban:	92
4.2.2.	Métodos de mejoras PDCA:.....	95
5.	Capítulo V: Estudio Empírico y Resultados	99
5.1.	Análisis de resultados.....	99
5.1.1.	Etapas V: Resultados y Mejoras:	99
5.2.	Validación o verificación del método propuesto.....	112
6.	Capítulo IV: Conclusiones Generales	115
6.1.	Hechos o resultados.....	115
6.2.	Con relación a los Objetivos de la Investigación	117
6.3.	Limitaciones	118
6.4.	Recomendaciones.....	118
6.5.	Futuras Líneas de Investigación.....	118
7.	Referencias bibliográficas.....	120
8.	Anexos	125
8.1.	Anexo A: ¿Qué son el On Boarding y Off Boarding?	125
8.1.1.	On Boarding.....	125

8.1.2.	Off Boarding	125
8.2.	Anexo B: Flujos de Trabajo	126
8.2.1.	Off Boarding Mutuo Acuerdo	126
8.2.2.	Off Boarding: Renuncia Voluntaria	126
8.2.3.	Off Boarding Término de contrato a plazo Fijo:	127
8.2.4.	Off Boarding Término de práctica	127
8.2.5.	Flujo On Boarding “Cuentas Generales”	128
8.2.6.	Flujo de Off Boarding “Cuentas Generales”	128
8.3.	Anexo C: Glosario.....	129
8.4.	Anexo E: Apartados de Jira.....	130

Índice de Gráficos

Gráfico 1 Levantamiento de brechas de normativa A.9 Control de acceso	16
Gráfico 2 Monto Transado total actual en Millones de dólares	20
Gráfico 3 Monto transado Mensual en millones de dólares	21
Gráfico 4 Cantidad de compradores por mensuales en la plataforma.....	21
Gráfico 5 Cantidad de proveedores mensuales en plataforma WherEX	22

Índice de Tablas

Tabla 1 Comparación de procesos	111
Tabla 2 Soluciones de brechas identificadas.....	114

Índice de Figuras

Figura 2.2.6.2.1 Objetivos de SGSI WherEX	28
Figura 3.1.7.2.1 Vista de portal de TA Plan.....	47
Figura 3.1.7.2.2 Vista de solicitud de proceso de práctica	47
Figura 3.1.7.2.3 Vista solicitud de búsqueda de colaborador	48
Figura 3.1.7.2.4 Mensaje de Penélope automatización de Zapier.....	49
Figura 3.1.7.2.5 Proceso On Boarding desde HR-Ops.....	50
Figura 3.1.7.2.1 Opción de crear proyecto y proyectos creados	55
Figura 3.1.7.2.2 Creación de proyecto Jira Service Management.....	56
Figura 3.1.7.2.3 Vista de lista de incidencias Proyecto de cuentas (PDC)	56
Figura 3.1.7.2.4 Vista PDC Tablero de incidencias	57
Figura 3.1.7.2.5 Vista de solicitudes dentro de "PDC"	57
Figura 3.1.7.2.6 Creación Jira Software Project	58
Figura 3.1.7.2.7 Vista tablero Kanban Cuentas Generales (CG)	58
Figura 3.1.7.2.8 Vista de Screen y Custom Fields Colaborador "CG"	59
Figura 3.1.7.2.9 Continuación de Screen y Custom Fields Colaborador "CG"	60
Figura 3.1.7.2.10 Screen y Custom Fields de Sistemas "CG"	60
Figura 3.1.7.2.11 Workflow de "Cuentas Generales"	61
Figura 3.1.7.2.12 Vista 1 de automatizaciones de "CG"	62
Figura 3.1.7.2.13 Vista 2 automatizaciones "CG"	62
Figura 3.1.7.2.14 Vista de Issue Colaborador en "CG"	66

Figura 3.1.7.2.15 Vista de Issue Sistema en "CG"	66
Figura 3.1.7.2.16 Vista de configuración de Webhook y el tipo de mensaje a Slack	68
Figura 3.1.7.2.17 Vista de canal para "Pruebas de Proyecto"	69
Figura 3.1.7.2.18 Creación de Proyecto IAM "Acceso Sistemas Wherex" (ASW).....	71
Figura 3.1.7.2.19 Screen y Custom Field Colaborador en "ASW" Información general	72
Figura 3.1.7.2.20 Screen y Custom fields de cuentas generales de colaborador en "ASW" ...	74
Figura 3.1.7.2.21 Screen y Custom Field de Sistemas en "ASW"	77
Figura 3.1.7.2.22 Vista de Workflow Colaborador en "ASW"	80
Figura 3.1.7.2.23 Workflow de Sistemas "ASW"	80
Figura 3.1.7.2.24 Importación de incidencias y elección de CSV General de Sistemas.....	81
Figura 3.1.7.2.25 Settings Importación de incidencias "ASW"	82
Figura 3.1.7.2.26 Map Fields de Importación de incidencias "ASW"	83
Figura 3.1.7.2.27 Map Values para confirmar valores de importación de incidencias.....	84
Figura 3.1.7.2.28 Selección de validación de datos de Map Values	84
Figura 3.1.7.2.29 Validación de incidencias listas para Importar a "ASW"	85
Figura 3.1.7.2.30 Automatizaciones 1 de "ASW"	86
Figura 3.1.7.2.31 Automatizaciones 2 de "ASW"	86
Figura 3.1.7.2.32 Automatizaciones "ASW" página 2.....	87
Figura 3.1.7.2.33 Aviso vía correo de término de práctica a líder	89
Figura 3.1.7.2.1 Vista de tablero Kanban ASW.....	93
Figura 3.1.7.2.2 Vista principal de panel "Resumen de Sistemas" y "Sistemas generales"	94
Figura 3.1.7.2.3 Vista de panel Resumen de Status	94
Figura 3.1.7.2.4 Vista de "Resumen de Tarjetas" y "Sistemas por Área"	95
Figura 3.1.7.2.1 Vista de incidencias "Tarjetas de Crédito" agregadas a "Inventarios"	97
Figura 3.1.7.2.2 Vista de anexo de Tarjeta de crédito a Issue de Colaborador en ASW	97
Figura 3.1.7.2.1 Vista de detalle de Tarjeta de crédito	98
Figura 5.1.1.1.1 Evidencia 1 de Onboardin Eitor en pruebas	100
Figura 5.1.1.1.2 Evidencia 2 de Onboardin Eitor.....	100
Figura 5.1.1.1.3 Evidencia 3 de Onboardin Eitor pruebas finales	101
Figura 5.1.1.1.4 Vista de Issue Colaborador información personal.....	102
Figura 5.1.1.1.5 Vista de cuentas generales de Issue y activos anexados desde "Inventarios"	102

Figura 5.1.1.1.6 Vista de ejemplo de Cuentas específicas de Issue Colaborador	103
Figura 5.1.1.1.7 Correo enviado a líder sobre credenciales creadas	103
Figura 5.1.1.1.8 Vista de Issue Sistema ASW y contador de usuarios	104
Figura 5.1.1.2.1 Mensaje de OffboardBot.....	105
Figura 5.1.1.2.2 Evidencia 2 de Mensajes de OffboardBot	105
Figura 5.1.1.2.3 Vista de Status "Por desvincular"	106
Figura 5.1.1.2.4 Selección de Status "Por desvincular" en Issue	106
Figura 5.1.1.2.5 Vista de Status "Desvinculado"	107
Figura 5.1.1.4.1 Diagrama de flujo Off Boarding Mutuo Acuerdo	126
Figura 5.1.1.4.1 Diagrama de Flujo Off Boarding Renuncia Voluntaria.....	126
Figura 5.1.1.4.1 Diagrama de Flujo Off Boarding Contrato a plazo Fijo	127
Figura 5.1.1.4.1 Diagrama de Flujo Off Boarding Término de contrato Práctica	127
Figura 5.1.1.4.1 Flujo de On Boarding y gestión de cuentas según "CG"	128
Figura 5.1.1.4.1 Flujo de Off Boarding Según "CG"	128
Figura 5.1.1.4.1 Vista de plantilla Jira Software Project.....	130
Figura 5.1.1.4.2 Portal principal de Internal Support (USS).....	131
Figura 5.1.1.4.3 Vista de opciones de Internal Support (USS)	131
Figura 5.1.1.4.4 Continuación de la vista portal de Internal Support (USS)	132
Figura 5.1.1.4.5 Vista de Solicitud de mantenimiento de equipos "USS"	132
Figura 5.1.1.4.6 Vista de Solicitud de Activos "USS"	133
Figura 5.1.1.4.7 Vista de solicitud Baja de Usuario "USS" (Flujo de Off Boarding)	133
Figura 5.1.1.4.8 Vista de solicitud de Nueva Licencia de Plataforma "USS"	134
Figura 5.1.1.4.9 Vista de solicitud Soporte de Equipos "USS"	134
Figura 5.1.1.4.10 Vista Solicitud de Informe de equipo (Hardware) Dañado "USS"	135
Figura 5.1.1.4.11 Vista de solicitud Gestión de cuentas "USS".....	135
Figura 5.1.1.4.12 Vista de solicitud Tarjetas de Accesos "USS".....	136
Figura 5.1.1.4.13 Vista de solicitud Otras solicitudes "USS"	136
Figura 5.1.1.4.14 Vista de solicitud Eliminación de licencia de plataforma suscrita "USS".	137
Figura 5.1.1.4.1 Reuniones semanales con Automation Engineer para estudio de Jira.....	137

1. Capítulo I: Introducción

1.1. Contexto

En el contexto actual, la gestión de la información se ha vuelto crucial para las organizaciones, especialmente cuando abarca áreas económicas, sociales, políticas, gubernamentales o tecnológicas. Las empresas enfrentan constantes amenazas de entidades ilegales que buscan acceder a sus activos de información mediante ataques cibernéticos, conocidos como “Malwares”. Estos ataques tienen como objetivo principal causar perjuicios financieros tanto a individuos como a organizaciones de distintos sectores. (Guaña Moya, y otros, 2022).

Para abordar estas problemáticas, las empresas han reconocido la necesidad de enfrentar las amenazas mediante la implementación de medidas que cumplan con las normativas legales, como la Norma ISO27001:2013. Esta norma comprende alrededor de 115 controles regulatorios diseñados para controlar y mitigar diversos riesgos en relación con la protección de los activos de información (Baldecchi Q., 2014). Dado que la información representa un recurso vital en cualquier entidad, ya sea en formato físico, digital o transmitido, su seguridad es crucial. En un entorno cada vez más interconectado, esta información está expuesta a una variedad de amenazas y vulnerabilidades. Por lo tanto, la seguridad de la información se convierte en un escudo protector esencial para mitigar pérdidas, aprovechar oportunidades comerciales, optimizar la inversión y asegurar la continuidad operativa. Este objetivo se logra mediante la implementación de políticas, procedimientos, controles y tecnología, pero también a través de la conducta ética de quienes gestionan la información.

Para satisfacer los requisitos normativos previamente mencionados, es esencial establecer un plan de acción conocido como Sistema de Gestión de Seguridad de la Información (SGSI) (Ladino A., Villa S., & López E., 2011). En este contexto, tal como

indican Ladino, Villa y López en su artículo, el SGSI garantiza el cumplimiento de la norma ISO27001 mediante una serie de procesos y acciones diseñadas para atender las necesidades y expectativas de la organización y las partes interesadas. Su principal objetivo es reducir los riesgos y mitigar las posibles brechas identificadas dentro de la empresa.

Aun así, a pesar de que varias organizaciones se encuentren certificadas en la norma ISO27001:2013, no implica una totalidad en la seguridad de la información, sino más bien, una disminución del riesgo, es decir, aún sigue siendo posible el robo de activos de información por ataques de cibernéticos. También por la usurpación de datos como el “Ransomware”, (Barker, Scarfone, Fisher, & Souppaya, 2022) en el cual la entidad atacante cifra los datos de la organización y exigen una cantidad de dinero para devolver la información sustraída. Esto implica que, en caso de robar información sensible, los atacantes presionen a la organización para que pague por no difundir la información a terceros no autorizados, como competencia o público en general.

Por otro lado, tener en cuenta que una medida de seguridad dentro de las empresas como lo es el registro de accesos a todos sus colaboradores; ya sea por medios de credenciales definidas, como el método de Single Sign – On (SSO), donde cada colaborador puede ingresar a una red empresarial y sus recursos, por medio de un usuario [25] y contraseña; como también es posible ingresar a partir de la autenticación de usuario (UAAW) (Pacheco, 2010). De esta manera se puede evitar la usurpación de identidad por “Ransomware” y el robo de datos dentro de las organizaciones.

Cabe destacar que ninguna organización se encuentra completamente libre de riesgos de ciberamenazas, como fue el caso de Chile en lo que indica Barría en su Tesis; de 545.231 ataques de ransomware en 157 países, Chile concentró alrededor del 1,8% de los ataques totales; situándolo en el puesto 10° de los países que fueron analizados (Barría Barrientos,

Actualización del sistema de gestión de seguridad de la información basado en la norma ISO27001:2013 en la empresa CCS SPA, 2021). Por esta razón, es prescindible para todas las organizaciones buscar la manera de combatir estas amenazas, implementando diversas metodologías de defensa y contramedidas para evitar sufrir algún ciberataque.

Debido a lo anterior, se contempla que la información representa un recurso invaluable, especialmente para Wherex, una empresa de tipo SaaS (Software As a Service) donde la información constituye su activo principal. Cada individuo y componente asociado al colaborador se convierte en un elemento de gran importancia para el funcionamiento integral de la empresa. Por ello, se requiere una sólida seguridad tanto dentro de la compañía como en las plataformas que emplea; medidas que, en ambos casos, están respaldadas por la certificación de la norma ISO27001:2013. La salvaguarda de los recursos de información resulta fundamental para el éxito organizacional. Sin embargo, aún existe el riesgo inherente de divulgación, mal uso, robo, eliminación o sabotaje de la información, lo que afecta su disponibilidad y la expone a diversas amenazas (Niño Morante, 2018).

Es por estas razones que surgen las siguientes preguntas: ¿Qué papel juega el control de acceso normativo en la protección de la integridad del sistema de WherEX?, ¿Qué vulnerabilidades y riesgos de seguridad se han identificado en WherEX como resultado de las deficiencias en la gestión de accesos?, ¿Cuáles son las medidas que se deben tomar de manera urgente en WherEX para abordar las vulnerabilidades y riesgos de seguridad identificados para proteger la integridad de la información de la empresa?, ¿Cómo se espera que el control de accesos contribuya a la seguridad de la información en WherEX y a su cumplimiento de las normativas de seguridad establecidas?

1.2. Origen o Justificación del problema

El problema de seguridad en los accesos a los sistemas de WherEX surge como resultado de varias deficiencias en los procesos de gestión de usuarios y desvinculación de colaboradores. Según la normativa ISO27001:2013, se establecen controles específicos para gestionar el monitoreo y registro de ingresos de usuarios, conocido como "A.9 Control de accesos" (International Organization for Standardization (2013a), 2013). Aunque estos controles fueron implementados en WherEX a través de plataformas como Amazon Web Services, Atlassian, Google Workspace, Microsoft 365 y Slack; se identificaron irregularidades durante la revisión de las credenciales de los usuarios. Se encontraron cuentas activas de colaboradores desvinculados, lo que representa una vulnerabilidad significativa que podría dar lugar a accesos no autorizados y comprometer la integridad del sistema.

Además, durante la evaluación de riesgos (**Gráfico 1**), se evidenció un margen de error significativo en el proceso de desvinculación de colaboradores (definido como **Off Boarding**). Se observaron fallos en la comunicación sobre la salida de excolaboradores, así como omisiones en la creación de “Tickets” para dar de baja las cuentas en el portal de Internal Support (USS). Este proceso manual de desactivación de cuentas contribuye al mantenimiento de cuentas habilitadas de manera indebida, lo que aumenta el riesgo de exposición de información sensible.

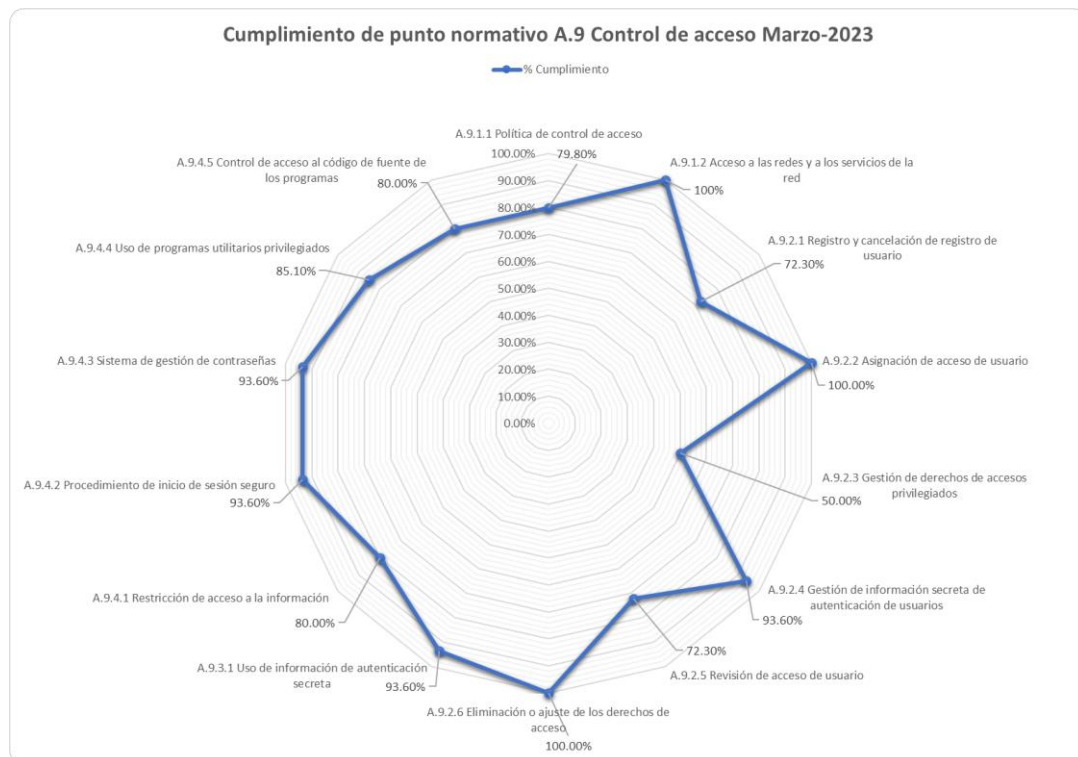


Gráfico 1 Levantamiento de brechas de normativa A.9 Control de acceso

Fuente: Elaboración propia, basado en la Norma ISO27002:2013

Una revisión adicional reveló la falta de un proceso definido y centralizado para regular y controlar los accesos a los sistemas de WherEX. Se identificó que algunos registros se realizan manualmente en hojas de cálculo, lo que puede llevar a inconsistencias y pérdida de información. Además, la desvinculación de colaboradores con proyectos en curso presenta desafíos para el traspaso de información sensible a cuentas generales de la empresa, lo que podría comprometer la seguridad de los datos.

Por estas causas, la ausencia de procesos claros y sistemas definidos para la gestión de accesos y desvinculación de colaboradores en WherEX ha generado una serie de vulnerabilidades y riesgos de seguridad que deben ser abordados de manera urgente para proteger la integridad de la información y garantizar el cumplimiento de las normativas de seguridad establecidas.

1.3. Objetivos

1.3.1. Objetivo General

Desarrollar e implementar un sistema de gestión e identidad de accesos (Identity and Access Management o IAM) de las plataformas de WherEX, que optimice la seguridad de la información y la eficiencia operativa, adaptándose a las necesidades crecientes de la empresa en un entorno de rápida expansión y cambio tecnológico.

1.3.2. Objetivos Específicos

1. Mejorar la seguridad de los datos y sistemas de WherEX, reduciendo el riesgo de accesos no autorizados y brechas de seguridad.
2. Facilitar la gestión de accesos durante los procesos de **On Boarding** y **Off Boarding** de colaboradores, asegurando la activación y desactivación eficiente y oportuna de cuentas y accesos.
3. Optimizar los recursos financieros mediante la reducción del gasto mensual en cuentas de usuarios desvinculados en plataformas pagas, contribuyendo así a la eficiencia operativa y la gestión responsable de costos.
4. Medir y evaluar continuamente la eficacia del sistema implementado, ajustando y mejorando los procesos y las tecnologías en función de las necesidades cambiantes y las mejores prácticas de la industria.

2. Capítulo II: Estado del Arte y Alcance

2.1. Estado actual del Conocimiento

Uno de los casos particulares que fue visto como pionero fue el proyecto de implementación del Sistema de Gestión de Identidades y Accesos (IAM) en la Universidad de Cuenca, Ecuador (Torres, De los Reyes, Espinoza, & Saquicela, 2017). El informe abordaba la necesidad de optimizar el acceso y la gestión de la información para los estudiantes y el personal administrativo. Se identificó que la duplicación de información y accesos, derivada de los múltiples dominios de autenticación de la institución, planteaba riesgos en el control de usuarios y la integridad de la información.

Inicialmente, la universidad gestionaba más de 40,000 cuentas de usuario distribuidas en dos dominios de autenticación: `ucuenca.edu.ec` y `ucuenca.ec`. Ante esta situación, se propuso fusionar los usuarios de ambos dominios en uno solo, “`ucuenca.edu.ec`”, para simplificar la gestión de credenciales e implementar un servicio de autenticación único.

Para abordar estos desafíos, se realizaron diversos análisis de los datos obtenidos de las fuentes de autenticación existentes, identificando problemas como nombres de usuario duplicados y la falta de una política institucional de gestión de usuarios. Además, se detectaron inconsistencias en las credenciales debido al uso de caracteres especiales, lo que dificultaba la creación y modificación de cuentas en algunos servicios.

El proyecto se llevó a cabo en fases, comenzando con pruebas de concepto de cada herramienta y su integración con los sistemas existentes. A través de este proceso, se fortaleció el conocimiento técnico del equipo y se refinaron los detalles de funcionalidad esperada.

Lograr la implementación del IAM en la Universidad de Cuenca representó un esfuerzo para modernizar y optimizar la gestión de identidades y accesos, con el objetivo de

mejorar la seguridad informática y facilitar el acceso a los recursos institucionales.

2.2. Antecedentes de la organización

2.2.1. Sobre la organización

Este estudio se realiza en CCS SpA, también reconocida como wherEX, una plataforma en línea de comercio electrónico B2B que enlaza las demandas de compañías de distintos sectores con las mejores ofertas disponibles. WherEX opera bajo el principio de "Where Exchange", con el propósito de ofrecer soluciones comerciales a través de su plataforma web, WherEX Sourcing. Esta plataforma simplifica la realización de licitaciones para productos y servicios industriales, abarcando una amplia variedad de necesidades empresariales. (WherEX, s.f.)

2.2.2. Origen

La empresa, que originalmente se llamaba AQmarket, surgió en 2015 en el sector acuícola y pesquero en Puerto Varas, Chile, con la intención de transformar los procesos de compra de grandes empresas. Bajo la dirección del Gerente General y Co Fundador Juan Carlos Hurtado; y en conjunto al director de Ventas y Marketing, Felipe Manterola (Barría Barrientos, Actualización del sistema de gestión de seguridad de la información basado en la norma ISO27001:2013 en la empresa CCS SPA, 2021).

Posteriormente, en 2018, la empresa se reestructuró como WherEX SpA. Con oficinas inaugurales en Puerto Varas y Santiago, ha experimentado un crecimiento significativo, aumentando su personal de 10 personas a aproximadamente 200 en la actualidad. (García Morales, 2023)

2.2.3. Desarrollo

En 2019, se expandió hacia las principales industrias productivas del país y se llevó a cabo un cambio de marca a WherEX, logrando un volumen de transacciones de 200 millones de dólares. Al año siguiente, en 2020, se abrieron nuevas oficinas en Lima, Perú. En 2021, la expansión continuó con la apertura de oficinas en México y Colombia, alcanzando nuevamente transacciones por 200 millones de dólares. Durante este periodo, el equipo creció a 40 personas y se gestionaron 300,000 ofertas de 7,500 proveedores en total (WherEX, s.f.).

A continuación, se presentan algunas estadísticas de actividad.

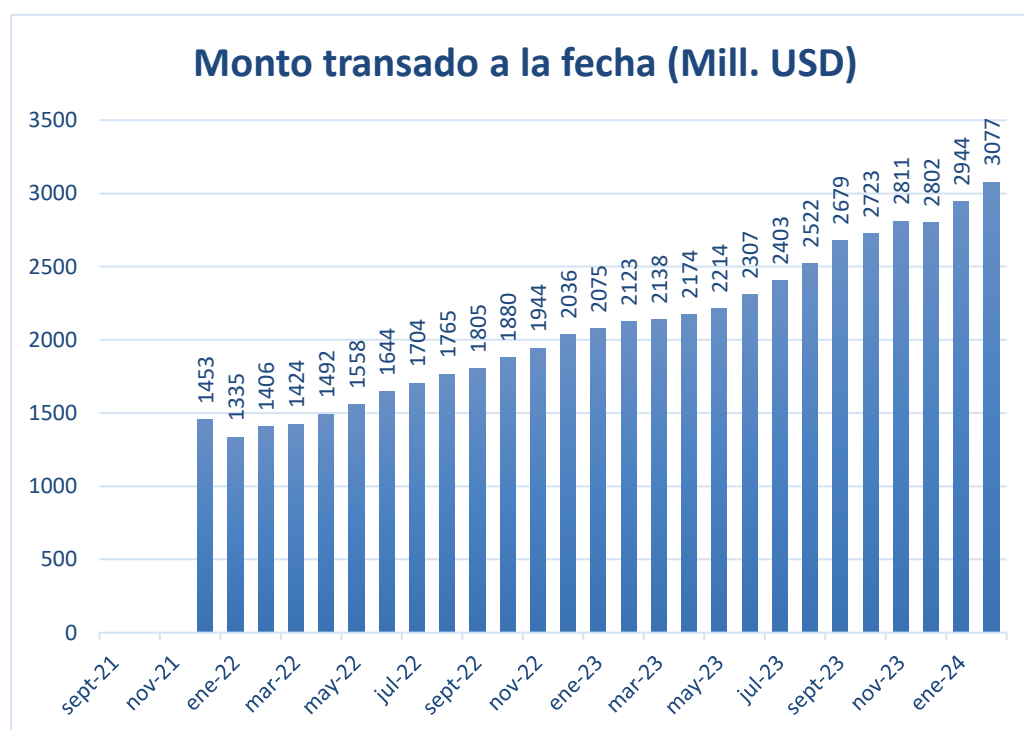


Gráfico 2 Monto Transado total actual en Millones de dólares

Fuente: Elaboración Propia, en base a datos otorgados por WherEX.

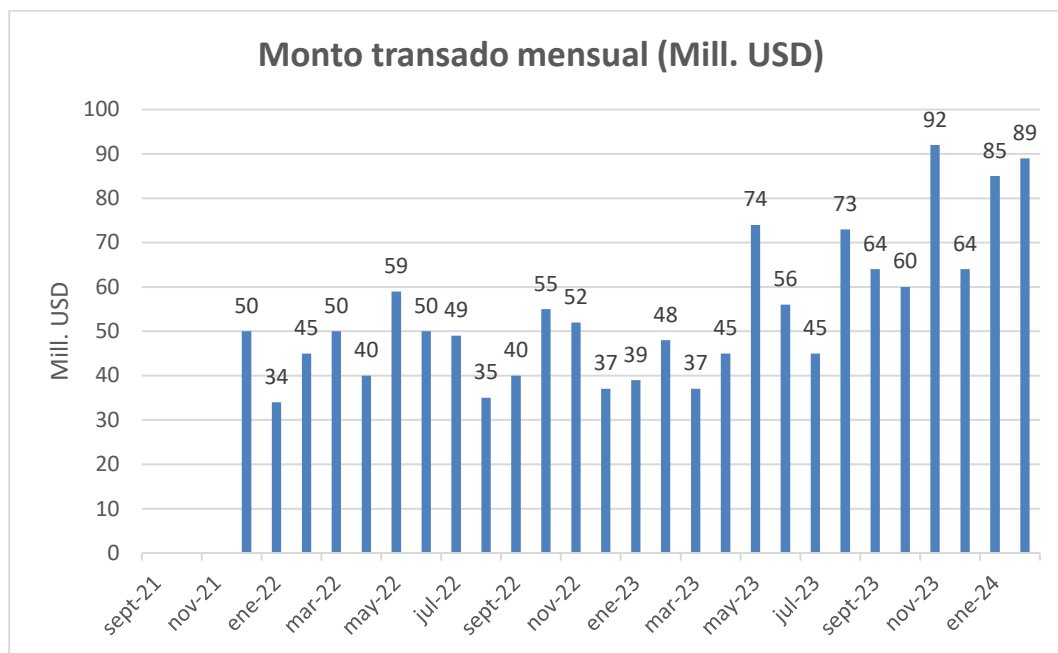


Gráfico 3 Monto transado Mensual en millones de dólares

Fuente: Elaboración Propia, en base a datos otorgados por WherEX.

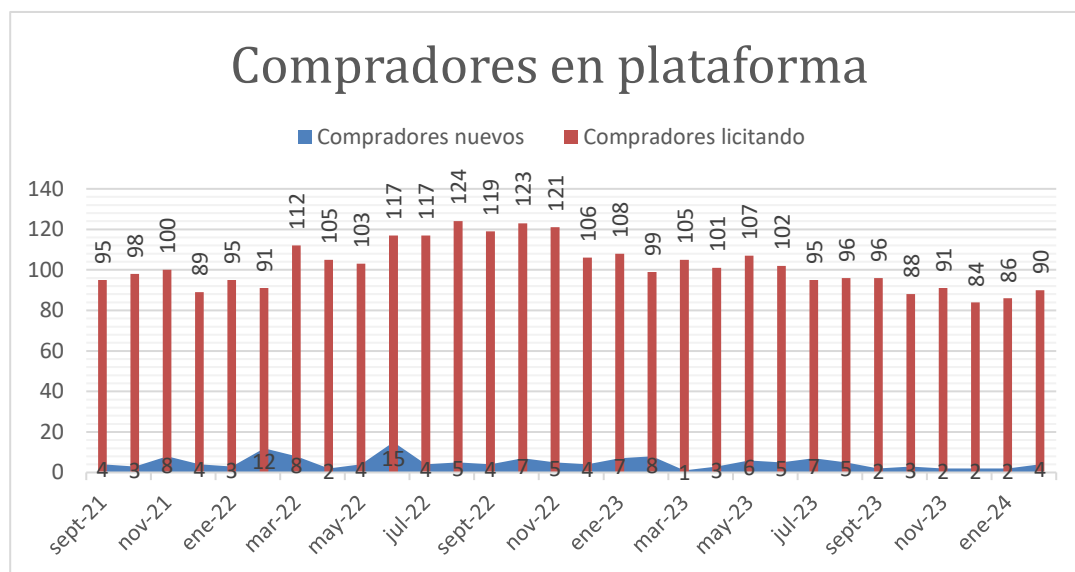


Gráfico 4 Cantidad de compradores por mensuales en la plataforma

Fuente: Elaboración Propia, en base a datos otorgados por WherEX.

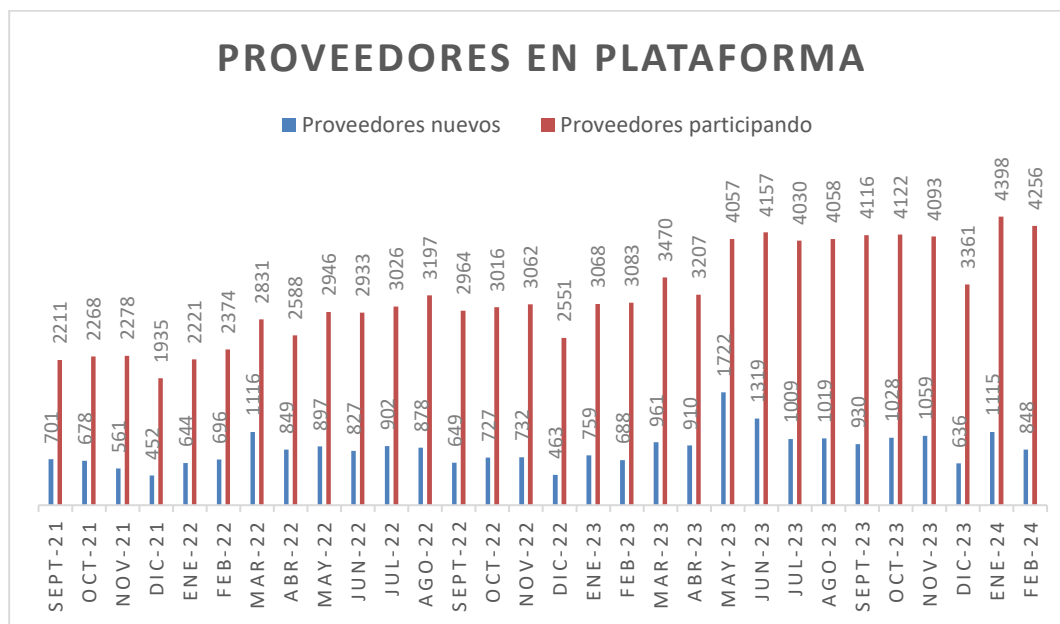


Gráfico 5 Cantidad de proveedores mensuales en plataforma WherEX

Fuente: Elaboración Propia, en base a datos otorgados por WherEX.

2.2.4. Misión

“Minimizar los costos de transacción de las compras industriales”.

2.2.5. Visión

“Ser el marketplace B2B líder de Latam”

2.2.6. Modelos de negocio

2.2.6.1. *WherEX Sourcing:*

Wherex Sourcing se configura como un centro de reunión para empresas de diversos campos, enlazándolas con una amplia variedad de proveedores a través del Marketplace de Wherex. Esta plataforma facilita la satisfacción de las necesidades de grandes corporaciones al proporcionarles acceso a una extensa red de distribuidores y proveedores. En este entorno,

los protagonistas son las empresas, los proveedores y los distribuidores. La esencia de su propuesta radica en llevar a cabo negociaciones competitivas, ofreciendo a los clientes una amplia gama de opciones para sus cotizaciones. Además, se promueve la transparencia y la trazabilidad, reduciendo el riesgo de fraudes mediante alertas integradas en la plataforma. La automatización de procesos simplifica la toma de decisiones y las compras, al tiempo que la mejora en la gestión de gastos conlleva ahorros y una guía basada en benchmarks. (Hurtado, 2023).

2.2.6.2. WherEX Pay:

Wherex Pay contribuye al manejo de las cuentas pendientes y por cobrar en las empresas, complementándolas con productos financieros como Factoring y Confirming. Según Hurtado en su presentación de “WherEX 101”; este enfoque comprende tres tipos de servicios distintos: (Hurtado, 2023)

- 1. Supply Chain Finance (SCF):** Dirigido a los proveedores clientes, este servicio genera ingresos a través de intereses en financiamiento. Utilizando productos como el "factoring", "confirming prórroga", "confirming pronto pago" y "descuento dinámico pronto pago", se adelanta el pago de facturas a los proveedores, agilizando el flujo de efectivo.
- 2. Cuentas por pagar:** Dirigido a los compradores, este servicio se accede a través del SCF. Incluye características como el portal de proveedores y el método "3-Ways-Match", diseñados para reducir la carga administrativa y los errores en los pagos mediante la digitalización y automatización del proceso.
- 3. Cuentas por cobrar:** Destinado nuevamente a los proveedores clientes, ofrece productos como acceso a financiamiento, análisis financiero, pronóstico de flujo

de efectivo y portal de cobranza. Su valor radica en la reducción de costos financieros y riesgos de liquidez, proporcionando una previsión precisa del flujo de efectivo y un acceso competitivo a financiamiento.

2.3. Propuesta de Valor del tema

La implementación del sistema propuesto tiene como objetivo principal proporcionar un control de los accesos a los activos de información en los sistemas de WherEX, permitiendo a la empresa tener una visión completa y detallada de su infraestructura tecnológica. Además, el sistema ayudaría a mitigar el riesgo asociado a la información sensible de excolaboradores, garantizando que sus accesos sean desactivados de manera oportuna y adecuada. También se esperaría una reducción de costos al eliminar usuarios con cobros extras de colaboradores desvinculados o cuentas en desuso, lo que optimizaría el uso de los recursos financieros de la empresa. Finalmente, la implementación del sistema abriría la posibilidad de crear nuevas mejoras y características automatizadas, lo que contribuiría a la continua optimización y evolución del sistema de gestión de identidad y accesos de las plataformas de WherEX.

2.4. Alcance de la memoria/proyecto

El alcance de esta memoria abarca la implementación de un sistema de gestión de identidad y accesos en la empresa WherEX SpA, diseñado para controlar y verificar el uso adecuado de los accesos a sus plataformas por parte de los diferentes tipos de usuarios y perfiles. Se detallará el proceso de análisis de los flujos de procesos de la empresa en colaboración con el equipo de Sistema de Gestión de la Seguridad de la Información (SGSI), identificando brechas en la gestión de ingreso y salida de colaboradores y proponiendo mejoras, automatizaciones y un método de monitoreo de los sistemas de WherEX.

Se promoverá la perspectiva de mejora continua mediante la implementación de metodologías orientadas a optimizar los flujos de trabajo, con el objetivo de desarrollar un sistema independiente con capacidad de autogestión, activando cada proceso de manera eficiente.

El proyecto se centra en gestionar los accesos de usuarios mediante el control de los encargados de Sysadmin, quienes manipulan las casillas de sistemas para llevar un registro detallado, asegurando que este control no interfiera con el registro de usuarios según los flujos de entrada y salida de colaboradores, para mitigar posibles riesgos de pérdida o robo de información.

3. Capítulo III: Marco Teórico

3.1. Marco de referencia a utilizar

3.1.1. Sistema

Según la información de la clase de “Teoría de sistemas” del profesor Oscar Saavedra (Saavedra Rodríguez, 2023), un sistema se define como un conjunto organizado de elementos o componentes que interactúan e interrelacionan de manera interdependiente, formando una estructura integral y compleja. Esta estructura exhibe propiedades emergentes que van más allá de las características individuales de sus partes constituyentes, dando lugar a una entidad holística donde la interacción de los componentes genera comportamientos y funciones distintivos.

Dos características esenciales de los sistemas son sus componentes y la estructura que regula las relaciones entre ellos. Además, los sistemas exhiben funciones específicas y mecanismos de integración que aseguran su estabilidad y coherencia, basándose en principios de cibernética y dirección. Otras propiedades notables incluyen relaciones interconectadas entre los elementos, delimitación de una frontera respecto a su entorno, sinergia resultante de la interacción de las partes, recursividad que permite subsistemas, homeostasis para mantener el equilibrio y adaptabilidad para ajustarse a cambios en el entorno.

Un sistema se define como una estructura integrada en la que sus partes interactúan de manera dinámica, creando propiedades nuevas que van más allá de las características individuales de cada parte. Esta forma de ver los sistemas es clave para entender la complejidad de entidades como las empresas, ya que proporciona un marco completo para estudiarlas y gestionarlas.

3.1.2. Riesgos para los sistemas: Ataques informáticos

Los ataques informáticos representan una amenaza persistente para la seguridad de las organizaciones, ya que explotan debilidades en el software, hardware y comportamiento humano con el fin de obtener ganancias económicas y causar daños a los sistemas y activos. Para hacer frente a esta problemática, es crucial que las organizaciones implementen procedimientos y prácticas que prevengan y mitiguen los riesgos. La educación juega un papel vital al permitir comprender las vulnerabilidades comunes y sus riesgos asociados, facilitando la identificación de debilidades y la implementación de estrategias de seguridad efectivas (Mieres, 2009).

Los datos proporcionados por la página Pauta.cl indican un incremento significativo en los ataques informáticos tanto en Chile como en América Latina durante el año 2018, con un aumento del 59% y 60%, respectivamente (Pauta, 2019). Este aumento se ilustra con el incidente de hackeo al Banco de Chile, donde se logró sustraer 10 millones de dólares en una operación compleja que se extendió por varios meses. Este episodio subraya la gravedad de la amenaza que enfrentan las instituciones financieras y resalta la evolución de los ataques, los cuales van más allá de la simple infiltración de virus en los sistemas informáticos (Pauta, 2018).

3.1.3. Sistema de gestión de seguridad de la información

El Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procesos, procedimientos y controles diseñados para administrar la seguridad de la información en una organización. Su establecimiento e implementación se basa en las necesidades y objetivos de la organización, así como en los requisitos de seguridad, los procesos organizacionales utilizados y la estructura de la organización. El SGSI tiene como

objetivo principal preservar la confidencialidad, integridad y disponibilidad de la información, considerados como los tres pilares fundamentales de la seguridad de la información. Para lograr esto, el SGSI se centra en proteger los activos de información, garantizar el cumplimiento de las políticas y normativas, así como en la revisión continua, la supervisión y la mejora de las directrices de seguridad (**Figura 2.2.6.2.1**). Además, busca asegurar el cumplimiento de la normativa vigente y proporcionar confianza a clientes, proveedores y otras partes interesadas en cuanto a la protección de los activos de información mediante un sistema de gestión de seguridad de la información (Barría Barrientos, Capacitación SGSI On Boarding Wherex [Documento compartido], 2023).

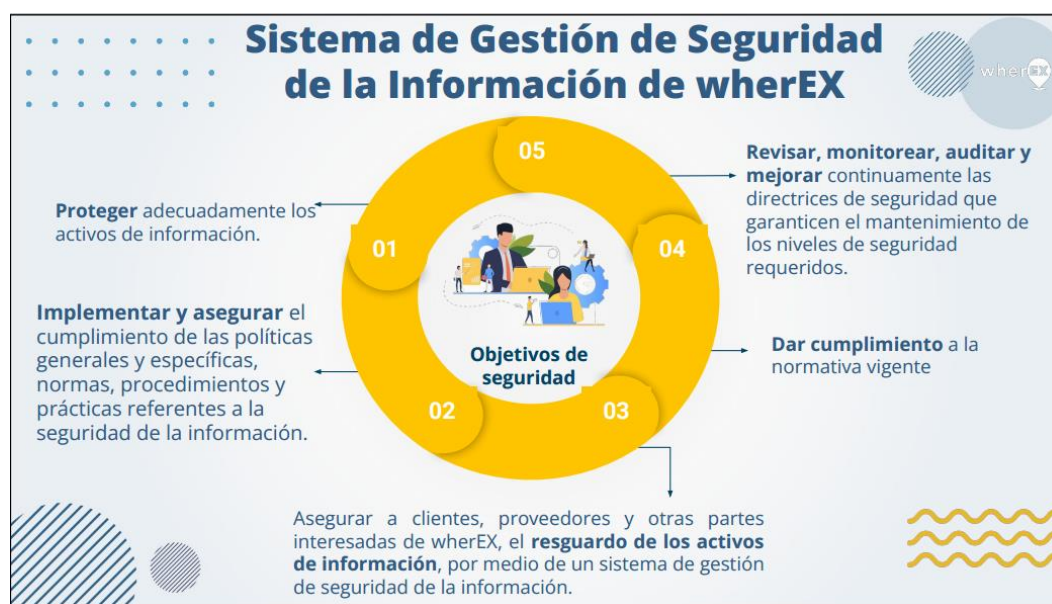


Figura 2.2.6.2.1 Objetivos de SGSI WherEX

Fuente: (Barría Barrientos, Capacitación SGSI On Boarding Wherex [Documento compartido], 2023)

3.1.4. Control de accesos

El control de accesos se define como el conjunto de políticas, procedimientos y controles técnicos implementados por una organización para garantizar que únicamente las personas autorizadas accedan a los recursos de información y sistemas.

La norma ISO 27001:2013 establece que el control de accesos busca prevenir accesos no autorizados que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Abarca áreas como gestión de contraseñas, autenticación de usuarios, autorización de acceso, monitoreo de accesos y protección de dispositivos (International Organization for Standardization (2013a), 2013).

La aplicación efectiva del control de accesos implica el establecimiento de políticas y procedimientos claros para la gestión de identidades y accesos, así como la implementación de controles técnicos como firewalls, sistemas de detección de intrusiones y gestión de accesos. Esto permite garantizar que solo las personas autorizadas tengan acceso a la información y los sistemas, reduciendo el riesgo de incidentes de seguridad (International Organization for Standardization (2013b), 2013).

El control de accesos se sustenta en tres actividades principales: autenticación, autorización y registro de auditoría. Requiere sistemas base (software) para administrar y controlar los accesos, así como personal alterno (backup) que pueda asumir funciones en caso de ausencia (Sacoto Mosquera, 2019).

3.1.5. Gestión de identidad y Accesos (IAM)

Un Sistema de Administración de Identidades y Accesos (IAM) representa una estrategia completa que abarca una serie de procesos, tecnologías y políticas empresariales

destinadas a gestionar de manera centralizada y automatizada las identidades de los usuarios, así como regular su acceso a los recursos de la organización. La implementación efectiva de un sistema IAM requiere la adopción de procesos y herramientas que permitan la gestión segura y eficiente de las identidades de los usuarios, garantizando que los permisos de acceso se asignen conforme a las políticas establecidas y que se mantengan registros detallados para fines de auditoría (Montoya & Restrepo, 2012).

Al implementar un sistema IAM sólido, no solo se fortalece la seguridad y el control de acceso, sino que también se optimiza la gestión de identidades, se reducen los riesgos y se mejora la eficiencia operativa, contribuyendo así al cumplimiento de regulaciones y normativas. Sin embargo, para alcanzar estos beneficios, es esencial contar con el compromiso y la colaboración de todos los niveles de la organización, desde la alta dirección hasta los equipos de soporte y apoyo (Castro, 2020).

3.1.5.1. Ventajas de la IAM.

Montoya, Restrepo y Castro señalan que la implementación de un Sistema de Gestión de Identidades y Accesos (IAM) conlleva una serie de beneficios significativos. En primer lugar, destaca el fortalecimiento de la seguridad de la información y la protección de datos al centralizar la gestión de identidades y controlar los accesos según roles, lo que reduce los riesgos asociados al robo de identidad y la divulgación de información confidencial.

Además, el sistema IAM permite asignar de manera eficiente los privilegios de acceso, garantizando que cada usuario acceda únicamente a los recursos necesarios para su función. Esto se alinea con el principio del menor privilegio y ayuda a mitigar los riesgos de accesos indebidos. Asimismo, la optimización de procesos administrativos y la reducción de costos

relacionados con la gestión de cuentas son ventajas notables de la implementación de IAM.

Por último, la adopción de IAM facilita el cumplimiento de regulaciones y normativas, ya que genera registros de auditoría que simplifican el monitoreo y la rendición de cuentas. Esto contribuye a mejorar la transparencia y la gestión de riesgos dentro de la organización, promoviendo un ambiente de seguridad y cumplimiento normativo.

3.1.5.2. Desventajas de la IAM

Sin embargo, como destacan los tres autores mencionados anteriormente, la implementación de IAM también presenta desafíos importantes. Uno de estos desafíos radica en el riesgo de vulnerabilidad asociado a contraseñas únicas, las cuales podrían comprometerse y utilizarse para suplantar identidades o robar información en ausencia de esquemas robustos de autenticación.

Además, la dependencia crítica del sistema IAM para la autenticación y autorización de accesos es otra desventaja significativa. Cualquier fallo en este sistema tendría un impacto directo en todas las aplicaciones integradas, lo que resalta la importancia de contar con componentes redundantes y mecanismos de alta disponibilidad para mitigar este riesgo.

Por otro lado, la implementación de IAM requiere una reestructuración completa de procesos y del modelo operativo de la organización, lo que demanda una considerable inversión de tiempo, esfuerzo y recursos. La definición precisa de roles de negocio y su correlación con roles técnicos es un proceso complejo que requiere atención meticulosa para evitar desviaciones y asegurar una gestión efectiva de los accesos.

Finalmente, la implementación de IAM representa una inversión considerable en términos de recursos económicos, tiempo y personal. Esto puede dificultar la formulación de

un caso de negocio sólido y el logro de un retorno de inversión a corto plazo, convirtiendo este proyecto en una iniciativa de retorno a largo plazo.

3.1.6. Encargado de gestión de accesos: Sysadmin

El rol del Sysadmin, o Administrador de Sistemas, se centra en garantizar el correcto funcionamiento de los sistemas informáticos en toda la empresa. Sus objetivos principales incluyen implementar, configurar, mantener, monitorear, documentar y asegurar el adecuado desempeño de estos sistemas, brindando soporte integral a los diferentes procesos transversales de la organización, como Recursos Humanos y Comercial, en conformidad con estándares como la norma ISO27001:2013. Entre sus funciones esenciales se encuentra la administración de cuentas, redes y sistemas, así como la instalación, configuración y mantenimiento de la infraestructura tecnológica. Además, proporciona apoyo tecnológico integral al área de desarrollo y colabora estrechamente con ingenieros de sistemas y desarrolladores (García Morales, 2023).

En términos de seguridad de la información, el Sysadmin actúa conforme a la política general de seguridad de la compañía, protegiendo los activos contra accesos no autorizados y reportando eventos o riesgos potenciales. También tiene la responsabilidad de administrar sistemas de seguridad informática en toda la organización y de energizar continuamente la protección contra ataques maliciosos o modalidades de trabajo a distancia. Este cargo desempeña un papel crucial en la gestión y el mantenimiento de la infraestructura tecnológica de la empresa, asegurando su operatividad y seguridad. Su experiencia y conocimientos en sistemas Windows, Linux, redes LAN y WLAN, administración de firewall, servidores de correo y aplicaciones en la nube son fundamentales para cumplir con sus responsabilidades y contribuir al éxito del área de Finanzas y la organización en general (WherEX, 2022).

3.1.7. Plataforma de integración: Jira Atlassian

JIRA, desarrollado por Atlassian Corporation a partir de 2002, es un sistema de seguimiento de incidencias que inicialmente se utilizó para el seguimiento de errores de software. Sin embargo, debido a sus avanzadas funciones de personalización, se adapta fácilmente a otros tipos de sistemas de gestión de “tickets” y proyectos. NIF ICCS comenzó a emplear JIRA en 2006 para el seguimiento del desarrollo de software, reemplazando un sistema local anterior debido a las limitaciones funcionales y de recursos. JIRA facilitó la migración de datos y ha permitido a ICCS mantener un historial completo de modificaciones de software (Fisher, Koning, & Ludwigsen, 2013). Actualmente, JIRA es una herramienta basada en la web ampliamente utilizada no solo en el ámbito técnico para el seguimiento de errores e incidentes, sino también en áreas no técnicas para la gestión de tareas y proyectos. Además, gracias a sus funciones para la organización de flujos de trabajo, JIRA puede ser utilizado para la gestión y mejora de procesos en diversos contextos operativos (Gatica Herrera, 2015).

3.1.7.1. ¿Por qué Jira?

Dentro del equipo se llevó a cabo una extensa discusión sobre cómo abordar la solución para cerrar la brecha relacionada con las cuentas que permanecían activas en la empresa. Durante estas conversaciones, se consideraron diversas plataformas que podrían ayudar a mitigar este riesgo. Sin embargo, todas estas opciones implicaban costos adicionales significativos que tendrían un impacto económico considerable en la organización. Entre las alternativas consideradas se encontraban Microsoft Azure, Okta, Ping Identity y Amazon Web Services (AWS) Directory Services. A pesar de que la empresa ya contaba con licencias para Microsoft Azure y AWS, estas estaban limitadas a ciertos sistemas bajo el dominio del área

de Ingeniería. En consecuencia, se tomó la decisión de dar de baja la licencia de Microsoft Azure y se determinó que la extensión de Directory Services de AWS no ofrecía las mismas características que las plataformas existentes en la empresa, lo que la convertía esencialmente en una nueva licencia de plataforma.

Por otro lado, al considerar el aspecto de la automatización y la conexión con el portal de Internal Support (USS), se llegó a la conclusión de que era factible gestionar el proyecto dentro de Jira, aprovechando las funciones y el conocimiento del equipo, enfatizando que la plataforma tiene su propia medida de seguridad. Jira opera mediante un sistema Kanban, que es una metodología ágil que prioriza el flujo y la mejora continua del trabajo. Este método limita el número de elementos que pueden estar en proceso al mismo tiempo (Work in Progress: WIP) para establecer un flujo de trabajo visible que facilite la gestión de la calidad y la entrega continua (Gatica Herrera, 2015). Además, esta metodología se alinea con el concepto de Kaizen, que se refiere a la mejora continua, lo que implica que en todo momento es posible introducir mejoras y actualizaciones que contribuyan a los proyectos. Por lo tanto, se determinó que un IAM dentro de Jira Atlassian sería una solución viable para abordar esta problemática (Fisher, Koning, & Ludwigsen, 2013).

3.1.7.2. Conocimientos de Jira:

Incidencias (Issues): constituyen registros detallados que reflejan problemas, errores, solicitudes de mejora o tareas en proyectos de desarrollo de software y otros tipos de proyectos. Estos registros son de vital importancia para la gestión eficaz del trabajo, dado que ofrecen una descripción exhaustiva del problema o tarea, asignan responsabilidades a los miembros del equipo y permiten un seguimiento claro del progreso a través de estados como "Abierto", "En Progreso" o "Resuelto". Asimismo, facilitan la colaboración entre los

integrantes del equipo al posibilitar la inclusión de comentarios y la programación eficiente del trabajo mediante la asignación de fechas límite. Las incidencias se convierten en herramientas esenciales para la organización y ejecución exitosa de proyectos, especialmente en el ámbito del desarrollo de software, al proporcionar un medio efectivo para identificar, abordar y resolver los desafíos que surgen durante el ciclo de vida del proyecto. (Li, 2018)

Internal Support (USS): En WherEX, se cuenta con un canal interno de soporte destinado a abordar consultas relacionadas con problemas técnicos en equipos, aplicaciones, creación o bloqueo de cuentas, así como para gestionar solicitudes relacionadas con el área, solicitar cotizaciones y tramitar bajas de licencias en plataformas, entre otros servicios. Este canal está disponible para satisfacer cualquier necesidad que puedan tener los usuarios. Está integrado con un proyecto de Jira Services Management que recopila todas las incidencias y solicitudes, las cuales son revisadas y gestionadas desde el backlog hasta el estado de "Por Atender" o "Cancelado". Si se selecciona la primera opción, la solicitud avanza a "En curso" y luego a "Resuelto". La administración de este portal recae completamente en el equipo de Sysadmin, en colaboración con el Automation Engineer, quienes han definido los flujos de trabajo para cada tipo de solicitud.

Tickets: son solicitudes generadas en el portal de Internal Support (USS) administrado por Jira. Un ticket hace referencia a una incidencia creada por un proyecto de servicio de Tecnologías de la Información (TI), gestionado por el equipo de Sysadmin. Estas incidencias pueden ser de diversos tipos, dependiendo de la naturaleza de la solicitud. Entre ellas se encuentran las incidencias relacionadas con equipos, la gestión de cuentas, la solicitud de nuevas licencias en plataformas y la baja de usuarios debido a desvinculaciones laborales.

Jira Software Management: se define como una estructura que representa el trabajo

de desarrollo de un producto, proyecto o servicio dentro de la plataforma Jira Software. En este contexto, Jira funciona como un rastreador central de problemas que ayuda a los equipos en la priorización, organización y gestión eficiente del trabajo asociado al desarrollo de software. Los proyectos de Jira Software consisten en colecciones de problemas que abarcan historias, errores, tareas y otros elementos relevantes. Estos proyectos tienen la flexibilidad de adoptar metodologías ágiles como Scrum o Kanban, así como de implementar un seguimiento de errores básico, dependiendo de los requisitos del equipo y la naturaleza del trabajo realizado. Asimismo, los proyectos de software administrados a través de Jira permiten una configuración y gestión colaborativas del trabajo, posibilitando que cualquier miembro del equipo pueda crear y administrar proyectos de manera sencilla, aunque solo los administradores tengan la capacidad de crear proyectos gestionados por la empresa. (Atlassian, s.f.)

Jira Service Management: se destaca como una plataforma integral diseñada para administrar las solicitudes de los clientes, permitiendo recibir, rastrear y resolver problemas de manera eficaz. Con atributos que incluyen la centralización de solicitudes en un único lugar, la colaboración entre equipos y la integración con otras herramientas de Atlassian, como Confluence y Opsgenie. Jira Service Management brinda una solución completa para la gestión de proyectos, facilitando la coordinación entre los equipos de TI, desarrollo, operaciones y negocios. Además, proporciona funcionalidades avanzadas como la gestión de incidentes y cambios, así como la capacidad de llevar a cabo acciones en masa para mejorar la eficiencia del trabajo del equipo. (Atlassian, s.f.)

Jira Query Language (JQL): El Lenguaje de Consulta de Jira (JQL) representa un lenguaje estructurado diseñado para construir consultas destinadas a buscar problemas dentro

de Jira Software. Este lenguaje brinda a los usuarios la capacidad de especificar criterios detallados para la búsqueda de problemas, basados en campos específicos, operadores y otros elementos relevantes. Esta funcionalidad posibilita la realización de búsquedas avanzadas y la obtención de información específica sobre los problemas dentro de un proyecto. JQL se caracteriza por ofrecer una sintaxis similar a SQL y proporcionar funciones como autocompletado, asistencia de sintaxis y sugerencias contextuales, lo que simplifica el proceso de construcción de consultas. Gracias a JQL, los usuarios tienen la capacidad de localizar problemas en función de diversos criterios, tales como el contenido textual de un campo, la fecha de creación o el estado del problema, entre otros. (Atlassian, s.f.)

Smart Values: En Jira, un "Smart Value" se define como un marcador de posición que posibilita la extracción de datos dinámicos y la manipulación de información vinculada a los problemas dentro de la plataforma. Estos valores inteligentes resultan fundamentales para la automatización y personalización de los flujos de trabajo, ya que permiten acceder a datos específicos de los problemas, lo que contribuye a mejorar la eficiencia y precisión en la gestión de proyectos. (Atlassian, s.f.)

Sandbox: es un espacio aislado donde los usuarios pueden realizar pruebas y experimentar con los productos de Atlassian antes de implementar cambios en el entorno de producción. Este entorno de pruebas replica el entorno de producción del producto seleccionado. Además de probar nuevas características, los entornos de pruebas pueden utilizarse para integrar y capacitar a nuevos usuarios, así como para evaluar nuevas aplicaciones, todo ello sin impactar en el entorno de producción. (Atlassian, s.f.)

3.2. Teorías y Metodologías de apoyo al tema

3.2.1. Metodología de investigación

Este estudio propone un enfoque completo para abordar las deficiencias identificadas en los accesos de la empresa WherEX o CCS SpA, con el fin de mejorar la eficiencia y efectividad de los procesos relacionados con el control de acceso normativo. El proyecto comprende una investigación exhaustiva y la implementación de soluciones diseñadas para optimizar el acceso de los colaboradores a varios sistemas, así como para gestionar la identificación de usuarios en la plataforma. Esto implica un análisis detallado de diversas áreas y tecnologías que intervienen en los sistemas de acceso.

Para llevar a cabo el estudio e implementación mencionados anteriormente, se identificaron cinco etapas clave que abarcan la totalidad del proyecto. Estos procesos son fundamentales para el éxito de la iniciativa y se estructuraron de la siguiente manera:

1. Etapa I: Planificación y estudio de plataforma a utilizar.

Esta fase implica identificar la plataforma principal para ejecutar el proyecto, que en este caso se ha seleccionado a Jira Atlassian. Se lleva a cabo un estudio exhaustivo de la estructura de la plataforma, sus características, el lenguaje utilizado y las posibles mejoras según la metodología Kanban. Además, se evalúa la idoneidad de la plataforma para los objetivos del proyecto, su viabilidad y capacidad para cumplir con los requisitos normativos correspondientes.

2. Etapa II: Análisis de los procesos de On Boarding, gestión de cuentas y Off Boarding de la empresa WherEX.

Para abordar esta etapa, se lleva a cabo un estudio colaborativo que involucra a varias

áreas, incluyendo People y Finance, con un enfoque particular en las subáreas de Process & Compliance y Human Resources Operations. Esta colaboración es esencial para comprender los detalles clave de los puntos de inicio de cada proceso, como el ingreso de nuevos colaboradores, la gestión de sus accesos y plataformas, así como el proceso de desvinculación y recuperación de sus accesos y equipos.

3. Etapa III: Levantamiento de sistemas de la organización.

Esta etapa es crucial y constituye la parte más amplia del proceso, ya que implica investigar todas las plataformas utilizadas por la organización y determinar qué colaboradores tienen acceso a estas. Para lograrlo, se llevó a cabo un exhaustivo relevamiento de todas las licencias y plataformas de la empresa, identificando a los administradores correspondientes de cada sistema. Este enfoque simplifica la recopilación de información sobre los usuarios al establecer contacto con cada administrador, lo que facilita la creación de una base de datos completa de los usuarios asociados a cada plataforma.

4. Etapa IV: Integración del sistema gestión e identidad de accesos.

En esta fase, se lleva a cabo la gestión de la creación del sistema y se establece su estructura básica para su funcionamiento. Se examina cómo está organizado el sistema y cómo se conecta con los diversos procesos, considerando su relación con otros proyectos en Jira asociados al ingreso de personal, las solicitudes desde un portal interno y el proceso de desvinculación de colaboradores. Además, se define la gestión y ejecución del proceso de salida de colaboradores desvinculados, incluyendo la revocación de sus credenciales y la recuperación de activos.

Durante esta etapa, también se desarrolla la visualización del proyecto, lo que incluye

cómo se presentan las incidencias, ya sea de la vista de las fichas de colaboradores, la organización de los tipos de accesos y los diferentes estados que distinguen cada una de las “issues”, tanto para colaboradores como para sistemas.

5. Etapa V: Resultados y mejoras.

Como fase final del proceso, el proyecto se encuentra completamente implementado en la organización, ejecutando de manera efectiva todo el flujo definido para la entrada y salida de colaboradores, así como para la solicitud de sus accesos a diferentes plataformas. Se examinan formas de mejorar y simplificar las responsabilidades de los Sysadmins encargados de gestionar y revisar el proyecto, lo cual es posible mediante automatizaciones configurables dentro de Jira. Esto abre diversas posibilidades de mejora dentro de la plataforma, con el propósito de reducir la carga laboral, alcanzar una independencia del proyecto en relación con el contacto humano e implementar la automatización de otros procesos asociados, utilizando la metodología PDCA. De esta manera, se evidencia la eficacia y eficiencia del sistema para controlar los accesos de los usuarios y monitorear los diversos sistemas de la organización.

Por otro lado, como se mencionó anteriormente en la primera y última etapa, existen 2 tipo de metodologías que beneficiaran constructivamente la implementación del proyecto; ya sea de forma de mejoras, automatizaciones o inclusión de otros procesos que estén relacionados con los flujos mencionados de ingreso y salida de colaboradores. Estas metodologías son:

3.2.2. Metodología KANBAN

Kanban es un método ágil enfocado en crear un sistema de producción efectivo y eficiente mediante la logística. Introducido originalmente por Toyota para controlar el avance del trabajo en su línea de producción, consiste en usar tarjetas visuales para señalar los pasos

en el proceso de fabricación. Este método enfatiza el flujo y la mejora continua del trabajo, limitando el número de ítems que pueden estar en proceso al mismo tiempo (Work in progress) para crear un flujo de trabajo visible que permita gestionar la calidad y entregar de forma continua. (Gatica Herrera, 2015)

La implementación de Kanban en el área de sistemas de proyectos de una empresa de IT incluyó definir actividades de trabajo, clases de servicio, limitar el WIP (Work in progress) y usar la herramienta JIRA para visualizar el trabajo. Los beneficios de esta implementación incluyen la reducción de tiempos de respuesta, la mejora de la comunicación, la mejor priorización de las tareas y el aumento de la visibilidad del trabajo para el equipo y los clientes.

Es fundamental el informe de Gatica, ya que menciona muchos atributos para la incorporación de un nuevo sistema dentro de una empresa que gestiona procesos mediante tickets de incidencias; donde a su vez, existe una opción de mejora continua. A pesar de que su finalidad es distinta, tienen similitud en la plataforma y el método de trabajo utilizado.

3.2.3. Metodología PDCA

Como se mencionó anteriormente, existe la posibilidad de incorporar nuevos procesos o flujos de trabajo al proyecto. Estos son objeto de análisis y metodología constante dentro del ámbito de Process & Compliance, donde se destaca la relevancia de la metodología PDCA, también conocida como el ciclo de Deming. El PDCA, que se desglosa en Plan (Planificar), Do (Hacer), Check (Verificar) y Act (Actuar), se convierte en una fase fundamental para la integración de otros procesos, ya que está diseñado para resolver problemas y mejorar continuamente los flujos, productos o servicios presentes en la empresa (Guerra Gutarra, 2020).

En la fase de Planificar (Plan), se investigarán y analizarán las problemáticas asociadas a otras líneas de trabajo, con el fin de recopilar información suficiente para comprender el contexto y las causas del problema de manera precisa. De acuerdo con Holguín, en su informe titulado "Metodología PDCA y su incidencia en la gestión de proyectos de la empresa Proemco S.A.C.", se mencionan cuatro indicadores para llevar a cabo esta fase: "Identificar Objetivos", "Priorizar Problemas" y "Analizar Causas" (Holguin Sánchez, 2021). Basándose en estos puntos, se podrán proponer diversas soluciones y elaborar un plan de acción que aborde el inconveniente inicial de manera efectiva.

Durante la etapa de Hacer (Do), se lleva a cabo la ejecución de la solución identificada, permitiendo realizar pruebas para validar el plan de acción propuesto en la fase anterior. Según Holguin, se destacan los siguientes indicadores para esta etapa: "Implementar acciones de mejora", "Supervisar la ejecución", "Medir los resultados" y "Verificar los resultados" (Holguin Sánchez, 2021).

En la fase de Verificación (Check), se realiza un análisis detallado de los resultados obtenidos para determinar su precisión y su correspondencia con los objetivos establecidos. Asimismo, se lleva a cabo una evaluación para verificar si los resultados alcanzaron el nivel de eficacia y eficiencia esperado. Una vez más, los indicadores propuestos por Holguin, como la "Retroalimentación de los profesionales" y el "Análisis de resultados", desempeñan un papel fundamental en esta etapa para obtener una evaluación completa y precisa (Holguin Sánchez, 2021).

Finalmente, en la fase de Actuar (Act), se lleva a cabo el registro y la estandarización del procedimiento utilizado para implementar la solución, lo que permite preservar los resultados en cuanto a efectividad y eficiencia. Holguin concluye con los indicadores de

"Detectar errores", "Documentar el proceso" y "Acciones de mejora de desempeño" (Holguin Sánchez, 2021). Posteriormente, se reinicia el ciclo para comparar los diferentes conjuntos de resultados obtenidos, lo que facilita el establecimiento de nuevos objetivos y la adecuación del flujo de trabajo hasta alcanzar el resultado deseado (Guerra Gutarra, 2020).

4. Capítulo IV: Propuesta de Metodología a Utilizar

4.1. Propuesta o Método teórico a utilizar

4.1.1. Etapa I: Planificación y estudio de plataforma a utilizar.

1. Búsqueda de soluciones

En el caso estudiado, se definió que la solución más factible es la creación de un sistema de gestión de identidad y accesos (IAM), en el cual, se estimó conveniente que existen diversas plataformas que ofrecen este servicio. Para ello, se investigaron opciones que pudieran cumplir con los requisitos que requería la empresa, entre ellas se encontraron las plataformas ya mencionadas anteriormente, pero que incurren en un gasto bastante alto para la empresa, también viendo los requisitos que requería el sistema, era bastante complejo encontrar algún sistema que pudiera abarcar el problema.

Luego de descartar las opciones de contratación de plataformas, se buscó otra solución, más aceptable y moldeable a lo que se buscaba el cual era la opción de crear un programa utilizando Visual Studio con formato HTML; no obstante, surgieron inquietudes en relación con el mantenimiento, el diseño y la seguridad de la plataforma propuesta.

2. Proyecto viable dentro de Jira y solución específica:

Simultáneamente, se estaba llevando a cabo una migración de datos desde otra plataforma hacia el espacio de Jira Software Management, en un proyecto denominado “Inventarios”. Este espacio, respaldado y gestionado por Atlassian, ofrece funcionalidades para la gestión integral de activos, incluyendo la identificación, personas asociadas, fechas de compra y mantenimiento, así como su disponibilidad. Destaca la capacidad de automatización de procesos, alineada con la categorización de incidentes por tipo y estado.

A partir de esta opción generada desde la subárea de Sysadmin, se inició una discusión con la responsable de Ingeniería de Automatización para abordar el monitoreo de sistemas dentro de la plataforma Jira y los requisitos necesarios para desarrollar el proyecto. Se organizaron reuniones con el equipo de Ingeniería para profundizar en aspectos clave como el lenguaje utilizado, las extensiones disponibles y el funcionamiento general de Jira. Tras estos intercambios, se determinó que era viable implementar el monitoreo y registro de sistemas dentro de la plataforma, aprovechando sus capacidades para ejecutar diversos procesos similares a un Sistema de Gestión de Identidad y Acceso (IAM).

3. Plataforma Jira y funciones:

Luego de ver la viabilidad del proyecto dentro Atlassian, se destinó a investigar y estudiar el funcionamiento del sistema, se llevó a cabo una inducción detallada con un Automation Engineer, con el objetivo de familiarizarse con la plataforma (**Figura 5.1.1.4.1**). Este proceso fue crucial para comprender la naturaleza de la plataforma, sus características principales y el lenguaje utilizado. Se destacó que Jira presenta una dinámica variada en varios aspectos, particularmente en el uso del lenguaje de la Jira Query Language (JQL por sus siglas en inglés), así como en la comprensión de los Smart Values. Estos últimos constituyen un lenguaje especializado para hacer referencia a los distintos componentes que componen las incidencias o Issues dentro del sistema.

Por otro lado, la capacidad de autogestión y autoaprendizaje se revelaron como habilidades fundamentales para adquirir un conocimiento profundo de todos los comandos, definiciones, lenguajes y estructuras relacionadas con Jira. Este aprendizaje se llevó a cabo mediante la consulta de libros que proporcionaban un manual de uso detallado de la plataforma. A través de esta fuente de información, se comprendió el propósito específico

requerido para cada proyecto, así como el procedimiento para comprender el comportamiento de las incidencias y, finalmente, organizarlas utilizando el método de panel Kanban. (Li, 2018)

Además, la plataforma en sí cuenta con una sección de soporte que alberga una base de datos documental detallada sobre su uso (Atlassian, s.f.). Esta base de datos proporciona información sobre cada proyecto y su propósito específico, así como herramientas para la visualización de proyectos, búsqueda de incidencias y exposición de los lenguajes utilizados, como JQL y Smart Values. Esta documentación es fundamental para la realización de mejoras en los proyectos y la implementación de automatizaciones que faciliten la autogestión del proyecto sin requerir interacciones del personal.

4.1.2. Etapa II: Análisis de los procesos de On Boarding, gestión de cuentas y Off Boarding de la empresa WherEX.

En esta fase, se compartió con los distintos equipos de wherEX los flujos de empleados, tanto de la integración como de la desvinculación de los colaboradores. Este proceso se llevó a cabo en conjunto con los equipos de People y Finance, que, a través de reuniones periódicas, se elaboró el flujo detallado de cada aspecto del proceso. En este sentido, se pueden describir los procedimientos previos a la implementación del nuevo sistema IAM era de la siguiente manera:

1. Flujo On Boarding:

El proceso de integración de un nuevo colaborador se inicia con la solicitud realizada por un líder a través del portal de TA Plan (**Figura 3.1.7.2.1**), donde se especifica si se trata de la búsqueda de un cargo específico o de un practicante. Una vez recibida la solicitud, se genera una incidencia en el proyecto de Jira de People, detallando el cargo solicitado, el líder responsable, el área y el motivo de la solicitud.

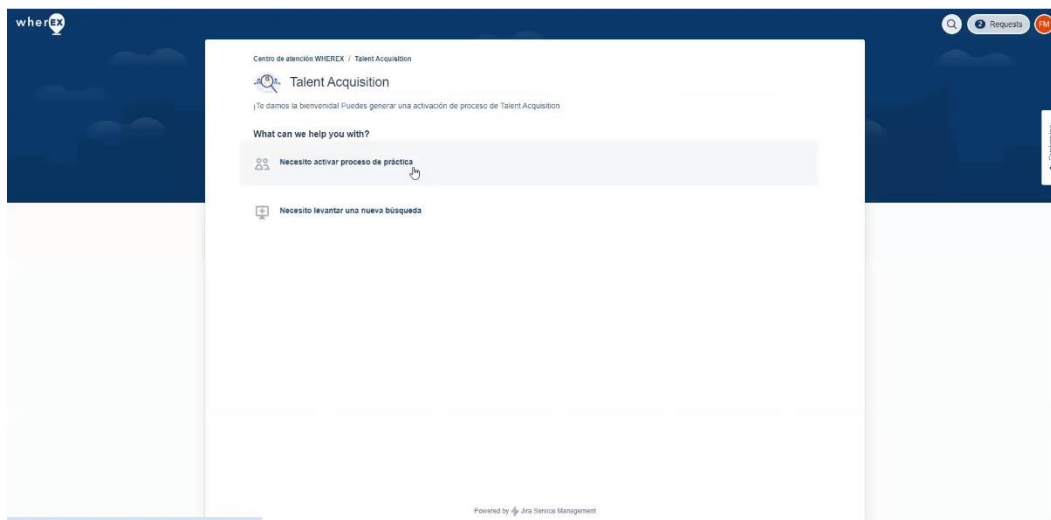


Figura 3.1.7.2.1 Vista de portal de TA Plan

Fuente: Espacio de trabajo en Jira.

Figura 3.1.7.2.2 Vista de solicitud de proceso de práctica

Fuente: Espacio de trabajo en Jira.

Centro de atención WHEREX / Talent Acquisition

Talent Acquisition

¡Te damos la bienvenida! Puedes generar una activación de proceso de Talent Acquisition

What can we help you with?

Raise this request on behalf of *

! Aquellas búsquedas no planificadas en el TA Plan deben pasar por un proceso de aprobación previo. A continuación te pediremos que completes la información correspondiente al cargo, la cual necesitaremos para llevar a cabo esta validación.

¿Cuál es la necesidad de la búsqueda que se está solicitando?

☐ Nuevo HC

☐ Reemplazo de cargo existente

☐ Reemplazo temporal de cargo existente (licencia médicas . permisos excepcional)

¿Se trata de una búsqueda confidencial? *

☐ No

☐ Si

Send Cancel

Powered by Jira Service Management

Figura 3.1.7.2.3 Vista solicitud de búsqueda de colaborador

Fuente: Espacio de trabajo en Jira.

En el caso de una nueva vacante, se organiza una reunión con el líder para discutir la remuneración líquida prevista para la contratación. Posteriormente, la gerente de finanzas analiza la solicitud y decide sobre la viabilidad de la contratación. Si se aprueba, se solicita la validación al equipo de People para iniciar la búsqueda del candidato adecuado.

Una vez seleccionada la persona, se envía un formulario de Google Forms para recopilar sus datos personales y cualquier información adicional que desee compartir con el equipo. A partir de este formulario, se inician los preparativos para su ingreso, notificando al equipo de Wherex a través de Slack mediante la plataforma de Zapier (**Figura 3.1.7.2.4**).

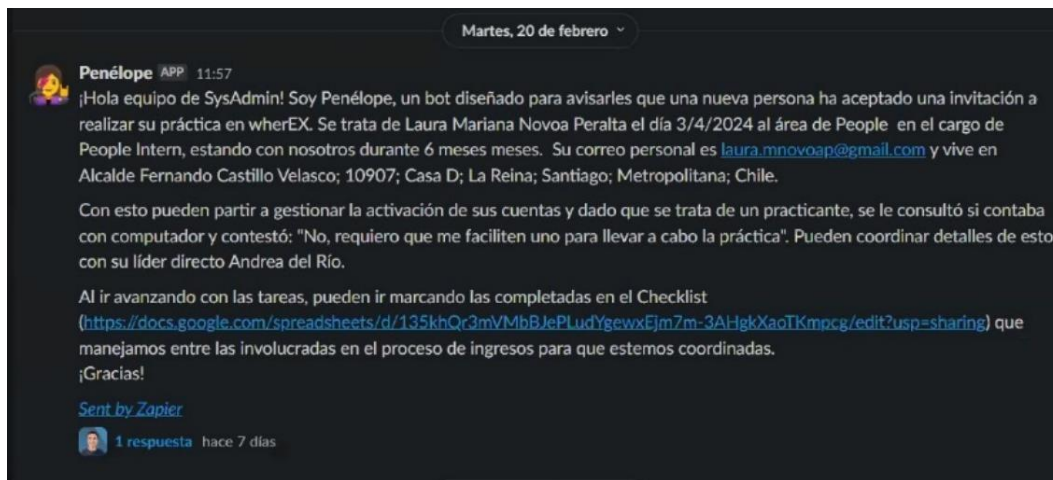


Figura 3.1.7.2.4 Mensaje de Penélope automatización de Zapier

Fuente: Espacio de trabajo en Slack.

Se coordina con el equipo de Sysadmin para asignar los activos necesarios, como un ordenador portátil, teléfono y tarjeta, así como cualquier otro equipo solicitado por el líder, como un monitor. Además, se generan las credenciales necesarias para el acceso a Gmail, Slack, Atlassian y Microsoft 365. Todo el proceso se documenta y se sigue a través de una lista de verificación en Excel.

El día de ingreso del nuevo colaborador, la encargada de Human Resources Operations (HR-Ops) gestiona la firma de los documentos pertinentes, como las actas de entrega de equipos y el acuerdo de confidencialidad (NDA). Una vez completado este proceso, el nuevo colaborador finaliza su proceso de Onboarding (**Figura 3.1.7.2.5**).

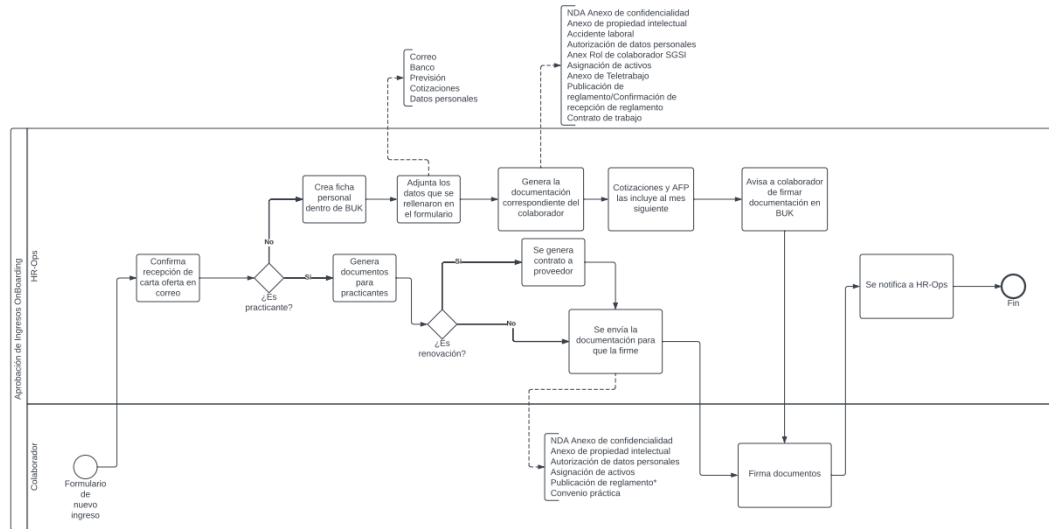


Figura 3.1.7.2.5 Proceso On Boarding desde HR-Ops

Fuente: Elaboración Propia, en base a datos otorgados por WherEX.

En caso de que se requieran cuentas adicionales en otros sistemas, el líder debe solicitarlas a través de Internal Support (USS).

2. Flujo de Off Boarding:

Para los casos de salida de colaboradores, se distinguen tres tipos: desvinculación urgente, renuncia voluntaria y término de contrato (aplicable tanto a colaboradores como a practicantes). En el caso de desvinculación urgente, se notifica a la persona el mismo día de la decisión y, una vez desvinculada, el Sysadmin procede a dar de baja todos sus accesos y eliminar sus credenciales de las cuentas generales, además de solicitar la devolución de los activos asignados. En el caso de renuncia voluntaria o término de contrato, se comunica con anticipación al colaborador, y el día de su salida, el Sysadmin realiza los mismos procedimientos de baja y el colaborador entrega los activos en la oficina para su recepción. Es importante mencionar que, en casos de desvinculación y situaciones particulares, se acompaña al excolaborador a la notaría para formalizar el finiquito.

3. Fallas en los flujos:

Es importante destacar que, dentro del análisis realizado, se identificaron algunas inconsistencias en estos flujos, las cuales pueden haber afectado a la organización o representar un riesgo directo para la misma. Entre estas irregularidades, se encuentran las siguientes:

- a. **Falla en “aviso de nuevo ingreso” a equipo de Sysadmin:** Se llevó a cabo un análisis exhaustivo de este error recurrente que consistía en notificar el ingreso del colaborador el mismo día, lo cual impedía al equipo de Sysadmin gestionar adecuadamente los equipos y las credenciales con antelación para que el nuevo miembro pudiera comenzar sus labores a tiempo. Esta situación generaba incomodidades en el equipo, dado que se veían obligados a cumplir estas responsabilidades de manera apresurada y sin la preparación adecuada para recibir al nuevo integrante. Además, se requerían modificaciones en los equipos asignados, tales como configuraciones pertinentes y actualizaciones necesarias para que el colaborador pudiera llevar a cabo sus tareas mediante otros sistemas que exigían un equipo de alta gama. Asimismo, esta situación resultaba en que los nuevos ingresos no contaran con tarjetas de acceso para ingresar a la oficina, lo que ocasionaba una dependencia constante de sus colegas para acceder al lugar de trabajo.
- b. **Activación de cuentas a sistemas no autorizados ni notificados al equipo de Sysadmin:** otro error recurrente era la falta de notificación al responsable sobre los accesos que tenían los colaboradores, lo que resultaba

en una pérdida de control sobre la información a la que tenían acceso los usuarios. Esta falta de comunicación también generaba inseguridad para el equipo de SGSI al desconocer el tratamiento de los activos de información. También implicaban costos adicionales por licencias, lo que requería alertar al equipo de Accounting para gestionar los pagos correspondientes y emitir la tarjeta para realizar el abono del dinero de manera efectiva.

- c. **Monitoreo de Sistemas por medios de Google Sheets:** El equipo responsable de la gestión de los sistemas realizaba manualmente todos los movimientos relacionados, tanto la incorporación de nuevos usuarios como la eliminación de cuentas, utilizando Google Sheets. En este documento, ingresaban manualmente las credenciales y los sistemas activos. Sin embargo, si surgía algún problema y el equipo de Sysadmin no actualizaba este documento, no se disponía de información actualizada sobre los usuarios por sistema.
- d. **No avisar sobre la salida del colaborador:** Este error, que constituyó el principal motivo del descubrimiento del problema, se relacionaba con la falta de notificación al equipo de Sysadmin cuando una persona era desvinculada. Esta omisión resultaba en la falta de desactivación de sus cuentas y la ausencia de restricciones correspondientes para evitar el acceso a archivos que pudieran contener información sensible. Además, ocasionaba que las cuentas permanecieran habilitadas en varios sistemas hasta que se realizara una revisión exhaustiva por cada uno de ellos, sin que se procediera a su desactivación. Esta situación representaba una brecha de

seguridad frente a posibles ataques cibernéticos que podrían acceder a estas cuentas para sustraer la información contenida en ellas.

- e. **Cuentas de usuarios desvinculados con proyectos asociados:** En algunas instancias, se evidenció la activación de cuentas pertenecientes a individuos que ya no formaban parte de la empresa. Esta situación surgía debido a la práctica incorrecta de asociar todos los proyectos o procesos a las cuentas personales, lo que dificultaba su traspaso o desactivación. Este escenario generaba una nueva brecha de seguridad, ya que la información confidencial y sensible relacionada con el modelo de negocio de la organización quedaba desprotegida debido a la falta de monitoreo constante de estas cuentas inactivas.

4.1.3. Etapa III: Levantamiento de sistemas de la organización.

Luego de realizar el análisis a los procesos, se prosiguió con otro apartado de la etapa que tiene relevancia con cierta información sensible de la organización, lo que es el levantamiento de los sistemas de la empresa y los usuarios que estos tienen. Para este proceso, se destacaron 2 fases para llevar a cabo el levantamiento

1. **Registro de todos los sistemas de WherEX:** En este primer apartado, se estableció una base de datos principal que, como se mencionó anteriormente, presentaba una inconsistencia, ya que estaba alojada en Google Sheets. Este documento contenía, en su mayoría, todos los sistemas con licencias pagas que poseía la organización. En él se registraban detalles como la tarjeta utilizada para el pago, el nombre del sistema, el monto pagado, la moneda utilizada, el

administrador del sistema y su respaldo, el área de negocio que utilizaba la plataforma y la periodicidad de pago. La acción prioritaria fue contactar al equipo de Accounting para confirmar el monto de cada sistema y verificar la tarjeta utilizada, así como para añadir el URL que redirigía a la plataforma.

2. **Registro de usuarios por plataforma:** Una vez completado el registro de los sistemas y sus respectivas características, se procedió a completar la base de datos de los colaboradores de la empresa. Este proceso se inició mediante el contacto con el administrador de cada sistema previamente registrado. Los administradores proporcionaron archivos, ya sea en formato CSV o imágenes, que contenían la información de los usuarios almacenados en cada plataforma. Además, indicaron el perfil correspondiente de cada usuario, clasificándolos en dos tipos: perfiles de usuario con accesos limitados y perfiles de administradores.

Ambos tipos de registros fueron documentados en un archivo Excel con el fin de facilitar su conversión a un formato CSV-UTF8. Esta decisión se tomó con el propósito de permitir la importación de los datos en la plataforma Jira para la creación de incidencias de manera eficiente y precisa.

4.1.4. Etapa IV: Integración del sistema de gestión e identidad y acceso.

Ya teniendo los estudios necesarios y los requisitos correspondientes para la creación de proyectos en Jira, de manera simultánea al levantamiento, se procedió a crear el IAM dentro de Atlassian. Este proceso se realizó de manera efectiva a partir de 3 fases correspondientes que abarcaron todo el proyecto.

1. Fase I: Creación de proyecto mínimo viable posible (MVP) en espacio apartado (Sandbox):

Para avanzar con mayor precisión, se estableció un espacio designado como Sandbox, exclusivo para pruebas y accesible únicamente por las personas asignadas y el administrador. En este entorno se inició la creación de proyectos conforme a la propuesta de la memoria.

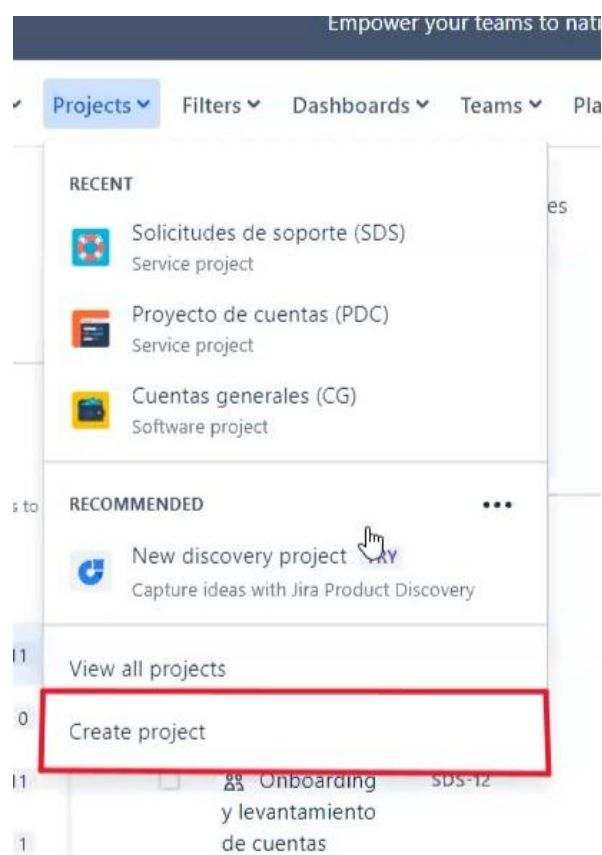


Figura 3.1.7.2.1 Opción de crear proyecto y proyectos creados

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

a. Configuración del sistema:

En primer lugar, se presentó el proyecto de Jira Services IT Project, conocido como Proyecto de Cuentas (PDC), destinado a gestionar incidencias y solicitudes desde un portal, con tres tipos de solicitudes: Onboarding, solicitud de cuentas y Offboarding, cada uno con su

respectivo formulario integrado en el espacio (**Figura 3.1.7.2.5**).

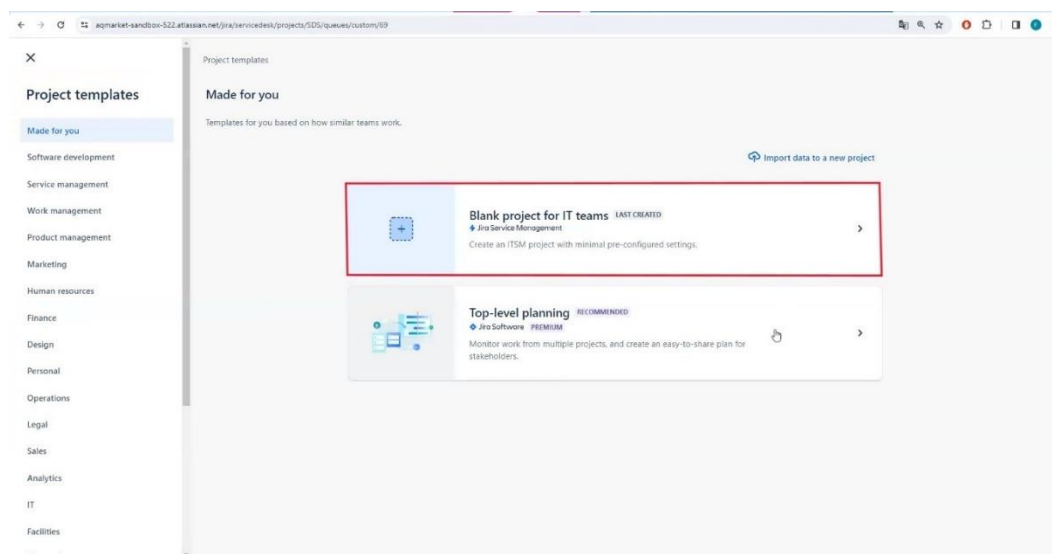


Figura 3.1.7.2.2 Creación de proyecto Jira Service Management

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

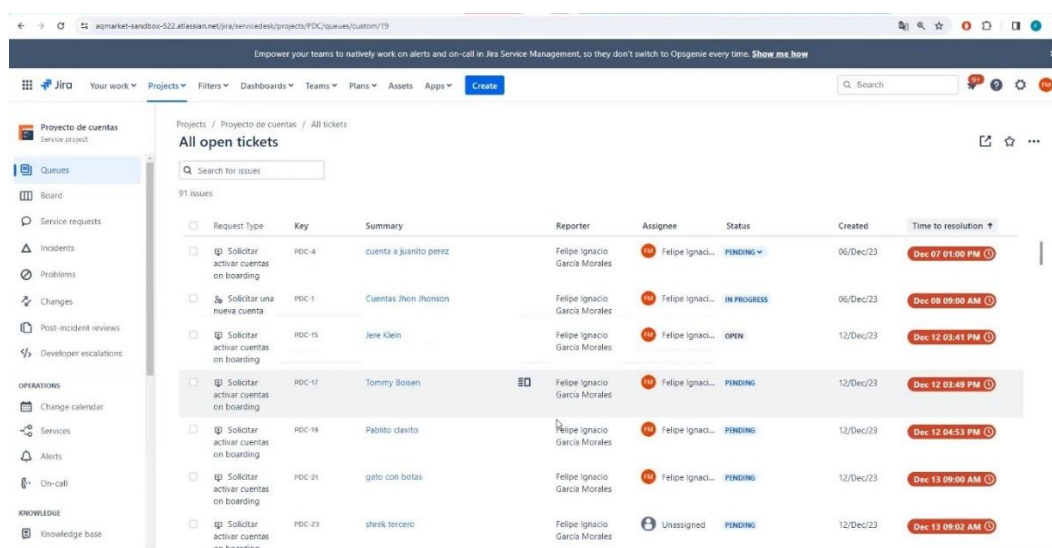


Figura 3.1.7.2.3 Vista de lista de incidencias Proyecto de cuentas (PDC)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

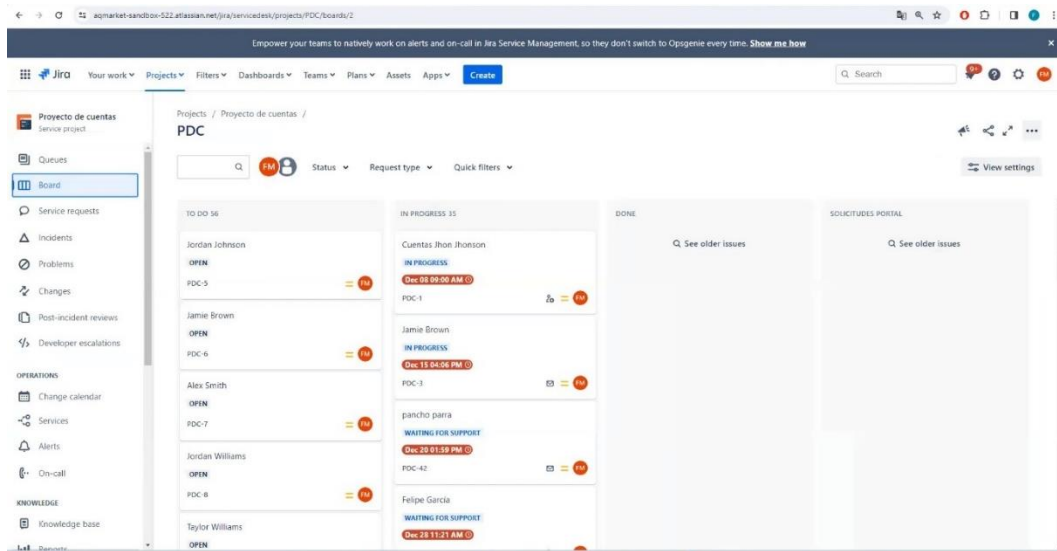


Figura 3.1.7.2.4 Vista PDC Tablero de incidencias

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

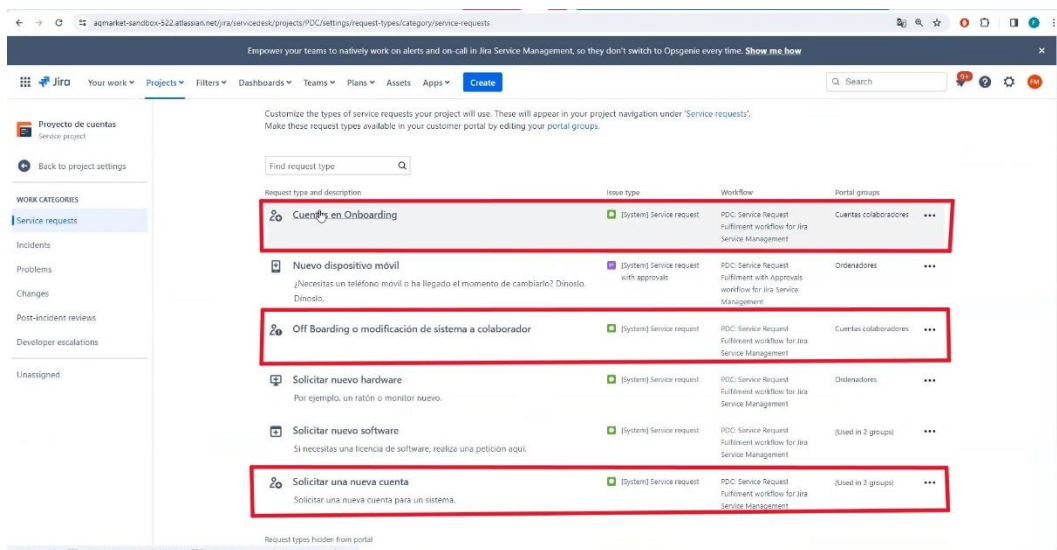


Figura 3.1.7.2.5 Vista de solicitudes dentro de "PDC"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

Por otra parte, se crearon Custom Fields, campos personalizados utilizados para completar las issues y guiar las automatizaciones posteriores. Aunque se lograron avances con el proyecto de Jira Services, se identificaron algunas limitaciones en sus funcionalidades, como la incapacidad de crear un resumen de incidencias en un tablero Kanban. Por lo tanto,

se creó un segundo proyecto denominado Jira Software Project, llamado Cuentas Generales (CG), que carecía de la opción de generar incidencias a partir de solicitudes, pero ofrecía una mejor gestión de incidencias y un resumen más claro del estado de las issues.

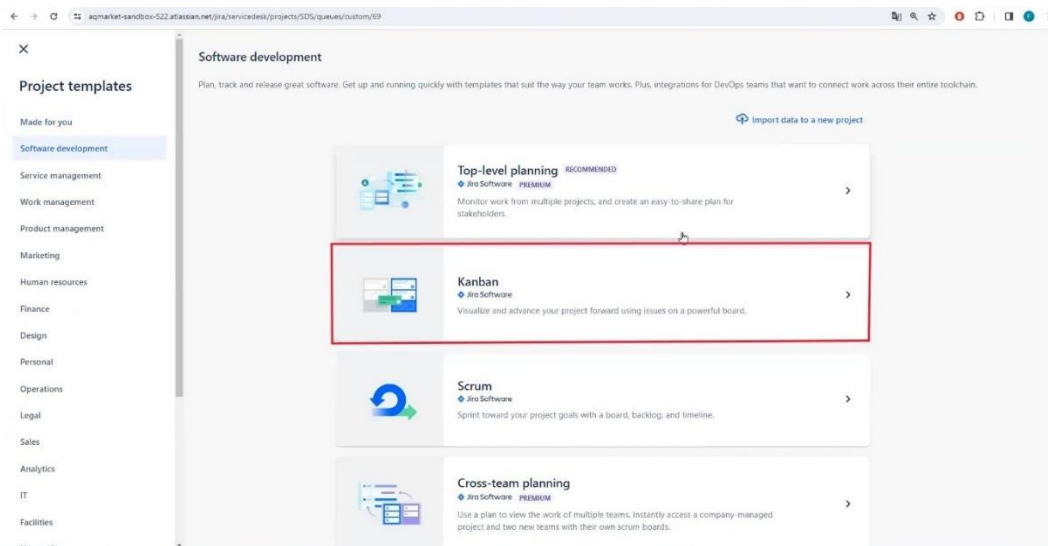


Figura 3.1.7.2.6 Creación Jira Software Project

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

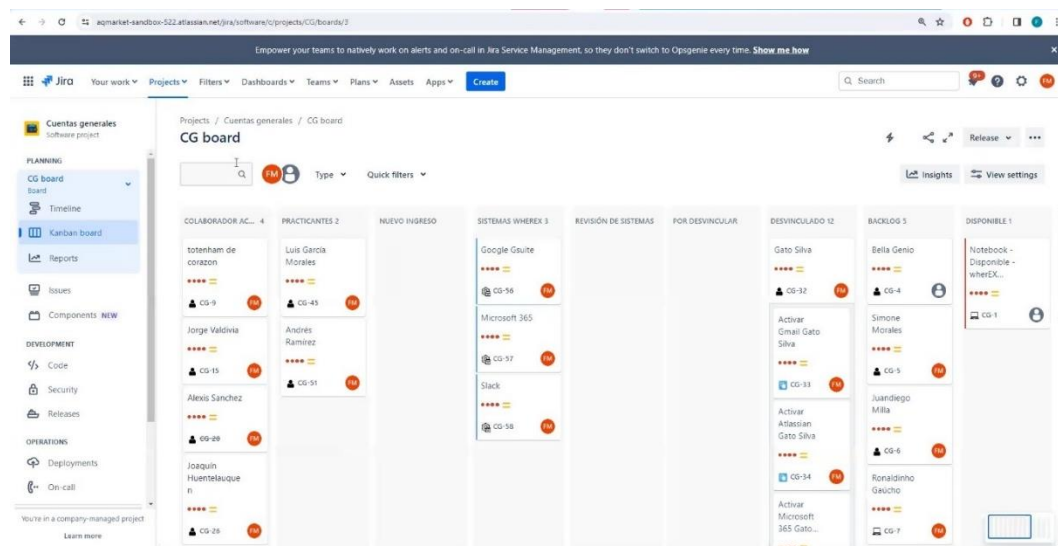


Figura 3.1.7.2.7 Vista tablero Kanban Cuentas Generales (CG)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

Para configurar este proyecto, se crearon Custom Fields relevantes, como campos de texto simple para información como "Gmail", "Bsale ID", "Microsoft 365" y "Ubicación", opciones de elección única para "Contrato", "Amazon Web Services", "Atlassian", "Slack" y "Área de negocio", y campos de fecha simple para "Fecha de ingreso" y "Fecha de Desvinculación". También se establecieron campos de asignación de usuarios como "Asignee", "Reporter", "Líder Directo" y "Nombre y apellido". Posteriormente, se definieron los IssueTypes, categorizando las incidencias en "Colaboradores" y "Sistemas", cada uno con sus propios Custom Fields, como se visualiza a continuación.

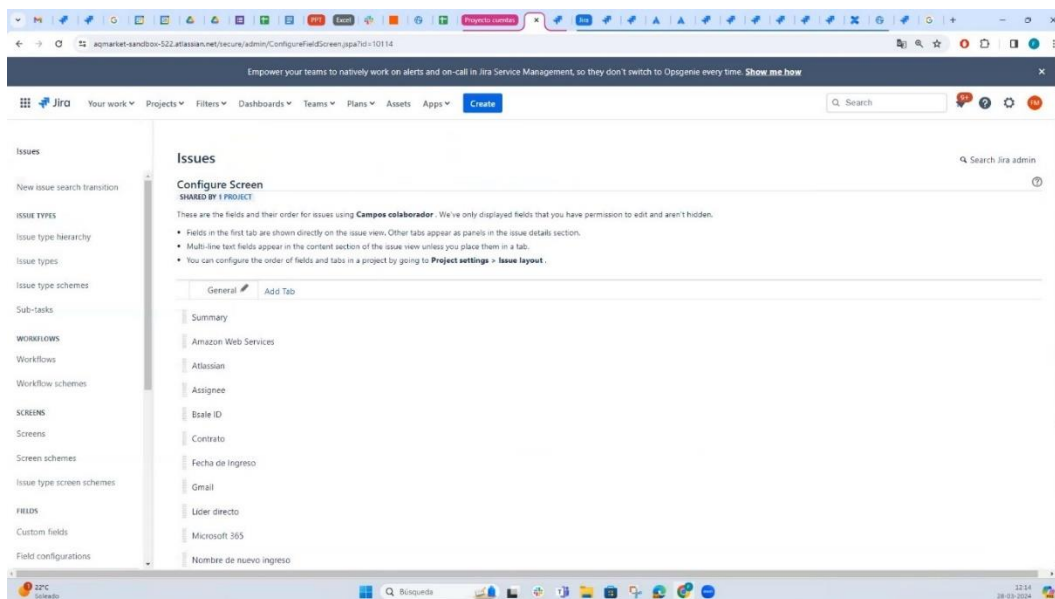


Figura 3.1.7.2.8 Vista de Screen y Custom Fields Colaborador "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

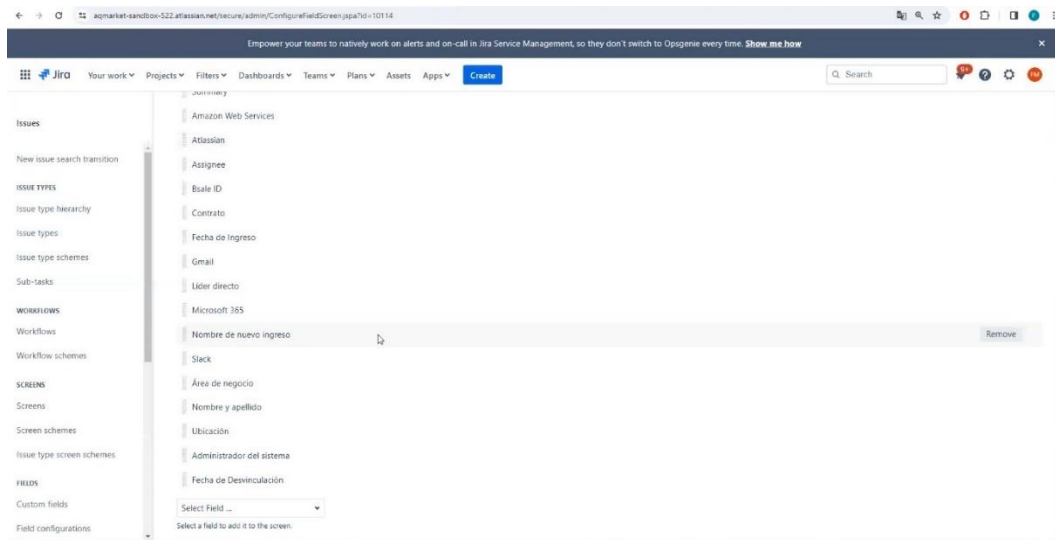


Figura 3.1.7.2.9 Continuación de Screen y Custom Fields Colaborador "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

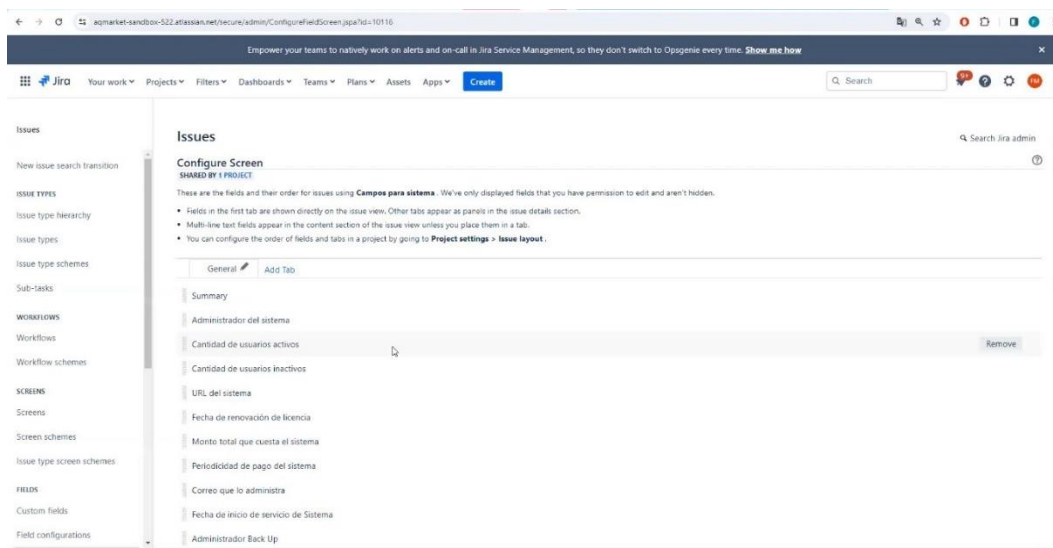


Figura 3.1.7.2.10 Screen y Custom Fields de Sistemas "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

Continuando con la configuración del sistema, se definió su funcionamiento como un registro y control de cuentas a través de las incidencias creadas, separadas según el tipo (colaborador o sistema) y distinguiendo entre colaboradores a contrato y practicantes. Los sistemas también tendrán su propio formato, con un Screen específico para cada uno, que

establece la estructura de las incidencias al momento de su creación. Para mantener la coherencia con el flujo de On Boarding, se creó un proyecto de Jira Software Management que refleja el proyecto de TA Plan, permitiendo así una gestión continua del proceso de On Boarding con las mismas condiciones y posibles mejoras dentro del proyecto.

Como el espacio Kanban se gestiona a partir de estados (o status), se realizaron diversas modificaciones como añadir los estados correspondientes al proyecto en su flujo denominado “Workflow”, las que se pueden ver a continuación.

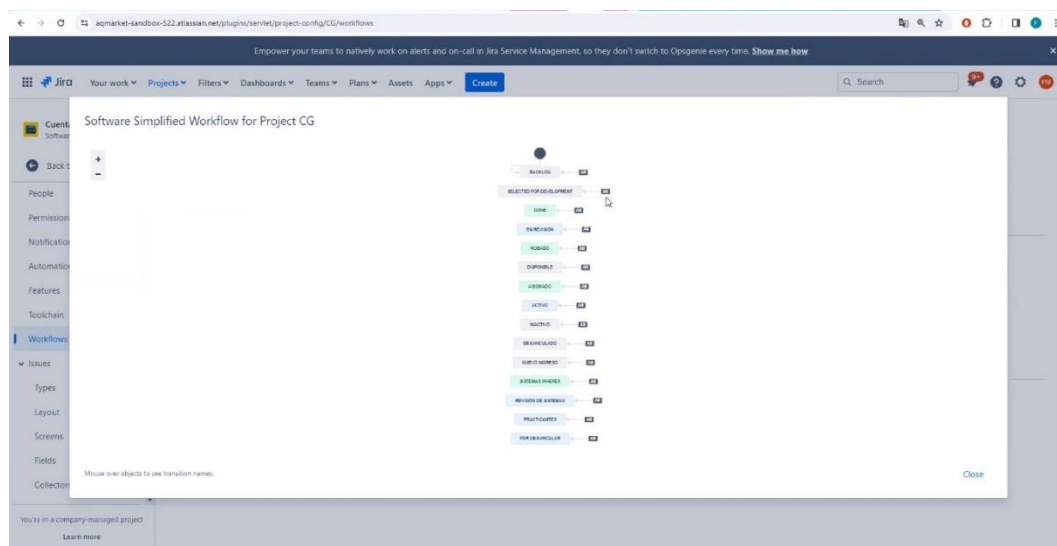


Figura 3.1.7.2.11 Workflow de "Cuentas Generales"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

b. Automatizaciones del proyecto:

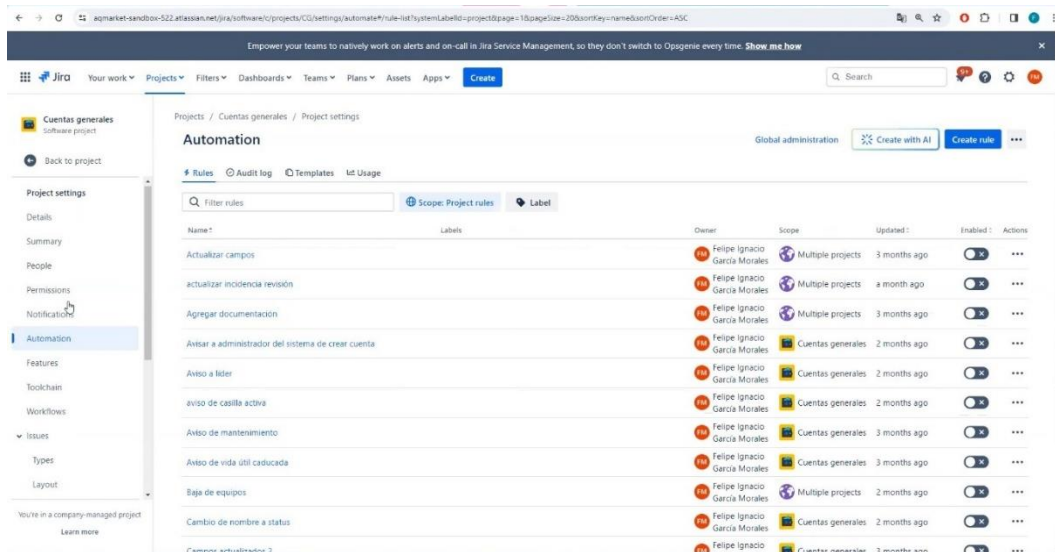


Figura 3.1.7.2.12 Vista 1 de automatizaciones de "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

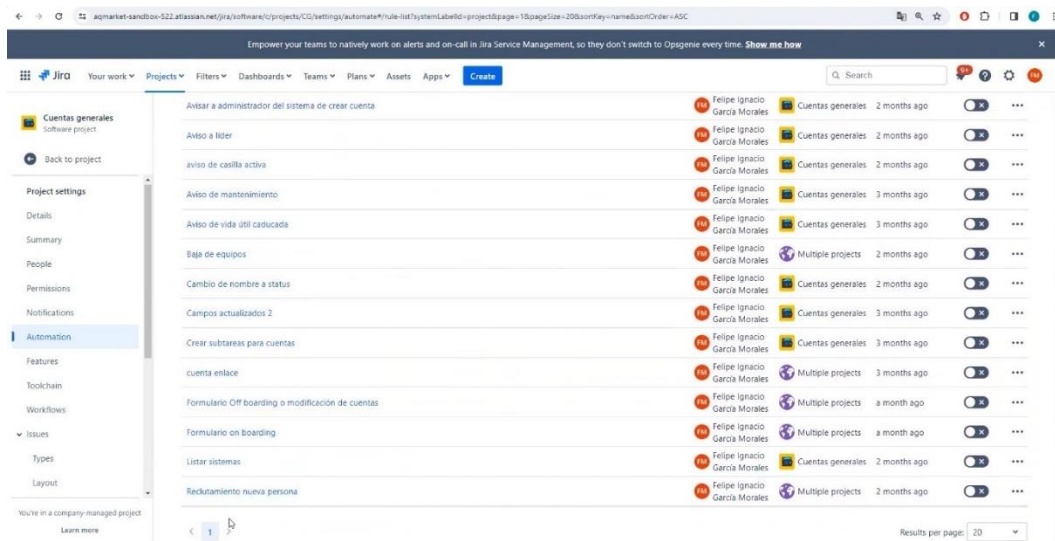


Figura 3.1.7.2.13 Vista 2 automatizaciones "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

- **Actualizar campos:** Se realizó una automatización de prueba para evaluar cómo un cambio de campo en una incidencia padre afecta a otras incidencias hijas, como las

subtareas.

- **Actualizar Incidencia Revisión:** Se llevó a cabo una prueba de automatización para la transición de estado cuando una incidencia de “Type Request” cambia a resuelta o cancelada.
- **Agregar documentación:** Se efectuó una prueba para enviar un mensaje a un grupo de Slack, notificando a la responsable de HR-Ops para adjuntar la documentación de la asignación de activos.
- **Avisar al administrador del sistema de crear cuenta:** Se realizó una prueba para notificar, vía correo, al administrador del sistema deseado cuando se levanta una solicitud de activación de cuenta, para que active la cuenta solicitada.
- **Aviso al Líder:** Se configuró un correo al líder del nuevo ingreso para que obtenga las credenciales y realice la solicitud de activar cuentas específicas.
- **Aviso de casilla activa:** Se implementó una prueba para asegurar que, al estar un usuario desvinculado, todas las casillas de los sistemas que tenía activas estén correctamente desactivadas.
- **Aviso de mantenimiento:** Se realizó una prueba para el proyecto de inventarios, donde se genera un aviso cuando un equipo alcance el fin de su vida útil o lleve un año sin mantenimiento preventivo.
- **Aviso de vida útil caducada:** Prueba para el proyecto de inventarios, donde se genera un aviso cuando un equipo alcanza el fin de su vida útil, indicando la necesidad de renovación.

- **Baja de equipos:** Se configuró una prueba de solicitud para que, al realizar una desvinculación, se genere un aviso al equipo de Sysadmin para listar y recuperar los activos que tenía en su poder la persona desvinculada.
- **Cambio de nombre a status:** Se implementó una automatización para cambiar el nombre del estado en ciertos casos específicos.
- **Crear subtareas para cuentas:** Se configuró una automatización para crear subtareas al momento de un nuevo ingreso, correspondientes a la activación de sistemas generales como Google Gsuite, Microsoft 365, Slack y Atlassian.
- **Cuenta enlace:** Se realizó una prueba para evaluar el comportamiento de conectar diferentes proyectos.
- **Formulario Off Boarding o modificación de cuentas:** Se configuró una prueba de solicitud para generar un aviso al equipo de Sysadmin al realizar una desvinculación, para desactivar todos los accesos a los sistemas de la persona desvinculada.
- **Formulario On Boarding:** Se estableció una solicitud para activar cuentas específicas al realizar un nuevo ingreso.
- **Listar sistemas:** Se implementó una automatización para listar los sistemas activos.
- **Reclutamiento de nueva persona:** Se realizó una conexión con un proyecto denominado “Solicitudes de Soporte” (SDS) para crear una incidencia en CG al ingresar el nombre de la persona seleccionada, además de alertar al equipo de Sysadmin sobre su fecha de ingreso y activación de credenciales.

c. Flujos de procesos:

i. Flujo Onboarding:

Para iniciar el proceso de Onboarding, se levanta una solicitud dentro de "Solicitudes de Soporte" (SDS) para un nuevo ingreso, incluyendo información como el líder solicitante, área, tipo de puesto, tipo de contrato y país solicitante, junto con los equipos requeridos. Una vez seleccionada la persona, se completan ciertos Custom Fields como "Fecha de ingreso" y "Fecha de desvinculación" en formato de fecha simple, y el "Nombre de la persona seleccionada". Automáticamente, se crea una incidencia en el proyecto "Cuentas Generales" copiando estos campos, con el tipo "Colaborador". Además, se envía una notificación vía Slack al equipo de Sysadmin para informar sobre la próxima incorporación. El equipo de Sysadmin gestiona internamente las credenciales de las cuentas principales, marcando los campos de Google Gsuite, Microsoft 365, Slack y Atlassian según corresponda. Cuando la incidencia se mueve al estado "Colaborador Activo" o "Practicante" (*Figura 3.1.7.2.14*), se envía un mensaje al líder con las credenciales asignadas y el enlace al portal de "Proyecto de Cuentas" (PDC) para solicitar activar cuentas en otras plataformas si es necesario.

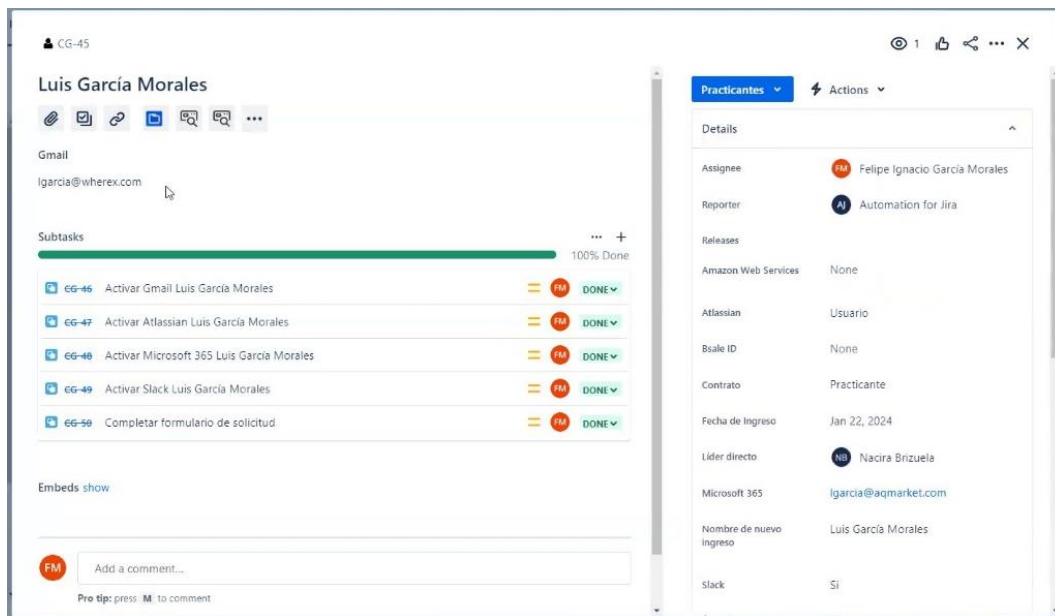


Figura 3.1.7.2.14 Vista de Issue Colaborador en "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

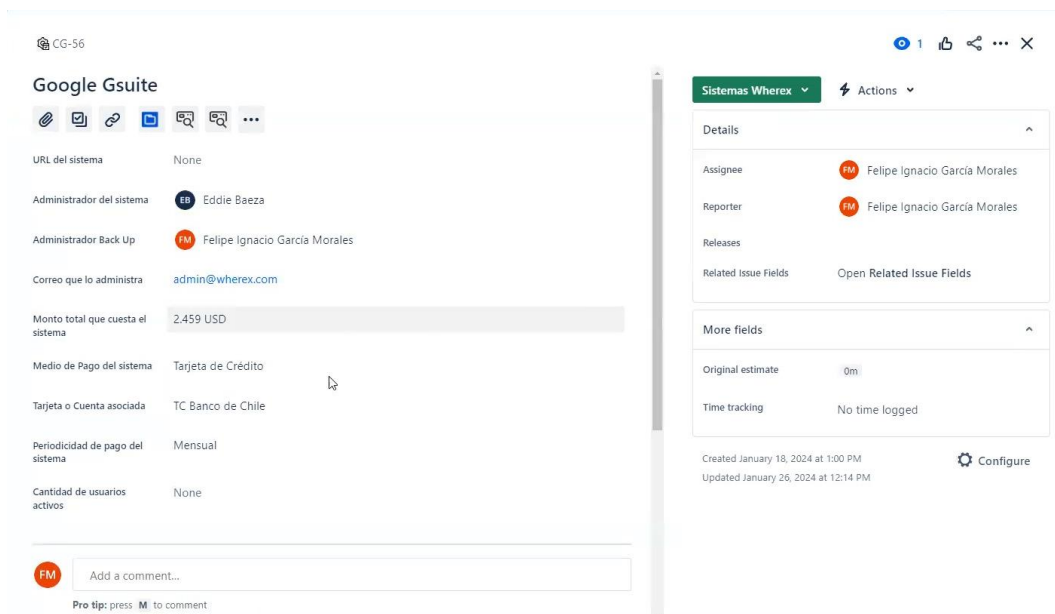


Figura 3.1.7.2.15 Vista de Issue Sistema en "CG"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

ii. Flujo de gestión de nuevas cuentas en plataformas:

Si se recibe una solicitud de activación de nuevas cuentas dentro de "PDC" (Solicitud

de gestión de cuentas), esta se anexa automáticamente a la incidencia correspondiente en "CG", que pasa al estado "Revisión de sistemas". Se notifica al equipo de Sysadmin a través de Slack para que atienda la solicitud. Cada vez que se solicite una nueva cuenta, se debe realizar la solicitud en el portal correspondiente y los encargados activan la cuenta, marcando la casilla del sistema correspondiente como "Activado Usuario".

iii. Flujo de Off Boarding:

Para el proceso de Offboarding, se levanta un ticket denominado "Formulario Offboarding" con los datos de la persona desvinculada y la fecha y hora exacta de la desvinculación. Esta solicitud alerta al equipo a través de una notificación en Slack y se añade la fecha de desvinculación a la incidencia de la persona en "CG", vinculando el ticket subido. El equipo de Sysadmin espera hasta la fecha de desvinculación y, una vez cumplida, se notifica nuevamente en Slack para proceder con la baja correspondiente. Se desactivan las casillas correspondientes y se añade "Suspendido" o "Eliminado" en los correos según sea necesario. Finalmente, cuando todas las casillas están desactivadas, la incidencia pasa al estado "Desvinculado", finalizando el flujo.

1. Fase II: Efectividad de MVP a partir de datos de pruebas:

Para el buen funcionamiento del proyecto se realizaron ciertos ajustes que gestionaban todo el proceso, entre ellos se pueden explicitar las siguientes características.

a. Creación de un canal para alertas de mensajes y repositorio de Bots.

En el contexto de las automatizaciones implementadas, se han incorporado diversas alertas mediante “Bots” generados en formato Webhook (**Figura 3.1.7.2.16**). Esta configuración se puede administrar mediante las propias automatizaciones en Jira. Al

seleccionar la opción de enviar mensajes a Slack, los usuarios son dirigidos al apartado de conexión con esta plataforma, donde pueden crear un bot personalizado que envíe mensajes específicos. Este bot genera un enlace tipo "Webhook", el cual debe ser copiado y pegado en la sección correspondiente de la automatización. De esta manera, se gestionan todas las alertas asociadas a cada automatización creada.

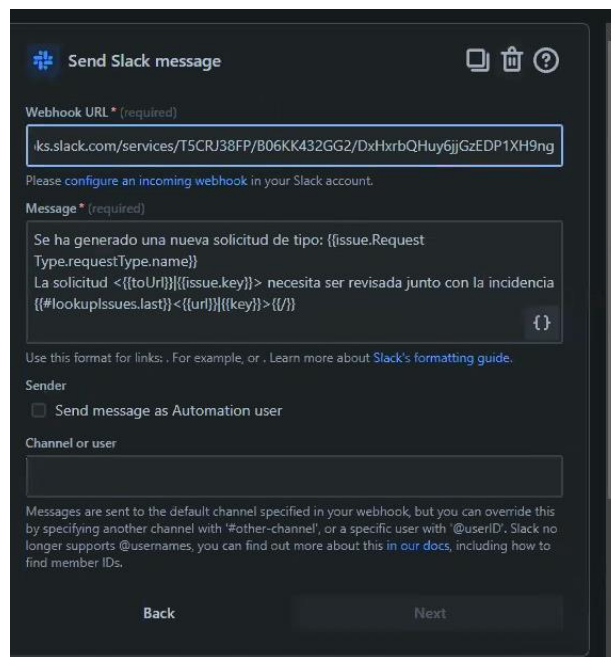


Figura 3.1.7.2.16 Vista de configuración de Webhook y el tipo de mensaje a Slack

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian Sandbox, 2024)

Asimismo, se estableció un canal específico que se utilizó como repositorio de alertas y mensajes provenientes de "CG"; este canal fue denominado "pruebas-de-proyecto" (**Figura 3.1.7.2.17**). A lo largo del tiempo, este canal recibió todas las pruebas necesarias para garantizar el correcto funcionamiento del proyecto y permitir la corrección de los errores pertinentes. Se incluyeron aspectos como el contenido de los mensajes, la presentación de los campos contenidos, y la capacidad de utilizar enlaces que redirijan a la página de la incidencia a la que hace referencia la automatización.

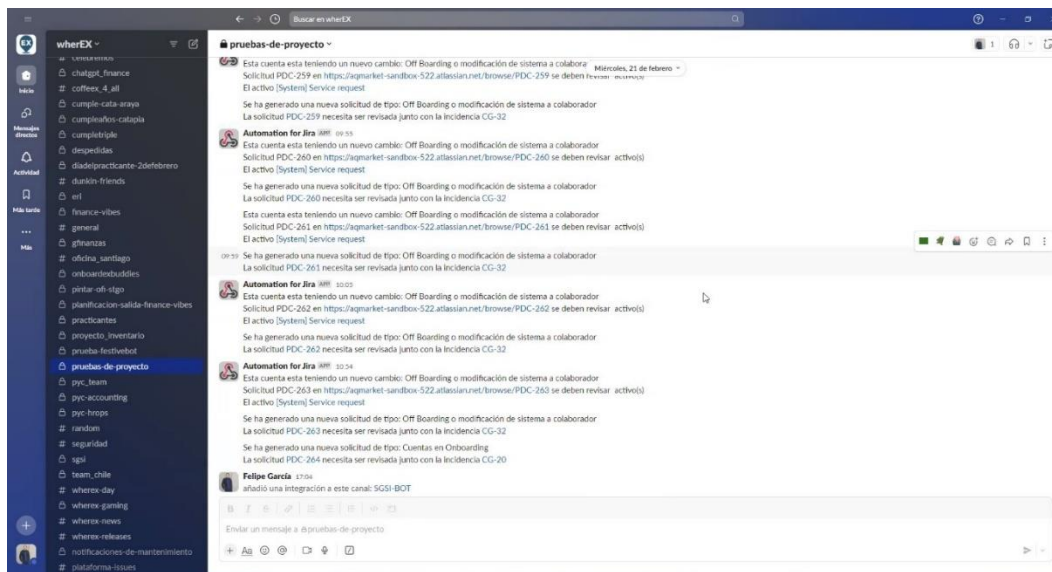


Figura 3.1.7.2.17 Vista de canal para "Pruebas de Proyecto"

Fuente: Espacio de trabajo en Slack.

b. Generación de base de datos ficticios

Efectivamente, una base de datos definida es fundamental para el correcto funcionamiento del proyecto. Inicialmente, esta base de datos fue creada de forma experimental por el responsable del proyecto, utilizando el método de "Ensayo y error". Se generaron nombres al azar y se incorporaron las características necesarias para la creación de cada incidencia, como el área, el cargo, la posición (en el caso de practicantes o colaboradores), los equipos requeridos, y las fechas de ingreso y salida. Es importante destacar que, en todo momento, el campo de líder se mantuvo asignado al mismo estudiante responsable del proyecto, con el fin de que todas las notificaciones fueran dirigidas a su correo personal y no causaran molestias a los demás colaboradores.

c. Pruebas con equipo de “Gobernanza de Sistemas”

Antes de obtener los resultados finales, se llevaron a cabo pruebas directas en colaboración con el equipo de "Gobernanza de Sistemas" con el fin de garantizar el correcto

funcionamiento de los proyectos implementados. Durante estas pruebas, los miembros del equipo evaluaron el desempeño de los proyectos y proporcionaron retroalimentación en caso de encontrar aspectos poco claros o funcionamientos incorrectos. Con el propósito de mantener un seguimiento continuo del progreso del sistema en desarrollo, se programaron reuniones regulares cada dos semanas con el equipo. Estas reuniones permitieron visualizar el avance del proyecto y abordar cualquier ajuste necesario para mejorar su funcionamiento.

A mediados de febrero de 2024, se llevó a cabo una reunión definitiva para evaluar el progreso del estudiante en el proyecto. Durante esta reunión, se realizaron pruebas detalladas para verificar el correcto funcionamiento del flujo establecido. Estas pruebas abarcaron todo el proceso, desde el Onboarding de nuevos colaboradores hasta la gestión de cuentas solicitadas y el Offboarding de colaboradores desvinculados. Se otorgó acceso a los integrantes del equipo para que pudieran crear solicitudes dentro de los portales previamente establecidos. Estas solicitudes se realizaron dentro del "Portal de Solicitudes de Soporte" (SDS) para solicitar nuevos ingresos, y dentro del "Proyecto de Cuentas" (PDC) para solicitar tanto la activación de nuevas cuentas como la baja de usuarios en el proceso de Offboarding.

2. Fase III: Integración del proyecto en espacio de wherEX como “Accesos Sistemas

WherEX (ASW):

Cuando el equipo de “Gobernanza de Sistemas” verificó el correcto funcionamiento de “CG” y dio su aprobación, se autorizó la creación del proyecto principal dentro del espacio de Jira Wherex. Se otorgaron los accesos necesarios al estudiante para que pudiera crear el proyecto y asegurar su correcto funcionamiento. En base a esto, se procedió a crear el proyecto denominado "Acceso Sistemas Wherex" o "ASW" por sus siglas, utilizando la misma metodología que en proyectos anteriores (**Figura 3.1.7.2.18**). Sin embargo, se optó por

categorizarlo como un Proyecto de Software Jira, permitiendo así el uso del tablero Kanban y aprovechando todas las funcionalidades de Jira para una mejor organización y gestión de las incidencias.

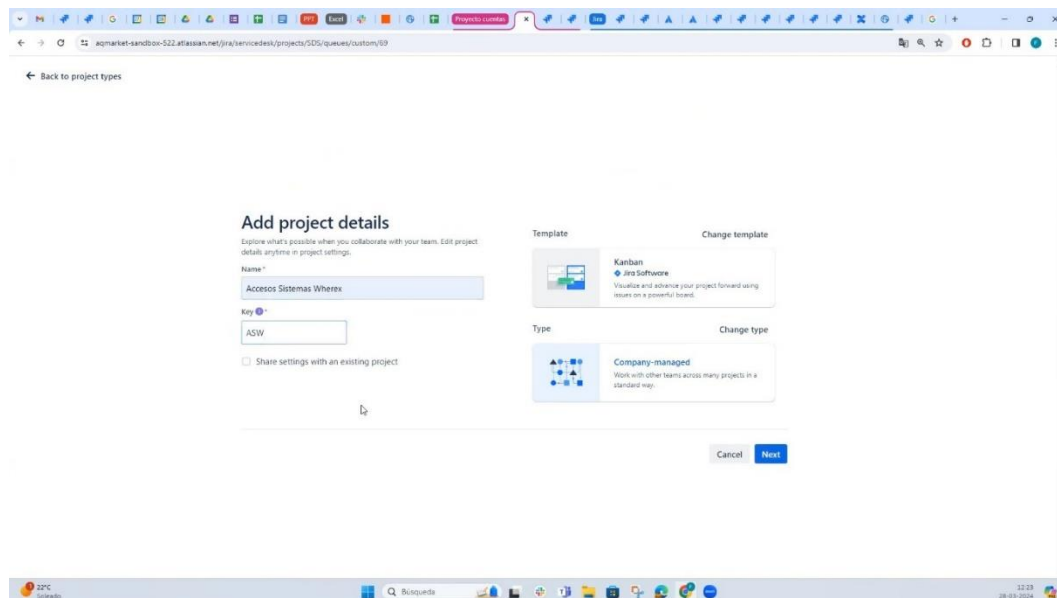


Figura 3.1.7.2.18 Creación de Proyecto IAM "Acceso Sistemas Wherex" (ASW)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

a. Configuración del sistema ASW:

Después de establecer el proyecto, se procedió a definir tres tipos de incidencias: "Colaboradores de Wherex", "Correos Generales" y "Sistemas de Wherex". Cada uno de estos tipos hace referencia a distintos aspectos a revisar dentro del sistema.

Los "Colaboradores de Wherex" abarcan tanto a las personas con contratos como a los practicantes dentro de la organización. Los "Correos Generales" se refieren a los correos de Gmail o Microsoft 365 bajo los dominios "@wherex" y "@aqmarket", los cuales están asociados a sistemas específicos para el trabajo. Por último, los "Sistemas de Wherex" engloban todas las plataformas de pago que cuentan con una licencia vigente, ya sea para

correos particulares de colaboradores o para correos generales.

Una vez definidos los tipos de incidencias, se procedió a crear campos personalizados para cada uno de ellos, los cuales permiten capturar información específica relacionada con cada tipo de situación a revisar dentro del sistema.

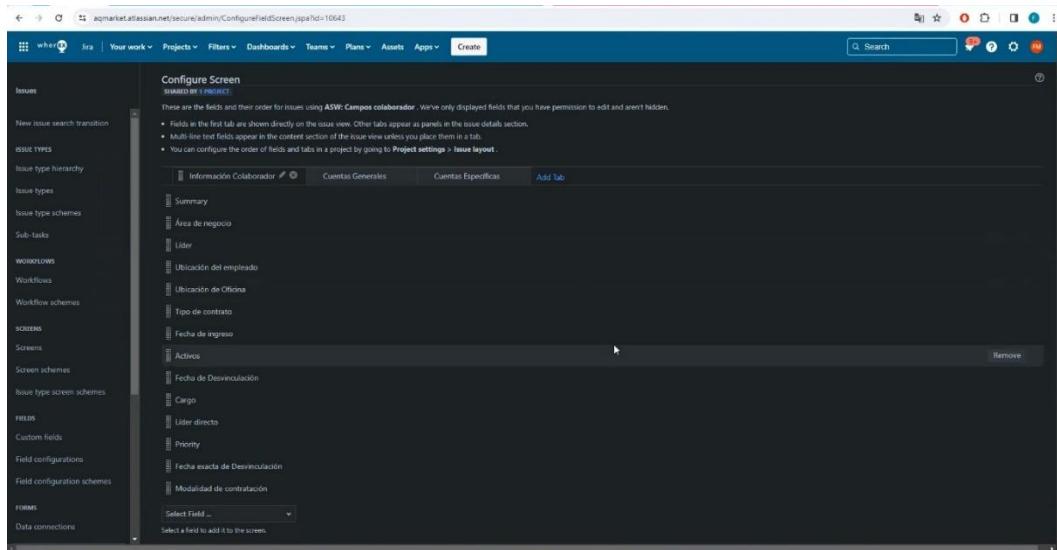


Figura 3.1.7.2.19 Screen y Custom Field Colaborador en "ASW" Información general

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Para los "Colaboradores", se diseñaron tres pestañas con diferentes campos personalizados:

- **Información Colaborador:**
 - **Área de Negocio:** Campo de selección múltiple que indica el equipo asignado dentro de la organización.
 - **Líder:** Campo de texto simple para ingresar el nombre de la persona que supervisa al colaborador, en caso de que no esté en la base de datos de Jira.
 - **Líder directo:** Campo de asignación de usuario donde se ingresa el correo del

líder del equipo del colaborador.

- **Ubicación del empleado:** Campo de texto simple para indicar la dirección particular del colaborador.
- **Ubicación de Oficina:** Campo de selección múltiple que ofrece opciones de las oficinas presentes en la organización.
- **Tipo de contrato:** Campo de selección múltiple que indica la situación contractual del colaborador.
- **Modalidad de contratación:** Campo de selección múltiple para indicar el tipo de contrato de ingreso a la organización.
- **Fecha de ingreso:** Campo de fecha simple que indica la fecha exacta en que el colaborador comienza a trabajar.
- **Fecha de Término de contrato:** Campo de fecha simple que indica la fecha exacta de finalización del contrato según TA plan.
- **Fecha exacta de Desvinculación (Ticket SI):** Campo de fecha exacta definida por el ticket de Internal Support (USS) en la solicitud de "Baja de usuarios". Se completa solo si el líder sube la solicitud de desvinculación.

- **Cuentas generales:**

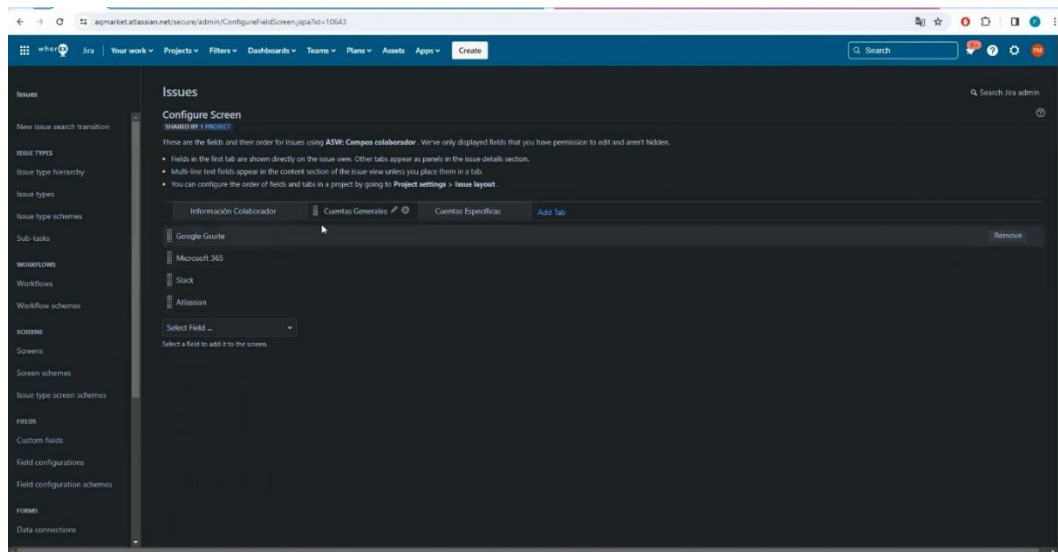


Figura 3.1.7.2.20 Screen y Custom fields de cuentas generales de colaborador en "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

- **Google Gsuite:** Campo de texto simple que se completa con el correo de Google Workspace del colaborador.
- **Microsoft 365:** Campo de texto simple donde se ingresa el correo asociado con el dominio "@aqmarket".
- **Slack:** Campo de selección múltiple con opciones como "Sin activar", "Desactivado", "Activado Usuario" y "Activado Administrador", asociado a la plataforma principal de comunicación de la empresa, Slack.
- **Atlassian:** Campo de selección múltiple con opciones similares a Slack, asociado a cuentas de Jira en Atlassian utilizadas por los colaboradores.
- **Cuentas específicas:** Estos campos permiten seleccionar el estado de acceso a cada uno de los sistemas mencionados, como "Sin activar", "Desactivado", "Activado

Usuario" o "Activado Administrador", dependiendo de las necesidades y permisos del colaborador en cada plataforma específica. Es importante destacar que no todos los colaboradores requerirán acceso a todas estas plataformas, por lo que no es obligatorio activar ninguna casilla en esta pestaña si no es relevante para el colaborador en cuestión.

- | | |
|---|--|
| ☐ Geisser Spa | ☐ Reforge INC |
| ☐ Bsale Chile | ☐ Brevo (Sendinblue) |
| ☐ BUK | ☐ Hotjar |
| ☐ Cardda | ☐ Lucidchart |
| ☐ Clay | ☐ Loom |
| ☐ Clara | ☐ Jasper |
| ☐ Genoma.work | ☐ Read.AI |
| ☐ Regcheq | ☐ GoDaddy |
| ☐ Datamart | ☐ Sonarsource |
| ☐ Tribal | ☐ VWO |
| ☐ Amazon Web Services | ☐ Figma |
| ☐ Salesforce | ☐ Adobe |
| ☐ Linkedin ADS | ☐ Apollo |
| ☐ Google ADS | ☐ Netreo |

- Docker
- Weglot
- Mailtrap
- New Relic
- UserPilot
- Duemint
- Bright Data
- A Cloud Guru
- Odoo
- Microsoft Azure
- MongoDB
- System
- Amplitude
- Snyk
- Aircall
- Stackify
- Ops Tracing
- OneDrive
- Zendes

Para los "Sistemas de Wherex", se creó una pestaña única que contiene los siguientes campos personalizados:

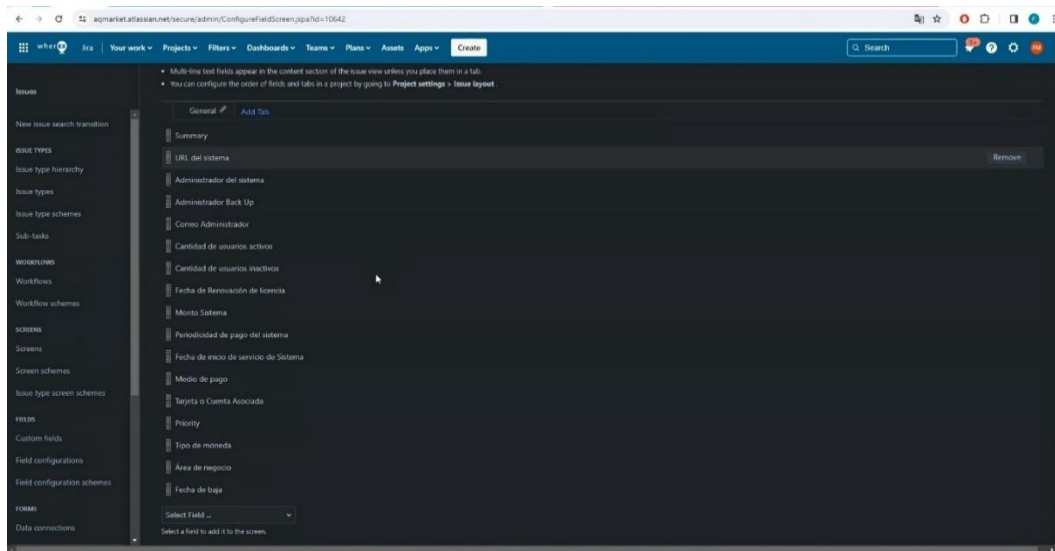


Figura 3.1.7.2.21 Screen y Custom Field de Sistemas en "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

- **URL del sistema:** Campo de dirección URL que hace referencia al enlace del sistema contratado.
- **Administrador del sistema:** Campo de asignación de usuario donde se ingresa el correo de la persona principal que administra la plataforma.
- **Administrador Back Up:** Campo de asignación de usuario donde se ingresa el correo de respaldo de la persona que administra la plataforma.
- **Correo administrador:** Campo de texto simple donde se ingresa el correo con el cual el administrador de la plataforma puede acceder a su cuenta.
- **Cantidad de usuarios activos:** Campo de número que indica la cantidad de usuarios activos en el sistema.
- **Cantidad de usuarios inactivos:** Campo de número que indica la cantidad de usuarios inactivos en el sistema.

- **Fecha de Renovación de licencia:** Campo de fecha simple que indica la fecha en que se renueva la licencia luego del pago.
- **Monto del sistema:** Campo de número donde se ingresa la totalidad del monto del sistema o la licencia.
- **Periodicidad de pago:** Campo de selección múltiple con opciones como "Mensual", "Trimestral", "Semestral", "Anual" e "Indefinido" para determinar la frecuencia de cobro de la plataforma.
- **Tarjeta o cuenta asociada:** Campo de selección múltiple que contiene las cuentas bancarias de la empresa y especifica con qué cuenta se paga el sistema.
- **Tipo de moneda:** Campo de selección múltiple que indica la moneda utilizada para realizar el pago del sistema, con opciones como "USD", "CLP", "COL", "MXN" y "SOL".
- **Área de negocio:** Campo de selección múltiple que contiene las áreas de la empresa, indicando el equipo principal que utiliza el sistema.
- **Fecha de baja:** Campo de fecha simple que se completa solo si se realiza la solicitud de baja del sistema.

Para el tipo de “Correo General”, sólo contiene los mismos campos de las pestañas de Cuentas generales y Cuentas específicas.

Después de la creación de todos los Custom Fields, se procede a la creación del Screen para cada tipo de incidencia. Este paso es fundamental, ya que garantiza que cada campo se visualice de manera adecuada dentro de la incidencia correspondiente. Para lograr esto, se

crean "Screens" personalizadas utilizando los Screen Scheme y Screen Scheme Issue Type. De esta manera, solo se mostrarán los campos relevantes para cada tipo de incidencia, evitando la sobrecarga de información.

Además, gestionar el "Layout" de cada incidencia es importante para mejorar la comprensión y la usabilidad del sistema. Esta sección determina cómo se presenta la incidencia al crearla, permitiendo organizar la información de manera más efectiva. Es posible agregar, quitar o reorganizar campos según sea necesario para mejorar la estructura y facilitar la navegación dentro del sistema. También ayuda a distinguir claramente entre los diferentes tipos de incidencias, lo que facilita su identificación y manejo por parte de los usuarios.

Finalmente, se ha establecido un flujo de trabajo o "Workflow" que consiste en los diversos estados que pueden tener tanto las incidencias de los colaboradores como las relacionadas con los sistemas. Esta estructura facilitará una revisión más eficiente y seguirá el enfoque de tablero Kanban para la modificación, visualización y seguimiento de las incidencias.

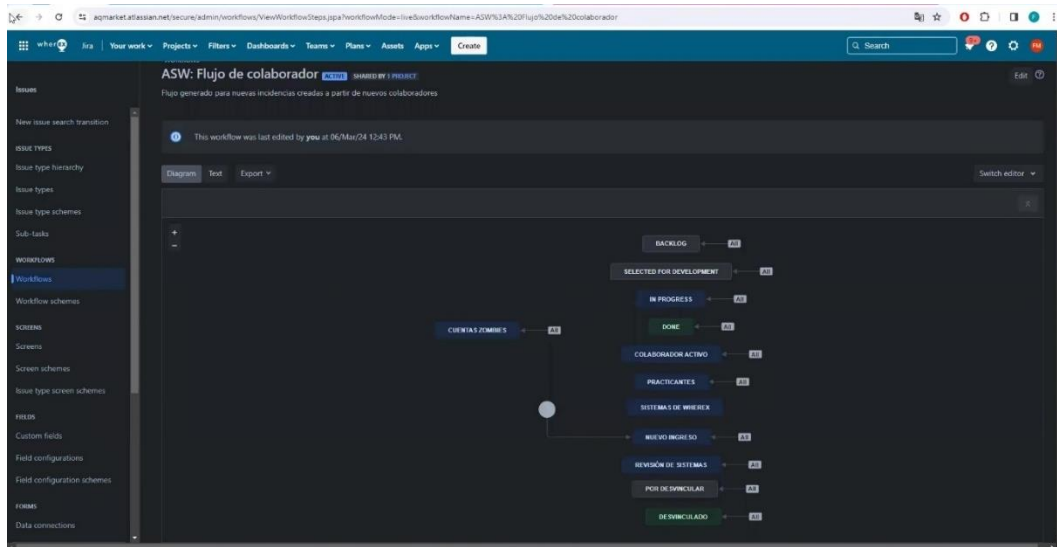


Figura 3.1.7.2.22 Vista de Workflow Colaborador en "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

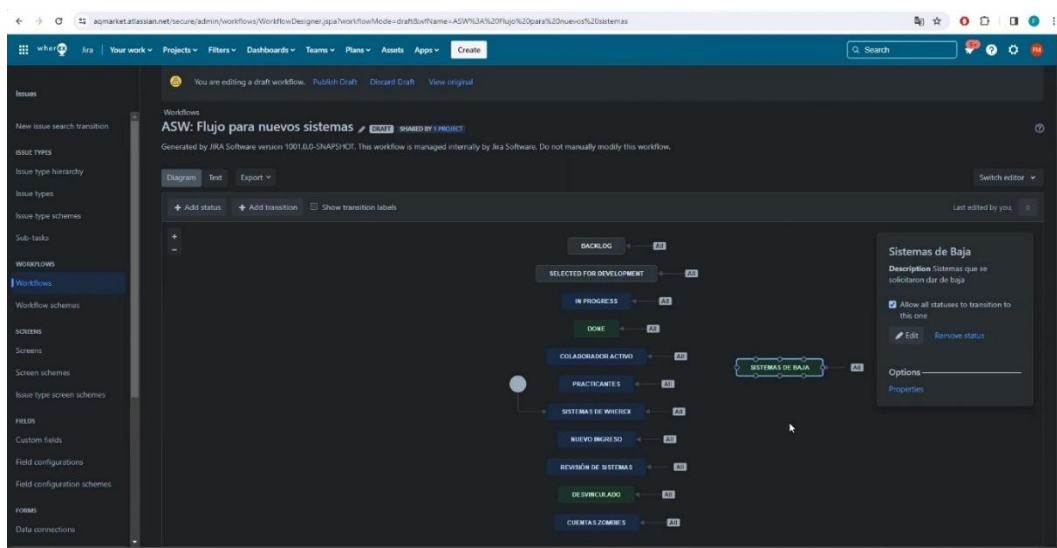


Figura 3.1.7.2.23 Workflow de Sistemas "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

b. Importación de base de datos de sistemas y usuarios:

Una vez completada la configuración adecuada de cada parte de las incidencias, se llevó a cabo la carga masiva de información de los colaboradores de Wherex, incluyendo

contratos, practicantes y correos generales. La recopilación de esta información fue realizada por el estudiante, quien se reunió con los administradores de los sistemas de la empresa para adquirir los datos de los usuarios de cada plataforma. Estos datos fueron recopilados en un archivo de Excel denominado "General de Sistemas", que contenía tanto la información personal de cada colaborador como sus accesos a los sistemas.

Este archivo Excel fue modificado para cumplir con los requisitos de los Custom Fields creados, asegurándose de ingresar los valores adecuados en cada campo, especialmente si se trataba de campos de selección múltiple. Una vez que se completó el archivo, se procedió a crear una réplica en formato CSV UTF-8 para su posterior carga en la plataforma de Jira, específicamente como incidencias en ASW.

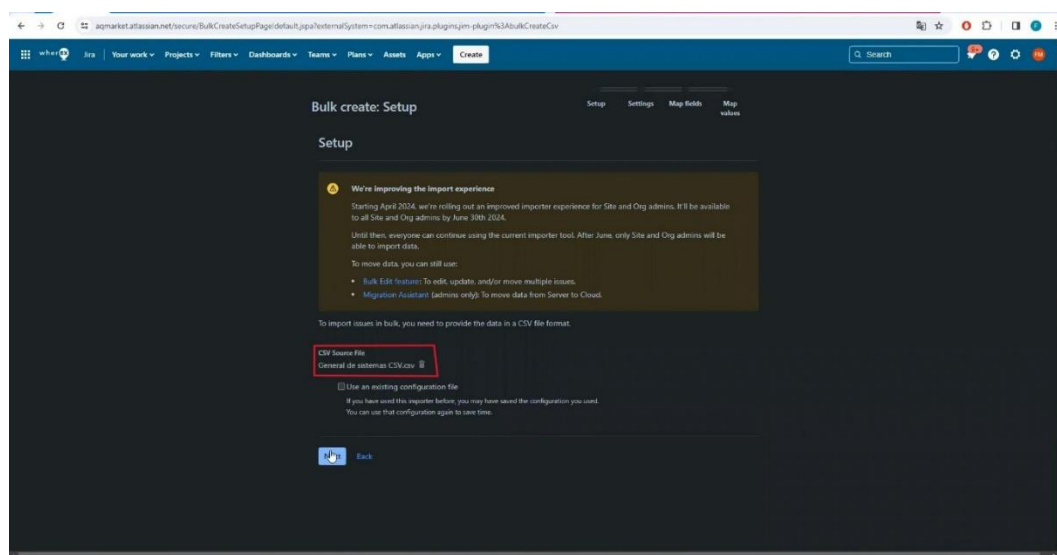


Figura 3.1.7.2.24 Importación de incidencias y elección de CSV General de Sistemas

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Para realizar la carga masiva, se seleccionó la opción "Crear", que despliega una vista predeterminada con la opción "Importar Incidencias" a la derecha. Esta opción, conocida como "Bulk Create: Setup", es el primer paso para la carga masiva. Al seleccionar el archivo

deseado y hacer clic en "Siguiente", se procede al segundo paso, donde se define el proyecto para la carga, el formato del archivo y el delimitador de campos, en este caso ";". También se especifica el formato de fecha, que por lo general es "dd-MM-yyyy".

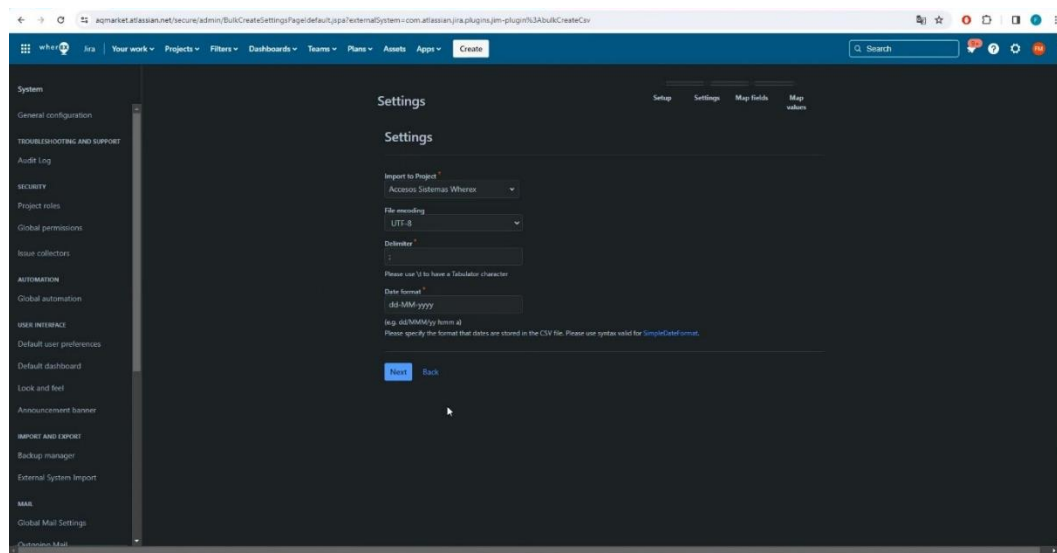


Figura 3.1.7.25 Settings Importación de incidencias "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Una vez completado este paso, al hacer clic en "Siguiente" se accede al módulo de "Map Fields" para seleccionar los campos que se llenarán a partir de las columnas del archivo subido. Es crucial ser meticuloso en esta etapa para asegurar que cada campo se mapee correctamente. Se debe activar la opción "Map Field Value" para cada campo seleccionado, lo que garantiza la correcta carga de datos y su análisis por parte del programa.

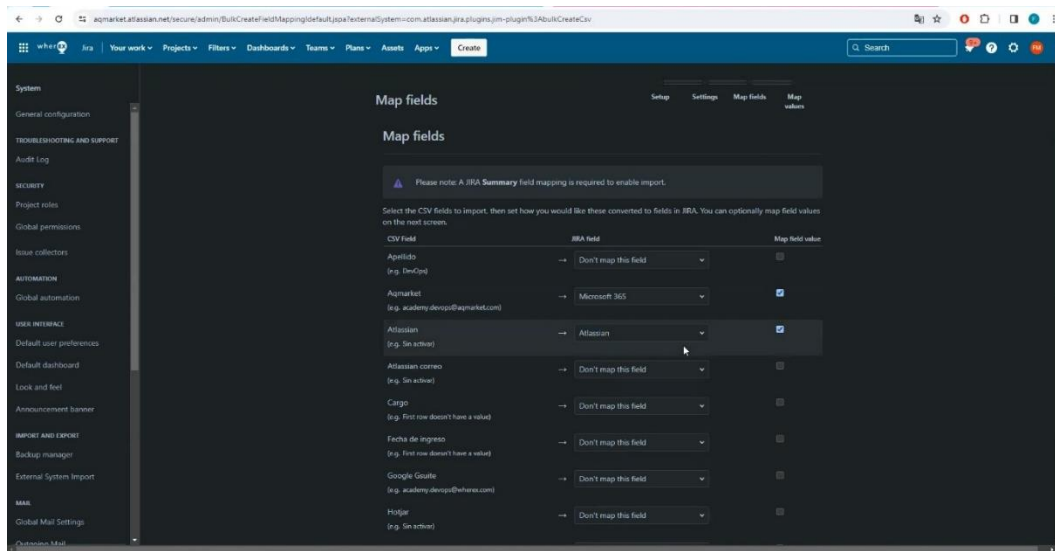


Figura 3.1.7.2.26 Map Fields de Importación de incidencias "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Después de seleccionar todos los campos, se pasa al último paso, la sección "Map Values", donde se verifica la disponibilidad y corrección de los datos dentro del proyecto. Es importante validar los datos con la opción "Validate" para evitar problemas en el proyecto. Si no hay problemas ni advertencias, se pueden subir las incidencias seleccionando la opción "Begin Import". Esto iniciará la carga de información, creando un Issue Type correspondiente para cada colaborador, practicante o correo general, y asignándoles el estado apropiado.

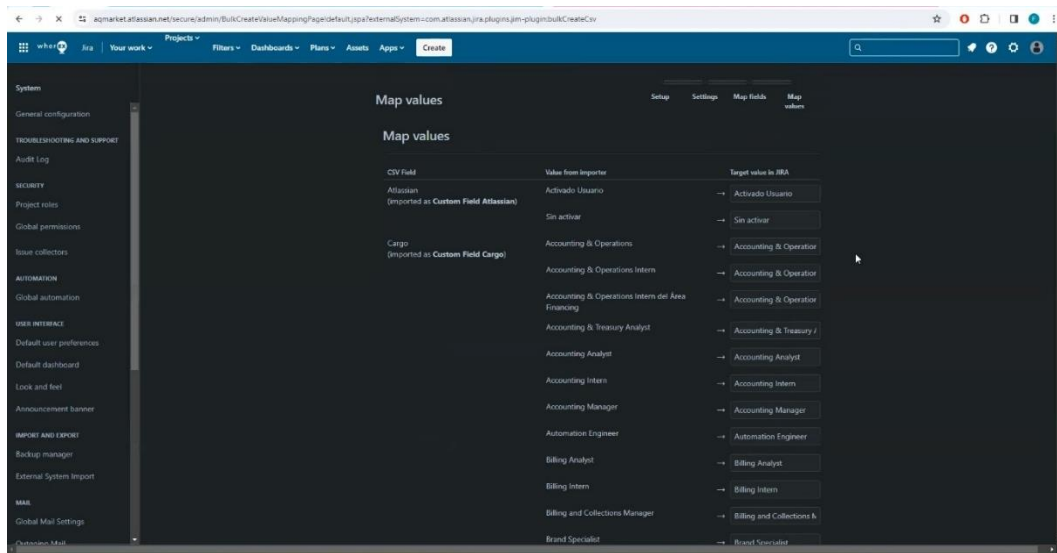


Figura 3.1.7.2.27 Map Values para confirmar valores de importación de incidencias

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

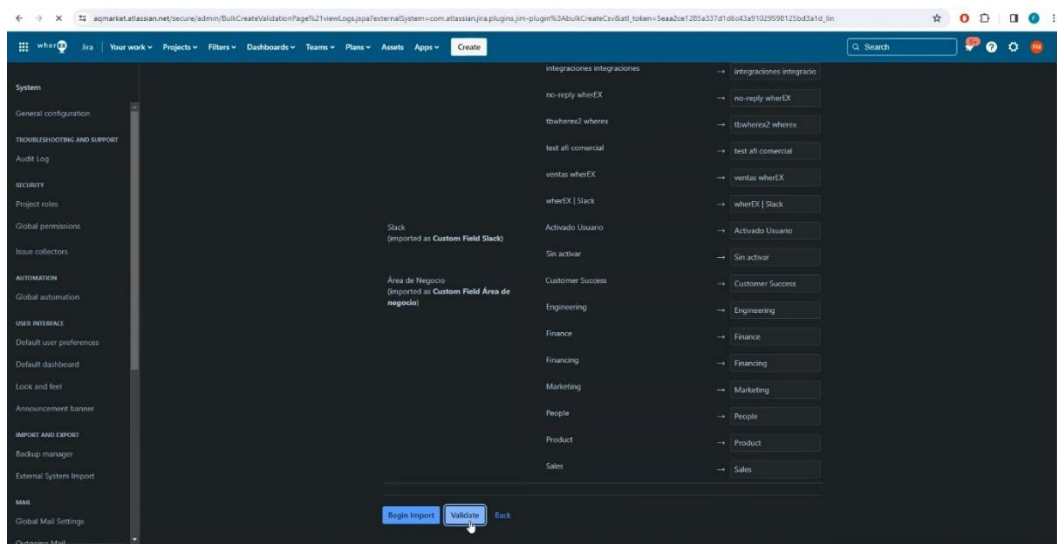


Figura 3.1.7.2.28 Selección de validación de datos de Map Values

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

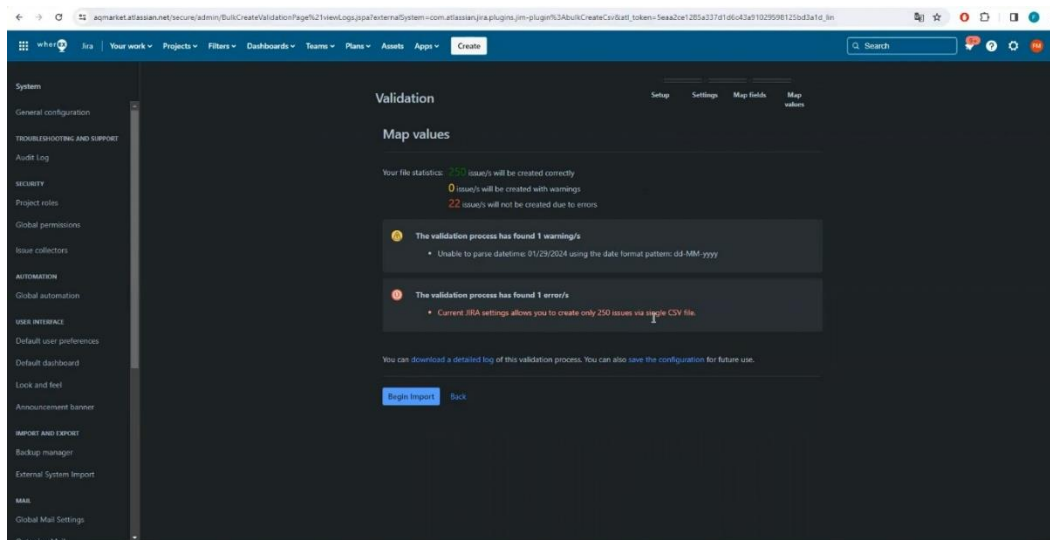


Figura 3.1.7.2.29 Validación de incidencias listas para Importar a "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Una vez completada la carga de información de los colaboradores, se procedió a realizar un procedimiento similar para la carga de sistemas. Para ello, se utilizó un archivo de Excel denominado "Datos de Sistemas", el cual fue recopilado de manera similar, aunque en este caso se contó con la asistencia del equipo de Accounting para acceder a información relevante sobre valores, tarjetas y periodicidades de pagos.

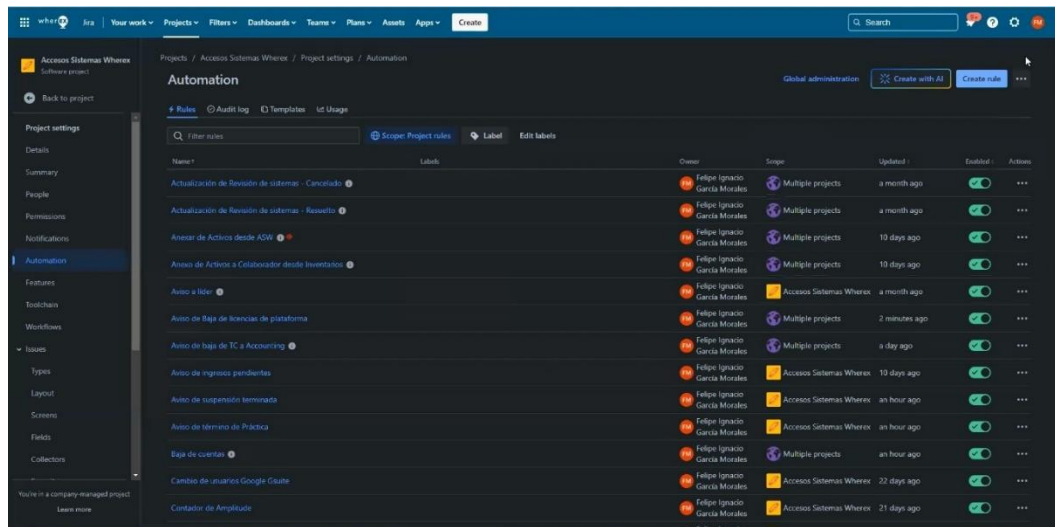
La información contenida en este archivo Excel fue subida como Issue Types "Sistemas de Wherex" y se ingresaron en el mismo estado o Status que los colaboradores. Este proceso aseguró que tanto la información de los colaboradores como la de los sistemas se integraran de manera coherente y consistente dentro del sistema de gestión de incidencias.

c. Conexión de proyectos:

Las automatizaciones implican la consideración de varios aspectos que conforman las funcionalidades del sistema. Entre estos aspectos, destaca la interacción de ASW con otros tres proyectos: Talent Acquisition Plan (TA Plan), Internal Support e Inventarios. Cada uno

de estos proyectos posee funcionalidades específicas que contribuyen al funcionamiento global del sistema.

d. Automatizaciones:

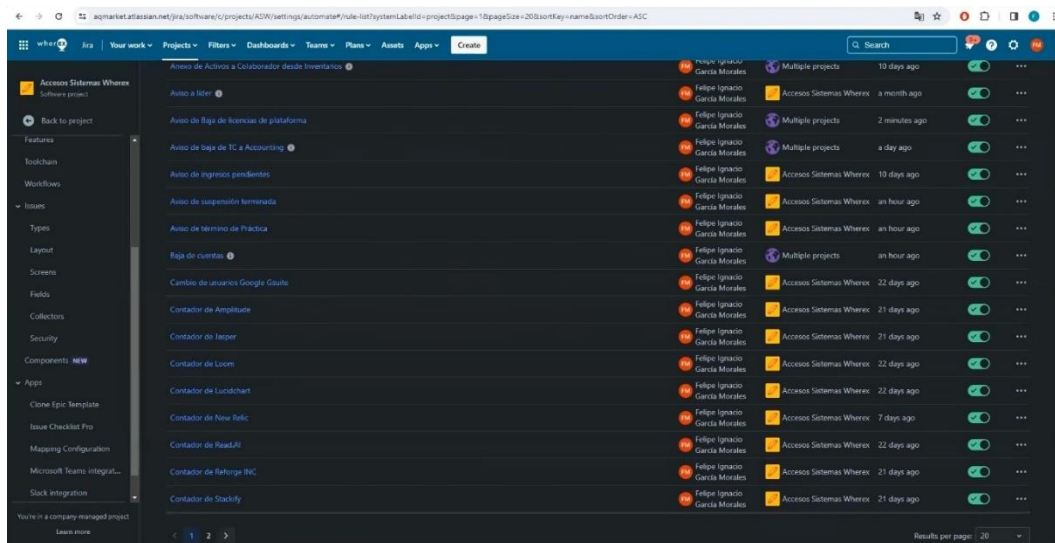


The screenshot shows the Jira Automation interface for the 'Accesos Sistemas Wheres' project. The left sidebar contains navigation options like 'Project settings', 'Details', 'Summary', 'People', 'Permissions', 'Notifications', 'Automation' (selected), 'Features', 'Toolchain', 'Workflows', 'Issues', 'Types', 'Layout', 'Screens', 'Fields', and 'Collectors'. The main area displays a list of automation rules under the 'Automation' tab. The rules are as follows:

Name	Labels	Owner	Scope	Updated	Enabled	Actions
Actualización de Revisión de sistemas - Cancelado		Felipe Ignacio García Morales	Multiple projects	a month ago	On	...
Actualización de Revisión de sistemas - Resuelto		Felipe Ignacio García Morales	Multiple projects	a month ago	On	...
Anexo de Activos desde ASW		Felipe Ignacio García Morales	Multiple projects	10 days ago	On	...
Anexo de Activos a Colaborador desde Inventario		Felipe Ignacio García Morales	Multiple projects	10 days ago	On	...
Anexo a líder		Felipe Ignacio García Morales	Accesos Sistemas Wheres	a month ago	On	...
Anexo de Ropa de licencias de plataforma		Felipe Ignacio García Morales	Multiple projects	2 minutes ago	On	...
Anexo de hoja de TC a Accounting		Felipe Ignacio García Morales	Multiple projects	a day ago	On	...
Anexo de ingresos pendientes		Felipe Ignacio García Morales	Accesos Sistemas Wheres	10 days ago	On	...
Anexo de suspension terminada		Felipe Ignacio García Morales	Accesos Sistemas Wheres	an hour ago	On	...
Anexo de término de Práctica		Felipe Ignacio García Morales	Accesos Sistemas Wheres	an hour ago	On	...
Ropa de cuentas		Felipe Ignacio García Morales	Multiple projects	an hour ago	On	...
Cambio de usuarios Google GSuite		Felipe Ignacio García Morales	Accesos Sistemas Wheres	22 days ago	On	...
Contador de Amplitud		Felipe Ignacio García Morales	Accesos Sistemas Wheres	21 days ago	On	...

Figura 3.1.7.2.30 Automatizaciones 1 de "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)



This screenshot shows the continuation of the Jira Automation rules list. The rules are as follows:

Name	Labels	Owner	Scope	Updated	Enabled	Actions
Anexo de Activos a Colaborador desde Inventario		Felipe Ignacio García Morales	Multiple projects	10 days ago	On	...
Anexo a líder		Felipe Ignacio García Morales	Accesos Sistemas Wheres	a month ago	On	...
Anexo de Ropa de licencias de plataforma		Felipe Ignacio García Morales	Multiple projects	2 minutes ago	On	...
Anexo de hoja de TC a Accounting		Felipe Ignacio García Morales	Multiple projects	a day ago	On	...
Anexo de ingresos pendientes		Felipe Ignacio García Morales	Accesos Sistemas Wheres	10 days ago	On	...
Anexo de suspension terminada		Felipe Ignacio García Morales	Accesos Sistemas Wheres	an hour ago	On	...
Anexo de término de Práctica		Felipe Ignacio García Morales	Accesos Sistemas Wheres	an hour ago	On	...
Ropa de cuentas		Felipe Ignacio García Morales	Multiple projects	an hour ago	On	...
Cambio de usuarios Google GSuite		Felipe Ignacio García Morales	Accesos Sistemas Wheres	22 days ago	On	...
Contador de Amplitud		Felipe Ignacio García Morales	Accesos Sistemas Wheres	21 days ago	On	...
Contador de lebar		Felipe Ignacio García Morales	Accesos Sistemas Wheres	21 days ago	On	...
Contador de Loom		Felipe Ignacio García Morales	Accesos Sistemas Wheres	22 days ago	On	...
Contador de Lucidchart		Felipe Ignacio García Morales	Accesos Sistemas Wheres	22 days ago	On	...
Contador de New Relic		Felipe Ignacio García Morales	Accesos Sistemas Wheres	7 days ago	On	...
Contador de ReadAI		Felipe Ignacio García Morales	Accesos Sistemas Wheres	22 days ago	On	...
Contador de Reforge INC		Felipe Ignacio García Morales	Accesos Sistemas Wheres	21 days ago	On	...
Contador de Stackify		Felipe Ignacio García Morales	Accesos Sistemas Wheres	21 days ago	On	...

Figura 3.1.7.2.31 Automatizaciones 2 de "ASW"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

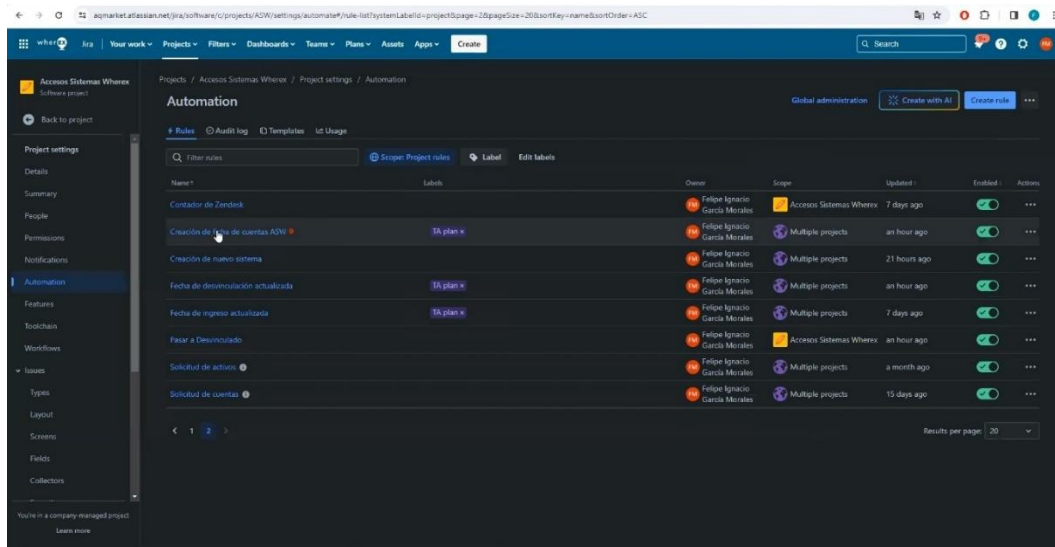


Figura 3.1.7.2.32 Automatizaciones "ASW" página 2

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

- **Actualización de Revisión de Sistemas - Cancelado:** Al generarse una solicitud en Internal Support, se vincula el correo ingresado con el de la persona en ASW. Posteriormente, si la solicitud es cancelada, el estado del ticket vuelve a "Colaborador Activo" o "Practicantes" sin realizar cambios adicionales.
- **Actualización de Revisión de Sistemas - Resuelto:** Tras la creación de una solicitud en Internal Support, se enlaza el correo ingresado con el de la persona en ASW. Si el ticket es cancelado, retorna al estado de "Colaborador Activo" o "Practicantes". Sin embargo, el Sysadmin debe activar la casilla del sistema del cual se solicitó el ticket de cuentas.
- **Anexar Activos desde ASW:** Al crear una incidencia de colaborador con las credenciales correspondientes, se busca en el proyecto de Inventario los activos asociados al correo de Google Gsuite y se enlazan con el nombre "Escalado en" todos los equipos que posea.

- **Anexo de Activos a Colaborador desde Inventarios:** Cuando se ingresa el correo de un colaborador en una incidencia de inventario, esta automatización busca en ASW el correo del colaborador o practicante para vincular el activo con la persona correspondiente.
- **Aviso a Líder:** Cuando las credenciales de cuentas generales están activas, se envía un correo electrónico al líder del usuario que las ingresó, confirmando la creación de las cuentas.
- **Aviso de Baja de Licencias de Plataforma:** Al subirse un ticket de solicitud de "Eliminación de licencia de plataforma suscrita" en Internal Support, se alerta al equipo de Sysadmin y Accounting para confirmar la baja de la plataforma y cancelar el pago asociado.
- **Aviso de Baja de TC a Accounting:** En el momento en que una persona se desvincula, se notifica al equipo de Accounting vía Slack, indicando la desvinculación y, si tiene una tarjeta de crédito asociada, que se cancele o quede disponible para otro colaborador.
- **Aviso de Ingresos Pendientes:** Si las incidencias no son revisadas durante 24 horas después de la fecha de ingreso, se envía una alerta al equipo de Sysadmin vía Slack para que genere las credenciales de la persona y designe la incidencia al estado de "Colaborador Activo".
- **Aviso de Suspensión Terminada:** Si se necesita realizar un respaldo en el espacio del correo de una persona desvinculada, su correo pasará a estar suspendido. Se avisa un día antes de que la cuenta se termine de suspender y pase a eliminarse.

- **Aviso de Término de Práctica:** Cuando ingresa un practicante, se alerta al equipo de Sysadmin por Slack y por correo al líder del practicante que su contrato está por terminar, instándolos a levantar un ticket de baja de cuentas o notificar el cambio de salida (*Figura 3.1.7.2.33*).

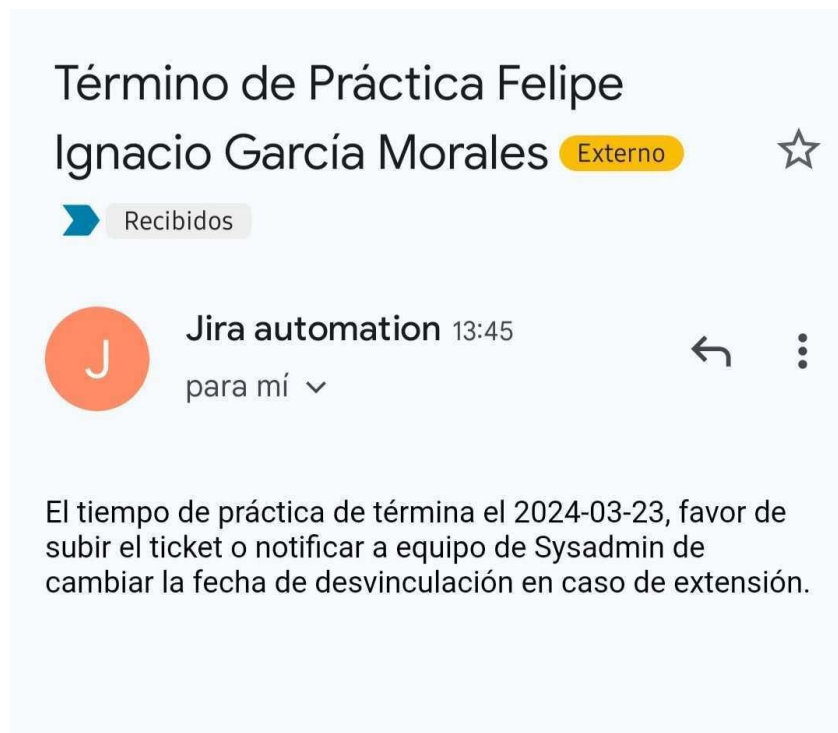


Figura 3.1.7.2.33 Aviso vía correo de término de práctica a líder

Fuente: Espacio de trabajo en Gmail.

- **Baja de Cuentas:** Al subirse un ticket de baja de cuentas por desvinculación, se genera una alerta para que el Sysadmin revise los sistemas activos asociados al usuario. La incidencia se vincula con el ticket subido y cambia su estado a "Por Desvincular" para que el Sysadmin dé de baja todas las cuentas en la fecha de salida.
- **Cambio de Usuarios Google Gsuite:** Si un colaborador pasa al estado de "Desvinculado" y sus cuentas siguen activas o no han sido modificadas, se alerta sobre la cuenta vigente y se indica que el Sysadmin debe cambiar el campo y verificar si la

cuenta fue dada de baja.

- **Contador de Amplitude, Jasper, Loom, New Relic, Read.AI, Reforge INC, Stackify y Zendesk:** Cada día a las 9 AM, se genera un registro de todas las incidencias (personas o correos generales) asociadas a una cuenta activa en el sistema respectivo. Se realiza un conteo y se actualiza la cantidad dentro del campo de Usuarios Activos en la incidencia correspondiente de cada sistema.
- **Creación de Ficha de Cuentas ASW:** Esta automatización conectada con el Proyecto de TA Plan, inicia el proceso del proyecto al ingresar el nombre de una persona contratada. Crea una nueva incidencia de "Colaborador" en ASW con los datos correspondientes, alertando al equipo del nuevo ingreso para gestionar la creación de credenciales y asignación de activos.
- **Creación de Nuevo Sistema:** Cuando se genera un ticket de "Solicitud de Nueva Licencia de Plataforma" en Internal Support y este avanza al estado "Pre-aprobado", se crea una incidencia tipo "Sistemas de Wherex" con el nombre de la plataforma solicitada. Se notifica al equipo de Accounting y Sysadmin para gestionar la activación y pago.
- **Fecha de Desvinculación Actualizada:** Conectada con TA Plan, actualiza automáticamente la fecha de término de contrato en la incidencia de la persona en ASW cuando se realiza un cambio en el campo correspondiente en la incidencia de búsqueda en TA.
- **Fecha de Ingreso Actualizada:** Conectada con TA Plan, actualiza automáticamente la fecha de ingreso en la incidencia de la persona en ASW cuando se modifica el campo

correspondiente en la incidencia de búsqueda en TA.

- **Pasar a Desvinculado:** Al crear el ticket de baja de cuentas, se ingresa la fecha y hora exacta de desvinculación. Cuando llega el momento definido, se alerta al equipo de Sysadmin para proceder con la baja de cuentas y eliminar los accesos, cambiando el estado a "Desvinculado".
- **Solicitud de Activos:** Al crearse un ticket de solicitud de activos en Internal Support, y este contenga el correo de la persona destinataria, se vincula con la incidencia de la persona en ASW y se alerta al equipo de Sysadmin para gestionar los activos correspondientes.
- **Solicitud de Cuentas:** Al generarse un ticket de "Gestión de Cuentas" en Internal Support, y este contenga el correo de la persona destinataria, se vincula con la incidencia de la persona en ASW y se alerta al equipo de Sysadmin para gestionar la activación de cuentas en la plataforma correspondiente, activando también la casilla del sistema.

4.2. Métodos y procedimientos por utilizar

Dentro del proyecto, teniendo en cuenta las funcionalidades que posee, es perfectamente viable para obtener mejoras, lo es así mediante las diferentes metodologías que fueron nombradas en un apartado del informe.

4.2.1. Métodos de aplicación de Kanban:

El proceso de gestión de incidencias, fundamentado en el uso del tablero Kanban (*Figura 3.1.7.2.1*), representa un enfoque sistemático y eficaz para organizar y abordar las tareas relacionadas con los sistemas de la empresa. Este tablero categoriza las incidencias en diferentes estados, lo que permite una visualización clara y ordenada de las actividades en curso, las pendientes y las completadas. Al ser accesible para todo el equipo, se promueve la transparencia y la colaboración, ya que cada miembro puede ver el estado de las incidencias y contribuir según sea necesario.

La asignación equitativa de incidencias a los miembros del equipo es fundamental para garantizar una distribución justa de la carga de trabajo y una atención adecuada a cada solicitud. Esto se logra mediante un proceso transparente y basado en criterios objetivos, lo que fomenta la participación de todos los miembros del equipo y evita la sobrecarga de trabajo de algunos individuos.

La eficiencia del proceso se ve reforzada por la utilización de automatizaciones que generan alertas sobre nuevos ingresos y salidas de colaboradores. Estas alertas permiten al equipo anticiparse a las necesidades de gestión de activos y credenciales, asegurando que todo esté preparado para la llegada de un nuevo colaborador o la salida de uno existente. Además, estas automatizaciones contribuyen a la trazabilidad de la información al proporcionar registros claros y detallados de todas las acciones realizadas.

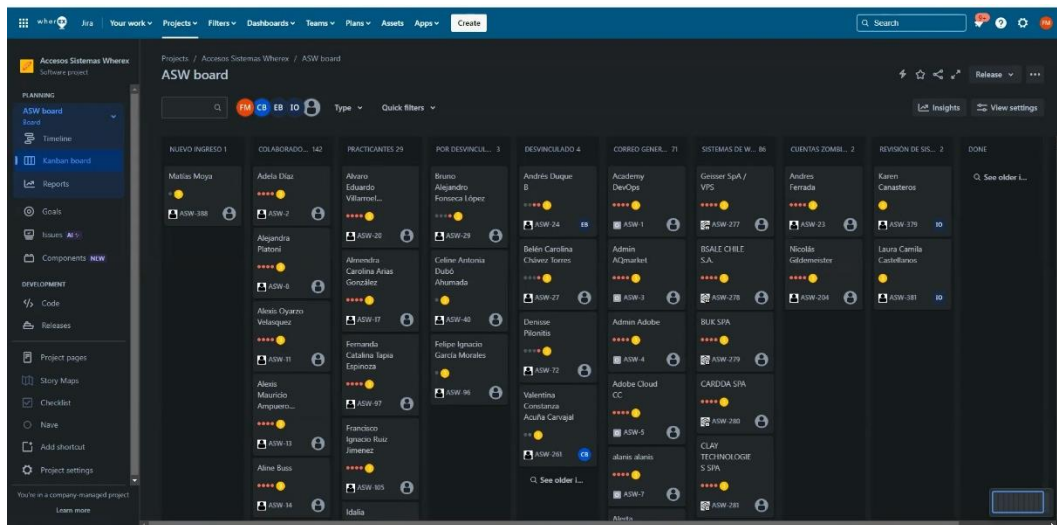


Figura 3.1.7.2.1 Vista de tablero Kanban ASW

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Finalmente, se logró la implementación de un panel en la plataforma Jira para realizar un seguimiento general de las incidencias de sistemas, esto representa un avance significativo en la capacidad de supervisar y controlar el estado de los accesos y las actividades relacionadas con los sistemas. Este panel proporciona métricas clave sobre usuarios, valores y administradores, lo que permite al equipo identificar tendencias, patrones y áreas de enfoque prioritario. Con esta información, el equipo de Sysadmin puede tomar decisiones informadas y proactivas para mejorar la eficiencia y la seguridad de los sistemas de la empresa.

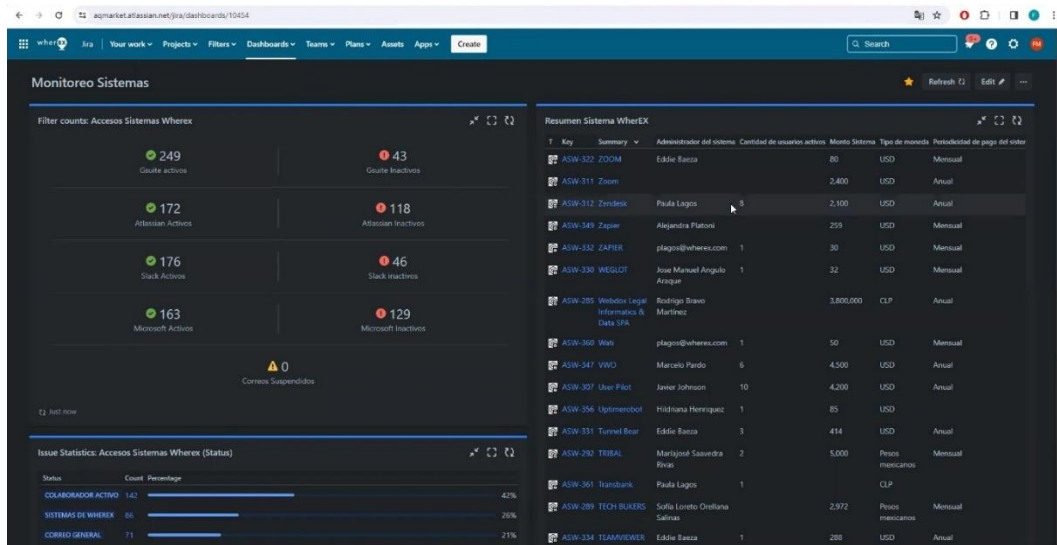


Figura 3.1.7.2.2 Vista principal de panel "Resumen de Sistemas" y "Sistemas generales"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

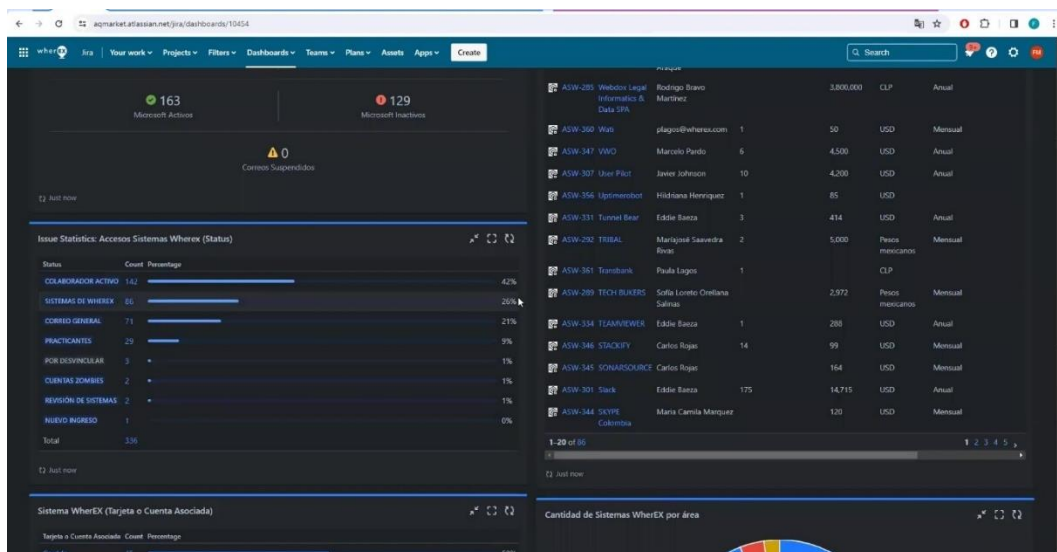


Figura 3.1.7.2.3 Vista de panel Resumen de Status

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

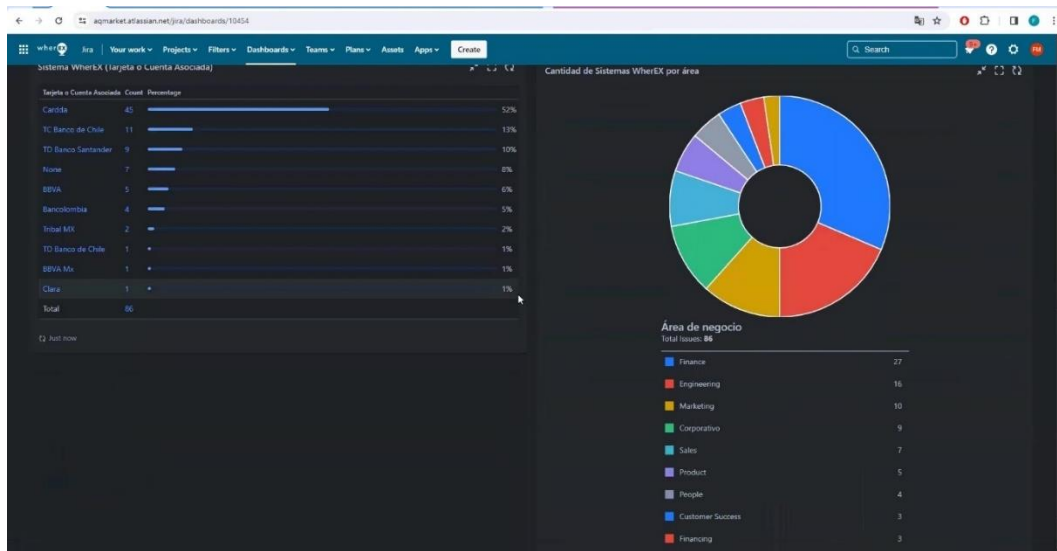


Figura 3.1.7.2.4 Vista de "Resumen de Tarjetas" y "Sistemas por Área"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

4.2.2. Métodos de mejoras PDCA:

En la fase inicial de integración del proyecto "ASW", se empleó la metodología PDCA (Planificar, Hacer, Verificar, Actuar) para identificar oportunidades de mejora y proporcionar beneficios adicionales a la empresa. Durante este proceso, se destacó una mejora significativa para el equipo de Finanzas, específicamente en la gestión de tarjetas de crédito asociadas a los colaboradores.

1. **Planning (Planificación):** se evaluó la viabilidad de integrar las tarjetas de crédito al sistema ASW con el fin de mantener un control preciso sobre estas. Se identificó que existía una falta de notificación cuando los colaboradores dejaban la empresa, lo que generaba riesgos en la gestión de las tarjetas. En colaboración con el equipo de Contabilidad, se determinó la necesidad de establecer una conexión que permitiera cargar la base de datos de tarjetas en el proyecto de "Inventarios" en Jira, con el propósito de registrar y controlar el estado de las tarjetas.

2. **Do (Hacer):** se implementó el apartado de tarjetas en el proyecto de Jira "Inventarios", permitiendo vincularlas como activos a las incidencias de los colaboradores. Asimismo, se desarrollaron automatizaciones en conjunto con el Soporte Interno para asignar tarjetas a nuevas plataformas, notificar la baja de una plataforma para cancelar el pago de la tarjeta y alertar al equipo de Contabilidad sobre la disponibilidad de tarjetas de colaboradores desvinculados.
3. **Check (Verificar):** se llevaron a cabo varias pruebas para confirmar el correcto funcionamiento del sistema. Se comprobó que, a través de las solicitudes gestionadas por el Soporte Interno, se notificaba de manera eficiente al equipo de Contabilidad sobre los movimientos relacionados con las tarjetas, adaptando los mensajes para satisfacer las necesidades específicas del equipo en la gestión de cuentas bancarias.
4. **Act (Actuar):** se verificó el funcionamiento óptimo del sistema y se reconoció su potencial para aplicarse en otros procesos de gestión de activos, como computadoras portátiles, teléfonos móviles, monitores, entre otros. La colaboración estrecha con el equipo de Contabilidad garantizó la disponibilidad de toda la información necesaria para una gestión efectiva de las tarjetas de crédito.

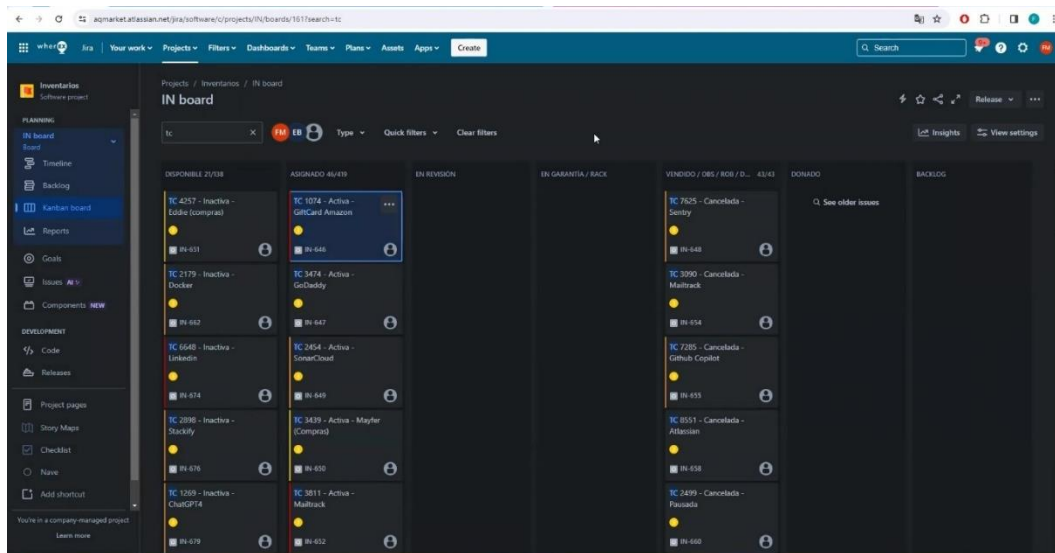


Figura 3.1.7.2.1 Vista de incidencias "Tarjetas de Crédito" agregadas a "Inventarios"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

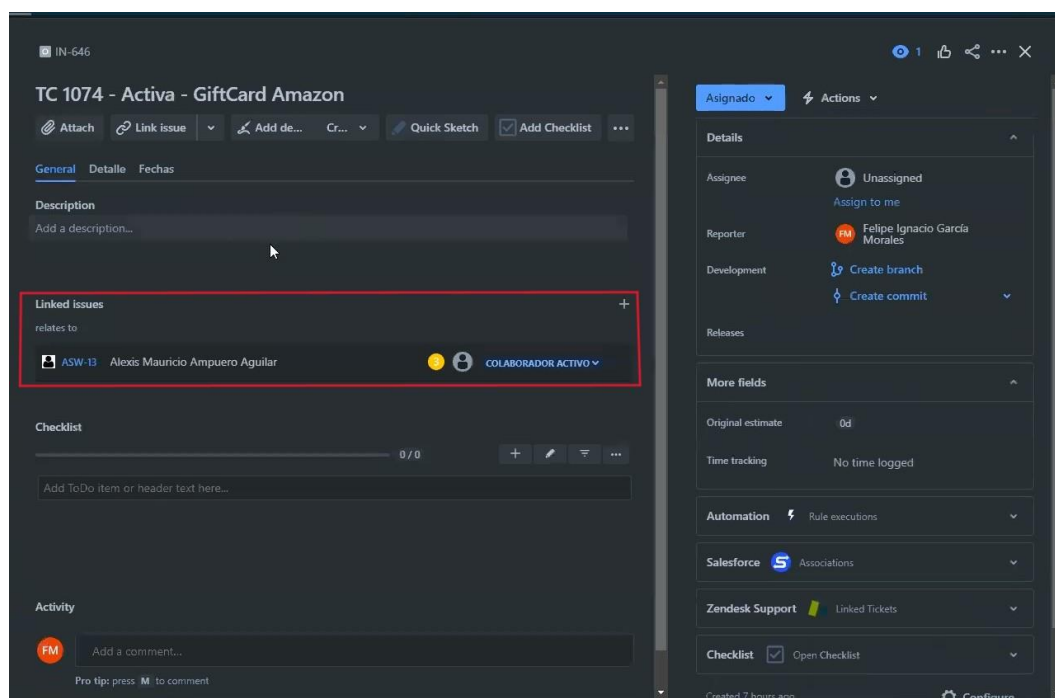


Figura 3.1.7.2.2 Vista de anexo de Tarjeta de crédito a Issue de Colaborador en ASW

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

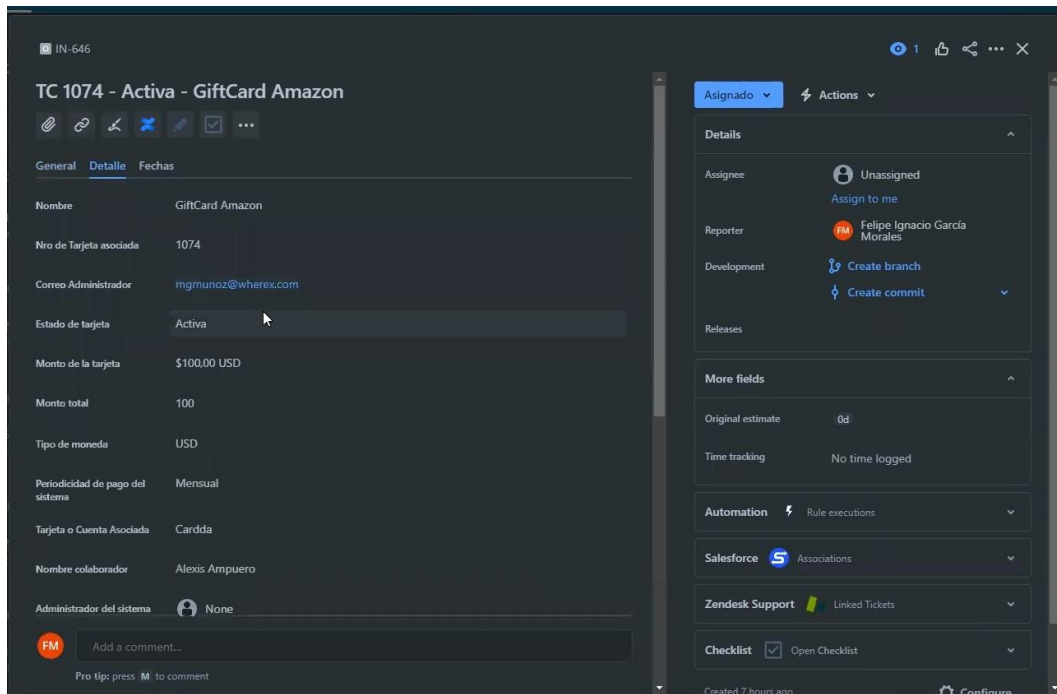


Figura 3.1.7.2.1 Vista de detalle de Tarjeta de crédito

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

5. Capítulo V: Estudio Empírico y Resultados

5.1. Análisis de resultados

A partir del proceso anterior, se llega a la última etapa de la metodología planteada, con la intención de lograr concentrar el análisis de los resultados, cuales fueron los cambios, el impacto que causó para la gestión de cuentas y como beneficia al equipo de Sysadmin.

5.1.1. Etapa V: Resultados y Mejoras:

Para este apartado, se verifica el correcto funcionamiento del proyecto “ASW”, que a partir de una solicitud de TA Plan, permite que todo el proceso funcione de manera independiente, gestionando la interacción con el equipo de Sysadmin para integración y eliminación de cuentas.

5.1.1.1. Nuevo Flujo de On Boarding:

El proceso comienza con la modificación del campo "Nombre de la persona seleccionada". Una vez completado este campo, se genera una incidencia en "ASW" y en el proyecto MVP. Se copian todos los campos definidos, incluyendo área, líder directo, tipo de contrato, cargo, fecha de ingreso y fecha de término de contrato. Simultáneamente, un bot designado como "Onboardin-eitor" envía una notificación al canal de Slack denominado "Atención Sysadmin", informando sobre la nueva persona que ingresará a la empresa. A partir de este punto, el equipo de sysadmins se encarga de distribuir las incidencias para crear las credenciales y gestionar los equipos necesarios para el día del ingreso, así como de recibir a la persona.

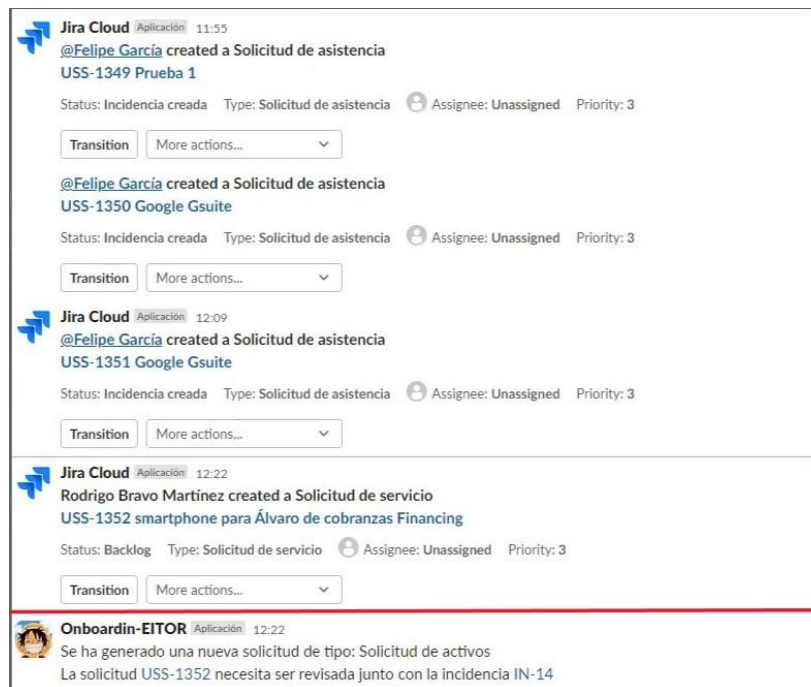


Figura 5.1.1.1.1 Evidencia 1 de Onboardin Eitor en pruebas

Fuente: Espacio de trabajo en Slack.

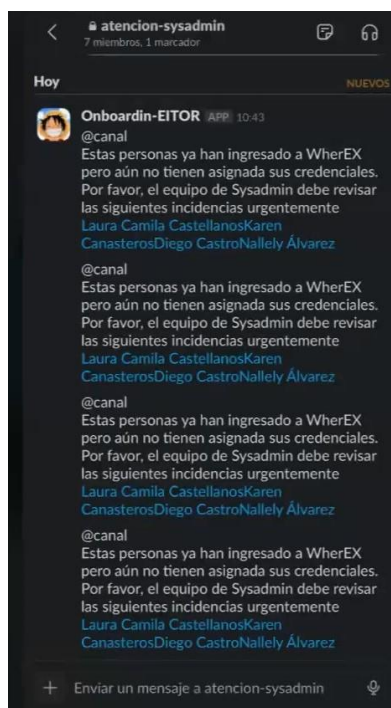


Figura 5.1.1.1.2 Evidencia 2 de Onboardin Eitor

Fuente: Espacio de trabajo en Slack.

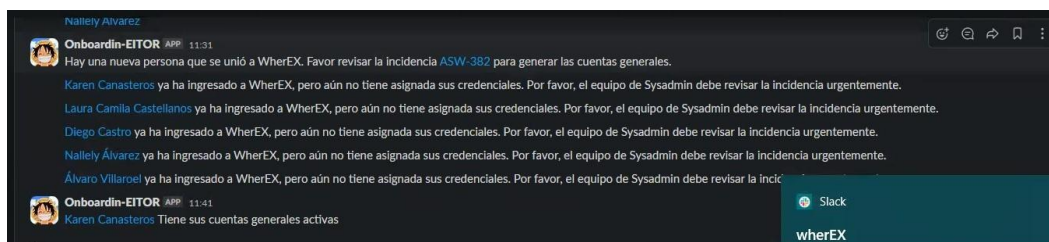


Figura 5.1.1.1.3 Evidencia 3 de Onboardin Eitor pruebas finales

Fuente: Espacio de trabajo en Slack.

Cuando se asignan los equipos desde el proyecto Inventario, estos se vinculan a la incidencia de la persona correspondiente para mantener un registro de los activos asignados (*Figura 5.1.1.1.5*), y también se adjunta el Acuerdo de No Divulgación (NDA, por sus siglas en inglés) definido por HR-Ops. Una vez que el sysadmin haya creado todas las credenciales necesarias, trasladará la incidencia a la categoría de "Colaborador activo" o "Practicante", según corresponda, y enviará un correo electrónico al líder correspondiente informando sobre las cuentas activadas (*Figura 5.1.1.1.7*). Con esto se completa el flujo del proceso. Es importante destacar que cada vez que se habilita una nueva cuenta, la cantidad de usuarios del sistema seleccionado se actualizará automáticamente, permitiendo así un registro y monitoreo completamente actualizados (*Figura 5.1.1.1.8*).

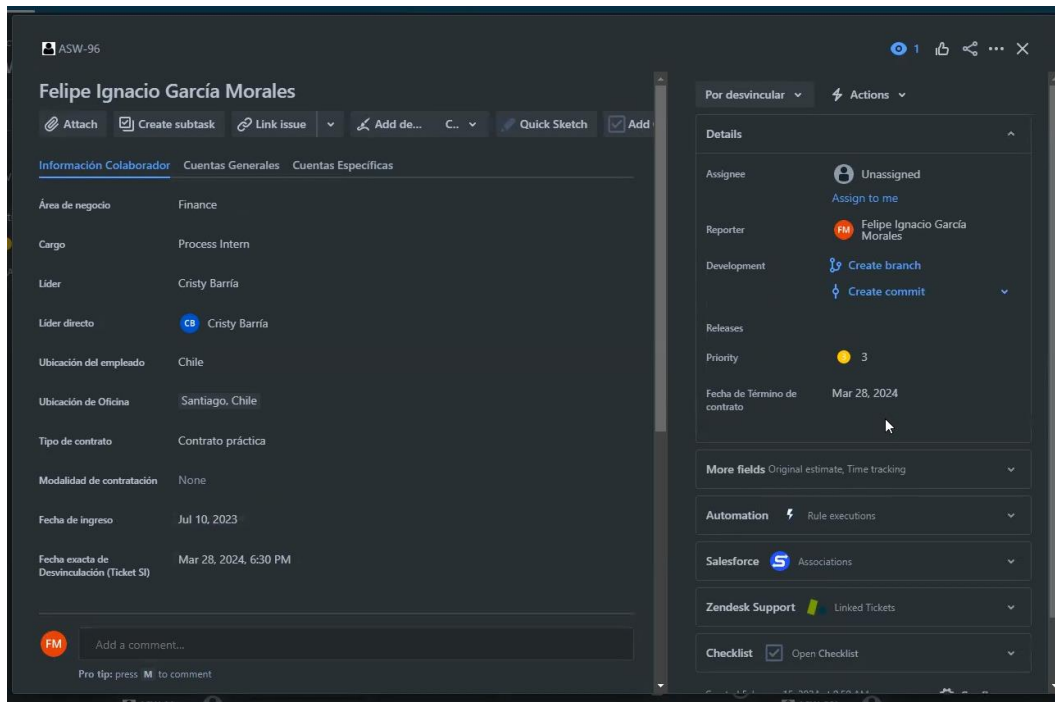


Figura 5.1.1.1.4 Vista de Issue Colaborador información personal

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

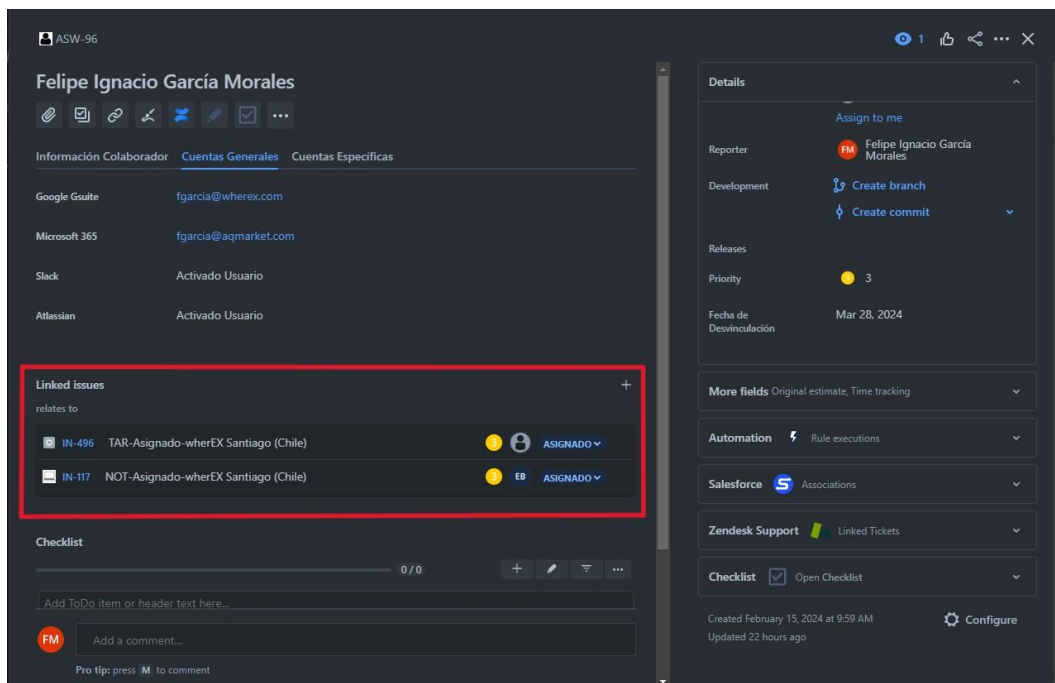


Figura 5.1.1.1.5 Vista de cuentas generales de Issue y activos anexados desde "Inventarios"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

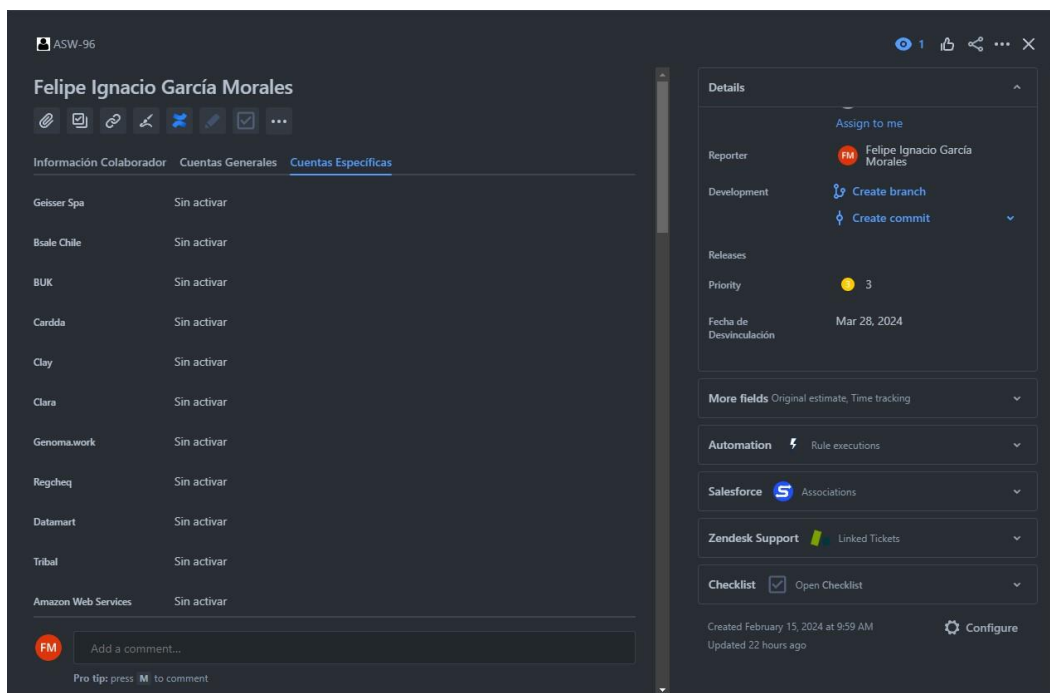


Figura 5.1.1.1.6 Vista de ejemplo de Cuentas específicas de Issue Colaborador

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

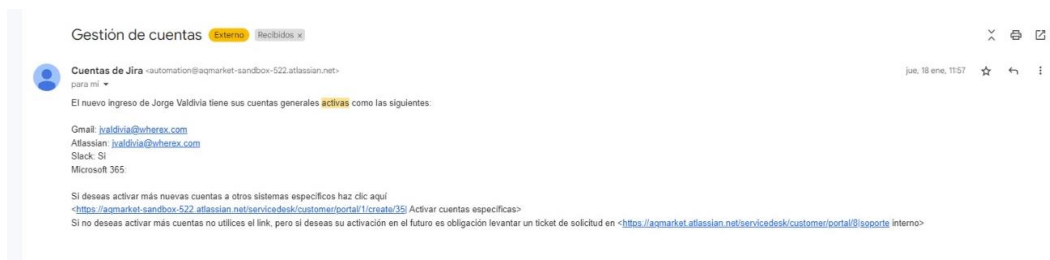


Figura 5.1.1.1.7 Correo enviado a líder sobre credenciales creadas

Fuente: Espacio de trabajo en Gmail.

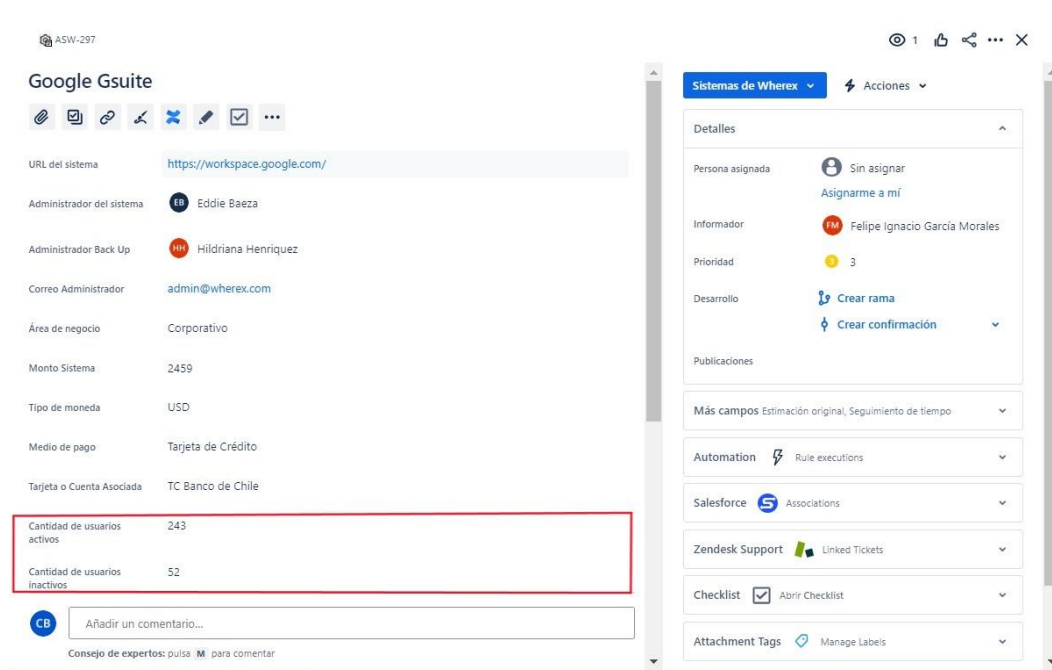


Figura 5.1.1.1.8 Vista de Issue Sistema ASW y contador de usuarios

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

5.1.1.2. Nuevo Flujo Off Boarding

Quando se procede a desvincular a una persona, el líder debe generar un ticket en Internal Support (USS). Este ticket, a su vez, genera una nueva alerta a través del bot "OffboardBot" (**Figura 5.1.1.2.1**) en el canal "Off Boarding", donde se registran todas las personas necesarias para el proceso de salida de un colaborador. Esta alerta indica la fecha de salida, cambia el estado de la incidencia a "Por desvincular" y notifica los equipos y otros activos asignados al colaborador para que el encargado pueda proceder con su recuperación (*Figura 5.1.1.2.3 y Figura 5.1.1.2.4*).

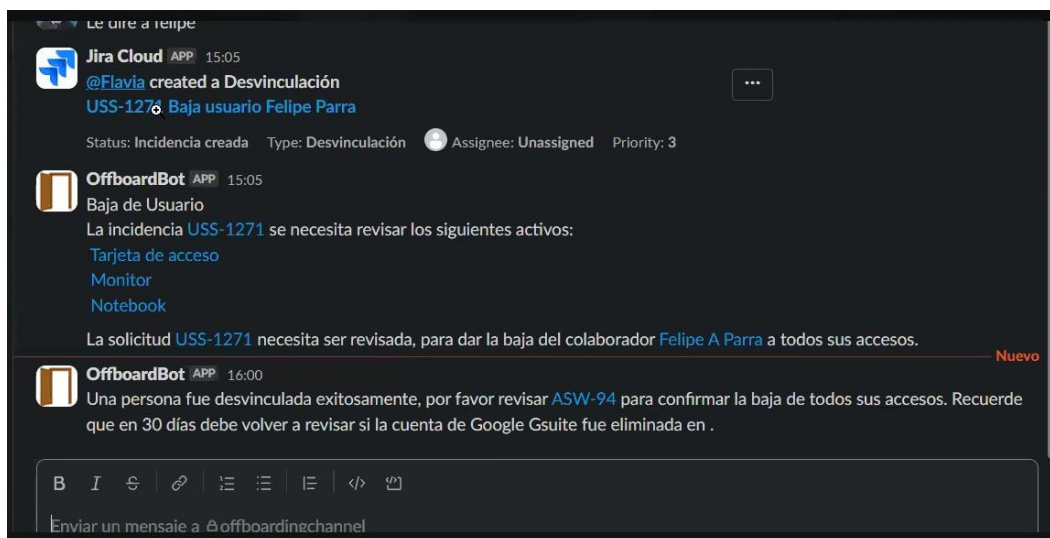


Figura 5.1.1.2.1 Mensaje de OffboardBot

Fuente: Espacio de trabajo en Slack.

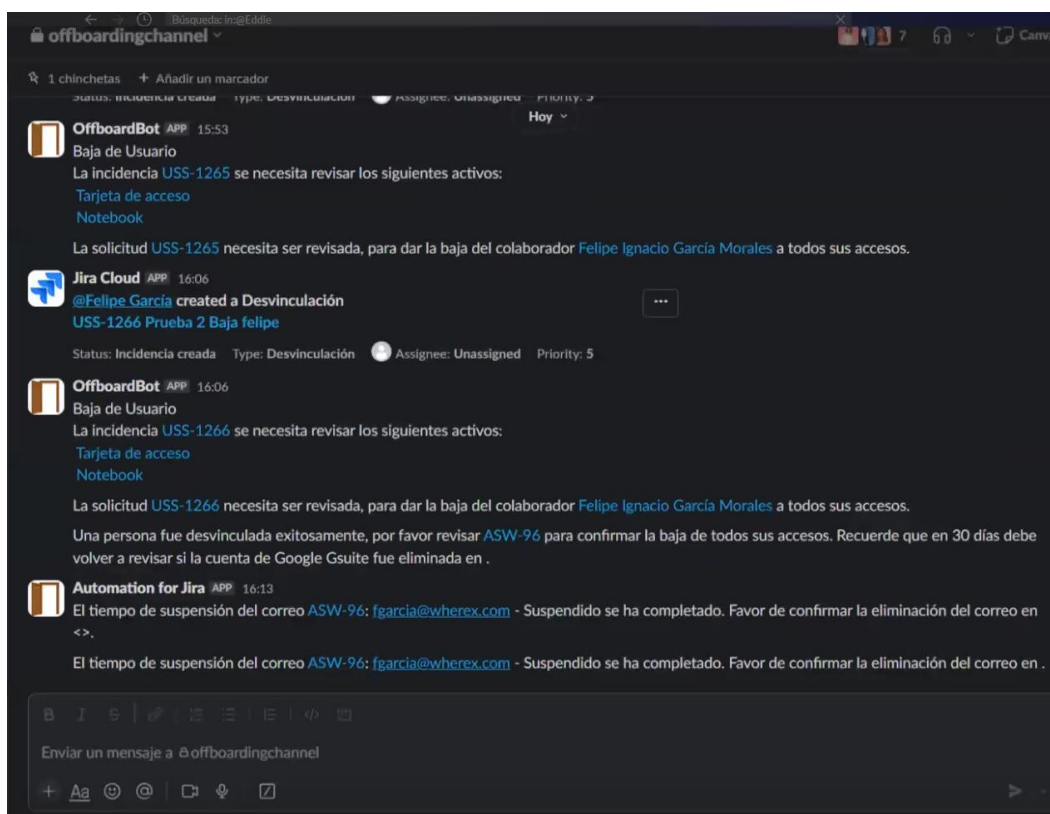


Figura 5.1.1.2.2 Evidencia 2 de Mensajes de OffboardBot

Fuente: Espacio de trabajo en Slack.

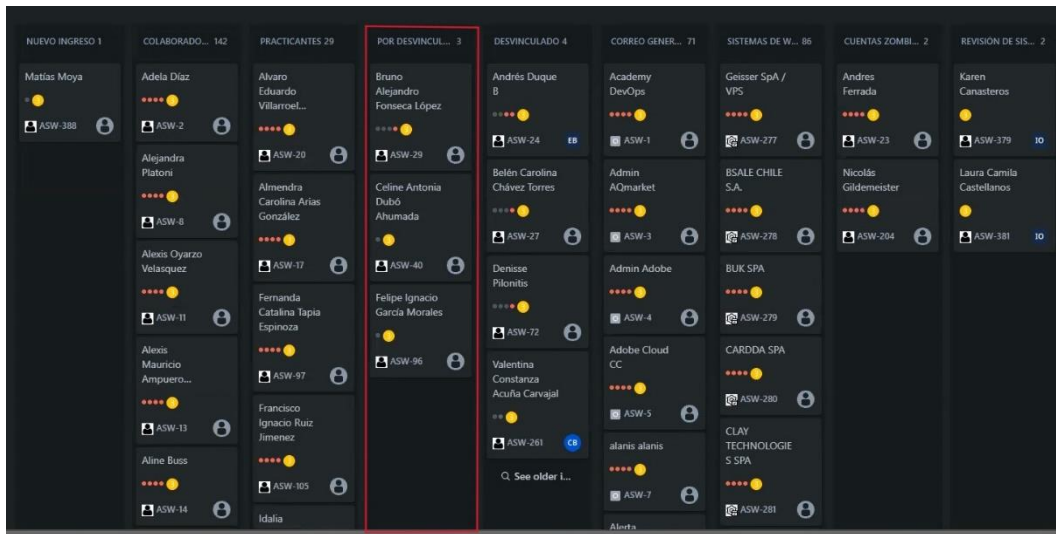


Figura 5.1.1.2.3 Vista de Status "Por desvincular"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

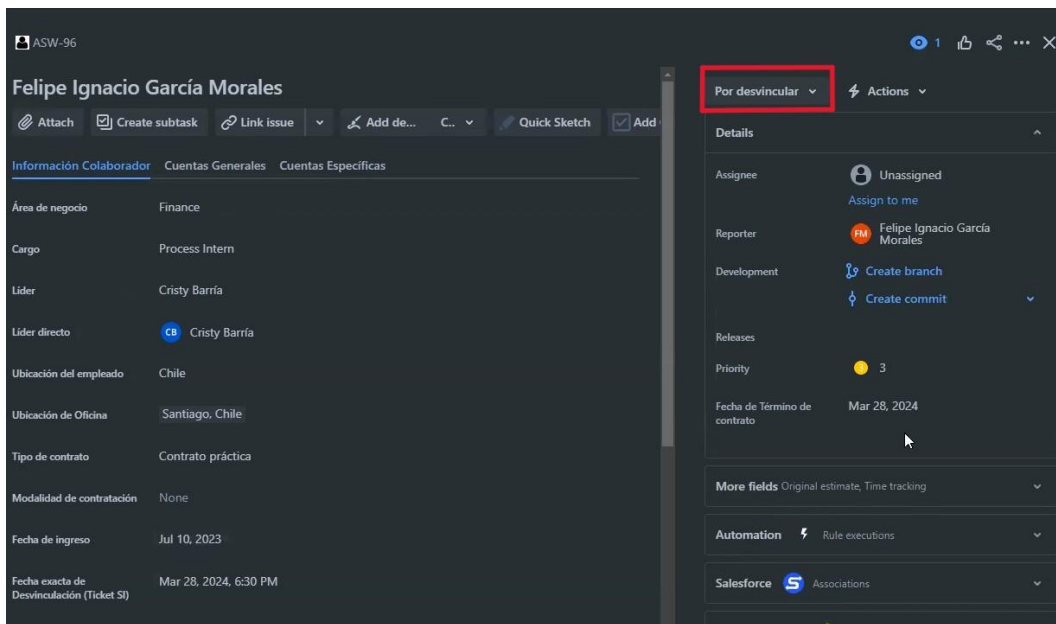


Figura 5.1.1.2.4 Selección de Status "Por desvincular" en Issue

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

Por otro lado, el Sysadmin debe llevar a cabo la desactivación de todos los accesos del colaborador, desmarcando las casillas correspondientes a los sistemas activos y seleccionando la opción "Desactivado". En el caso de que el colaborador esté asociado a un proyecto

importante o posea información sensible en su cuenta de Google Workspace, esta cuenta pasará al modo "suspendido", lo que indica al líder la necesidad de iniciar el proceso de recuperación. Transcurridos 30 días, se enviará una notificación adicional informando que la cuenta será eliminada.

Una vez que el Sysadmin haya completado la desactivación de todas las cuentas, el estado de la incidencia cambiará a "Desvinculado", finalizando así el flujo del proceso (Figura 5.1.1.2.5). Es importante destacar que, gracias a las automatizaciones implementadas, las cantidades de usuarios se actualizarán automáticamente al deshabilitar las casillas, lo que garantiza un control preciso de todos los sistemas.

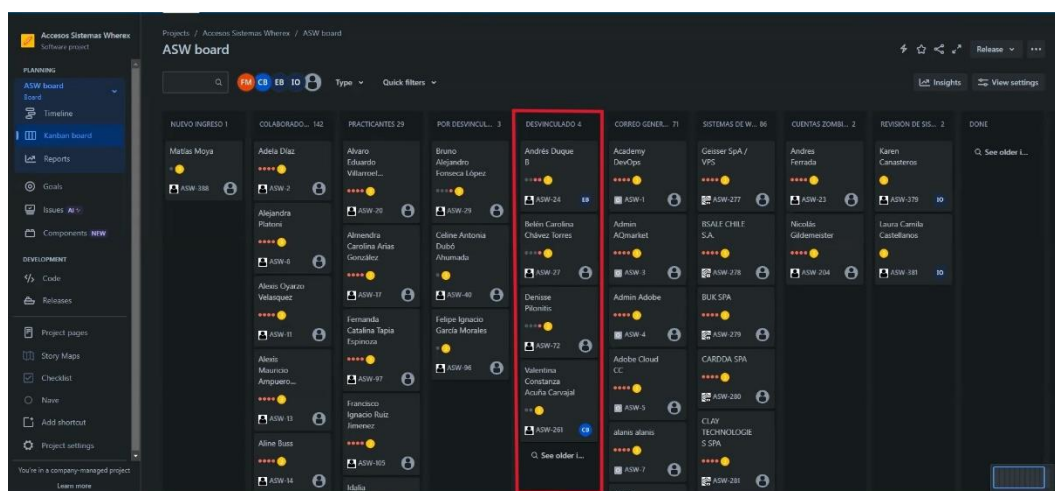


Figura 5.1.1.2.5 Vista de Status "Desvinculado"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

5.1.1.3. Comparación entre los diferentes flujos:

Tras analizar el flujo completo de "ASW", se demuestran que los resultados son satisfactorios, ya que se observa el correcto funcionamiento de las alertas y los procesos asociados a cada estado. Este hallazgo permite establecer una comparación entre los flujos de

los procesos de incorporación (On Boarding) y desvinculación (Off Boarding).

Flujo del proceso	Antes	Ahora
On Boarding	El proceso anteriormente implementado se basaba en un formulario alojado en Google Forms, desde donde se generaban recordatorios al personal de People mediante Slack. En este proceso, la activación de las cuentas se llevaba a cabo el mismo día del ingreso del colaborador, lo que implicaba que la responsabilidad recaía únicamente en un encargado de Sysadmin. Este encargado debía gestionar tanto la activación de las credenciales como la preparación de los equipos necesarios, lo que podría resultar en una falta de previsión al no tenerlos listos para cuando el colaborador llegara.	El proceso actualmente gestionado por Jira en el Portal de TA plan permite notificar al equipo de Sysadmin en el momento de la selección de una persona. Esta funcionalidad proporciona el tiempo necesario para que el equipo pueda distribuir cada ingreso a los integrantes correspondientes, al mismo tiempo que visualiza la ficha del nuevo colaborador, su área, líder y fecha de ingreso. Además, este proceso facilita la activación de las credenciales y la gestión anticipada de los equipos necesarios, garantizando así que estén preparados para el ingreso del colaborador.
Gestión de cuentas	El proceso anteriormente gestionado mediante una solicitud a través de un mensaje en Slack, el cual, carecía de	La activación de cuentas se gestiona a través de una solicitud dentro del portal de Internal

	un registro de la persona que solicitaba el acceso. Además, los accesos se registraban en una hoja de cálculo de Google, lo que requería una interacción manual y dejaba el proceso vulnerable a inconvenientes. Esta metodología resultaba engorrosa en caso de surgir algún problema y no se actualizaba automáticamente en caso de eliminar una cuenta.	Support (USS), lo que permite adjuntar la solicitud a la incidencia de la persona que requiere activar la cuenta. Además, al activar el usuario, se puede habilitar el campo correspondiente al sistema activado y al perfil del usuario. En el caso de solicitar la baja, también es posible marcar el campo del sistema como "Desactivado", lo que facilita el control de la cantidad de usuarios por plataforma.
Gestión de Sistemas	Los sistemas se almacenaban en Google Sheets, lo que implicaba un proceso manual y engorroso, sin conocer si la plataforma era utilizada. Además, no se tenía información sobre el administrador de la plataforma ni la cantidad de usuarios asociados al sistema. Esto generaba un desperdicio de recursos, ya que representaba un costo adicional por un sistema ineficiente.	Los sistemas se registran dentro del proyecto ASW, incorporando todas las características requeridas de la plataforma. Además, mediante automatizaciones, se lleva un registro de la cantidad de usuarios que tienen acceso a la plataforma. En caso de ser necesario realizar la baja de un sistema, esto puede realizarse a través de una solicitud desde Internal Support. Esta acción alerta

		tanto al equipo de Sysadmin como al equipo de Accounting, quienes se encargan de deshabilitar el pago asociado a la tarjeta correspondiente.
Off Boarding	El aviso de salida de un colaborador solía enviarse como un mensaje de Slack el mismo día de su salida, pero este proceso carecía de información detallada sobre todos los accesos que el colaborador poseía. Únicamente se tenía certeza de que la baja de sus cuentas de Google Workspace y Microsoft impedía el acceso desde otros dispositivos electrónicos. Sin embargo, al desconocer las plataformas específicas que el colaborador utilizaba, existía el riesgo de incurrir en gastos innecesarios al mantener cuentas de licencia de pago activas. Además, este método no proporcionaba el tiempo necesario para realizar la recuperación de equipos, por no conocer que tipos de activos	Ahora, los avisos de salida de colaboradores se gestionan a través de solicitudes en Internal Support, las cuales se asocian a la incidencia de la persona correspondiente. Este enfoque permite conocer todas las plataformas a las que el colaborador tenía acceso, facilitando la tarea de dar de baja todas las cuentas que pudieran contener información sensible o requerir pagos. Además, este método proporciona el tiempo necesario para que el equipo de Sysadmin pueda gestionar adecuadamente la recuperación de activos. Gracias a la vinculación de los equipos con el inventario de Jira, se sabe exactamente cuáles

	(computador, teléfono, monitor o tarjeta) poseía el colaborador.	activos debe recuperar, lo que mejora la eficiencia del proceso.
--	--	--

Tabla 1 Comparación de procesos

Fuente: Elaboración propia.

5.1.1.4. Principales indicadores de resultados obtenidos.

Según los resultados esperados, se obtienen los siguientes indicadores:

- **Control Integral de Sistemas y Monitoreo de Accesos:** Implementación de un sistema de control integral de los sistemas, con monitoreo constante de los usuarios y sus respectivos accesos.
- **Mejora de la Eficacia del Monitoreo de Sistemas:** mejora del 300% en la eficacia del control de sistemas. Se sustituirían los monitoreos trimestrales por frecuencias mensuales o incluso semanales, facilitando la detección temprana de posibles problemas o vulnerabilidades.
- **Gestión de Tarjetas de Crédito Asociadas a Colaboradores:** control de las tarjetas de crédito asociadas a los colaboradores para evitar pagos indebidos o pérdidas económicas por licencias no utilizadas en plataformas.
- **Reducción de Costos por Usuarios Inactivos:** disminución de costos o pérdidas financieras por cobros adicionales de excolaboradores o cuentas en desuso. Este caso se ilustra mediante la reducción de aproximadamente 2000 USD dentro de la plataforma Atlassian, donde se revocaron permisos y licencias de los espacios (Confluence, Jira Software y otros) a usuarios que no hacían uso de la plataforma, lo cual ocasionaba un gasto adicional.

- **Resguardo de Activos de Información de Colaboradores:** protección de los activos de información de los colaboradores ante posibles problemas o accesos no autorizados a las cuentas.
- **Agilización de Procesos de Ingreso y Salida de Colaboradores:** rapidez y mejora en los procesos de ingreso y salida de colaboradores para optimizar la gestión de equipos y prevenir pérdidas o daños materiales que puedan requerir gastos adicionales para su reposición.
- **Promoción de Conciencia sobre el Uso de Activos de Información:** promover la conciencia sobre el uso adecuado de activos de información, equipos y sistemas dentro de la empresa, adaptándose a las normativas y políticas establecidas por el Sistema de Gestión de Seguridad de la Información (SGSI), y fomentando buenas prácticas en WherEX.

5.2. Validación o verificación del método propuesto

La metodología empleada puede ser validada mediante el correcto funcionamiento del proyecto, lo que evidencia que los resultados obtenidos son consistentes con las expectativas. Además, la comparación con otras metodologías estudiadas indica que el proyecto tiene el potencial de ser eficaz, ya que ofrece diversas oportunidades de mejora. Sin embargo, para una verificación más precisa, se puede generar un cuadro que muestre los resultados obtenidos en relación con las brechas identificadas.

Brecha detectada	Resultado de solución propuesta
Falla en aviso de nuevo ingreso a equipo de Sysadmin	Ahora, cada vez que se realice una selección del personal, se generará automáticamente una alerta al equipo de Sysadmin, sin necesidad de dirigirse al área de People. Esto permitirá que el equipo pueda preparar tanto los equipos como las credenciales necesarias para el día de ingreso del nuevo colaborador de manera oportuna y eficiente.
Activación de cuentas a sistemas no autorizados ni notificados al equipo de Sysadmin	La administración recae principalmente en el equipo de Sysadmin y en el de gobernanza de sistemas. Además, la propiedad de cada plataforma también está a cargo de estos equipos. Por lo tanto, para solicitar la activación de una nueva cuenta, es necesario levantar una solicitud, siguiendo un flujo continuo y manteniendo un registro de qué persona debe activar la nueva cuenta y qué acceso tiene.
Monitoreo de Sistemas por medios de Google Sheets	Ahora es posible medir el uso de los sistemas, tanto a través de las automatizaciones de conteo de usuarios como del monitoreo mediante el panel creado en Jira denominado "Panel de ASW". Este panel proporciona toda la información relevante de cada plataforma y se actualiza automáticamente. Además, es posible gestionar los sistemas mediante la conexión a Power BI, que puede ofrecer indicadores más precisos y resultados acordes a los requerimientos. Esto incluye la capacidad de enviar informes a los administradores de sistemas para que verifiquen la integridad de sus plataformas y fomentar una cultura de uso adecuado de las mismas.
No avisar sobre la salida del colaborador	Para activar el proceso de Off Boarding, es necesario presentar una solicitud obligatoria de "Baja de Cuentas", en el portal de Internal

	Support (USS). Esta solicitud desencadenará todo el procedimiento para que el equipo de Sysadmin pueda desactivar todos los accesos del usuario y, si es necesario, realizar un respaldo de la información. Asimismo, este proceso permite al equipo de Sysadmin recuperar los equipos que fueron asignados al colaborador, facilitando su posterior formateo y reasignación. Por último, este procedimiento permite al equipo de Sysadmin mantener actualizada la cantidad de colaboradores, incorporando los equipos disponibles en inventario en caso de nuevas compras o actualizaciones necesarias.
Cuentas de usuarios desvinculados con proyectos asociados	Cuando un colaborador sea desvinculado pero su cuenta permanezca activa, se enviarán alertas periódicas cada 7 días, tanto al líder correspondiente como al equipo de Sysadmin. Estas alertas servirán como recordatorio para que realicen el traspaso y respaldo de los proyectos asociados al colaborador desvinculado. Este enfoque proporciona un período de tiempo adecuado y fomenta la conciencia entre los líderes, permitiéndoles hacerse cargo de los activos del excolaborador. El objetivo es evitar posibles irregularidades en la empresa en caso de eliminación de las cuentas del colaborador, asegurando que la información y los proyectos asociados no se eliminen inadvertidamente.

Tabla 2 Soluciones de brechas identificadas

Fuente: Elaboración propia.

6. Capítulo IV: Conclusiones Generales

6.1. Hechos o resultados

En respuesta al complejo entorno enfrentado por la empresa y la identificación temprana de una brecha significativa, se decidió de manera directa implementar y desarrollar un sistema de gestión de identidad y acceso en colaboración con el equipo de Sysadmin. Esta acción fue tomada con el objetivo de mitigar el riesgo de pérdida o robo de información debido a posibles ataques dirigidos a usuarios de la empresa. Se reconoce la importancia de poseer un conocimiento detallado sobre los distintos accesos y plataformas en las que la empresa participa, así como la necesidad de distinguir los diversos flujos de información y asegurar su protección.

Desde la perspectiva presentada anteriormente, se puede afirmar que la implementación del proyecto ha sido exitosa en todos los aspectos, como se evidencia en la mitigación de las diversas brechas detectadas en la organización. Esta eficacia se refleja en la tabla X, donde se muestra la reducción de todo tipo de riesgos mediante la solución propuesta previamente. Además, se observa un cambio satisfactorio en los flujos de entrada y salida de colaboradores, lo que ha generado resultados acordes a las expectativas. Esto ha facilitado y organizado el acceso dentro de la empresa, así como el monitoreo de todos los sistemas a cargo del equipo de Sysadmin.

Se implementó un rediseño específico en el proceso de entrada de colaboradores, donde todo el procedimiento está conectado a través de Jira y gestionado mediante automatizaciones. Desde la solicitud inicial en TA plan, el equipo de Sysadmin puede gestionar adecuadamente los equipos y accesos asignados al nuevo colaborador anticipadamente y de manera correcta para su llegada, como se muestra en la imagen X.

Además, se pueden determinar los gastos necesarios en caso de activar una cuenta paga o adquirir un nuevo equipo.

También se realizaron modificaciones en el proceso de salida de los colaboradores, asegurando que se registre cada acceso que poseía el excolaborador y confirmando la eliminación de sus cuentas, junto con el traslado y resguardo de la información contenida en sus accesos para proteger la integridad de los activos.

En cuanto al monitoreo de los accesos, se supervisó el uso de las diversas plataformas de la empresa, lo que permitió evaluar su efectividad para el buen funcionamiento de la organización. Se llevó a cabo un monitoreo de usuarios de manera semanal, lo que incrementó en un 300% la eficacia del control de sistemas. Esto permitió eliminar los accesos de los excolaboradores y gestionar todos los activos de información dentro de la plataforma, visualizando la cantidad de usuarios por plataforma y el área a la que pertenecían.

En términos económico-financieros, mediante la visualización de la cantidad de usuarios y el conocimiento del tipo de plataforma que utilizaban, se logró controlar los costos asociados a cuentas inactivas o de excolaboradores que seguían activas. Estas cuentas generaban un gasto adicional que afectaba a la organización, por lo que el monitoreo del IAM implementado evitó este desperdicio de recursos y controló la utilización de las plataformas pagas, como el caso evidenciado de Atlassian.

En conclusión, se logra asegurar un control completo de los accesos de los usuarios, ya sea en términos económicos o en relación con el conocimiento de las tarjetas y medios de pago que los usuarios poseen. Se tiene conocimiento de todos los sistemas que la empresa utiliza, quiénes los administran o utilizan, qué información contienen y si está protegida o no. Finalmente, se garantiza la desactivación de todos los accesos de las personas que fueron

desvinculadas para prevenir riesgos de usurpación de datos o ataques dentro de la organización por cuentas sin supervisión.

6.2. Con relación a los Objetivos de la Investigación

En base al objetivo general establecido, se evidencia la ejecución completa y exitosa del sistema propuesto para la gestión de identidad y accesos en las plataformas de WherEX. Este sistema proporciona funciones clave para la gestión, control, eficiencia y seguridad necesarias en la actualidad para resguardar los diversos activos de información de la empresa. Además, su flexibilidad permite adaptaciones futuras para mantenerse al día con los avances tecnológicos y las necesidades cambiantes del entorno empresarial.

En relación con los objetivos específicos planteados, se destaca la efectiva reducción del riesgo de exposición de datos gracias al adecuado monitoreo y gestión de los accesos a las plataformas de la empresa. Este enfoque fortalece la seguridad de los usuarios y la información que manejan. Además, se ha logrado simplificar y optimizar los flujos de On Boarding y Off Boarding, permitiendo al equipo de Sysadmin realizar estas tareas de manera más eficiente y funcional.

El tercer objetivo específico ha contribuido significativamente a la optimización de los recursos financieros mediante la reducción del gasto mensual en cuentas de usuarios desvinculados en plataformas pagas. Esto se logra mediante un control más efectivo de las cuentas inactivas o sin supervisión, así como la evaluación de la viabilidad de las plataformas para determinar su utilidad continua.

Por último, gracias a las metodologías de Kanban y PDCA, se ha establecido un proceso continuo de mejora y avance tecnológico que permite a WherEX mantenerse actualizada y eficiente en sus operaciones. Estas metodologías facilitan la automatización y la

implementación de mejoras necesarias para un funcionamiento óptimo del sistema IAM.

6.3. Limitaciones

Durante la ejecución del proyecto, se identificaron varias limitaciones que influyeron en el proceso. Una de estas limitaciones fue la falta de interacción adecuada entre las diversas áreas involucradas. Se observó una comunicación insuficiente en los flujos de entrada y salida de personal, así como en la coordinación con la alta dirección para definir qué plataformas utilizar y cuáles cancelar.

Otra limitación significativa fue la falta de conocimiento y comprensión de la plataforma por parte de otras áreas. Esto dificultó que pudieran visualizar todas las funciones y características disponibles, lo que habría permitido mejorar los procesos de trabajo y simplificar las tareas mediante la implementación de automatizaciones.

6.4. Recomendaciones

En el contexto de mejoras continuas, resulta crucial continuar aplicando un análisis del ciclo de Deming. Este enfoque es esencial para identificar nuevas oportunidades que impulsen una ejecución más eficiente de las tareas repetitivas presentes en la empresa. La implementación de automatizaciones se presenta como un medio para mejorar y modernizar los métodos de trabajo. Además, es de vital importancia la integración de nuevos aspectos procedentes de distintas áreas, fomentando así una colaboración conjunta y simplificada entre ellas.

6.5. Futuras Líneas de Investigación

En el ámbito de la gestión de identidades y accesos, el enfoque predominante se centra en el control del uso de la información por parte de los colaboradores. No obstante, se

considera importante continuar explorando el proceso para mejorar la gestión económica, posiblemente integrándola con los procesos financieros de la empresa. Esta integración permitiría una gestión más efectiva de los recursos financieros de la organización, garantizando un uso adecuado del dinero en aspectos tangibles e intangibles, como equipos, personal y otros aspectos de interés para la empresa.

Asimismo, se está trabajando en la implementación de una interacción automatizada para la eliminación de información redundante, en colaboración con el equipo de ingeniería que está desarrollando un bot diseñado para facilitar esta tarea al equipo de Sysadmin. Esto no solo agilizará el trabajo del equipo, sino que también asegurará la protección adecuada de los activos de información de la empresa.

Finalmente, al considerar estas perspectivas, se observa un potencial prometedor para identificar diversas funciones y mejoras que optimicen los procesos de la empresa. Esto abre la puerta a un nuevo mundo de automatización y eficiencia laboral para todas las áreas implicadas.

7. Referencias bibliográficas

- Atlassian ASW. (2024). *Espacio de trabajo*. Obtenido de Jira: <<https://aqmarket.atlassian.net/browse/ASW>>
- Atlassian. (s.f.). *Jira Software Cloud resources*. Recuperado el 10 de Marzo de 2024, de Jira Software Support: <https://support.atlassian.com/jira-software-cloud/resources/>
- Atlassian Sandbox. (2024). *Sandbox*. Obtenido de Jira: <<https://aqmarket-sandbox-522.atlassian.net/jira>>
- Atlassian USS. (2024). *Portal Internal Support (USS)*. Obtenido de <<https://aqmarket.atlassian.net/servicedesk/customer/portal/8>>
- Atlassian. (s.f.). *What are Sandboxes?* Recuperado el 6 de Marzo de 2024, de Atlassian Support : <<https://support.atlassian.com/organization-administration/docs/what-are-sandboxes/>>
- Atlassian. (s.f.). *What is a Jira Software project?* Recuperado el 6 de Marzo de 2024, de Jira Software Support [en línea]: <<https://support.atlassian.com/jira-software-cloud/docs/what-is-a-jira-software-project/>>
- Atlassian. (s.f.). *What is advanced search in Jira Cloud?* Recuperado el 6 de Marzo de 2024, de Jira Software Support: <<https://support.atlassian.com/jira-software-cloud/docs/what-is-advanced-search-in-jira-cloud/>>
- Atlassian. (s.f.). *What is Jira Service Management?* Recuperado el 6 de Marzo de 2024, de Jira Service Management Support [en línea]: <<https://support.atlassian.com/jira-service-management-cloud/docs/what-is-jira-service-management/>>
- Badilla Lagos, S. (2023). *Gestión y control de indicadores de abastecimiento en locales extremos en Walmart Chile S.A.* Memoria para optar a título de ingeniero, Universidad Técnica Federico Santa María [Documento Compartido], Industrias, Santiago de Chile. Recuperado el 6 de Marzo de 2024
- Baldecchi Q., R. (4 de Sep de 2014). *Implementación efectiva de un SGSI*. Recuperado el 16 de Enero de 2024, de Google Académico [en línea]: <<http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%20%20CIGRAS%20ISO%2027001%20-%20rbq.pdf>>
- Barker, W. C., Scarfone, K., Fisher, W., & Souppaya, M. (Febrero de 2022). Gestión de riesgo de Ransomware: un perfil de marco de ciberseguridad. *NIST(8374)*, 31.

doi:<<https://doi.org/10.6028/NIST.IR.8374.spa>>

- Barría Barrientos, C. A. (2021). *Actualización del sistema de gestión de seguridad de la información basado en la norma ISO27001:2013 en la empresa CCS SPA*. Universidad de la frontera, FACULTAD DE INGENIERÍA Y CIENCIAS. Temuco: Universidad de la frontera. Recuperado el 20 de Noviembre de 2023
- Barría Barrientos, C. A. (2021). *Actualización del sistema de gestión de seguridad de la información basado en la norma ISO27001:2013 en la empresa CCS SPA*. Universidad de la frontera, FACULTAD DE INGENIERÍA Y CIENCIAS. Temuco: Universidad de la frontera [Documento compartido]. Recuperado el 20 de Noviembre de 2023
- Barría Barrientos, C. A. (1 de Marzo de 2023). Capacitación SGSI On Boarding Wherex [Documento compartido]. Puerto Varas, Chile. Recuperado el 5 de Marzo de 2024
- Bisbé, R. L. (2021). *Offboarding*. Editorial Libros. com. Recuperado el 4 de Abril de 2024, de <https://books.google.com.mx/books?hl=es&lr=&id=7QMueAAAQBAJ&oi=fnd&pg=PT3&dq=que+es+el+Off+Boarding&ots=DaEgLQhiUj&sig=Ey8b3SW-kZ-N_hblB7tEvJslbss#v=onepage&q&f=false>
- Castro, F. S. (2020). *Gestión de identidades y accesos unificados*. Tesis de Grado, Universidad Nacional de La Plata, Facultad de Informática. Recuperado el 1 de Marzo de 2024, de <<http://sedici.unlp.edu.ar/handle/10915/118390>>
- Fisher, J., Koning, D., & Ludwigsen, A. (2013). *Utilizing Atlassian JIRA for large-scale software development management*. San Francisco, CA, United States: r Lawrence Livermore National Security. Recuperado el 5 de Marzo de 2024, de <<https://www.osti.gov/servlets/purl/1097750>>
- García Morales, F. I. (2023). *Informe de Práctica Profesional WherEX [Elaboración propia]*. [Práctica Profesional], Santiago. Recuperado el 1 de Marzo de 2024
- Gatica Herrera, V. M. (2015). *Aplicación de una metodología Kanban en el área de Operaciones IT*. Tesis de Pregrado, Universidad Técnica Federico Santa María, Informática, Valparaíso. Recuperado el 6 de Marzo de 2024, de <<http://hdl.handle.net/11673/12850>>
- Guaña Moya, E. J., Sánchez Zumba, A., Chérrez Vintimilla, P., Chulde Obando, L., Jaramillo Flores, P., & Pillajo Rea, C. (16 de Agosto de 2022). *Ataques informáticos más comunes en el mundo*. doi:<http://190.57.147.202:90/xmlui/handle/123456789/3445>
- Guerra Gutarra, R. G. (Agosto de 2020). Kaizen en la gestión de entrega de una empresa

- automotriz aplicando la metodología PDCA. *Pontificia Universidad Católica del Perú [en línea]*, 1-20. Recuperado el 6 de Marzo de 2024, de <https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/16830>
- Holguín Sánchez, B. (2021). *Metodología PDCA y su incidencia en la gestión de proyectos de la empresa Proemco SAC*. Tesis de grado académico, Universidad César Vallejo, Lima. Recuperado el 6 de Marzo de 2024, de <https://repositorio.ucv.edu.pe/handle/20.500.12692/57545>
- Hurtado, J. C. (31 de Enero de 2023). WherEX 101: Entendiendo el modelo de negocio y algunos términos asociados. [Diapositivas]. Puerto Varas, Chile. Recuperado el 1 de Marzo de 2024
- International Organization for Standardization (2013a). (2013). *Norma Chilena NCh-ISO 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos*. (Segunda ed.). Santiago de Chile [Documento compartido]. Recuperado el 1 de Marzo de 2024
- International Organization for Standardization (2013b). (2013). *Norma Chilena NCh-ISO 27002:2013. Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información*. (Segunda ed.). Santiago de Chile [Documento Compartido]. Recuperado el 1 de Marzo de 2024
- Ladino A., M. I., Villa S., P. A., & López E., A. M. (Abril de 2011). FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. *Scientia Et Technica [en línea]*, XVII(47), 334-339. Recuperado el 16 de Enero de 2024, de <<https://www.redalyc.org/articulo.oa?id=84921327061>>
- Li, P. (2018). Issues and issue Types. En P. Li, R. Tripathi, N. Dasan, N. Borkar, J. Maliyekal, & S. Editing (Edits.), *Jira Software Essentials [en línea]* (2 ed., Vol. 1, pág. 98). Birmingham, Mumbai: Packt Publishing Ltd. Recuperado el 6 de Marzo de 2024, de <https://books.google.com.mx/books?hl=es&lr=&id=sSZKDwAAQBAJ&oi=fnd&pg=PP1&dq=jira+software&ots=sUkQIIaDDs&sig=RCx2gHsi1Iy5oI9_mkk9cNDjZ0g#v=onepage&q&f=false>
- Mieres, J. (2009). Ataques informáticos. *Evil Fingers*, 17. Recuperado el 1 de Marzo de 2024, de <https://www.evilmfingers.org/publications/white_AR/01_Atques_informaticos.pdf>
- Montoya, J., & Restrepo, Z. (9 de Abril de 2012). Gestión de identidades y control de acceso

- desde una perspectiva organizacional. *Ingenierías USBMed*, 3, 23-34. Recuperado el 1 de Marzo de 2024, de <<https://revistas.usb.edu.co/index.php/IngUSBmed/article/view/261>>
- Niño Morante, N. R. (2018). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque*. Tesis, Universidad Nacional Pedro Ruiz Gallo, Lambayeque. Recuperado el 16 de Enero de 2024, de <<https://repositorio.unprg.edu.pe/handle/20.500.12893/5935?show=full>>
- Pacheco, C. R. (2010). Implementación de autenticación de usuarios con múltiples credenciales. *Concurso de Trabajos Estudiantiles (EST 2010) - JAIIO 39 (UADE, 30 de agosto al 3 de septiembre de 2010) [en línea]* (págs. 854-865). Puerto Madryn: Sociedad Argentina de Informática e Investigación Operativa. Recuperado el 16 de Enero de 2024, de <<http://sedici.unlp.edu.ar/handle/10915/153090>>
- Pauta. (11 de Junio de 2018). *Cómo fue el hackeo al Banco de Chile*. Recuperado el 1 de Marzo de 2024, de Pauta100.5: <<https://www.pauta.cl/actualidad/2018/06/11/como-fue-el-hackeo-al-banco-de-chile.html>>
- Pauta. (18 de Marzo de 2019). *Chile fue el décimo país con más ciberataques en 2018*. Recuperado el 1 de Marzo de 2024, de Pauta 100.5: <<https://www.pauta.cl/entretencion/2019/03/18/chile-fue-el-decimo-pais-con-mas-ciberataques-en-2018.html>>
- Rosas Custodio, M. E. (2015). *Propuesta de Implementación del proceso de On Boarding como apoyo a la gestión del talento humano*. Obtención de grado de maestría, Universidad Panamericana, FACULTAD DE FILOSOFÍA Y CIENCIAS SOCIALES. Recuperado el 4 de Abril de 2024, de <<https://biblio.upmx.mx/tesis/150831.pdf>>
- Saavedra Rodríguez, Ó. (Marzo de 2023). *Teoría de Sistemas y Gestión*. Recuperado el 1 de Abril de 2024, de Aula USM: <<https://aula.usm.cl/>>
- Sacoto Mosquera, V. H. (2019). *Implementación De Un Esquema De Seguridad Informática Para Una Entidad Financiera, Con El Propósito De Mitigar Los Riesgos Que Podrían Presentarse A Causa De Ataques Cibernéticos, Internos O Externos Y Salvaguardar La Integridad De La Información*. Trabajo de Titulación de Magister, ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, FACULTAD DE INGENIERÍA EN

ELECTRICIDAD Y COMPUTACIÓN, Guayaquil. Recuperado el 10 de Abril de 2024, de <<http://www.dspace.espol.edu.ec/xmlui/handle/123456789/47048>>

Torres, M. J., De los Reyes, A., Espinoza, L., & Saquicela, V. (2017). Plataforma de Gestión de Identidad y Acceso Federado para la Universidad de Cuenca. *Séptima Conferencia de Directores de Tecnología de Información, TICAL 2017 Gestión de las TICs para la Investigación y la Colaboración*, (pág. 12). San José. Recuperado el 1 de Marzo de 2024, de <<https://dspace.redclara.net/bitstream/10786/1261/1/30-3-4Plataforma%20de%20Gesti%C3%B3n%20de%20Identidad%20y%20Acceso%20Federado%20para%20la%20Universidad%20de%20Cuenca.pdf>>

WherEX. (s.f.). Recuperado el 1 de Marzo de 2024, de WherEX: <<https://wherex.cl/>>

WherEX. (1 de Octubre de 2022). Job Description Sysadmin [Documento compartido]. Santiago, Chile. Recuperado el 5 de Marzo de 2024

8. Anexos

8.1. Anexo A: ¿Qué son el On Boarding y Off Boarding?

8.1.1. On Boarding

El Onboarding es el proceso de integración y bienvenida de nuevos colaboradores a una empresa. Este proceso abarca desde el momento en que el empleado es contratado hasta que se familiariza completamente con su rol, su equipo de trabajo y la cultura organizacional. Durante el Onboarding, se brinda al nuevo empleado toda la información, herramientas y recursos necesarios para que pueda desempeñar sus funciones de manera efectiva y contribuir al éxito de la organización. Esto incluye la realización de trámites administrativos, la entrega de equipos y materiales de trabajo, la capacitación sobre políticas y procedimientos internos, así como la presentación a colegas y la asignación de un mentor o buddy que lo oriente en sus primeros días. El objetivo del Onboarding es facilitar la integración del nuevo colaborador, promover su sentido de pertenencia y asegurar una transición exitosa hacia su nuevo rol dentro de la empresa. (Rosas Custodio, 2015)

8.1.2. Off Boarding

El Offboarding se refiere al proceso formal y estructurado que una organización lleva a cabo al finalizar la relación laboral de un empleado o practicante. Este proceso abarca todas las actividades necesarias para desvincular al individuo de la empresa de manera ordenada y eficiente. Incluye la gestión de varios aspectos, como la comunicación de la salida, la cancelación de accesos y credenciales, la devolución de activos de la empresa y la finalización de trámites administrativos (Bisbé, 2021). Dependiendo de las circunstancias de la salida (desvinculación urgente, renuncia voluntaria o término de contrato), el Offboarding puede variar en cuanto a la notificación previa, la realización de trámites y la entrega de activos.

8.2. Anexo B: Flujos de Trabajo

8.2.1. Off Boarding Mutuo Acuerdo

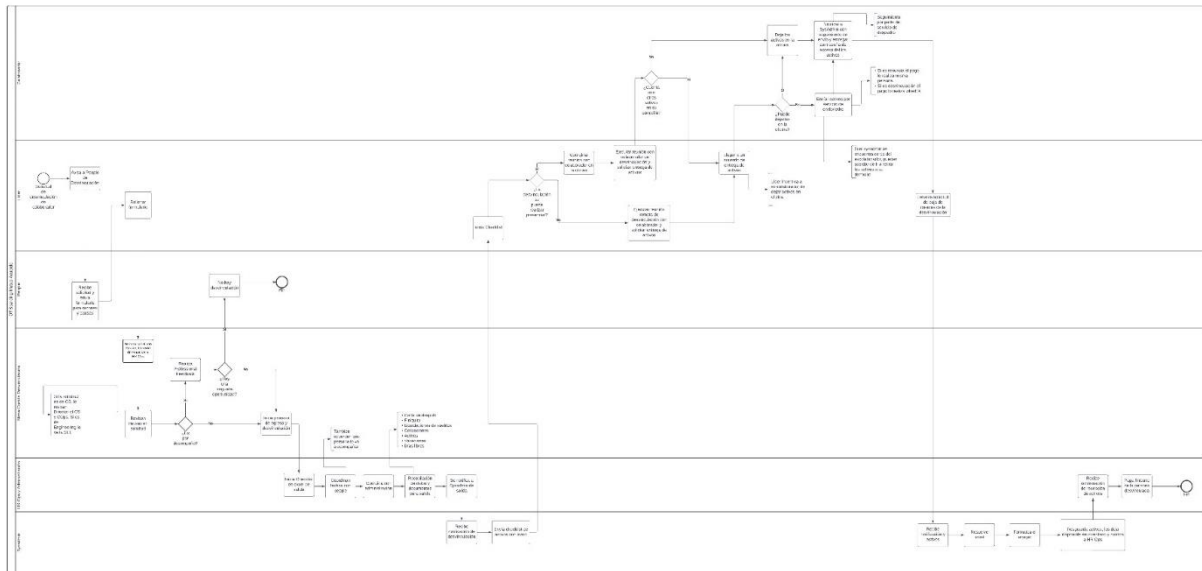


Figura 5.1.1.4.1 Diagrama de flujo Off Boarding Mutuo Acuerdo

Fuente: Elaboración propia.

8.2.2. Off Boarding: Renuncia Voluntaria

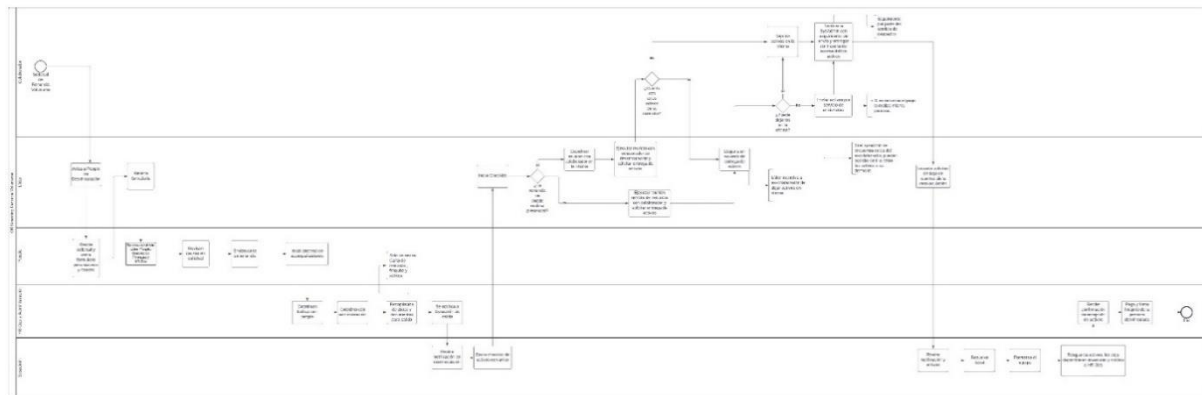


Figura 5.1.1.4.1 Diagrama de Flujo Off Boarding Renuncia Voluntaria

Fuente: Elaboración propia.

8.2.5. Flujo On Boarding “Cuentas Generales”

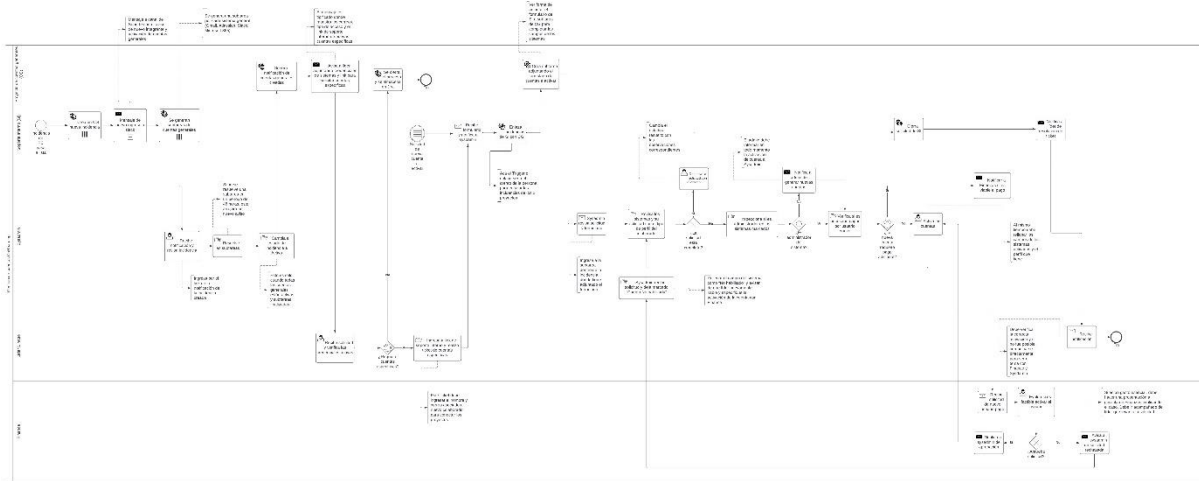


Figura 5.1.1.4.1 Flujo de On Boarding y gestión de cuentas según "CG"

Fuente: Elaboración propia.

8.2.6. Flujo de Off Boarding “Cuentas Generales”

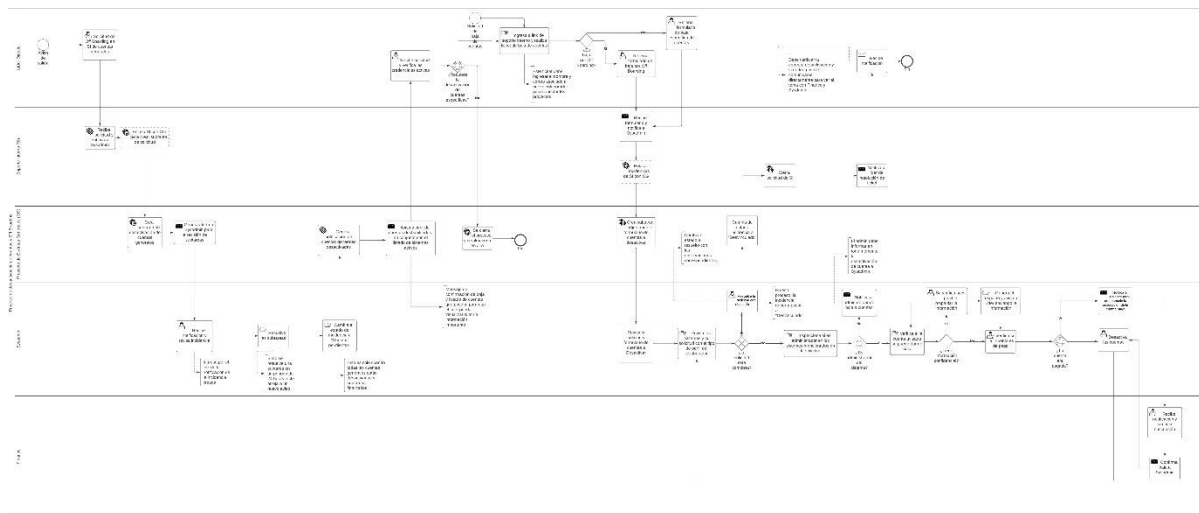


Figura 5.1.1.4.1 Flujo de Off Boarding Según "CG"

Fuente: Elaboración propia.

8.3. Anexo C: Glosario

1. **Activo de información:** es cualquier recurso valioso relacionado con el procesamiento, almacenamiento o transmisión de datos, como equipos informáticos o documentos, que tiene importancia para una organización.
2. **Ataque cibernético:** Intento malicioso de comprometer la seguridad de sistemas informáticos, redes o dispositivos electrónicos para robar información, causar daños o interrumpir operaciones.
3. **Benchmarks:** Puntos de referencia o estándares utilizados para evaluar y comparar el rendimiento o las prácticas.
4. **Brecha:** Vulnerabilidad o fallo en la seguridad de un sistema, red o aplicación que puede ser explotado por un atacante para obtener acceso no autorizado o comprometer la integridad de datos.
5. **CSV UTF-8:** Formato de archivo de valores separados por comas (CSV) que utiliza la codificación de caracteres UTF-8.
6. **Custom Field:** Campos personalizados que se pueden agregar en Jira para capturar información adicional.
7. **Dominio:** Nombre único que se utiliza para identificar una ubicación específica en Internet, como un sitio web o una dirección de correo electrónico, compuesto por un nombre de dominio y una extensión.
8. **Finance:** Área de Finanzas de WherEX.
9. **Gobernanza de Sistemas:** equipo de trabajo que coordina la gestión de acceso a sistemas, abarcando políticas, flujos y estructuras. Su labor se centra en administrar y controlar los sistemas de información de la organización de manera efectiva.
10. **Hardware:** todos los dispositivos físicos que componen un sistema tecnológico, como computadoras, teléfonos móviles, impresoras, entre otros. Es la parte tangible de la tecnología que se puede tocar y manipular físicamente.
11. **Jira Service Management Talent Acquisition Plan (TA Plan):** Se trata de un sistema implementado en Jira que actúa como una plataforma central para facilitar la contratación de nuevos empleados a través de solicitudes presentadas por los líderes de los distintos departamentos. Este sistema administra todo el proceso de selección de personal.
12. **Layout:** Diseño o disposición de los elementos en las pantallas o interfaces de Jira.
13. **Licencias:** Autorizaciones o permisos otorgados para el uso legítimo de software o servicios.
14. **Malware:** Software malicioso que se infiltra en sistemas informáticos sin permiso, causando daños o robando información.
15. **People:** Área de WherEX que comprende la gestión de personas, como recursos humanos.
16. **Perfiles:** Conjuntos de características, configuraciones y permisos asociados a un usuario o rol específico.
17. **Plataformas:** Sistemas o entornos informáticos que brindan una base para ejecutar aplicaciones o servicios.

18. **Portal:** Sitio web o aplicación que actúa como punto de acceso centralizado a información, servicios o recursos.
19. **Process & Compliance (P&C):** Sub-área dedicada a gestionar los procesos dentro de una organización, apoyando y ayudando a diferentes áreas.
20. **Screen:** Pantallas o interfaces visuales en la plataforma Jira.
21. **SaaS:** Software as a Service es un modelo de distribución de software en el que las aplicaciones son alojadas por un proveedor de servicios en la nube y se accede a ellas a través de Internet, generalmente mediante un navegador web, sin necesidad de descargar ni instalar el software en dispositivos locales.
22. **Software:** conjunto de programas, aplicaciones y datos que dirigen el funcionamiento de los dispositivos informáticos, permitiendo realizar diversas tareas sin necesidad de componentes físicos adicionales. Es la parte intangible de la tecnología que interactúa con el hardware para ejecutar funciones específicas y satisfacer necesidades del usuario.
23. **Solicitudes de soporte (SDS):** Proyecto de Jira Service Management, que trata de replicar el funcionamiento de TA Plan.
24. **Status:** Estados o etapas que pueden tener las tareas o incidentes en Jira.
25. **Usuarios:** Personas o entidades que tienen acceso y utilizan los sistemas, plataformas o servicios.
26. **Webhook:** Mecanismo que permite la comunicación entre diferentes aplicaciones o servicios web mediante notificaciones.
27. **Work in progress (WIP):** Tareas o incidentes que se encuentran en proceso o en curso en Jira. Es el trabajo que se ha iniciado, pero todavía no se ha realizado.

8.4. Anexo E: Apartados de Jira

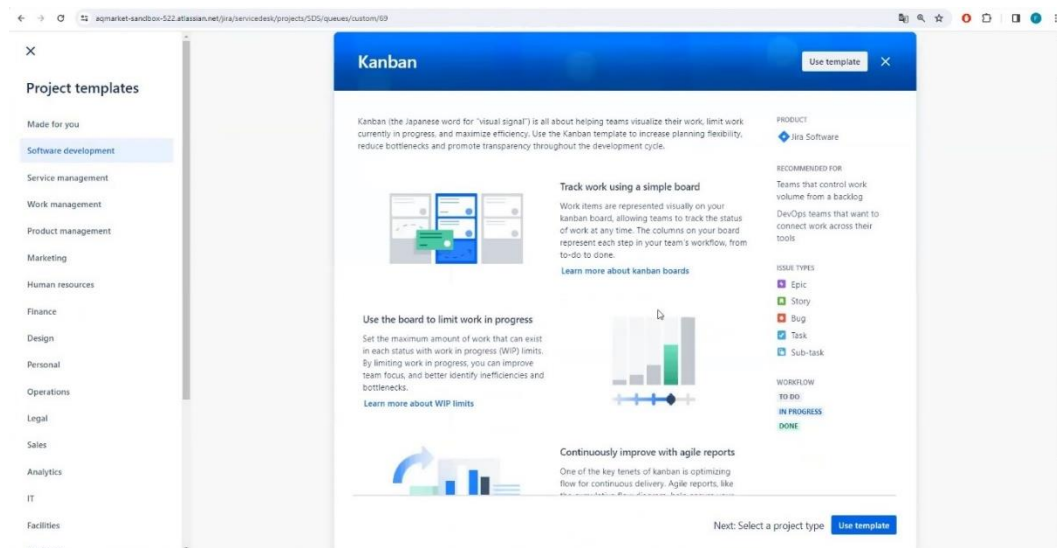


Figura 5.1.1.4.1 Vista de plantilla Jira Software Project

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian ASW, 2024)

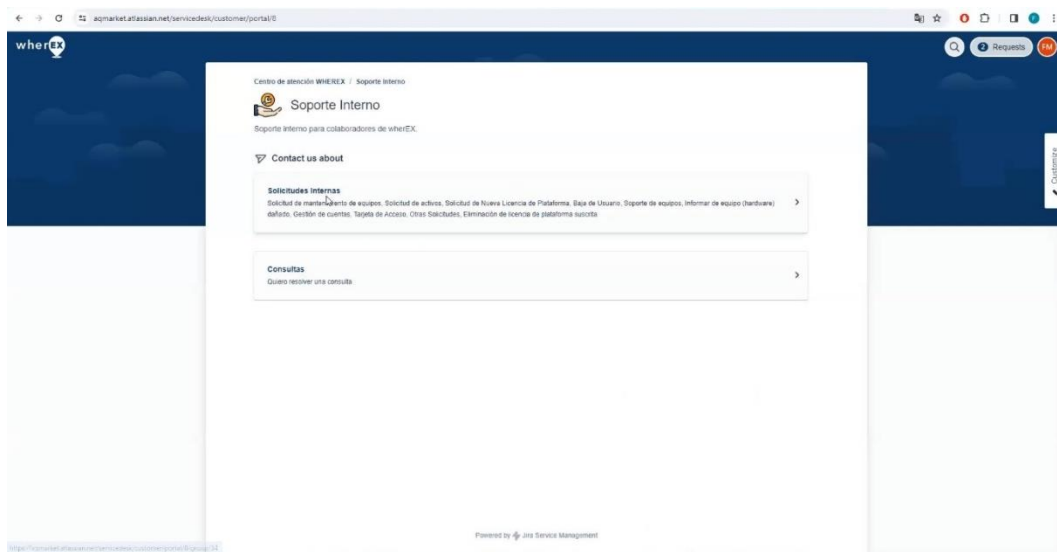


Figura 5.1.1.4.2 Portal principal de Internal Support (USS)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

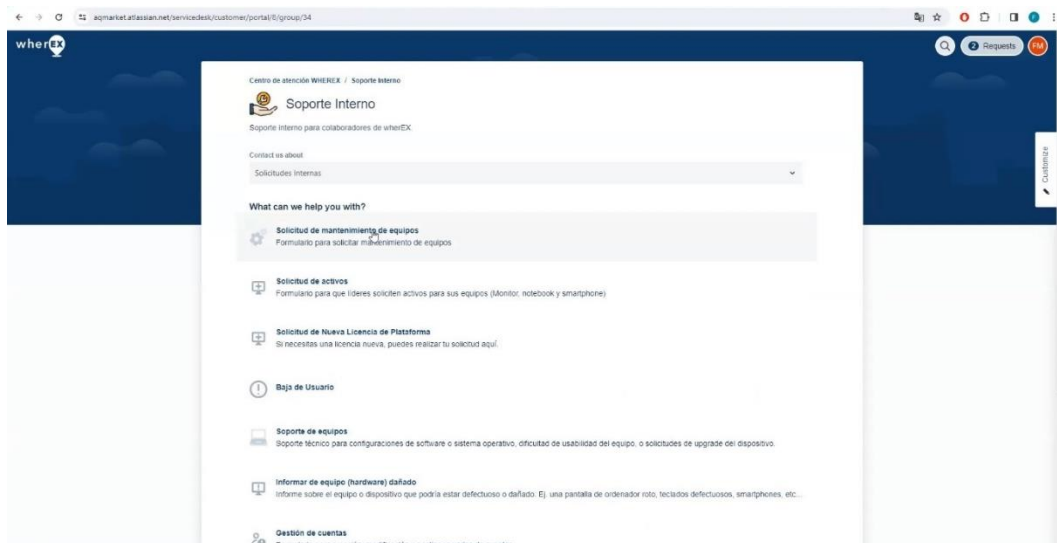


Figura 5.1.1.4.3 Vista de opciones de Internal Support (USS)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

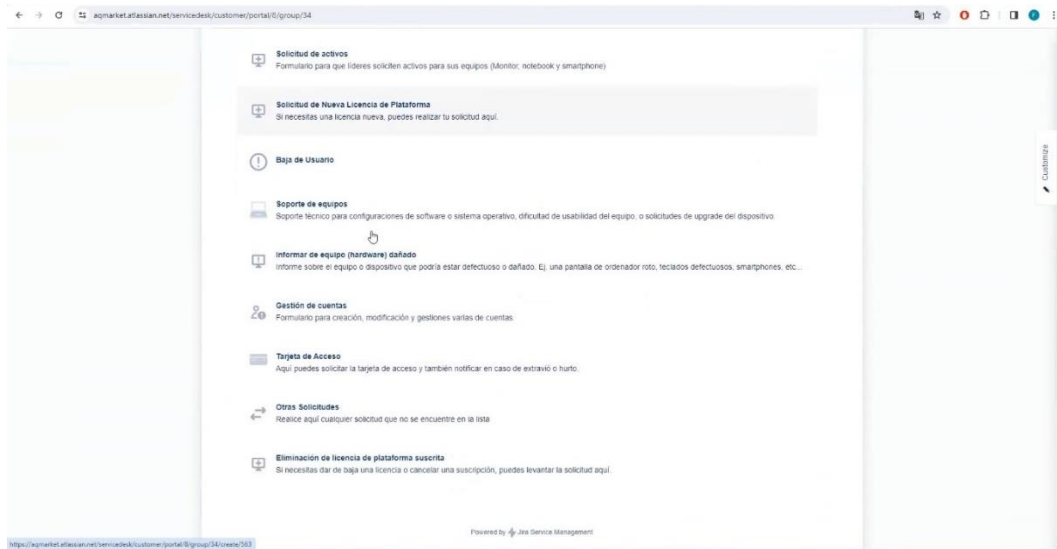


Figura 5.1.1.4.4 Continuación de la vista portal de Internal Support (USS)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

 A screenshot of the Jira Service Management portal showing the "Soporte Interno" section. The page title is "Soporte Interno" and the subtitle is "Soporte interno para colaboradores de whereEX". The form includes the following fields:

- Contact us about**: A dropdown menu with "Solicitudes Internas" selected.
- What can we help you with?**: A dropdown menu with "Solicitud de mantenimiento de equipos" selected. Below it is the text "Formulario para solicitar mantenimiento de equipos".
- Rate this request on behalf of***: A dropdown menu with "Felipe Ignacio García Morales (fgarcia@where.com)" selected.
- Resumen***: A text input field.
- Nombre y apellido***: A text input field.
- Correo electrónico***: A text input field.
- Describe brevemente el problema detectado con tu computadora***: A text input field.
- Agrega una fecha tentativa para dar mantenimiento***: A date and time picker showing "e.g. 3/26/2024" and "e.g. 12:30 PM".

 At the bottom of the form are "Send" and "Cancel" buttons.

Figura 5.1.1.4.5 Vista de Solicitud de mantenimiento de equipos "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

Centro de atención WHEREX / Soporte Interno

Soporte Interno
Soporte interno para colaboradores de whereX.

Contact us about
Solicitudes internas

What can we help you with?
Solicitud de activos
Formulario para que líderes soliciten activos para sus equipos (Monitor, notebook y smartphone)

Rate this request on behalf of?
Felipe Ignacio García Morales (fgarcia@wherex.com)

Resumen*

Añade un breve resumen de la solicitud

Descripción:
Añade una breve descripción de la solicitud

Normal text | B | I | U | Link | Image | Video | Attachments

Usuarios final*

Ingresar el nombre de la persona que utilizará el activo

Figura 5.1.1.4.6 Vista de Solicitud de Activos "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

Centro de atención WHEREX / Soporte Interno

Soporte Interno
Soporte interno para colaboradores de whereX.

Contact us about
Solicitudes internas

What can we help you with?
Baja de Usuario

Rate this request on behalf of?
Felipe Ignacio García Morales (fgarcia@wherex.com)

Resumen de solicitud*

Resumen corto de la solicitud

Nombre y Apellido*

Nombre completo del colaborador

Correo de la persona a dar de baja*

Ingresar la fecha de baja de cuentas*
e.g. 26/Mar/24 e.g. 12:31 PM
Indica la fecha y hora EXACTA en la que la persona finaliza sus labores en WhereX, recuerda que debes ser dentro del horario laboral de cada país para que nuestro equipo pueda ver la solicitud.

Área de negocio*

País solicitud*

Prioridad de desactivación*

3

Procesos/Flujo usual del nivel de prioridad para la desactivación de la cuenta: desde 1 en la alta prioridad a 5 la más baja.

Figura 5.1.1.4.7 Vista de solicitud Baja de Usuario “USS” (Flujo de Off Boarding)

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

Centro de atención WHEREX / Soporte Interno

Soporte Interno
Soporte interno para colaboradores de whereX.

Contact us about:
Solicitudes Internas

What can we help you with?
Solicitud de Nueva Licencia de Plataforma
Si necesitas una licencia nueva, puedes realizar tu solicitud aquí.

Rate this request on behalf of:
Felipe Ignacio García Morales (fgarcia@wherex.com)

Área de negocio*

País*

¿Está aprobado?*

Enter name (or email...)

Ingrese el nombre de la primera opción a contactar*

Motivo de la solicitud*

Figura 5.1.1.4.8 Vista de solicitud de Nueva Licencia de Plataforma "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

Centro de atención WHEREX / Soporte Interno

Soporte Interno
Soporte interno para colaboradores de whereX.

Contact us about:
Solicitudes Internas

What can we help you with?
Soporte de equipos
Soporte técnico para configuraciones de software o sistema operativo, dificultad de usabilidad del equipo, o solicitudes de upgrade del...

Rate this request on behalf of:
Felipe Ignacio García Morales (fgarcia@wherex.com)

Título*

Tipo de soporte*
☐ Configuración
☐ Defecto

Motivo

Normal text | B | I | A | [Icons]

Send Cancel

Powered by Jira Service Management

Figura 5.1.1.4.9 Vista de solicitud Soporte de Equipos "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

Centro de atención WHEREX / Soporte Interno

Soporte Interno
Soporte interno para colaboradores de wherEX.

Contact us about
Solicitudes Internas

What can we help you with?

Informe de equipo (hardware) dañado
Informe sobre el equipo o dispositivo que podría estar defectuoso o dañado. Ej: una pantalla de ordenador roto, teclados defectuosos,...

Rate this request on behalf of:
Felipe Ignacio García Morales (fgarcia@wherex.com)

Resuma el problema *

Describe what has occurred and how has occurred *

Normal text | B | I | ... | Attachments | ...

Archivos adjuntos

Drag and drop files, paste screenshots, or browse

Browse

¿En qué medida te afecta el problema o te o a la organización?

Figura 5.1.1.4.10 Vista Solicitud de Informe de equipo (Hardware) Dañado "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

Centro de atención WHEREX / Soporte Interno

Soporte Interno
Soporte interno para colaboradores de wherEX.

Contact us about
Solicitudes Internas

What can we help you with?

Gestión de cuentas
Formulario para creación, modificación y gestiones varias de cuentas.

Rate this request on behalf of:
Felipe Ignacio García Morales (fgarcia@wherex.com)

Título *

Tipo de cuenta *

Introduzca el tipo de cuenta. Ej: O suite, System, Private ID, etc.

Gestión de cuentas *

Correo *

Archivos adjuntos

Drag and drop files, paste screenshots, or browse

Browse

Figura 5.1.1.4.11 Vista de solicitud Gestión de cuentas "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

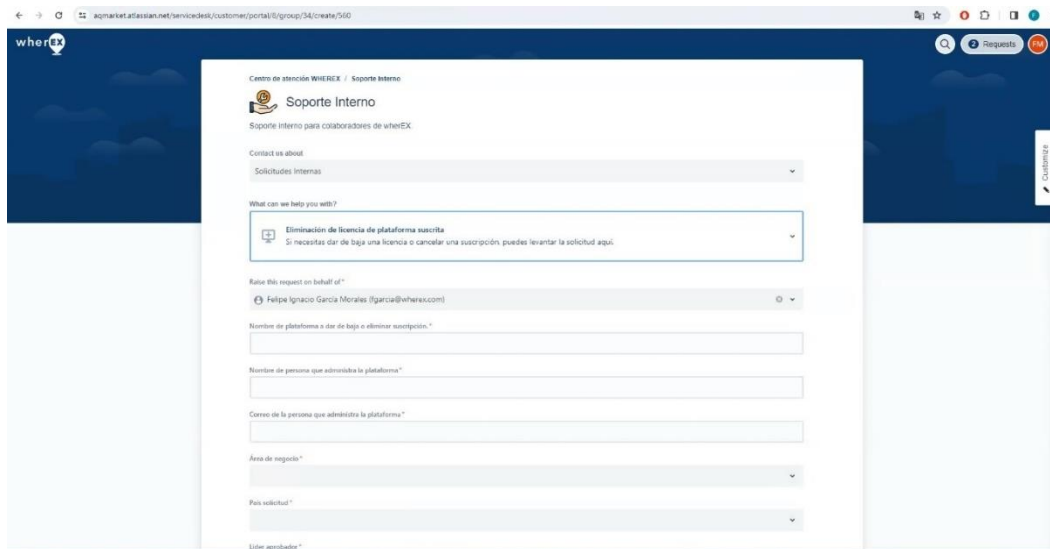


Figura 5.1.1.4.14 Vista de solicitud Eliminación de licencia de plataforma suscrita "USS"

Fuente: Espacio de trabajo en Jira. Recuperado de: (Atlassian USS, 2024)

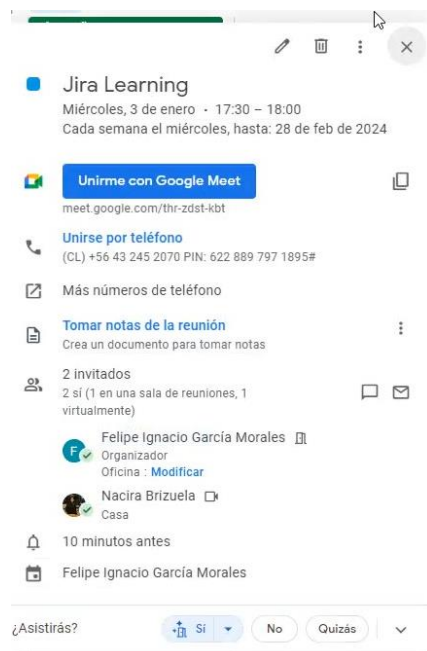


Figura 5.1.1.4.1 Reuniones semanales con Automation Engineer para estudio de Jira

Fuente: Espacio de trabajo en Google Calendar.