UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROCESO DE GESTIÓN INTERNA PARA LA INTERACCIÓN DE CIBERSEGURIDAD CON PROYECTOS TECNOLÓGICOS

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

PEDRO ALEJANDRO SALAS VERGARA

PROFESORA GUÍA:
MARÍA CECILIA BASTARRICA PIÑEYRO

MIEMBROS DE LA COMISIÓN:
FEDERICO OLMEDO BERÓN
EDUARDO GRAELLS GARRIDO
RAUL MONGE ANWANDTER

SANTIAGO DE CHILE
2023

Resumen

Este trabajo de tesis se realiza en un Banco del País. Esta es una institución financiera, ubicada con su edificio central en una comuna del sector oriente. Actualmente es uno de los bancos más importantes del país y de la región en términos de activos, colocaciones, patrimonio y número de clientes.

Un hecho relevante, en el año 2016 inicia el proceso de Transformación Digital, proyecto que abordó todos los productos y servicios para entregar una experiencia omnicanal diferenciadora, lo que significó un aumento en la cantidad de proyectos tecnológicos vinculados a una potente inversión estratégica.

Para alcanzar este objetivo de una rápida digitalización y transformación, este Banco se ha obligado a acelerar sus procesos de transformación digital, entre ellos los de la Gerencia de Seguridad Informática y su participación en proyectos a través de los Especialistas en Ciberseguridad.

Este trabajo de tesis se focalizó en la creación de un proceso de gestión interna en la Gerencia de Seguridad Informática, para la interacción de Ciberseguridad con proyectos tecnológicos realizados, implementando 14 puntos de control.

La problemática se centra en la interacción que existe entre el Especialista en Ciberseguridad y los proyectos, donde no existe un proceso estandarizado que permita dar seguimiento a los controles entregados y mucho menos documentarlos. Haber continuado con el actual método de participación en los proyectos, hubiese generado distintas formas de gestión, según experiencia y conocimiento organizacional, provocando una alta dependencia en las personas.

El desarrollo de este proyecto implicó un levantamiento, investigación, además de distintos diseños e implementaciones, todos con una coordinación del equipo de proyecto, los equipos de la Gerencia de Seguridad Informática y los equipos que se vinculan a los proyectos dentro de la Institución.

Durante el proyecto, se realizaron una serie de actividades, entre ellas el entendimiento de la situación actual, con el objetivo de modelar el proceso futuro, la creación del concepto de puntos de control con su detalle y la creación de una etapa previa de implementación llamada Pre-Jira.

Finalmente, se realizó la implementación del proceso en el equipo Especialistas en Ciberseguridad, la que contempló desde el diseño de arquitectura hasta la creación de un dashboard para la visualización de la ciberseguridad en los proyectos tecnológicos. Esto permitió validar las herramientas utilizadas y el proceso en la práctica comprobando el resultado final de este trabajo de tesis.

Dedicatoria

“No sigas el camino; ve por donde no haya vereda y deja una huella”

Este trabajo está dedicado a mis padres, por haberme enseñado a alcanzar mis metas.

Agradecimientos

Mi primer agradecimiento es sin duda para mi familia que me ha brindado el apoyo necesario para estar donde me encuentro ahora, a su educación y formación, sus valores y principios, los cuales hoy me tienen finalizando este proceso. A Flavia mi pareja, porque ha sido muy importante para terminar este proceso, por estar conmigo, apoyándome, escuchando, comprendiendo y por el amor y cariño entregado.

Me permito agregar a todas aquellas personas que no serán mencionadas en esta hoja, quienes de una u otra forma dejaron huella, por sus conversaciones y aprendizajes, no es porque no las tenga presente, es simplemente que no me alcanzaría el papel para decirles gracias.

Me gustaría agradecer también a la comunidad académica de la Universidad de Chile, a la FCFM y al DCC por su apoyo en la realización de esta tesis, en especial a mi profesora Guía PhD. Cecilia Bastarrica, por encauzar mi inspiración y aportar al desarrollo de mi trabajo con sus comentarios y sesiones, las cuales fueron de un gran valor para mí.

Quiero incluir en este agradecimiento a la Institución Financiera donde se aplicó este trabajo quien constantemente nos vincula al hecho de ser protagonistas de nuestro desarrollo. A todos aquellos que de una forma u otra me ayudaron a lograr este objetivo, sobre todo a Pancho Toro y Tito Silva quienes me apoyaron para el ingreso.

Un especial agradecimiento al equipo Especialistas en Ciberseguridad quienes vivieron la implementación de este trabajo, destacando mi agradecimiento a mi amigo Sebastián Cerón, quien me acompañó en este proceso con su apoyo y respaldo a lo largo de este trabajo.

Agradecido de la vida y de poder aprovecharla.

Tabla de Contenido

Índice de Figuras

1. INTRODUCCIÓN

La transformación digital se ha convertido en un objetivo estratégico para muchas organizaciones, ya que puede ayudar a mejorar la eficiencia operativa, reducir costos y aumentar la satisfacción del cliente. Sin embargo, a medida que las empresas se vuelven cada vez más dependientes de la tecnología digital, también se vuelven más vulnerables a los ciberataques.

La ciberseguridad ha evolucionado significativamente en los últimos años debido al aumento en el uso de tecnología en nuestras vidas cotidianas. Con la creciente dependencia de la tecnología en los negocios y en nuestras vidas personales, la protección contra ataques cibernéticos y la seguridad de los datos se ha vuelto cada vez más importante. Esta importancia se refleja en términos de competitividad. Una empresa que cuenta con una adecuada protección cibernética puede destacarse en un mercado cada vez más competitivo, ya que los clientes buscan empresas en las que puedan confiar y que ofrezcan una seguridad adecuada.

En el sector financiero, la ciberseguridad puede asegurar que las operaciones bancarias y financieras se lleven a cabo de manera segura y confiable. También puede evitar la exposición de información confidencial y proteger la integridad de los sistemas y datos financieros. Es por esta razón que la ciberseguridad es de vital importancia en proyectos tecnológicos, sobre todo del sector financiero, debido a la cantidad de información valiosa y confidencial que se maneja en estos ámbitos. Si esta información no es protegida adecuadamente, puede ser vulnerable a ataques cibernéticos que pueden resultar en pérdida de datos, fraude y robo de identidad.

El presente trabajo de tesis se desarrolla en una Institución Financiera y toma como desafío abordar un proyecto que cree un proceso de gestión interna para la interacción de ciberseguridad que estandarice la implementación de medidas de seguridad adecuadas, desde el inicio de un proyecto tecnológico, para continuar evaluando y mejorando estos controles a medida que avanza y evoluciona este proyecto.

1.1 Motivación del trabajo

El Banco en el año 2016 inicia su proceso de Transformación Digital, proyecto que abordó todos los productos y servicios para entregar una experiencia omnicanal diferenciadora, destacando como el primer banco chileno que permitió abrir una cuenta corriente 100% digital en 20 minutos, además de la posibilidad de optar por un crédito para consolidar deudas del sistema financiero a través de un smartphone, tablet o computador. Esta experiencia diferenciadora llamada Viaje del Cliente reflejó el camino de la estrategia de cara al 2020 y marcó la evolución de cara a su propósito de atreverse a hacer una diferencia.

Dada la rápida digitalización y transformación de la industria, el Banco se ha obligado a acelerar sus procesos de transformación digital. Sin embargo, al margen de los beneficios derivados de la implementación de soluciones de vanguardia, hay riesgos que vale la pena gestionar desde un comienzo, por lo que la ciberseguridad debe ser una prioridad.

La ciberseguridad debe ser vista como un habilitador de negocio, entendiendo que la seguridad es un factor clave en la confianza que tienen los clientes en todos los productos y servicios, por lo tanto esta prioridad que la hace un desafío, es la motivación central de este trabajo.

La importancia de la ciberseguridad en los proyectos tecnológicos de la organización, fundamental para una transformación digital segura y con foco en resguardar a sus clientes, genera que este trabajo se centre en la mirada de procesos internos. Este proceso de gestión interna será un primer paso que permitirá crear un clima de confiabilidad en la operación y de resultados en torno a la seguridad de un proyecto tecnológico, ya que entregará una mirada integral de los controles implementados que permitirán evidenciar el resultado de un proyecto seguro dentro de la Institución.

El desafío de este trabajo es que dada la evolución constante de la Industria Financiera, la implementación del proceso de gestión interna para la interacción de ciberseguridad no deberá ser estático, sino que escalable y flexible lo que permitirá una constante evolución ajustándose a las necesidades internas para la entrega de valor, lo que lo transforma aún más en una motivación.

1.2 Problema a Resolver

La Gerencia de Seguridad Informática del Banco, tiene como misión reducir el riesgo y promover la resiliencia mediante procesos de mejora continua en la ciberseguridad de colaboradores, procesos y tecnologías. Esta mejora en los procesos de ciberseguridad se encuentra disponible en todo momento, pero se vuelve fundamental en los proyectos tecnológicos que la corporación genera de cara a su transformación digital.

Uno de los principales enfoques del equipo de Especialistas en Ciberseguridad pertenecientes a la Gerencia de Seguridad informática, es prevenir cualquier evento de seguridad que se pueda generar por algún incumplimiento de controles en sus distintos proyectos tecnológicos. Desafortunadamente la entrega y seguimiento de lineamientos, buenas prácticas y controles en torno a ciberseguridad, requiere de un alto conocimiento previo del negocio donde se realiza el proyecto tecnológico, además de una alta vinculación con las unidades de negocio e internas. Esto genera que todas las revisiones se realicen mediante criterio del juicio experto del Especialista en Ciberseguridad, generando un problema de interpretación y de nula estandarización.

Continuar con este actual método de participación en los proyectos, genera distintas formas de gestión, según experiencia y conocimiento organizacional, provocando una alta dependencia en las personas. Además se impide la evolución sistemática en torno a los controles de ciberseguridad basados en la documentación histórica de la participación en los proyectos tecnológicos.

El desarrollo de un proceso que estandarice la participación de ciberseguridad en proyectos tecnológicos, ayudará a implementar seguimientos que entreguen una mejor certeza y enfoque, al mismo tiempo que se disponibilizan los controles aplicados en dichos proyectos.

1.3 Alcance

El alcance de este trabajo de tesis está centrado en crear un proceso de gestión interna en la Gerencia de Seguridad Informática, que específicamente sea utilizado por los Especialistas en Ciberseguridad. La necesidad de la estandarización para el manejo actual en la interacción de ciberseguridad con proyectos, iniciativas y mejoras previo a su paso a producción, hace que sea necesario crear un proceso que considere los distintos tipos de proyectos y adecuar el seguimiento con herramientas tecnológicas.

La solución aborda la importancia de la revisión a través de controles de ciberseguridad en proyectos, la que a través de un proceso nuevo y estándar se hace cargo de mejorar la manualidad actual. Junto con la creación del proceso, la solución implementará un conjunto de herramientas que permitirán dar seguimiento y continuidad a las tareas de este nuevo proceso.

Esta solución tendrá en cuenta factores tecnológicos que no generen una carga en la gestión de este proceso y así permitir una continuidad no burocrática en la prioridad del rol del Especialista en Ciberseguridad, que es la de garantizar que todos los proyectos de esta Institución Financiera se encuentren seguros.

No es parte del alcance de este trabajo detallar en específico los controles de ciberseguridad creados para este propósito, ya que su foco se orienta en la creación de un proceso y no en la profundización de la aplicabilidad de los puntos de control de ciberseguridad.

1.4 Objetivos

Para el proyecto de tesis se definió el siguiente objetivo general y objetivos específicos.

1.4.1 Objetivo General

El objetivo general de este trabajo de tesis es crear un proceso de gestión interna en la Gerencia de Seguridad Informática que permita aumentar los controles de seguridad preventiva vinculados a lineamientos y buenas prácticas para proyectos tecnológicos, mediante la estandarización del manejo actual en la interacción de ciberseguridad con proyectos, iniciativas y mejoras previo a su paso a producción.

1.4.2 Objetivos Específicos

Los objetivos específicos para materializar el objetivo general son:

- Definir y crear un proceso que permita dar seguimiento a los controles de seguridad elegidos para la implementación en los proyectos.

- Estandarizar la entrega de controles de ciberseguridad en los proyectos.

- Elegir un conjunto de herramientas que permitan dar prioridad, seguimiento y continuidad de los controles de ciberseguridad en los distintos proyectos tecnológicos.

- Facilitar la disponibilidad de los controles de seguridad implementados en los proyectos de manera transversal para el equipo.

El autor de este trabajo de tesis trabaja en la Gerencia de Seguridad Informática específicamente como Arquitecto Senior de Seguridad TI, llamado a la interna Especialista en Ciberseguridad. Dentro del alcance de su responsabilidad está la ejecución del proyecto, validar el alcance de la solución junto con liderar la implementación en su equipo de trabajo.

2. MARCO TEÓRICO

El marco teórico se apoyó en cuatro temas para sustentar el presente trabajo. El primer tema se basa en la ciberseguridad que es el punto de partida para el entendimiento de los conceptos vinculados a las distintas tecnologías.

El segundo tema recoge la importancia de la ciberseguridad, un tema que en los últimos años y sobre todo en el desarrollo de la industria 4.0 está tomando más importancia, para así desarrollar una actividad económica de manera mucho más segura.

El tercer tema aborda la ciberseguridad en proyectos tecnológicos, que debe ser incorporada desde el concepto de la solución y por ende asumir los desafíos que esto significa en todas las etapas de un proyecto.

El cuarto tema aborda el rol y responsabilidad del perfil de un Especialista en Ciberseguridad donde se desempeña la solución y su relación con el diseño de la seguridad de un proyecto.

2.1 ¿Qué es la ciberseguridad?

El término ciberseguridad ha tomado mucha fuerza y relevancia últimamente, aunque pareciera algo más abstracto que tangible. Una definición dentro de las pocas existentes es la del NIST (National Institute of Standards and Technology), la define como “La habilidad de proteger o defender el uso del ciberespacio de ciberataques” [1]. Como concepto general se puede aperturar también como el conjunto de prácticas, herramientas y procedimientos que buscan proteger los activos de información pertenecientes a personas como empresas, de ataques maliciosos generados por ciberdelincuentes. Esta información principalmente se crea y/o almacena en dispositivos móviles, computadores, sistemas electrónicos, o cualquier cosa en la que almacenamos datos que queramos proteger.

El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes [2], estas son:

- **La seguridad de red** es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista. Esta es fundamental, ya que las redes son utilizadas para transmitir información valiosa y confidencial, desde datos personales hasta información financiera y de negocios.

- **La seguridad de las aplicaciones** se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

- **La seguridad de la información** protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.

- **La seguridad operativa** incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- **La recuperación ante desastres y la continuidad del negocio** definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

- **La capacitación del usuario final** aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

2.2 ¿Por qué es importante la ciberseguridad?

Los ataques informáticos son en la actualidad uno de los problemas de mayor impacto para las grandes, pequeñas y medianas empresas. Dado que las distintas empresas dependen cada vez más de diferentes tecnologías, el riesgo de amenazas informáticas se mantiene al alza, por lo que se hace necesario comprender la importancia de la ciberseguridad y sus implicancias.

Muchas organizaciones toman la protección en torno a la ciberseguridad a la ligera y como consecuencia son víctimas de ciberataques. Estas no implementan siquiera las medidas básicas de seguridad porque no las consideran como inversiones necesarias.

A continuación se describen algunas razones por las que la ciberseguridad es importante para las empresas de hoy en día, estas son:

1. **Los Ciberataques no discriminan**

   Los ataques no son dirigidos de manera específica hacia una persona u organización, trabajan con scripts automatizados que están buscando indistintamente vulnerabilidades, lo que implica que existiendo un computador con internet, existen ciberataques. Lo anterior, demuestra que redes y computadores están recibiendo de manera permanente un promedio de 39 ataques por segundo [3], utilizando botnets para realizar fraudes, robo de identidad, interrumpir otras redes o dañar archivos del computador. Este promedio se hace cada vez mayor a medida que los avances tecnológicos crecen y la tecnología se masifica.

2. **Los datos confidenciales se están digitalizando cada vez más**

   La forma en que las personas interactúan a través de las redes sociales y cómo las organizaciones se interconectan con sus clientes ha cambiado drásticamente. En lugar de optar por documentos obsoletos en lápiz y papel, la tecnología ofrece la comodidad de transferir y almacenar información en un sistema basado en la nube. Esta conectividad mejorada y de mayor acceso aumenta la regularidad de la información confidencial comprometida, robada y filtrada, como datos personales, secretos comerciales y detalles de cuentas bancarias.

3. **Un auge en el comercio electrónico indica un auge en las ciberamenazas**

   La pandemia vivida (COVID-19) provocó una serie de cambios en los comercios y la entrada de múltiples actores al mundo del e-commerce. Con las restricciones a nivel estatal y los protocolos de distanciamiento social, los consumidores recurrieron masivamente a las compras en línea. En una transacción de comercio electrónico, las empresas pueden tener acceso a datos confidenciales, datos de clientes, incluidos detalles de comunicación, direcciones, comportamiento del cliente, información de tarjetas de crédito y almacenamiento de una cadena de suministro. Cualquier violación de la seguridad de estos datos puede causar una exposición significativa y daños en los procesos de marketing. Estos problemas son evitables con una adecuada cuota de ciberseguridad.

4. **Las soluciones a los ciberataques son económicamente costosas**

   Los delitos informáticos son costosos para las empresas de todo tipo y para la economía. El informe de IBM sobre el costo de las violaciones de datos menciona que estas aumentaron de USD 3,86 millones a USD 4,24 millones en 2021[4]. Los gastos que siguen a un ataque cibernético, particularmente después de una violación de datos, incluyen la contratación de especialistas forenses para investigar el punto de violación, la revisión del proceso de remediación de la red y el sistema de una empresa, el monitoreo de crédito, sanciones y multas.

5. **Los ciberataques dañan la reputación**

   Las organizaciones que son víctimas de ciberataques a menudo sufren daños en su reputación. Las marcas dependen de la confianza del consumidor, y la falla organizacional de una marca para proteger los datos de sus clientes y su sistema operativo de TI puede dañar su credibilidad. Las empresas pueden experimentar una caída en el valor de las acciones y las ventas a medida que los clientes recurren a otras marcas con mayor confiabilidad. En una era en la que la información se vuelve más digitalizada, la reputación de una empresa depende en gran medida de cómo previene y mitiga las ciberamenazas.

6. **Las amenazas de ciberataques personales son intrusivas**

   Los niveles de amenazas de la seguridad cibernética no se limitan solo al daño virtual, sino que pueden corromper la privacidad de la vida de las personas de todos los ámbitos de la vida. Cualquiera que compre, se comunique y juegue en una plataforma digital es vulnerable a amenazas cibernéticas como virus, robo de identidad, phishing, ataques de ransomware y fraude. Los correos electrónicos maliciosos exponen regularmente a los usuarios de Internet a riesgos de datos en su información personal. Los delitos cibernéticos más complejos implican el rescate de datos y el chantaje, en los que los delincuentes obligan a las víctimas a sacrificar algo para detener el acoso.

7. **Litigar los delitos cibernéticos es un proceso dificil**

   Además del costo económico inicial de las amenazas cibernéticas, las empresas afectadas por un delito cibernético a menudo enfrentan un proceso de litigio costoso. A pesar de ser la víctima, una empresa violada puede incurrir en costos adicionales de litigio y honorarios de abogados además del pago de multas. Por ejemplo, muchas empresas están bajo contrato para compensar a los accionistas

por una reducción en el valor de las acciones debido a que la empresa no operó de manera responsable. Desafortunadamente, una brecha en la seguridad podría caer bajo esta cláusula y obligar a las empresas a llegar a un gran acuerdo para resolver el problema.

8. **El cibercrimen es una amenaza a la seguridad nacional**

   Dado que todo el mundo está conectado a Internet, no sorprende que la seguridad cibernética sea una prioridad principal para la administración de un país en todos los niveles, Chile no es la excepción con 410 millones de intentos de ciberataques [5]. Las bases de datos y los sistemas de red desprotegidos corren el riesgo de sufrir intrusiones por parte de naciones extranjeras y terroristas que pueden aprovechar las debilidades de seguridad de un país y acceder a su información confidencial. Los atacantes pueden usar esta información para dañar la infraestructura, dañar las funciones económicas, robar secretos de estado e infundir terror entre la gente.

9. **La interrupción del negocio es un resultado directo del ciberdelito**

   Un ataque cibernético podría tener un efecto devastador en el sistema operativo de una organización, ya que la mayoría de las empresas dependen en gran medida de computadores y redes para funcionar. Cuando una empresa sospecha sobre una violación de datos, tiene que limitar su acceso a la red y al almacenamiento en la nube para contener los niveles de amenaza de malware o la fuga de información. La sofisticación de la amenaza y el tiempo requerido para solucionar el problema pueden resultar en una disminución de la productividad, lo que resulta en una pérdida de ganancias y una interrupción en las actividades comerciales.

10. **La disponibilidad generalizada de la web oscura plantea nuevos desafíos para los sistemas de seguridad cibernética**

    La web oscura es una colección de sitios de Internet accesibles desde un navegador web especializado [6]. Un componente clave de la web oscura es su anonimato, lo que permite a los usuarios aventurarse de forma anónima en contenido web no indexado y realizar actividades ilegales. Un interés cada vez mayor en la web oscura subraya la importancia de la resiliencia cibernética en los usuarios de Internet, lo que implica el uso de prácticas seguras y software de protección para defenderse de los segmentos web maliciosos.

2.3 Ciberseguridad en Proyectos Tecnológicos

Es frecuente que los líderes de proyectos tecnológicos en el desarrollo de sus actividades ubiquen los temas de ciberseguridad y control como un atraso que demora la puesta en producción de sus soluciones. Al momento en que se les menciona un requerimiento de seguridad, piensan en los tiempos para entregar oportunamente y los costos en torno al esfuerzo que esto implica. El argumento sobre el cumplimiento de los tiempos, los recursos que inicialmente fueron comprometidos, genera una resistencia generalizada que será tomada recién en una etapa posterior a la puesta en producción.

La figura 1 muestra el porcentaje de organizaciones que incluye la ciberseguridad en la fase de planificación de los programas de transformación digital.

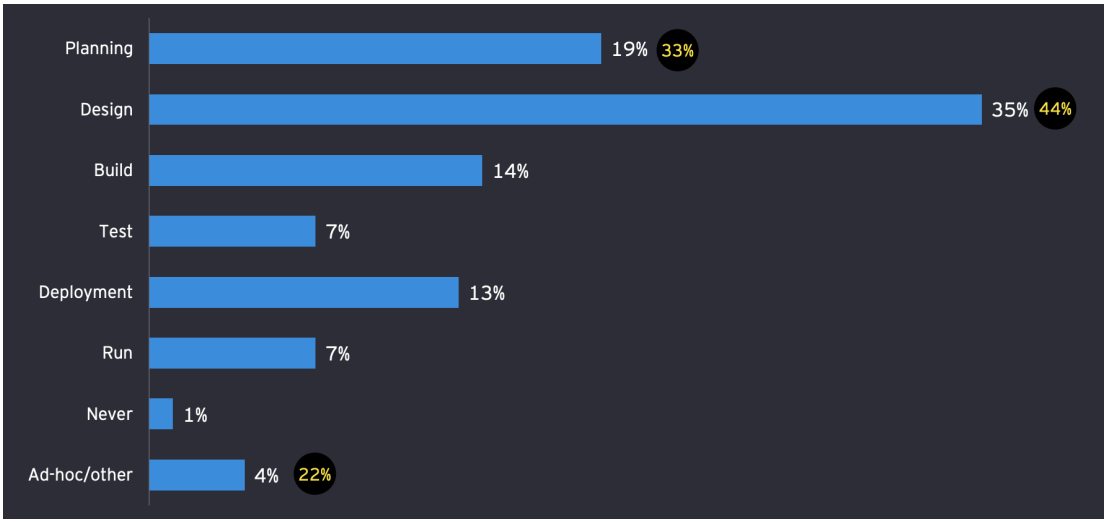


Figura 1: Etapas del proyecto donde se incluye ciberseguridad [7]

Cuando la ciberseguridad no se hace parte de las especificaciones y requisitos iniciales de un proyecto desde su concepción como idea, esto solo aumentará los riesgos actuales y futuros presentes al momento del paso a producción del proyecto.

Para ser realmente eficaz, la ciberseguridad debe integrarse desde cero. Los proyectos deben diseñarse para resistir ataques físicos y proporcionar seguridad para todos sus componentes con un diseño seguro desde cero.

Secure by Default [8] adopta un enfoque holístico para resolver los problemas de seguridad desde la raíz en lugar de tratar los síntomas, actuar a escala para reducir el daño general a un sistema en particular o tipo de componente. Secure by Default cubre el esfuerzo técnico a largo plazo para garantizar que los requisitos de seguridad

correctos estén integrados en el software y el hardware. También cubre la tarea igualmente exigente de garantizar que esos requisitos estén disponibles y se puedan usar de tal manera que el proyecto pueda adoptarlas fácilmente.

A continuación se describen algunos principios de seguridad por defecto [9] como:

- La seguridad debe estar integrada en los productos desde el principio, no se puede agregar más tarde

- Se debe agregar seguridad para tratar la causa raíz de un problema, no sus síntomas.

- La seguridad nunca es un objetivo en sí mismo, es un proceso y debe continuar a lo largo de la vida útil del producto.

- La seguridad nunca debe comprometer la usabilidad, los productos deben ser lo suficientemente seguros y luego maximizar la usabilidad.

- La seguridad no debe requerir una configuración extensa para funcionar y solo debe funcionar de manera confiable donde se implemente.

- La seguridad debe evolucionar constantemente para enfrentar y vencer las amenazas más recientes, las nuevas funciones de seguridad deben ser más rápidas en solucionar que en construirse.

- La seguridad no debe requerir una comprensión técnica específica o un comportamiento no obvio por parte del usuario.

Dado lo anterior, cuando un líder de proyecto establece las condiciones necesarias para los requisitos de seguridad, este se encuentra estableciendo un compromiso ético con los datos de las personas y empresas, así como con la responsabilidad digital de la organización, que entiende que los sistemas de información son puentes que habilitan nuevas oportunidades de negocio.

2.4 Especialista en Ciberseguridad y la Arquitectura de Seguridad

La importancia de que el líder del proyecto y todos los participantes en las distintas etapas de un proyecto tomen los requerimientos de seguridad es fundamental para un

paso a producción, habilitando entornos más seguros donde se disminuyen las brechas no previstas y que podrían impactar la imagen de la empresa.

En su rol, desde el acompañamiento al proyecto para generar un paso a producción seguro, es donde entra el Especialista en Ciberseguridad quien tiene una visión preventiva capaz de anticipar amenazas futuras y asesorar sobre cómo enfrentarlas [10]. Esto genera una serie de requerimientos de seguridad que se implementan en todo el ciclo de vida del proyecto, entregando seguridad desde una mirada holística con foco en una arquitectura de seguridad.

La arquitectura de seguridad tiene como propósito separar los componentes tecnológicos y de información más críticos de una organización y protegerla de las amenazas y daños cibernéticos. Los Especialistas en Ciberseguridad son entonces los responsables del análisis, diseño e implementación de los arquetipos y distintos componentes de ciberseguridad en la compañía.

Este rol debe garantizar que los requisitos de seguridad de las partes interesadas necesarios para proteger la misión y los procesos comerciales de la organización se aborden adecuadamente en todos los aspectos de la arquitectura empresarial. Estos aspectos deben incluir los modelos de referencia, arquitectura de soluciones y segmentos, además de los sistemas resultantes que respaldan esas misiones y procesos comerciales. [11]

En consecuencia, tanto el liderazgo como el acompañamiento de un proyecto en torno a la ciberseguridad son fundamentales para el cumplimiento de los objetivos de un proyecto tecnológico y los objetivos orientados a la ciberseguridad, abordados desde un proceso a lo largo de este trabajo.

3. SITUACIÓN ACTUAL EN LA EMPRESA

El presente trabajo de tesis se desarrolla en una Institución Financiera. Esta es una institución privada chilena, con presencia en territorio nacional, así como también en Estados Unidos y Perú. Su edificio corporativo se encuentra en el sector oriente de la Región Metropolitana con sucursales repartidas a lo largo del territorio nacional. Considerado un Banco de Familia, fue fundado por una familia y un grupo de emprendedores con el fin de apoyar a las pequeñas y medianas empresas de Chile. Actualmente, a nivel industria, se posiciona en el país en términos de colocaciones y por su número de clientes.

3.1 Misión y Visión

Su misión es ser líderes regionales en innovación, cercanía y experiencia de clientes, además de ser reconocidos como la mejor empresa para trabajar y desarrollarse. En su visión, se define como una Corporación de Soluciones Financieras que participa en todos los negocios y operaciones financieras que la Ley General de Bancos le permite, ofreciendo a la comunidad productos y servicios con procesos de alta eficiencia operacional y excelencia en la calidad, con una permanente innovación tecnológica, prudentes políticas de administración de riesgos y exigentes estándares éticos, los que deben ser respetados por todas las personas que se desempeñan en sus empresas. En este marco, y con el propósito de cumplir sus objetivos y políticas, la Corporación se compromete a cuidar que dichos logros se obtengan con especial énfasis en los que considera sus cuatro pilares fundamentales:

1. Accionistas
2. Clientes y Proveedores
3. Colaboradores y sus Familias
4. Sociedad.

En línea con su misión y visión, además del constante avance de la transformación digital y búsqueda permanente de su propósito “atrevernos a hacer una diferencia”, La Corporación ha definido para el logro de sus objetivos estratégicos y cumplir los resultados esperados, dos vehículos estratégicos:

- Planes Corporativos
- Flujos de Valor

3.2 Estructura Organizacional

Para alcanzar los objetivos corporativos, cada una de las diez Gerencias mencionadas en la Figura 2 y que reportan al Gerente General deben estar alineadas al cumplimiento de sus resultados, acorde a los dos vehículos estratégicos mencionados anteriormente en la Misión y Visión.

Apalancados en los objetivos corporativos se desprenden desde estas Gerencias una serie de proyectos, iniciativas y/o mejoras que serán necesarias de implementar para la ejecución y progreso de la estrategia.

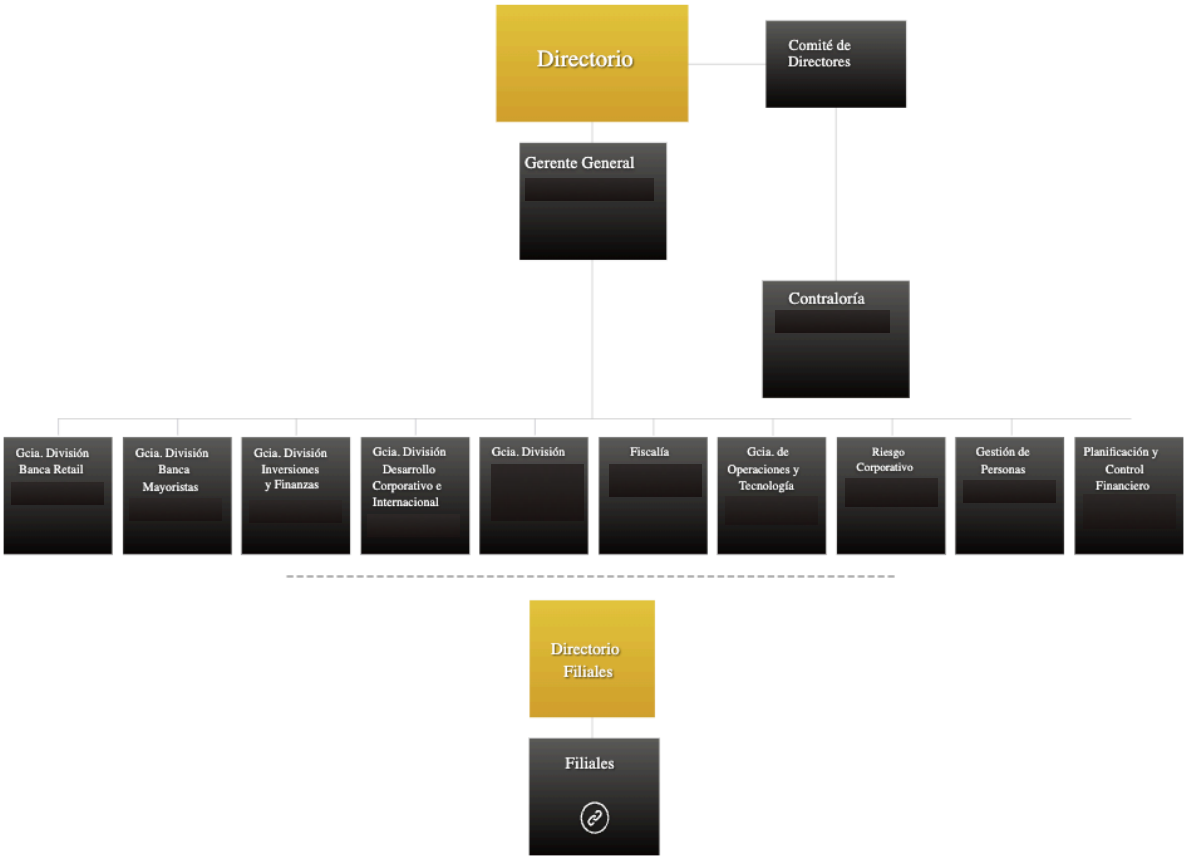


Figura 2: Estructura Organizacional del Banco

Es necesario detallar las Filiales del Banco mencionadas en la Figura 3, donde además se incluye indirectamente a la Fintech desarrollada por la Institución. Estas Filiales amplifican el cumplimiento de los objetivos estratégicos, por lo que también representan una suma importante de proyectos, iniciativas y/o mejoras que serán necesarias de implementar para la ejecución y progreso de la estrategia.

Figura 3: Detalle de las Filiales del Banco

Dentro de las diez Gerencias de primer reporte visualizadas en la Figura 4 se encuentra Operaciones y Tecnología, la cual posee dentro de sus filas a la Gerencia de Tecnología y Seguridad Informática, que contiene a su vez a la Gerencia de Seguridad Informática, creada el 2016 y vinculada de manera transversal a la Corporación.

La Gerencia de Seguridad Informática contiene a la Subgerencia de Especialistas en Ciberseguridad y Continuidad DRP, importante ya que aquí se encuentra el equipo de los Especialistas en Ciberseguridad quienes serán claves en la solución e implementación de este trabajo de tesis.

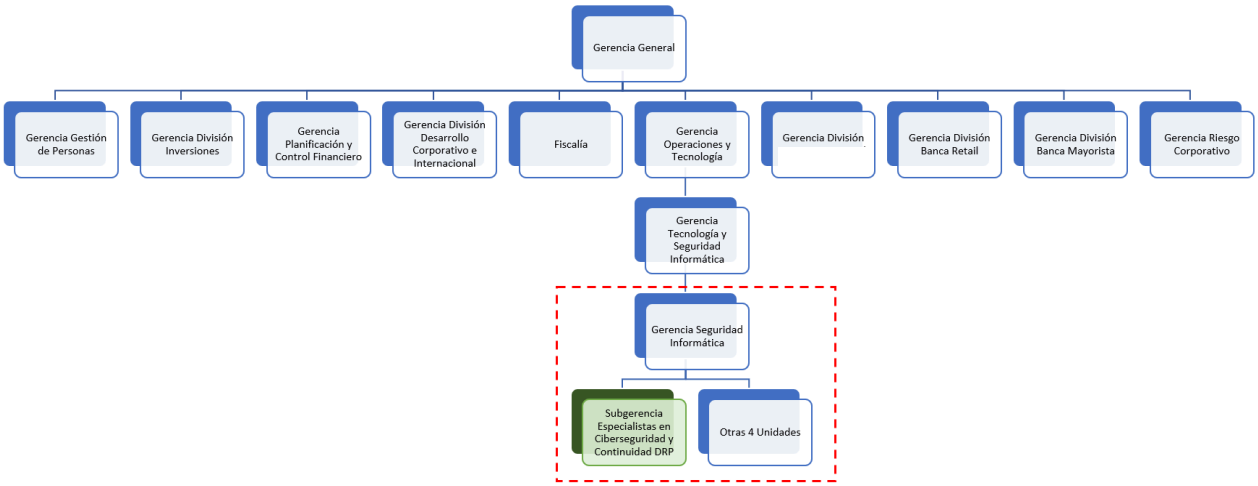


Figura 4: Estructura Organizacional objetivo de la solución

El objetivo de la Gerencia de Seguridad Informática es ser habilitadores en la transformación digital asegurando la continuidad operacional y protegiendo los activos de información de las amenazas existentes.

Dado lo anterior y para el cumplimiento de este objetivo, se define a nivel corporativo que todo proyecto, iniciativa y/o mejora generada por cualquiera de las Gerencias que componen a la Corporación, debe interactuar con la Gerencia de Seguridad Informática antes de su paso a producción, para uso de un usuario final, ya sea interno o externo.

3.3 Situación de los Proyectos Tecnológicos

La estructura general de un proyecto, iniciativa y/o mejora contempla una serie de actividades que son independientes del alcance, objetivo y particularidades. Éstas son descritas a continuación y forman parte del ciclo de vida descrito en fases de participación con distintos roles y responsabilidades de los equipos involucrados.

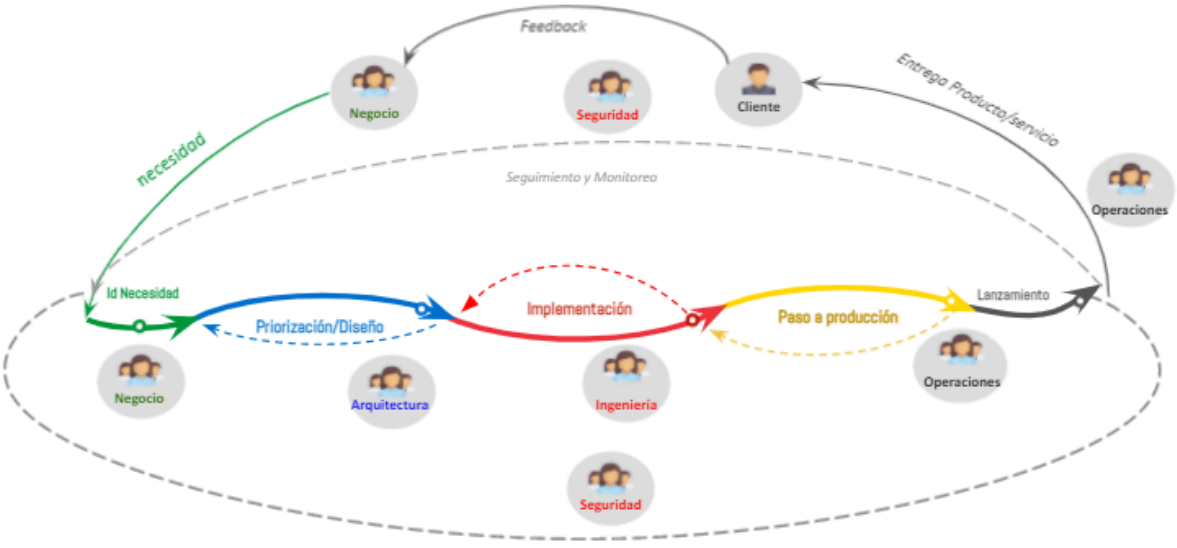


Figura 5: Diagrama general para las etapas de un proyecto, iniciativa y/o mejora.

La Figura 5 presenta la visión general en alto nivel de las etapas de un proyecto, iniciativa o mejora, donde debe existir la revisión de seguridad y cuyas principales actividades son las siguientes:

1. **Identificación (Id) de la Necesidad:** Las unidades del negocio bancario o tecnológicas identifican una necesidad que presenten los clientes, ya sean internos (otras unidades) o externos (clientes Bancarios).

2. **Priorización / Diseño:** La Gerencia de Arquitectura Tecnológica que contiene las distintas unidades de Arquitectura, es la responsable de priorizar en conjunto con las distintas unidades de negocio o unidades que presentaron la necesidad, la forma en que se realizará el proyecto tomando en consideración variables de negocio y tecnológicas.

3. **Implementación:** Dependerá de cómo se haya diseñado tecnológicamente la solución para la necesidad, además de la metodología a utilizar para su desarrollo. Ésta puede ser por ejemplo en Cloud, on premise o híbrida y de metodología tradicional o ágil. Las Gerencias y unidades involucradas dependen de los objetivos del proyecto y su alcance.

4. **Paso a producción:** Se deben cumplir una serie de requerimientos que son revisados por la unidad de control de cambios, que valida el cumplimiento de todos los requisitos a través de vistos buenos, de las unidades participantes en los flujos por categorías según el tipo de cambio.

5. **Lanzamiento:** La operación del proyecto desde la visión de continuidad y también de seguridad son fundamentales. El lanzamiento se puede generar de manera interna a un grupo acotado de personas para luego ser masificado al público objetivo o directamente publicado a clientes, esto independiente de la metodología.

3.4 Participación de Seguridad en los Proyectos Tecnológicos

La participación de la Gerencia de Seguridad Informática en estas etapas del proyecto es parte de su objetivo. Cuando un proyecto tecnológico llega a la Gerencia de Seguridad Informática, este debe ser revisado para su puesta en producción. La complejidad de la revisión radica en la etapa en que el Especialista de Ciberseguridad interactúa con el proyecto, la cual depende de las Gerencias que lleven los proyectos, iniciativas o mejoras y de la información disponible para el entendimiento del contexto. El manejo del contexto ya sea de negocio, de proceso o tecnológico se vuelve fundamental para la entrega de lineamientos de seguridad completos.

La forma de revisión actualmente queda a criterio del juicio experto del Especialista en Ciberseguridad y de su capacidad de vinculación con las unidades internas de la Gerencia de Seguridad Informática, quienes son responsables según su rol de ejecutar los distintos controles de ciberseguridad.

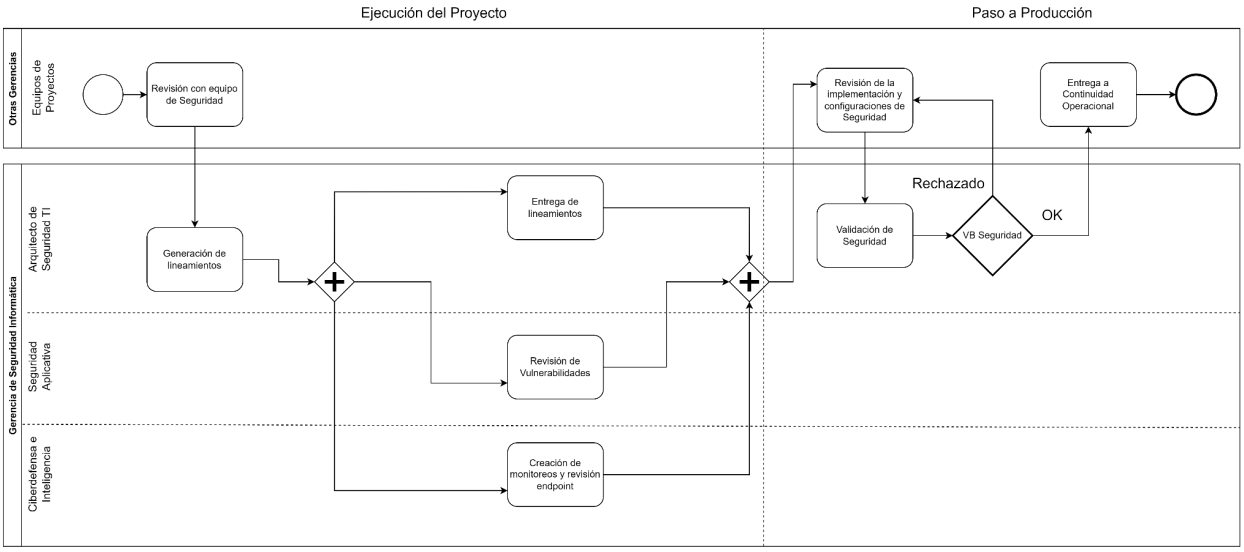


Figura 6: Proceso actual para la interacción de ciberseguridad con proyectos tecnológicos

La figura 6 muestra las distintas revisiones que se realizan actualmente en las etapas del proyecto y que generan una serie de lineamientos y buenas prácticas tecnológicas orientadas a ciberseguridad. Estos lineamientos son revisados por el Especialista en Ciberseguridad según su experiencia y/o según su interacción con el equipo de Riesgo quien los ha identificado previamente.

Es responsabilidad de quienes ejecutan los proyectos tomar las consideraciones levantadas por la Gerencia de Seguridad y es responsabilidad de Seguridad ir realizando la gestión de esa implementación, lo que genera distintas formas de gestión y seguimiento de las soluciones entregadas, según experiencia y conocimiento organizacional con directa dependencia del Especialista en Ciberseguridad.

Las consecuencias de la situación actual y de la forma en que se lleva a cabo la seguridad de los proyectos tecnológicos, radica en una muy alta complejidad para las revisiones de ciberseguridad vinculadas a las personas como a procedimientos. Respecto a las personas, existe una alta dependencia al Especialista en Ciberseguridad que participa en los proyectos, considerando el contexto y tiempo que involucran sus actividades junto con una alta dependencia a su expertise técnica y su antigüedad en la organización. Respecto a los procedimientos, existe un alto criterio al juicio experto y al conocimiento organizacional para resolver lineamientos y prácticas no estandarizadas, así como también existe una debilidad para dar seguimiento y visibilidad a las interacciones de ciberseguridad.

Los principales desafíos al construir esta solución son la definición de controles transversales de la arquitectura de seguridad, el levantamiento de las prácticas actuales

no estandarizadas y los requerimientos funcionales y tecnológicos. También se encuentran las limitaciones propias de la implementación en la alineación con la forma y participación que tienen los proyectos en toda la Corporación. La adopción inicial del proceso es parte importante, ya que debe considerar la gestión del cambio para garantizar una correcta implementación.

4. ESTRUCTURA PARA EL DESARROLLO DEL PROYECTO

4.1 Equipo de Trabajo

En primera instancia se conformó un equipo de trabajo adecuado para la realización del proyecto, con interacción directa del equipo de Especialistas en Ciberseguridad. Este equipo dentro de la Gerencia de Seguridad Informática y perteneciente a la Subgerencia detallada en la figura 7, es quien entrega las definiciones de seguridad a toda la Corporación por lo que se definió la siguiente estructura de trabajo:

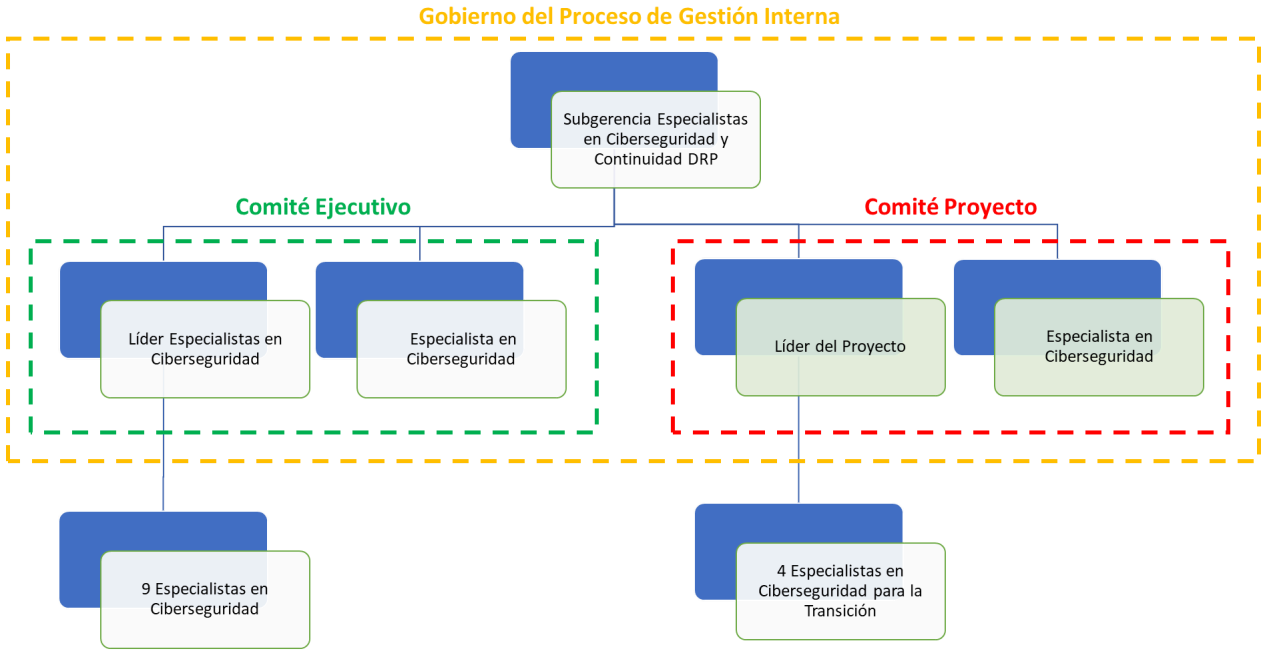


Figura 7 : Equipo del Proyecto

Los roles que se establecen en el equipo de trabajo se definen en torno a su responsabilidad, estos son según orden de interacción:

1. **Gobierno del Proceso de Gestión Interna:** El Gobierno se centra en la comunicación directa entre los líderes de los comités y el subgerente.
    a. **Subgerente Especialistas en Ciberseguridad y Continuidad DRP:** Define la necesidad del proceso en conjunto con el Gerente de Seguridad Informática, además de validar los alcances para su implementación en el equipo.

2. **Comité Ejecutivo:** Realiza la revisión de las decisiones para la correcta implementación en el resto del equipo.
    a. **Líder Especialistas en Ciberseguridad:** Impulsa el cambio y apertura espacios transversales para el cumplimiento de los objetivos.
    b. **Especialista en Ciberseguridad:** Entrega feedback y apoya en la gestión del cambio del equipo.

3. **Comité Proyecto:** Encargado de crear el proceso, definir alcances e implementación, responsable de la metodología y sus ajustes.
    a. **Líder del Proyecto:** Lidera el proceso, sus definiciones y la implementación.
    b. **Especialista en Ciberseguridad:** Fundamental en la gestión interna, feedback e implementación de la solución aportando directamente al cumplimiento de los objetivos.

4. **4 Especialistas en Ciberseguridad para la Transición:** Equipo pionero en implementar el proceso y su metodología de trabajo, es quien entrega el feedback constante. Reportan directamente al Líder del Proyecto.

5. **9 Especialistas en Ciberseguridad:** Resto del equipo Especialista quien debe declarar y posteriormente agregar a la solución los distintos proyectos en los que participa, con el objetivo de alimentar la plataforma definida para la implementación del proceso. Reportan los avances al Líder Especialistas en Ciberseguridad en las reuniones de equipo.

El rol del tesista se encuentra específicamente dentro del Comité de Proyecto, el cual es un equipo formado por 2 personas en donde la responsabilidad se presenta como Líder del Proyecto. Además de sus funciones como Especialista en Ciberseguridad, es el responsable del éxito de este proyecto. En concreto el tesista es quien crea, define e implementa el proceso.

El rol de los Especialistas en Ciberseguridad es utilizar el proceso de gestión interna aplicado a los proyectos que cada uno tiene asignado por sus funciones y además aplicado a su rol en este proyecto según las definiciones anteriores.

4.2 Metodología de Trabajo

La metodología ágil aplicada en este proyecto se centró en la misma metodología adoptada de manera transversal en la Corporación para el desarrollo de proyectos vinculados a la transformación digital, esta es la metodología ágil.

La metodología ágil es un enfoque iterativo de la gestión de proyectos y el desarrollo de software que ayuda a los equipos a aportar valor a los clientes de forma más rápida y con menos molestias. En lugar de centrarse en un lanzamiento de gran envergadura, un equipo ágil entrega el trabajo en incrementos pequeños, pero que se pueden consumir. Los requisitos, los planes y los resultados se evalúan de forma continua, de modo que los equipos disponen de un mecanismo natural para responder con rapidez ante los cambios [12].

Desde sus inicios, la metodología Agile reivindica 4 valores, que son utilizados a lo largo de este trabajo:

- Las interacciones de las personas sobre los procesos y las herramientas.
- Un software en funcionamiento frente a documentación exhaustiva.
- La participación activa del cliente durante todo el proceso de desarrollo.
- La capacidad de respuesta ante los cambios e imprevistos.

Lo más importante para implementar una metodología Agile es el liderazgo y el cambio cultural, más aún cuando se trata sobre la creación de un proceso. Saber dialogar y motivar a los equipos para vencer sus reticencias, convencerlos de los beneficios e involucrarlos en el cambio. El compromiso con el modelo es fundamental para su éxito.

La aplicación de Agile para este proyecto llevó a cumplir estos 12 principios, todos basados en el manifiesto ágil [13]:

1. La prioridad es que el cliente esté satisfecho y siempre informado del estado del proceso.
2. Los requisitos del proyecto pueden cambiar y no se verá como un problema, sino como una ventaja competitiva.
3. Las entregas se realizan periódicamente y en periodos cortos. La planificación se realizará desde las dos semanas, a los dos meses.
4. El equipo debe trabajar de forma conjunta y coordinada.
5. Es prioritario motivar al equipo, confiar en los miembros y proporcionarles los recursos o apoyos que necesiten.

6. Las reuniones son el método más efectivo para comunicarse.
7. El éxito depende de si el producto final funciona y es satisfactorio.
8. Los procesos deben ser sostenibles, tanto en recursos materiales, como en la gestión del tiempo y el ritmo de trabajo.
9. En todo proceso o etapa debe prevalecer la excelencia técnica.
10. Prevalece la ley de la simplicidad: menos es más.
11. La organización de los equipos es esencial para dar con un buen diseño.
12. Los tiempos para la reflexión y buscar mejoras es necesario e igual que importante que el resto de fases.

Este proyecto se dividió en 5 fases, que contemplaron su evolución constante basado en iteraciones mencionadas en la figura 8, estas son:

Figura 8 : Metodología Ágil

1. La primera fase se hará cargo de entender la situación actual de la Gerencia de Seguridad Informática y su interacción con las unidades vinculadas a los proyectos, con el objetivo de determinar el punto de partida.

2. La segunda fase tomará las sugerencias de mejora con el fin de optimizar la situación actual en torno al proceso, considerando una combinación correcta entre procesos y tecnologías.

3. La tercera fase de diseño de la solución considerará la participación fundamental del usuario final, Especialista de Ciberseguridad, como parte del proyecto desde su inicio, tomando su feedback como puntos de mejora y revisando siempre las opciones desde el punto de vista proceso y tecnología.

4. La cuarta fase tomará la construcción e implementación como entregables constantes para que los usuarios finales puedan utilizar la solución y solicitar cambios, aumentando la entrega de valor.

5. La quinta fase considera la evaluación y monitoreo midiendo que el proceso se esté cumpliento según lo acordado desde su inicio, además de controlar los feedbacks entregados.

4.3 Cronograma General

El cronograma general del proyecto considera las principales etapas y tareas, tales como los puntos de control de ciberseguridad para proyectos, la creación del proceso de gestión interna, el trabajo en confluence, la matriz de trabajo llamada pre-Jira, la construcción del modelo en Jira y los distintos dashboard de visualización. Todo separado en trimestres para lograr un mejor cumplimientos de las etapas.

El alcance de este trabajo de tesis no considera la posterior implementación de los subprocesos de cada equipo con rol participante de este sistema en el resto de las unidades de la Gerencia de Seguridad Informática, por lo que no fueron considerados en el cronograma presentado en la figura 9 a continuación.

Cronograma Planificado 2022 del Proyecto

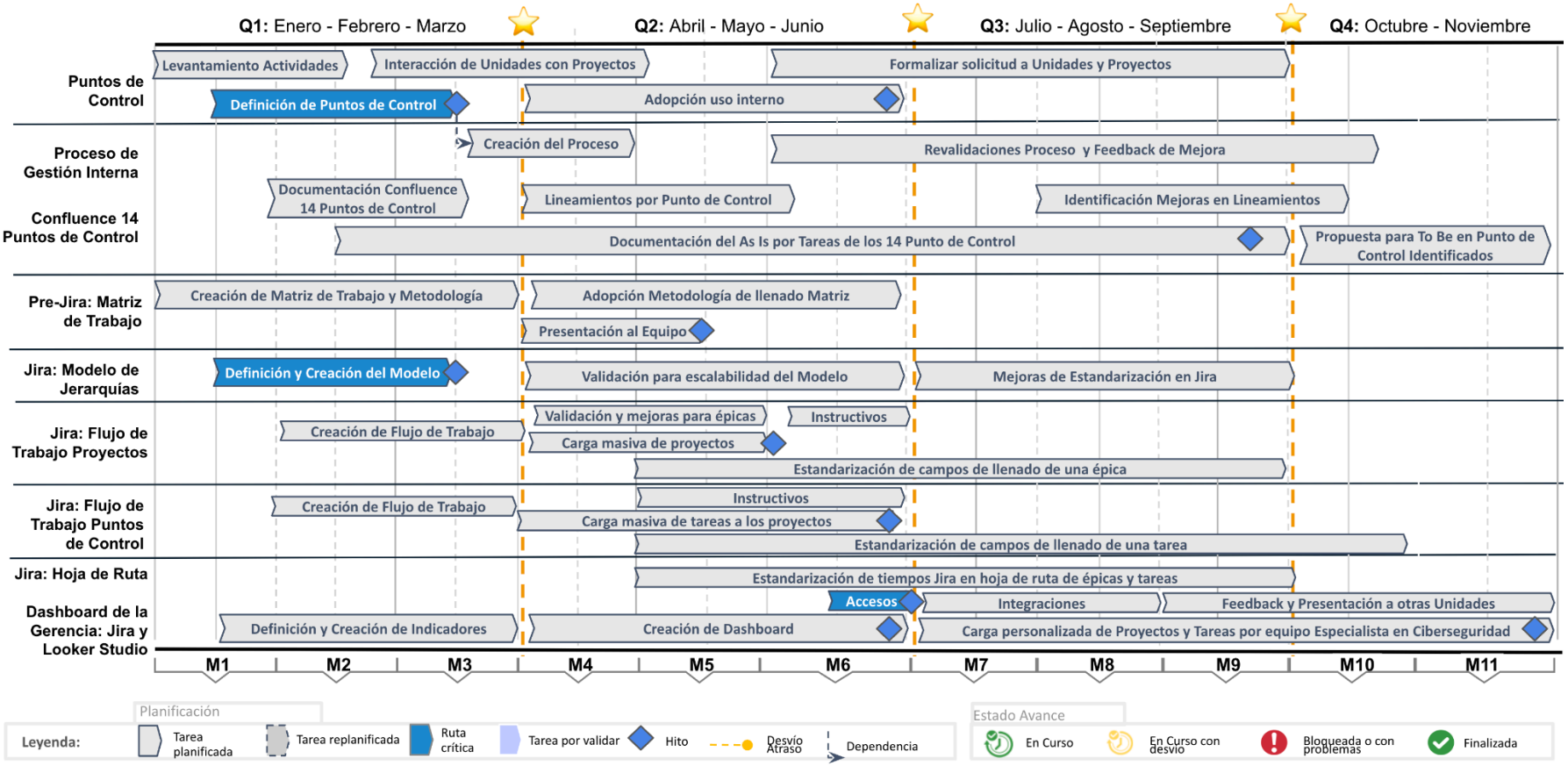


Figura 9 : Cronograma General

5. SOLUCIÓN

El diseño de la solución se enfocará en el proceso interno de la Gerencia de Seguridad Informática el cual tomará un conjunto de fases y operaciones con el objetivo de estandarizar y transformar la forma en que se interactúa con proyectos tecnológicos. La solución debe conectar pero también evidenciar las distintas fases sucesivas o paralelas que se crearán para la entrega de un lineamiento y/o buena práctica de ciberseguridad, a las distintas Unidades que ejecutan proyectos, iniciativas o mejoras dentro de la Corporación.

Para el desarrollo de la solución se abordaron tres temas para sustentar el presente trabajo. El primer tema trata sobre la creación de los puntos de control redefiniendo conceptos existentes en la industria y la organización para aplicarlos como tareas necesarias que se deben incorporar en este proceso.

El segundo tema aborda la creación del proceso de gestión interna explicando sus interacciones en torno a las actividades.

El tercer tema es la creación del denominado Pre-Jira, como mecanismo de seguimiento a la interacción de ciberseguridad, a través de los puntos de control, con los distintos proyectos.

5.1 Creación de los Puntos de Control

Un punto de control de seguridad es un conjunto de tareas o medidas aplicadas en proyectos que se toman para proteger a una Institución de posibles ataques maliciosos. Para comprender a la perfección este concepto, debemos tener en consideración que un punto de control hace referencia a todo el entorno de trabajo vinculado a un proyecto tecnológico. Estos entornos de trabajo, comprenden un grupo de personas o unidades dentro de la organización, stack tecnológicos, procesos y en general todo lo que se encuentre vinculado a los distintos proyectos por revisar.

La agrupación de los puntos de control generada, responde a la estructura organizacional interna de la Gerencia de Seguridad Informática de esta Institución Financiera, pero cada punto podría ser organizado de manera independiente respetando un proceso de gestión interna y su madurez organizacional. Esta estructura del proceso permite afrontar los cambios organizacionales que ocurren con el objetivo de alcanzar un mayor grado de madurez dentro de la organización o sus unidades en torno a la ciberseguridad.

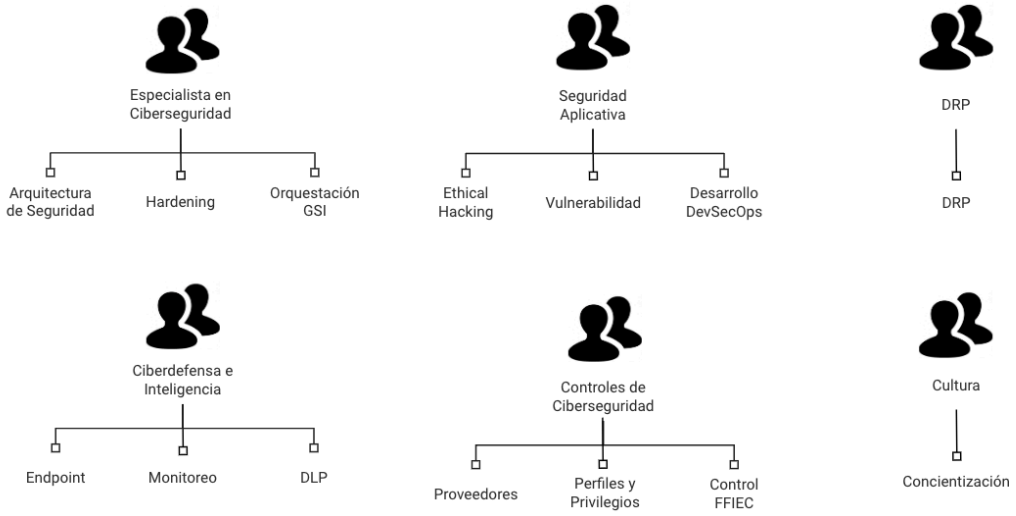


Figura 10: Puntos de Control de Seguridad para proyectos tecnológicos

Puntos de Control

- Equipo Especialista en Ciberseguridad

    - **Arquitectura de Seguridad:** El objetivo de este punto de control es que se realice una revisión de la seguridad en la arquitectura y diseños declarados por los proyectos. Este punto garantiza que las partes interesadas tomen buenas decisiones informadas en torno a un proyecto seguro desde su diseño, determinando acciones de corrección cuando existan incumplimientos.

    - **Hardening:** El hardening o endurecimiento de los sistemas se refiere a las herramientas, los métodos y las mejores prácticas utilizadas para reducir la superficie de ataque en la infraestructura tecnológica, incluyendo el software, los sistemas de datos y el hardware. El objetivo de este punto de control es reducir el "perfil de amenaza" general o las áreas vulnerables del sistema. Esto implica la revisión metódica, la identificación y la corrección de las posibles vulnerabilidades de seguridad en toda la organización, haciendo hincapié en la adaptación de diversos ajustes y configuraciones por defecto para hacerlos más seguros.

    - **Orquestación GSI:** El objetivo de este punto de control es ordenar, gestionar, y por lo tanto guiar a las unidades de la Gerencia de Seguridad Informática para el cumplimiento de su rol y responsabilidad en los distintos proyectos, considerando los puntos de control pertenecientes a cada unidad de seguridad.

- Equipo DRP

    - **DRP Tecnológico:** Un plan de recuperación ante desastres (Disaster Recovery Plan o DRP) es un enfoque estructurado y documentado que describe cómo una Institución puede reanudar el trabajo rápidamente después de un incidente no planificado.
      La ejecución de un DRP se aplica solo para las plataformas BIA (Business Impact Analysis), incluyendo plataformas que hayan sido declaradas como críticas y que formen parte de una solicitud de alguna Gerencia. Esto no impide que la etapa de levantamiento se lleve a cabo ya que corresponde a recopilación de información que todo proyecto debe manejar.

- Equipo Seguridad Aplicativa

    - **Ethical Hacking:** El objetivo de este punto de control es detectar las vulnerabilidades de los distintos sistemas y aplicaciones de una Institución, a través de ataques informáticos simulados realizados por los proveedores de Ethical Hacking. Realizar estos test permite anteponerse a eventuales ataques informáticos reales, y de esta manera proteger los sistemas de la Corporación antes de que estos ataques ocurran a mano de verdaderos delincuentes informáticos.

    - **Vulnerabilidades:** Una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.
      El objetivo de este punto de control es que todo proyecto antes de salir a producción debe considerar la revisión de vulnerabilidades para prevenir alguna explotación con fin malicioso. Si existen vulnerabilidades estas deben ser corregidas según un acuerdo de nivel de servicio (SLA por si sigla en Inglés) de Resolución.

    - **Seguridad en los Desarrollos:** Este punto de control tiene por objetivo asegurar la homogeneidad y conformidad de los requerimientos de seguridad en los sistemas, integrando los principios de seguridad en el ciclo de vida de desarrollo de un sistema (SDLC por su sigla en inglés), lineamientos regulatorios o propios de la Institución.
      Otro objetivo es el de garantizar que todo producto de software generado cuente con las suficientes revisiones y pruebas de seguridad en su código e infraestructura, que garanticen evidenciar los riesgos y maximizar su mitigación, previo a su paso a producción.

- Equipo Ciberdefensa e Inteligencia

    - **Seguridad Endpoint (Servidores y Estaciones de Trabajo):** Este punto de control tiene por objetivo securitizar los servidores, estaciones de trabajo y equipos móviles ante cualquier amenazas para el sistema, evitando que se transmitan a los dispositivos conectados mitigando problemas con amenazas de virus o de robo de datos.
      Los proyectos siempre deben considerar la instalación de los agentes de seguridad como línea base en la creación de servidores o estaciones de trabajo.

    - **Monitoreo:** Este punto de control tiene por objetivo incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información de la Corporación para analizar los ataques o posibles amenazas. El Monitoreo de ciberseguridad e inteligencia suma la tecnología, los procesos y las personas que apoyan la gestión integral de las amenazas a las que puede estar expuesta una Institución.
      Los proyectos siempre deben considerar el monitoreo de ciberseguridad basado en los riesgos declarados en la matriz de riesgo entregada por el equipo de Riesgo No Financiero.

    - **Fuga de Información - DLP (Data Loss Prevention):** Este punto de control tiene por objetivo prevenir la pérdida y fuga de datos, asegurando la implementación de los controles de seguridad necesarios para disminuir el riesgo de fuga o pérdida de información clasificada como sensible.
      Los proyectos siempre deben considerar el nivel de exposición de datos, según la clasificación de la información declarada por el equipo de Riesgo No Financiero y Gobierno de Datos.

- Equipo Controles de Ciberseguridad

    - **Control de Proveedores:** Este punto de control tiene como objetivo identificar, registrar, analizar, corregir y controlar los hallazgos u observaciones obtenidos de la evaluación de seguridad realizada a los proveedores, así mismo de cómo brindar reporte de la criticidad de los hallazgos en dicho proceso.
      Además, pretende fijar las medidas para el tratamiento de control y seguimiento de planes de acción correctivas a mitigar, con el objetivo de lograr un alto estándar en lo que seguridad se trata con los proveedores

que presten servicio a la Corporación.

- **Perfiles y Privilegios:** Este punto funciona como un control por oposición a la labor de Gestión de Identidades en su proceso de Alta, Baja y Modificación (ABM) de usuarios.
  Su objetivo es revisar las cuentas de usuarios (casos de uso) en plataformas, sistemas y aplicaciones, levantando hallazgos y gestionando sus remediaciones.

- **CAT - FFIEC:** Cybersecurity Assessment Tool (CAT) del Federal Financial Institutions Examination Council's (FFIEC) es un Framework adoptado por la Corporación en 2017, el cual debe ser cumplido por todas las áreas involucradas con algún control.
  Se aplica esta metodología como una forma unificada de controlar el cumplimiento de la ciberseguridad en las distintas áreas, con el fin de detectar, mitigar y cubrir posibles vulnerabilidades según lo descrito en cada control.
  Un control CAT es una declaración respecto a las actividades que se deben realizar dentro de un área y que tiene como fin definir si cumple o no con lo establecido en la definición del control. En el caso del modelo CAT-FFIEC no existe el cumplimiento parcial de una actividad.
  Su objetivo es ayudar a las instituciones financieras a identificar sus riesgos y determinar su preparación en ciberseguridad.

- Equipo de Sensibilización y Cultura

  - **Concientización:** Este punto de control tiene por objetivo mejorar las conductas de los colaboradores en el ámbito de ciberseguridad mediante capacitaciones operativas y técnicas, colabora en temas de formación canalizando los requerimientos de las unidades de la Gerencia de Seguridad Informática con el área de Formación. Este punto impulsa un programa de toma de conciencia dirigido a todos los colaboradores de la Corporación.

5.2 Creación del Proceso de Gestión Interna

La creación del proceso de gestión interna para resolver la necesidad de interacción de ciberseguridad con proyectos tecnológicos en el ciclo de vida (Figura 11) de un proyecto, iniciativa o mejora tecnológica se abordará como una iniciativa interna.

En las tareas dentro del proceso creado corresponden a la interacción con los puntos de control previamente definidos, los cuales definen la coordinación entre la Gerencia de Seguridad Informática y las Otras Gerencias que disponen de proyectos para revisar.

Proceso de Gestión Interna

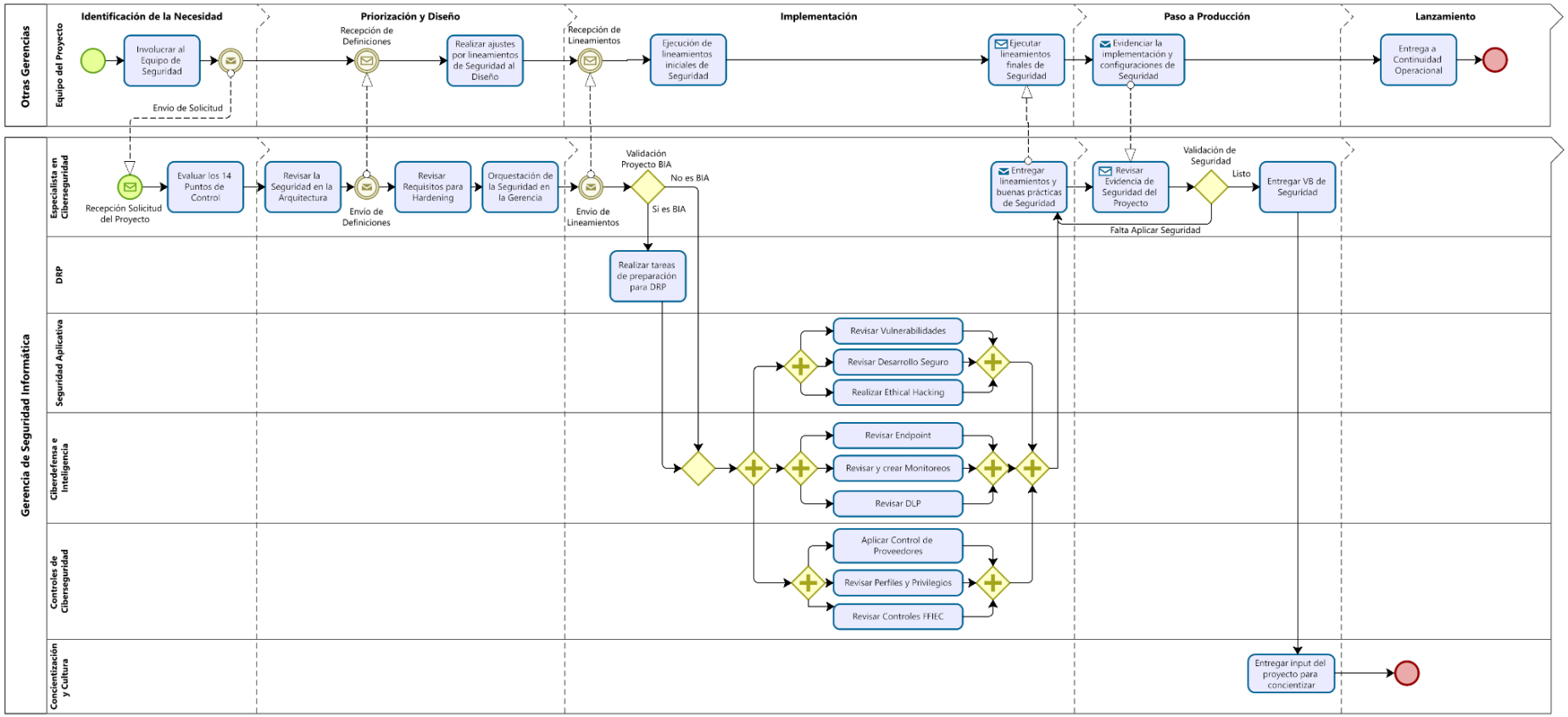


Figura 11: Proceso para la Interacción de Ciberseguridad con Proyectos Tecnológicos

La Figura 11 muestra la creación del proceso donde interactúa la Gerencia de Seguridad Informática con las distintas etapas de un proyecto para este nuevo escenario. A diferencia del actual funcionamiento, explicado en la situación actual, se incorporan puntos de control estandarizados como línea base de ciberseguridad, los que se implementan con una serie de herramientas que permitirán registrar y dar seguimiento a los lineamientos y buenas prácticas entregadas en cada punto de control. El proceso propuesto cuenta con las siguientes actividades desde la visión de ciberseguridad:

<table>
<tr><th>Entidad</th><th>Institución Financiera</th></tr>
<tr><td>Proceso</td><td>Interacción de Ciberseguridad con Proyectos Tecnológicos</td></tr>
<tr><td>Código Proceso</td><td></td></tr>
<tr><td>Responsable del Proceso</td><td>Equipo Especialista en Ciberseguridad</td></tr>
<tr><td colspan="2">Objetivo:

Realizar registro de la interacción de ciberseguridad con proyectos tecnológicos en la Gerencia de Seguridad Informática.</td></tr>
<tr><td colspan="2">Condiciones de Inicio:

● Proyectos tecnológicos con ingreso formalizado para revisión
● Proyectos tecnológicos que convocan proactivamente a Seguridad</td></tr>
<tr><td>Entradas:

● Proyectos que solicitan revisiones de Seguridad
● Proyectos donde Seguridad pide participación y revisión directa.</td><td>Salidas:

● Proyectos con interacción de ciberseguridad controlados, validados y registrados.
● Registro de ficha de proyecto con interacciones en puntos de control realizadas.</td></tr>
<tr><td colspan="2">Roles Participantes:

● Especialista en Ciberseguridad</td></tr>
</table>

- DRP
- Seguridad Aplicativa
- Ciberdefensa e Inteligencia
- Controles de Ciberseguridad
- Concientización y Cultura

Descripción de Actividades:

Actividad	**Descripción**
1. Identificación de la necesidad	El proyecto tecnológico genera una solicitud de revisión de seguridad que llega al Especialista en Ciberseguridad.
2. Priorización y Diseño	El Especialista en Ciberseguridad debe interactuar con el proyecto en 3 puntos de control: 1- Revisar la Seguridad en la Arquitectura enviando las definiciones en caso de que existan. 2- Revisar el Hardening de los componentes del proyecto 3- Realizar la Orquestación de la Seguridad en la Gerencia que es donde se apertura la revisión en conjunto con las otras unidades.
3. Implementación	El Especialista en Ciberseguridad envía los lineamientos al Equipo de Proyecto para su ejecución y luego valida si el proyecto es BIA, dando paso al punto de control vinculado al DRP donde se realizan las tareas de levantamiento para su preparación. En la etapa siguiente se paralelizan 9 puntos de control para la revisión en el proyecto, entregando lineamientos y buenas prácticas de seguridad que garanticen una ejecución por parte del Equipo del Proyecto.

4. Paso a Producción	El Equipo de Proyecto hace entrega de las evidencias de implementación y configuraciones de seguridad al Especialista en Ciberseguridad, el cual se encarga de revisar e iterar las veces que sea necesario para validar los puntos de control aplicados en el proyecto. Si se encuentran completados los puntos se entrega el visto bueno (VB) de Seguridad, para luego entregar los input generados para concientizar por parte de Concientización y Cultura.
5. Lanzamiento	El lanzamiento seguro de un proyecto es producto de las implementaciones de los distintos puntos de control, que se traducen en la entrega a continuidad operacional por parte del Equipo del Proyecto, quien administra y sustenta en el tiempo todos los controles realizados.

5.3 Creación del Pre - Jira

El Pre-Jira es un concepto creado para referirse a la etapa previa de la implementación con distintas herramientas tecnológicas. Se refiere a una hoja de Google Sheet creada con los puntos de control, definidos en la sección 5.2, que contiene los distintos proyectos en asignación del Especialista en Ciberseguridad. Esta Matriz de Trabajo para la adopción del proceso y gestión de los puntos de control, es un esfuerzo que permite un rápido ajuste por su diseño minimalista.

La creación del Pre - Jira es una forma de limitar posibles efectos negativos y sus consiguientes costos, así al exponerse la solución a la visión acotada de personas que serán usuarios, es posible determinar la viabilidad de la solución entre otros efectos positivos, como por ejemplo la obtención de feedback de manera temprana.

Se establecen los siguientes aspectos para monitorear el Pre-Jira:

- La comprensión de los usuarios a la adopción del proceso

- La comprensión de los usuarios a los estados de gestión de los puntos de control
- La validación de del diseño de la solución
- La escalabilidad con los distintos tipos de proyectos tecnológicos

5.3.1 Objetivos

Los objetivos planteados están referidos al Pre-Jira y complementan el seguimiento de las tareas del proceso.

- Determinar la forma correcta para realizar el seguimiento a los puntos de control dentro del proceso.

- Recoger oportunidades de mejora y ajustar el impacto de la creación del proceso en la gestión de la seguridad en proyectos tecnológicos.

- Obtener información que permita llevar la solución a una implementación con herramientas tecnológicas de centralización.

- Apoyar la formación del equipo en tiempo real al facilitar el contacto directo con el seguimiento previa implementación.

5.3.2 Ejecución del Pre-Jira

La ejecución de la matriz de trabajo Pre-Jira se inició en el mes de abril del 2022 con una reunión ejecutiva donde se dió el vamos para su uso. Se presentaron los objetivos y alcances de la ejecución, junto con la visión de los Especialistas en Ciberseguridad participantes en la transición.

A continuación se describen los aspectos generales del trabajo realizado.

El primer mes se capacitó a los Especialistas en Ciberseguridad para la transición en la adopción de la metodología de llenado de la matriz de trabajo, con los estados de un punto de control y su significado. Las presentaciones de capacitación consistieron en explicar la forma en que se debía anotar un proyecto y la interacción con un punto de control.

Los Especialistas en Ciberseguridad interactuaron directamente con el Pre-Jira llevando a la matriz ejemplos prácticos de los proyectos con los que interactúan día a día, lo que permitió facilitar la adopción de la matriz y acelerar el cambio en el proceso de gestión.

El inicio de la ejecución fue acompañado en todo momento por el comité del proyecto, utilizando la metodología ágil. Durante todo el mes se reforzó el uso de la matriz de Pre-Jira y su llenado, se resolvieron problemas y dudas que se fueron presentando, el equipo comité del proyecto resolvió complicaciones presentadas con la edición y realizó ajustes en la visualización de los puntos de control dentro de la matriz.

Los siguientes dos meses correspondientes al cronograma, se realizaron varios puntos de encuentro entre el Equipo de Especialistas en Ciberseguridad, considerando a los Especialistas en Ciberseguridad para la transición y al resto del equipo. En estas sesiones se transmitió el conocimiento de manera general, se evaluó el funcionamiento del Pre-Jira en los proyectos y se compartieron experiencias. Se acordaron colectivamente soluciones para la adopción en los distintos proyectos y se iban ajustando formas según requerimientos levantados en las sesiones.

Durante la operación del Pre-Jira se recibieron distintas observaciones de los Especialistas en Ciberseguridad. Estas básicamente fueron referidas a la forma de anotar un proyecto y los estados de los puntos de control. Con esta información el Comité del Proyecto analizó y realizó los ajustes necesarios liberando las correcciones rápidamente gracias al modelo de agilidad, permitiendo recabar información que sirvió para la siguiente etapa de implementación.

El resultado de la matriz de trabajo Pre-Jira se refleja a continuación en la Figura 12, donde en las filas se ven reflejados los proyectos (color azul) y en las columnas se ven reflejados los puntos de control (color verde). Además se agregaron campos adicionales en las columnas (color verde) como Plataforma, Fecha de Entrega, Líder del Proyecto y Documento de Evidencia, que aportaron información adicional de los proyectos y su proceso para la gestión interna de los puntos de control.

Matriz de Trabajo Pre-Jira

		Plataforma	Fecha	Lider	Documento	Especialistas de Ciberseguridad			DRP	Seguridad Aplicativa			Ciberdefensa e Inteligencia			Controles de Ciberseguridad			Sensibilización y Cultura
TEMAS	PROYECTOS	Tipo	Entrega	Proyecto	Evidencia	Arquitectura	Hardening	Orquestación	DRP	Ethical Hacking	Vulnerabilidad	Desarrollo	Endpoint	Monitoreo	DLP	Proveedores	Perfiles y Privilegios	FFIEC	Concientización
Data & Analytics	1- Nombre del Proyecto	PaaS	15 Feb (Prod)	Arquitecto	Link Documento							-							
	2- Nombre del Proyecto			Jefe de Proyecto															
	3- Nombre del Proyecto	IaaS		Arquitecto Ingeniero	Link Documento														
	4- Nombre del Proyecto	PaaS		Subgerente	Link Documento														
	5- Nombre del Proyecto			Colaborador Lider	Link Documento														
	6- Nombre del Proyecto	OnPrem		Colaborador Lider	Link Documento							-							
	7- Nombre del Proyecto	OnPrem		Colaborador Lider								-							
	8- Nombre del Proyecto	SaaS		Colaborador Lider								-							
	9- Nombre del Proyecto			Colaborador Lider								-							
	10- Nombre del Proyecto			Colaborador Lider															
Technology	1- Nombre del Proyecto	SaaS	Q1	Jefe de Proyecto	Link Documento							-				-			
	2- Nombre del Proyecto		Q4 2021 Q1 2022	Arquitecto Ingeniero	Link Documento							-				-	-		
	3- Nombre del Proyecto	PaaS		Arquitecto	Link Documento														
	4- Nombre del Proyecto	Onprem PaaS		Colaborador Lider						-		-				-			
	5- Nombre del Proyecto	FaaS		Colaborador Lider											-		-		
	6- Nombre del Proyecto			Colaborador Lider						-		-	-		-				
Governance & Central Systems	1- Nombre del Proyecto	DaaS (BIA)	14 Ene (Prod)	Arquitecto Ingeniero	Link Documento							-							
	2- Nombre del Proyecto	IaaS	14 Mar (Prod)	Arquitecto								-							
	3- Nombre del Proyecto			Arquitecto	Link Documento														
	4- Nombre del Proyecto	Proceso		Arquitecto	Link Documento	-	-		-			-	-		-	-	-	-	
	5- Nombre del Proyecto			Jefe de Proyecto	Link Documento							-							
	6- Nombre del Proyecto	Agentes		Jefe de Proyecto			-		-	-		-			-	-	-		

Figura 12: Pre-Jira para la gestión de los puntos de control

El llenado de la matriz en torno a los puntos de control revisados en un proyecto se realiza acorde a la Figura, la que representa los estados posibles de un punto de control expresados a continuación:

- **No OK:** Aún no se comienza a trabajar
- **En Progreso:** Hay trabajo que se está realizando
- **OK, Con Hallazgo:** Finalicé el punto con alguna observación
- **OK:** Finalicé el trabajo
- **No Aplica:** No es necesario el punto de control

Simbología	
🔴	No OK
🔵	En Proceso
🟡	OK, Con Hallazgo
🟢	OK
-	No Aplica

Figura 13: Simbología de los estados de un punto de control

6. IMPLEMENTACIÓN

La implementación se abordó como un proyecto tecnológico. En las etapas iniciales se coordinó y definió el gobierno del proyecto, junto con la planificación y calendarización de actividades, entre las cuales se destaca: El entendimiento de la situación actual a través del relevamiento de procesos, la especificación de las necesidades de revisión de ciberseguridad con su forma de dar seguimiento y la continuidad de las definiciones entregadas a los distintos proyectos tecnológicos.

La solución consideró la implementación de un conjunto de herramientas tecnológicas que recogen las necesidades relevadas para dar seguimiento y continuidad a los puntos de control, a través del cumplimiento de las buenas prácticas y lineamientos de ciberseguridad. Esto contempló la utilización de componentes desplegados del tipo Software as a Service (SaaS) que se encuentran en el Banco y comunicados entre sí por medio de distintas integraciones del tipo conectores, extensiones y enlaces.

La solución requirió de una adopción en un nuevo proceso de gestión interna por parte del equipo de Especialistas en Ciberseguridad. Para apoyar esto y lograr la adhesión necesaria del equipo, se consideraron distintas jornadas de adopción y sensibilización con el equipo, las que sumadas al material entregado por la Corporación sobre agilidad y gestión del cambio permitieron avanzar hacia el éxito del proyecto.

6.1 Diseño General de la Implementación

El diseño de la solución tecnológica fue enfocado en la estandarización del proceso de gestión del Especialista en Ciberseguridad al momento de participar en los proyectos tecnológicos. La solución conecta los distintos puntos de control de ciberseguridad que son aplicados en la interacción con proyectos tecnológicos.

La implementación tiene tres componentes centrales: la primera un espacio de centralización de definiciones para los puntos de control en la herramienta Confluence, la segunda es la materialización del seguimiento de los puntos de control a través de flujos de trabajo creados en la plataforma Jira y la tercera es la plataforma de presentación realizada en Looker Studio donde se muestran las distintas métricas obtenidas en el cumplimiento de la ciberseguridad por parte de los proyectos tecnológicos.

La siguiente figura representa el esquema de la solución de alto nivel, aquí se

encuentran representadas las interacciones de los componentes centrales confluence, Jira y Looker Studio.

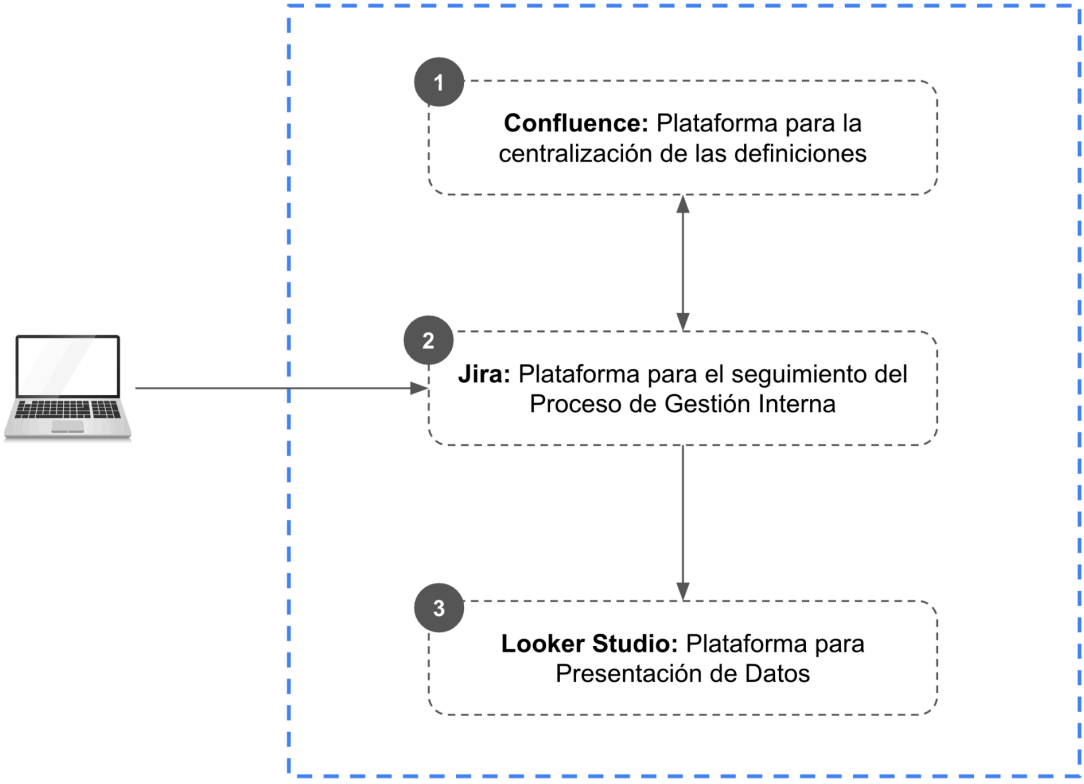


Figura 14: Diseño General de la Solución

La figura ilustra un diagrama general de la solución donde se visualizan las interacciones entre las plataformas. En ésta se representa la comunicación entre plataformas, además de identificar el uso de cada una. La plataforma Jira almacena todas las interacciones de ciberseguridad con los proyectos tecnológicos de la Corporación, es por eso que el usuario ingresa desde el punto 2 para la validación del proceso de gestión interna. El Especialista en Ciberseguridad tiene acceso a los tres componentes del diseño que interactúan entre sí, ya sea de forma separada o integrados a través de Jira.

6.2 Diseño Arquitectónico

La Arquitectura para la solución que sustenta el proceso de gestión interna se basa en la necesidad de contar con componentes que permitan entregar una implementación robusta pero amigable al uso, que sea capaz de escalar según las necesidades actuales y futuras de ciberseguridad, así como también a las necesidades orientadas a los tipos de proyectos tecnológicos y cambios organizacionales de estructura.

6.2.1 Arquitectura de Componentes

El Banco cuenta con una Arquitectura Tecnológica variada para sus sistemas, estos pueden ser de manera local (on premise) o en la nube (Cloud) en sus distintos tipos de servicios (as a Service), estos son: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Dado este escenario, es que la solución desde un principio se plantea bajo el concepto de SaaS, considerando la adaptabilidad y escalabilidad que necesita el modelo, además de los costos reducidos e integrados en la facturación total por utilización de las plataformas en toda la Institución.

La arquitectura de esta solución se diseñó a partir de tres grupos de componentes centralizados por Jira Work Management y que dan visibilidad a la gestión del proceso interno, de acuerdo al siguiente diagrama:

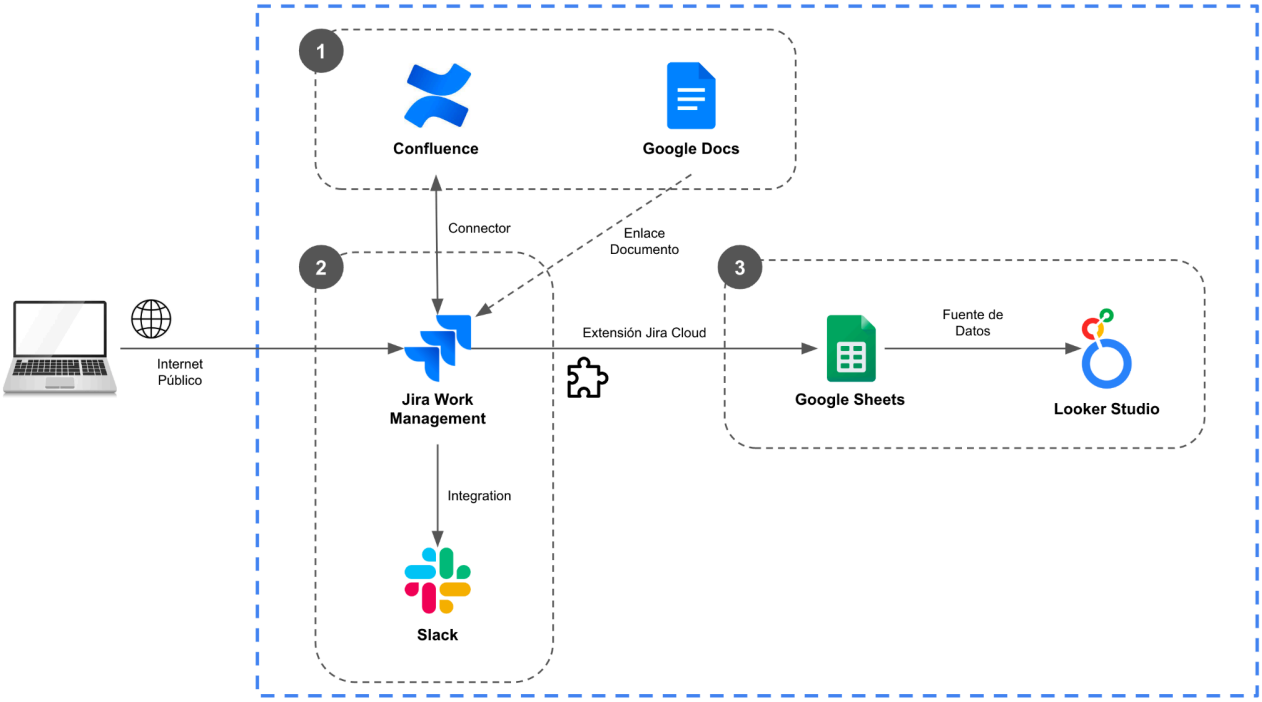


Figura 15: Arquitectura de Componentes de la Solución

En la figura se representa la arquitectura de componentes como modelo de construcción de la solución, aperturada en los tres componentes centrales y sus interacciones. A continuación se describen cada uno de los componentes.

6.2.2 Componentes de centralización de las definiciones

El conocimiento juega un papel relevante en los proyectos dentro de una Institución, ya que determina la capacidad de acción que tiene un Especialista en Ciberseguridad en la entrega de un punto de control y del seguimiento para su cumplimiento. Es por esto que se hizo importante documentar tanto las definiciones entregadas como también los avances generados.

Para la centralización y documentación de las definiciones de los puntos de control de Ciberseguridad se utilizó Confluence y para la documentación del avance y cumplimiento de un proyecto se utilizó Google Docs, ambas plataformas descritas a continuación:

- **Confluence:** Atlassian compañía detrás de esta plataforma describe Confluence como un espacio de trabajo en equipo donde el conocimiento y la colaboración se encuentran [14]. En otras palabras, es una plataforma en línea donde las personas pueden trabajar desde una serie de documentos compartidos en Cloud.

  La característica principal que se trabajó en esta tesis y desde la que trabajan los usuarios son las páginas. Estos son documentos que los miembros del equipo crean en Confluence Cloud y que se pueden editar en tiempo real, con comentarios y notificaciones de colegas.

  Las páginas se almacenan en espacios de trabajo donde los equipos pueden colaborar en proyectos y mantener todo el contenido organizado. Los usuarios pueden crear tantos espacios como necesite un equipo y los espacios se pueden personalizar con nombres, imágenes, enlaces, calendarios y más.

- **Google Docs:** Es una herramienta de Google que permite crear y editar documentos en línea y a la que se accede a través de cualquier dispositivo conectado a internet. Con este procesador de textos, cualquier usuario puede redactar documentos que se almacenan en la nube y que pueden ser trabajados colaborativamente.

  La importancia tomada en esta implementación es la de almacenar automáticamente los avances de un proyecto dentro de un documento que permita el trabajo colaborativo. Además la de restringir su acceso a personas externas de la Gerencia de Seguridad Informática, siendo esta última una característica fundamental para la implementación de esta plataforma.

6.2.3 Componentes del proceso de gestión interna

Los componentes del proceso de gestión interna creado, necesariamente se potencian con herramientas tecnológicas que permitan dar seguimiento e historia de los trabajos realizados. Lo anterior, como forma de enfocar el trabajo de ciberseguridad, que persigue un mejoramiento continuo de las actividades realizadas a través de los puntos de control en un proyecto.

Para el seguimiento de los puntos de control dentro de un proyecto se utilizó Jira y para la historia de los trabajos realizados se utilizó Slack, ambas plataformas descritas a continuación:

- **Jira Work Management:** Es una plataforma Cloud de Atlassian dirigida hacia la gestión de proyectos, seguimiento de errores e incidencias, que permite supervisar, administrar, rastrear y manejar todo tipo de proyectos dentro de la organización [15].

  Jira permite llevar a cabo una planificación personalizada, con una evolución escalable que se adapte a la comodidad de todos los miembros del equipo, teniendo una estructura clara y priorizando las tareas y/o incidencias, permitiendo contar con una visión globalizada respecto al trabajo del equipo involucrado en este proyecto.

  Con la utilización en este proyecto de Jira Work Management en específico, es posible gestionar tanto el proyecto como al equipo de trabajo, a través de workflows (flujos de trabajo), donde se definen todos aquellos procesos, tareas y responsables a través de paneles Kanban. Esta versión es un BPM (Business Project Management).

- **Slack:** Es una aplicación de mensajería para empresas que conecta a las personas con la información que necesitan [16]. Está pensada para equipos y lugares de trabajo, puede utilizarse en múltiples dispositivos y plataformas, y está equipada con sólidas funciones que permiten no sólo chatear uno a uno con los asociados, sino también en grupo. También es posible subir y compartir archivos con los distintos miembros del equipo, así como integrarse con otras aplicaciones y servicios. Además permite controlar de forma granular casi todos los ajustes, incluida la posibilidad de crear emoji personalizados.

  Esta herramienta permite la colaboración en las comunicaciones a través de mensajes, canales, menciones y reacciones, entre otros, pero como principal

función en este trabajo de tesis es por su capacidad de integrarse con múltiples herramientas en particular con Jira lo que la vuelve una plataforma potenciadora para el desarrollo de este proyecto aplicándola principalmente como registro de auditoría con un canal de logs.

6.2.4 Componentes para la presentación de datos

La presentación de los datos es fundamental para la toma de decisiones, ya que estos deben contar la historia de lo sucedido en los proyectos en torno a los puntos de control de ciberseguridad.

Para presentar un dato también fue necesario implementar una fuente de datos que permitiera almacenar y verificar los datos previa configuración. Para el almacenamiento se utilizó Google Sheet y para la presentación se utilizó Looker Studio, ambas plataformas descritas a continuación:

- **Google Sheet:** Es una herramienta de Google que permite trabajar con hojas de cálculo de manera online. Esta sirve para organizar y analizar una gran cantidad de datos, crear informes personalizados, automatizar cálculos, colaborar con diferentes equipos, etc. Otra característica de esta herramienta es que se puede almacenar datos, hacer seguimiento de métricas de rendimiento y crear paneles.

  Su capacidad para integrarse con Looker Studio y presentarse como una fuente de almacenamiento de datos exportados de Jira Work Management a través de Jira Cloud for Sheets hacen de Google Sheet una herramienta fundamental para la presentación de los datos de esta tesis.

- **Looker Studio:** Es una herramienta de Google, la que hasta hace poco era llamada Data Studio lanzada en el año 2016. Se utiliza principalmente para la visualización y análisis de datos, ya que convierte datos en informes y paneles claros, totalmente personalizables, fáciles de consultar y compartir [17].

  Su capacidad de integración y vinculación con fuentes de datos en almacenamiento, hace de Looker Studio una herramienta completa para el trabajo de esta tesis. Existe una infinidad de alternativas para la creación de informes y dashboard de control, destaca por su variedad de opciones de personalización para el trabajo de datos en vivo y controles interactivos donde es posible centralizar los datos según clasificación y visualización.

6.3 Implementación en Confluence

Todos los puntos de control previamente definidos en la sección 5.1 de la solución fueron creados y profundizados en Confluence, con la finalidad de que cualquier proyecto consulte proactivamente estos controles y los aplique bajo la mirada de ciberseguridad y este nuevo proceso de gestión.

La justificación de la implementación en confluence de una estructura jerárquica para la documentación de los puntos de control de seguridad, se presenta en:

- La complejidad para encontrar un documento, sin estar familiarizado con el árbol jerárquico
- El alto volumen de documentos que no se encuentran vinculados a los puntos de control de seguridad

La implementación permitió dar una solución a los dos puntos anteriores, ya que la estructura implica una modificación directa al árbol jerárquico en Confluence del Equipo Especialistas en Ciberseguridad, disminuyendo la complejidad que significa actualmente encontrar un documento. Lo anterior debido a que Confluence se utiliza para la publicación de múltiples documentos del equipo, los que representan un total de más de 300 páginas no categorizadas. Para entender la organización de la documentación de los puntos de control es necesario revisar los puntos a continuación.

6.3.1 Funcionamiento del árbol jerárquico

La idea base de la organización e implementación de la documentación en Confluence se encuentra estructurada en un árbol [18] el cual se irá balanceando y reestructurando según el siguiente criterio:

Si para un mismo Ni de nivel Li hay más de un nodo que contiene los mismos tipos de documentos vinculados a un punto de control (más de un nodo que contenga a Ni) entonces, el nodo Ni disminuye en uno la profundidad ubicándose en el nivel Li-1 y todos los nodos que tenían a Ni pasarán a ser hijos de Ni.

Supongamos que tenemos el siguiente árbol jerárquico:

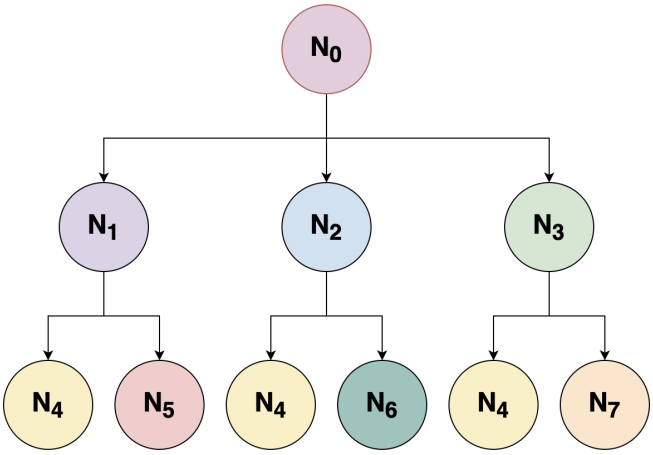


Figura 16: Ejemplo árbol jerárquico

La Figura 16 muestra la ubicación en el segundo nivel que tiene el nodo N4, el cual se repite como hijo de todos los nodos del primer nivel (N1, N2 y N3). Eso implica que el nodo N4 por importancia debe subir un nivel y puede (o no) tener como hijos a los nodos que anteriormente eran el nodo padre de N4. Esto depende exclusivamente de si todas las versiones del nodo N4 se pueden mezclar, o bien si aún así requieren estar divididas. Si este caso se vuelve necesario, estaríamos en presencia de un posible nuevo punto de control de seguridad.

Dependiendo de la posibilidad de mezclar los nodos N4, el árbol jerárquico original puede quedar como alguna de las siguientes dos figuras:

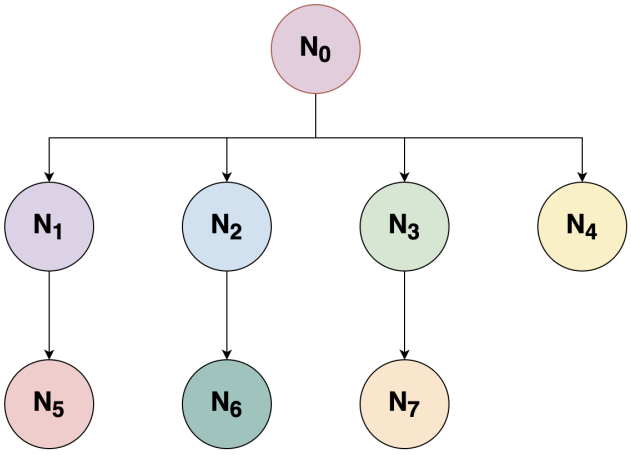


Figura 17: Opción 1 nuevo árbol jerárquico

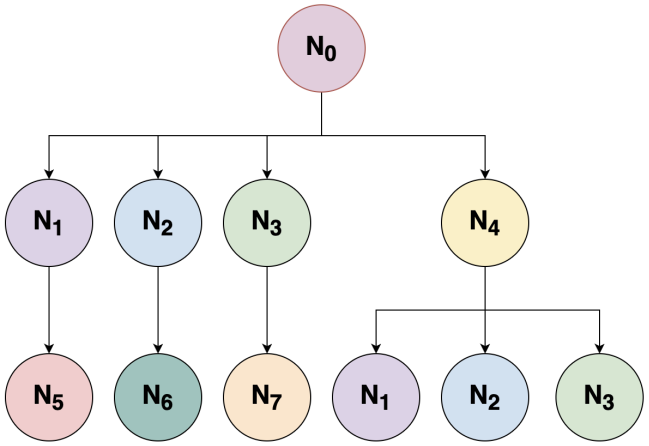


Figura 18: Opción 2 nuevo árbol jerárquico

Las nuevas versiones del árbol jerárquico no tienen como objetivo simplificar el árbol en términos de anchura o amplitud (número de nodos en un nivel y el número de hojas respectivamente). El objetivo de este balanceo y reestructuración del árbol es tener en los niveles más cercanos a la raíz los documentos vinculados a los puntos de control que, por repetirse en más de un nodo, requieran ser encontrados más rápido, o con una menor navegación dentro del árbol.

6.3.2 Clasificación de los puntos de control

Siguiendo la lógica del funcionamiento jerárquico de la sección anterior, se agruparon los puntos de control bajo el modelo de la opción 2 nuevo árbol jerárquico de la figura 18, con el objetivo de ordenar las distintas categorías dentro del Confluence y así normar la forma de documentar del equipo Especialista en Ciberseguridad. Del mismo modo, se presenta como una manera de consultar los diferentes puntos de control por parte de los equipos de proyectos.

Esta clasificación de los puntos de control, en color naranja, se ve reflejada en la Figura 19 de la siguiente manera:

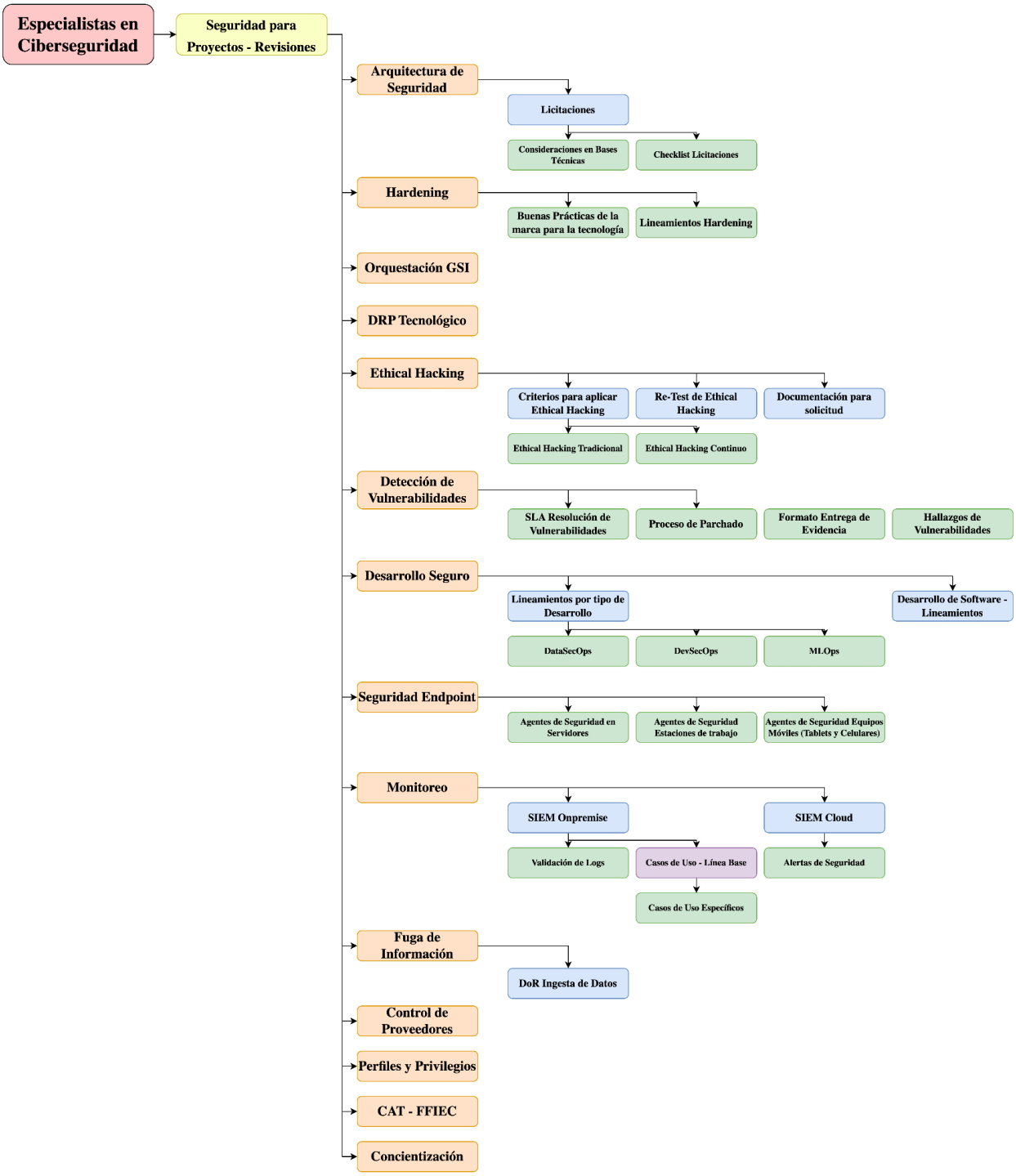


Figura 19: Clasificación de documentación de los puntos de control

La visualización de la clasificación dentro de la herramienta Confluence se presenta en el lado izquierdo de la siguiente figura:

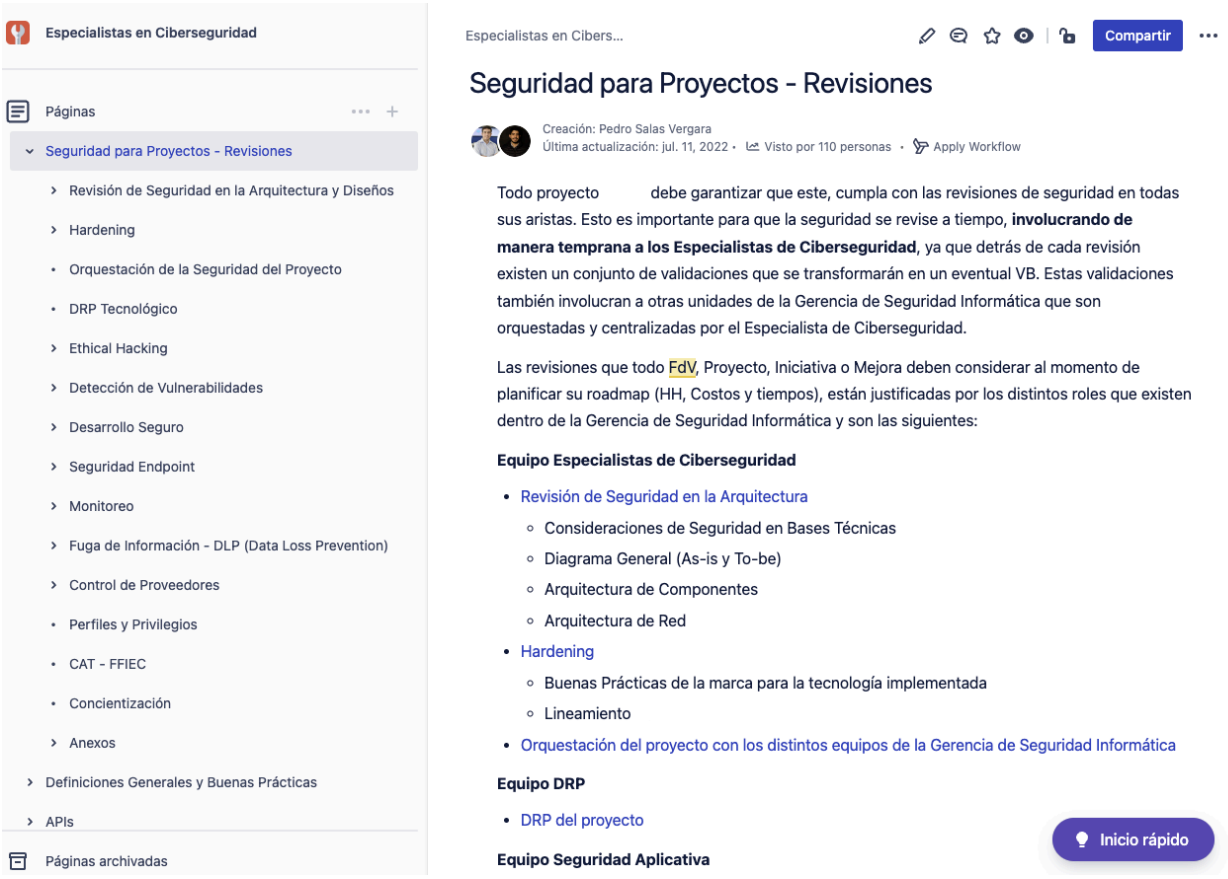


Figura 20: Confluence de los Puntos de Control de Seguridad

6.4 Implementación en Jira Work Management

La implementación en Jira recoge lo aprendido en la etapa del Pre-Jira descrita en el capítulo 5.3 y llevado a la herramienta de Atlassian Jira. Esta herramienta registra y evoluciona el seguimiento de los proyectos para dar mayor visibilidad del trabajo realizado, para ello fue necesario contemplar los siguientes puntos:

6.4.1 Modelo de Jerarquía

Para definir correctamente la implementación de los puntos de control en Jira, se realizó la definición de un modelo jerárquico basado en la estructura de gestión de proyectos de Atlassian [19]. Para llevar a cabo el modelo se agruparon los proyectos y puntos de control bajo 3 conceptos claves:

1. **Épica:** Una Épica es una gran cantidad de trabajo que se desglosa en varias tareas, por lo tanto una épica representa cualquier proyecto, iniciativa o mejora

en las que participe un Especialista en Ciberseguridad y de las que se desglosan tareas.
Las definiciones de proyecto, iniciativa o mejora descritas a continuación consisten en una breve estandarización de los conceptos:

- **Proyecto:** Conjunto de objetivos que llevan a un resultado. Un proyecto es clasificable según su ámbito de acción y siempre debe considerar el factor tecnológico.

- **Iniciativa:** Propuesta que impulsa una persona o unidad para una acción específica.

- **Mejora:** Cambio o progreso de una condición menor hacia un estado mejor en un plataforma o ambiente tecnológico.

2. **Tarea:** Una tarea es el equivalente a un punto de control y se encuentra siempre asociada a un proyecto. Un proyecto contiene las 14 tareas definidas como puntos de control, las que requieren ser realizadas dentro del proceso para la revisión de ciberseguridad. Una tarea en un proyecto puede definir sub-tareas si fuera necesario.

3. **Etiqueta:** Una etiqueta es una palabra clave que se agrega para categorizar un concepto relevante para su medición. Una etiqueta puede contener otras etiquetas catalogadas como subetiquetas sucesivamente.
   Se categorizaron en etiquetas los Equipos responsables que manejan un punto de control dentro de la Gerencia de Seguridad Informática y la clasificación de los vehículos estratégicos explicado en la sección 3.1 dentro de la situación actual.

A continuación la figura 21 muestra la estructura del modelo tomando como referencia los puntos anteriormente mencionados:

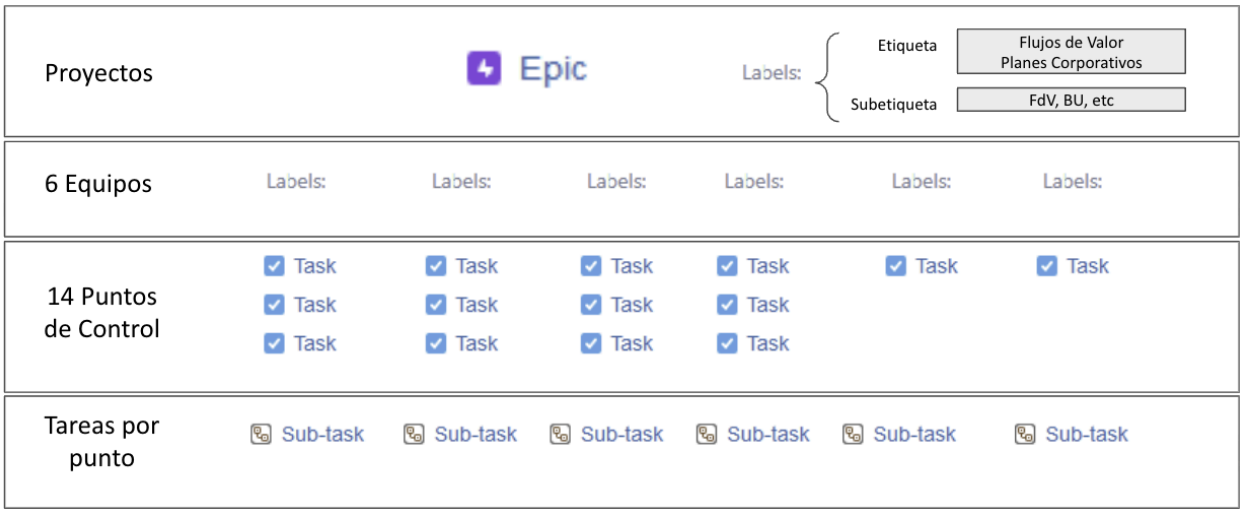


Figura 21: Modelo de Jerarquía para la implementación en Jira

6.4.2 Flujo de Trabajo para Proyectos

El flujo de trabajo para proyectos se refiere al conjunto específico y ordenado de estados que deben completarse para declarar que un proyecto ha finalizado. Cada cambio de estado del proyecto depende de la finalización de un estado anterior.

La siguiente figura muestra el flujo de trabajo de un proyecto con todos sus cambios de estados posibles:

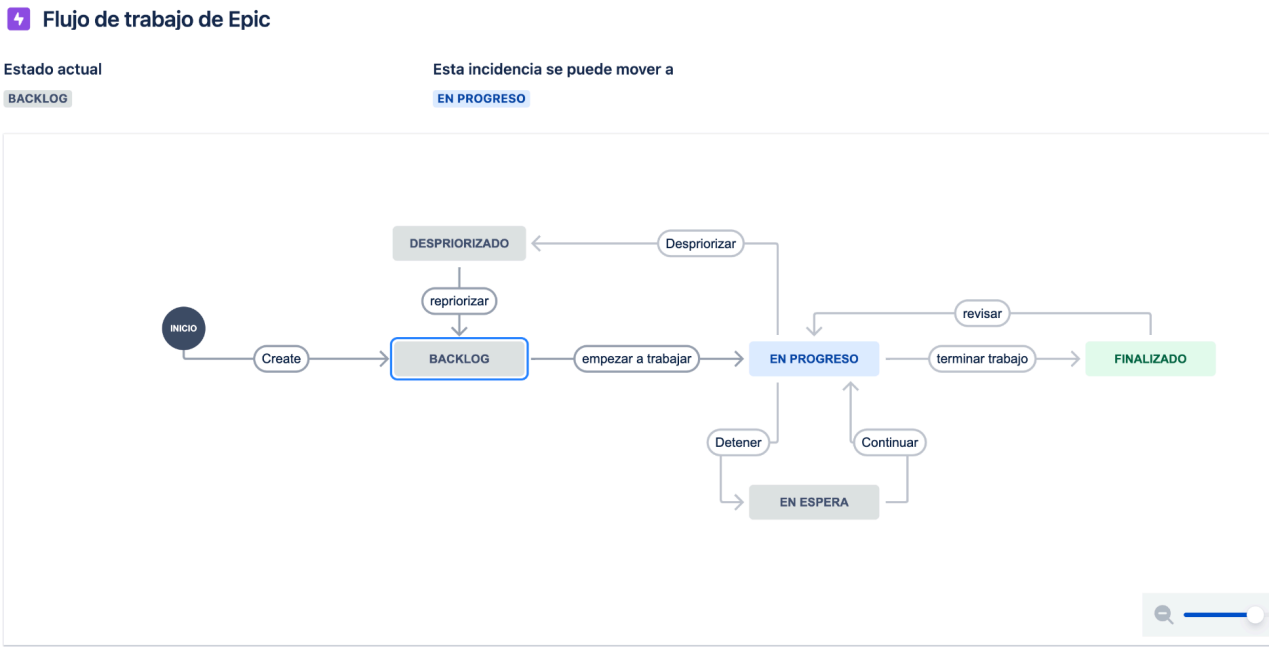


Figura 22: Flujo de Trabajo de un Proyecto

A continuación se describen las definiciones de un estado en el proyecto que sustentan el flujo de trabajo de la figura 22:

- **BACKLOG (GSI):** Cuando se crea un proyecto, se le asigna por defecto este estado. Se debe mantener en este estado hasta que exista la primera interacción con los involucrados del Proyecto.

- **EN PROGRESO (GSI):** Se debe cambiar a este estado siempre y cuando haya existido la primera interacción con el equipo involucrado en el Proyecto.

- **EN ESPERA(GSI):** Se utiliza este estado cuando ocurre una actividad en el proyecto que genera dependencia en las actividades de Seguridad.

- **FINALIZADO (GSI):** Se utiliza este estado cuando un proyecto finaliza la ejecución de los 14 Puntos de Control, en sus estados No Aplica o Finalizado.

- **DESPRIORIZADO (GSI):** Se utiliza este estado cuando un proyecto se desprioriza formalmente con evidencia adjunta que lo respalde.

6.4.3 Flujo de Trabajo para Puntos de Control

El flujo de trabajo para puntos de control se refiere al conjunto específico y ordenado de estados que deben completarse para declarar que un punto de control ha finalizado. Cada cambio de estado del proyecto depende de la finalización de un estado anterior.

La siguiente figura muestra el flujo de trabajo de un punto de control con todos sus cambios de estados posibles:

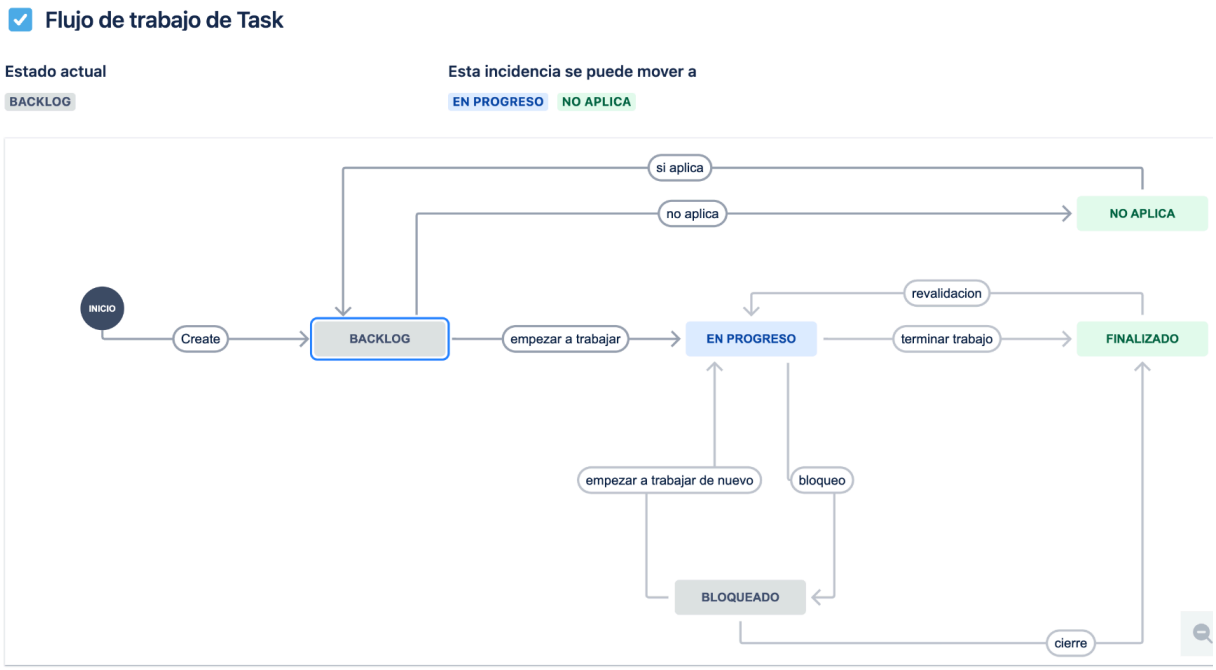


Figura 23: Flujo de Trabajo de un Punto de Control

A continuación se describen las definiciones de un estado en los puntos de control que sustentan el flujo de trabajo de la figura 23:

- **BACKLOG (GSI):** Cuando se crean los puntos de control dentro del proyecto, se les asigna por defecto este estado. Se debe mantener en este estado hasta que exista la primera interacción con las personas involucradas en el punto de control.

- **EN PROGRESO (GSI):** Cuando generé la primera interacción con las personas involucradas (responsables).

- **BLOQUEADO (GSI):** Cuando tengo o se me declara un problema para avanzar.

- **FINALIZADO (GSI):** Cuando soy capaz de evidenciar las tareas involucradas en el término del Punto de Control.

- **NO APLICA (GSI):** Cuando el contexto del Proyecto entrega información suficiente como para determinar que no aplica el Punto de Control según juicio experto.

6.4.4 Visualización en Fichas de Proyectos

La figura 24 muestra la configuración realizada para un proyecto directamente desde Jira categorizado bajo el modelo de jerarquías con los campos agregados. Todos los proyectos tienen esta vista estándar creando así una ficha de proyecto con las revisiones de sus estados para los distintos puntos de control.

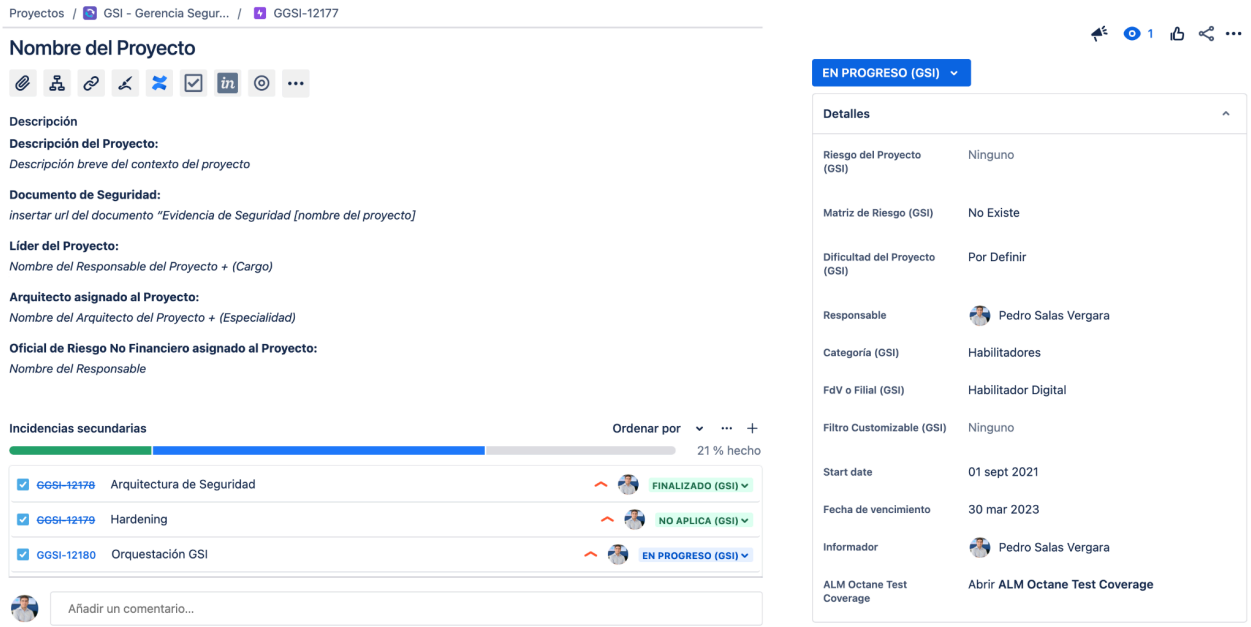


Figura 24: Ficha de un proyecto en Jira

Para una ficha de un proyecto se consideraron los siguientes temas:

- Información de Contexto del Proyecto (Descripción y Stakeholders)
- Generación del Documento de Evidencia de Seguridad del Proyecto.
- Definición inicial de qué tareas aplican y cuáles no aplican según proceso.
- Conocimiento del Riesgo del Proyecto
- Conocimiento de la Dificultad del Proyecto (*previa fórmula)
- Categoría y Flujo de Valor o Filial
- Fecha de inicio de participación del Especialista en Ciberseguridad
- Fecha de Término de participación del Especialista en Ciberseguridad
- Definición del Especialista responsable de la Seguridad en el Proyecto.
- Definición de un informador para los casos en que existan proyectos con participación de múltiples Especialistas en Ciberseguridad.

6.4.5 Visualización en Fichas de Puntos de Control

La figura 25 muestra la configuración realizada para un punto de control directamente desde Jira categorizado bajo el modelo de jerarquías con los campos agregados. Todos los puntos de control tienen esta vista estándar creando así una ficha de punto de control con su respectivo estado de avance.

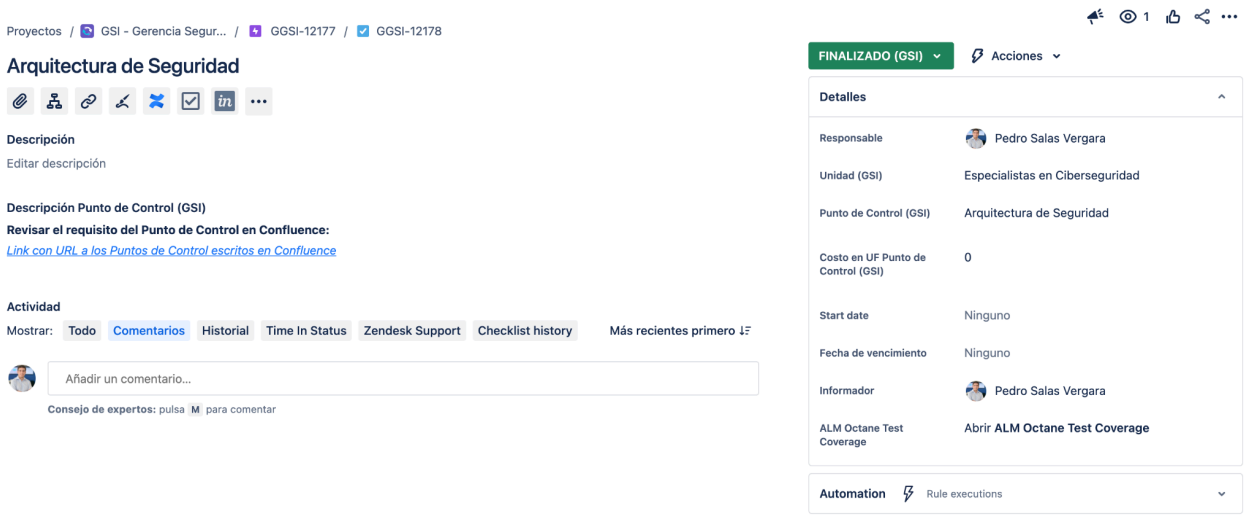


Figura 25: Ficha de un Punto de Control en Jira

Para una ficha de un punto de control se consideraron los siguientes temas:

- Descripción de la definición del Punto de Control en Confluence adjunto en cada ficha del Punto de Control.
- Unidad responsable e involucrada en el punto de control.
- Fecha de inicio de la interacción con las unidades responsables de los puntos de control.
- Fecha de entrega con evidencia del punto de control Finalizado.
- El informador siempre será el Especialista en Ciberseguridad dando seguimiento al avance del Punto de Control.
- Registro de todas las evidencias que llevaron al cumplimiento de un punto de control en el Documento de Evidencia del Proyecto. Este Documento será entregado como un informe de auditoría y solo debe ser de uso interno.

6.4.6 Funciones de Planificación para Proyectos

El software de Jira es personalizable, por lo que se configuraron una serie de funciones para la visualización de los proyectos con sus distintos puntos de control. Estas funciones permiten adaptar las vistas dependiendo del tipo de información relacionada exclusivamente con proyectos, exclusivamente con puntos de control o vinculada directamente a un Especialista en Ciberseguridad.

Las funciones habilitadas para la visualización de los proyectos son las siguientes:

1. **Tablero:** Disponibilizada para mostrar los proyectos bajo una vista Kanban
2. **Lista:** Disponibilizada para mostrar los proyectos con sus correspondientes puntos de control en forma de listas.
3. **Calendario:** Disponibilizada para mostrar las fecha de inicio y término de los proyectos en formato de calendario mensual.
4. **Cronograma:** Disponibilizada para mostrar los proyectos en formato carta gantt.
5. **Incidencias:** Disponibilizada para mostrar todos los proyectos y puntos de control (épicas y tareas) en una misma vista, con la opción de generar filtros para búsquedas avanzadas.

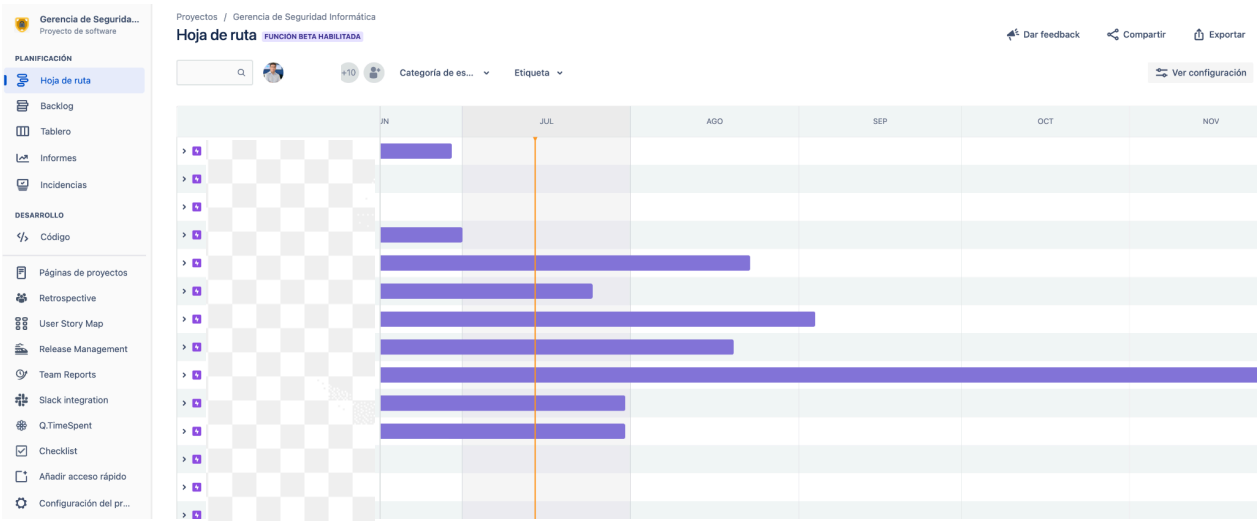


Figura 26: Funciones de planificación para proyectos

La figura 26 muestra específicamente la función de vista cronograma, herramienta gráfica cuyo objetivo es exponer el tiempo de dedicación previsto para la realización de los distintos proyectos con sus puntos de control, a lo largo de la fecha de inicio y de término previamente declaradas.

6.5 Dashboard de la Gerencia en Jira

Una organización como un Banco que crece constantemente, tiene un volumen cada vez mayor de proyectos que visualizar a los que se les debe aplicar ciberseguridad. La importancia de centralizar el trabajo realizado y mostrarlo de una manera simple, hace que esta implementación sea fundamental para dar seguimiento y tomar decisiones.

Para llevar a cabo este propósito, fue necesario realizar las siguientes acciones que permitieron configurar un dashboard disponible para el equipo de Especialistas en Ciberseguridad y sus Jefaturas.

6.5.1 Creación del panel y utilización de gadgets

Un panel es una página creada en Jira que para este trabajo es un dashboard y que tiene por objetivo mostrar los datos de los proyectos, los puntos de control y etiquetas a través de gadgets.

Un gadget es un objeto pequeño, es decir una pieza de funcionalidad que ofrece contenido dinámico que se visualiza en el panel del dashboard. El objetivo de los gadgets es agregar o resumir información que permita a los Especialistas en Ciberseguridad y Jefaturas hacer seguimiento en tiempo real de todo lo que está ocurriendo en los proyectos en torno a los puntos de control. Estos gadgets pueden ser listas, resúmenes o gráficos estadísticos.

Se construyó un panel llamado Dashboard Gerencia de Seguridad Informática que presenta en detalle una serie de datos, tales como:

- Categoría de los proyectos
- Estado de avance de los proyectos
- Dificultad de los proyectos
- Riesgo de los proyectos
- Cantidad de proyectos por etiqueta de clasificación
- Estado de los proyectos por etiqueta de clasificación
- Estado total de los puntos de control
- Detalle por estado de avance de los puntos de control
- Cantidad de puntos de control por unidad
- Cantidad y estado de proyectos por Especialista en Ciberseguridad
- Dificultad de proyectos por Especialista en Ciberseguridad
- Estado total de los puntos de control de los Especialistas en Ciberseguridad

- Cantidad y estado de puntos de control por Especialista en Ciberseguridad

Estos datos presentados en el dashboard provienen de la implementación del Jira de las épicas, tareas y etiquetas basadas en el modelo de jerarquías y que representan todos los proyectos trabajados por los Especialistas en Ciberseguridad y su interacción con los distintos puntos de control.

La siguiente figura muestra la forma de presentación que tiene el dashboard configurado con los distintos gadgets en Jira y que obtiene sus datos mediante la creación de distintos filtros de búsqueda.

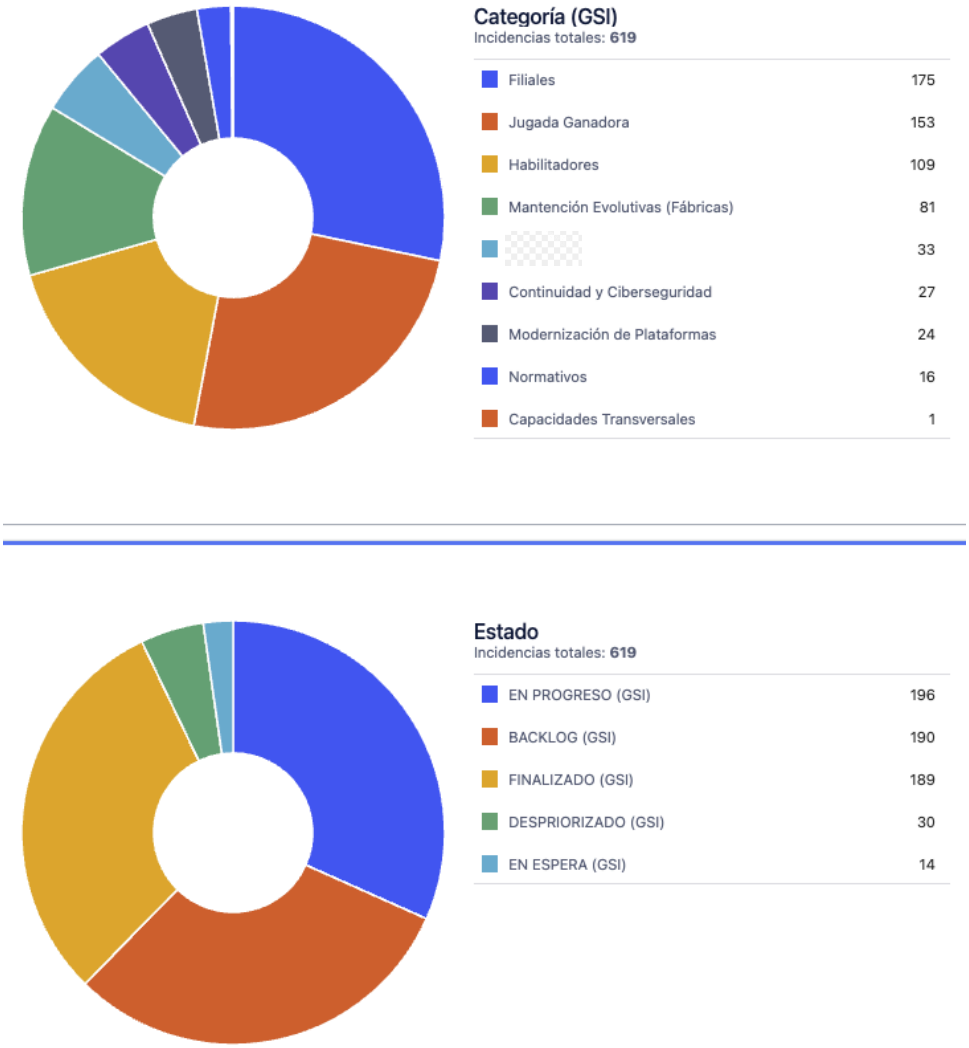


Figura 27: Visualización Dashboard Gerencia Seguridad Informática

6.5.2 Creación de los filtros con JQL

JQL significa Jira Query Language (Lenguaje de consulta de Jira) y es la forma más potente y flexible de buscar incidencias en cualquier proyecto en Jira. Los resultados de las consultas se guardaron y utilizaron como filtros y vistas en todo Jira (incluidos los tableros) en la implantación de esta tesis.

A través del cuadro de búsqueda de Jira se utilizaron búsquedas para incidencias que corresponden a épicas y tareas, que según la definición creada para el modelo de jerarquías corresponden a los proyectos y puntos de control. Estas queries para búsquedas se dividen en dos tipos, básicas y avanzadas explicadas a continuación:

- Las **búsquedas básicas** presentan un conjunto de formularios que pueden rellenar, como el nombre del proyecto, el tipo de incidencia, el estado y la persona asignada. Las búsquedas básicas se utilizaron para obtener una visualización de prioridad para las épicas, tareas, su estado y responsables.

- Las **búsquedas avanzadas** son el fuerte para la implementación de este dashboard y donde hubo que adentrarse en JQL, usándolo para hacer consultas. Las consultas son una serie de elementos simples encadenados para formar una pregunta más compleja. Se utilizaron consultas con cuatro partes básicas: campos, operadores, valores y palabras clave, explicadas a continuación:

    - **Campo:** Los campos son diferentes tipos de información en el sistema. Los campos de Jira incluyeron prioridad, etiqueta, tipo de incidencia, entre otros.

    - **Operador:** Los operadores son el corazón de la consulta. Relacionan el campo con el valor. Los operadores que más se utilizaron incluyen al igual (=), no igual (¡!), menos que (<), entre otros.

    - **Valor**: Los valores son los datos reales de la consulta. Son el elemento que se busca.

    - **Palabra clave**: Las palabras clave son palabras específicas del lenguaje que tienen un significado especial, las más utilizadas en este proyecto son el AND y OR.

Todas las búsquedas creadas bajo la sintaxis de JQL representadas en la figura 28,

fueron guardadas en Jira las cuales se utilizaron para ser vinculadas con los gadgets y alimentar la presentación de sus resultados en el panel Dashboard.

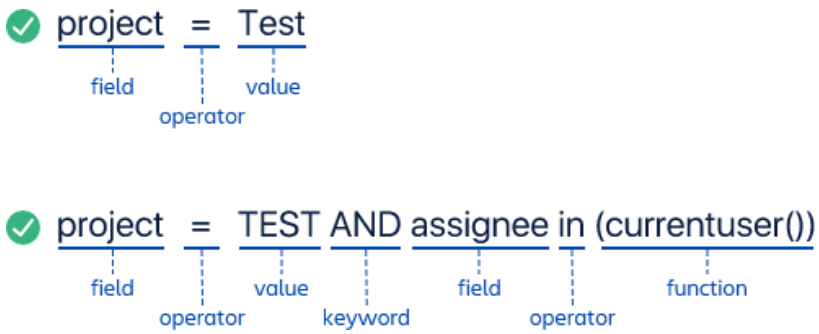


Figura 28: Sintaxis JQL utilizada para los filtros en Jira

6.6 Implementación en Looker Studio

La necesidad de una presentación para la Gerencia de Seguridad Informática generó la creación de un panel de control o dashboard que permite la obtención de datos para el apoyo a la toma de decisiones.

Al momento de implementar la gran cantidad de datos generados en Jira y llevados a la fuente de datos consumibles por Looker Studio, generó el riesgo de una sobrecarga de información que fue mitigada con grupos de datos previamente definidos y métricas relevantes para una toma de decisiones inicial.

La importancia de consolidar los datos de las revisiones de ciberseguridad a través de los puntos de control, generó la necesidad de hablar de un mapeado de datos como la mejor manera de construir una imagen clara del cumplimiento de los proyectos dentro de la Corporación.

La implementación consideró una evolución en las fuentes de datos cargadas, la que llevó a requerir combinar las distintas fuentes de datos para generar gráficos más representativos y dinámicos en su interacción.

La figura 29 muestra una vista general de una de las 12 hojas por temática del dashboard creado con las fuentes de datos combinadas y que apertura una serie de datos con gráficos dinámicos.

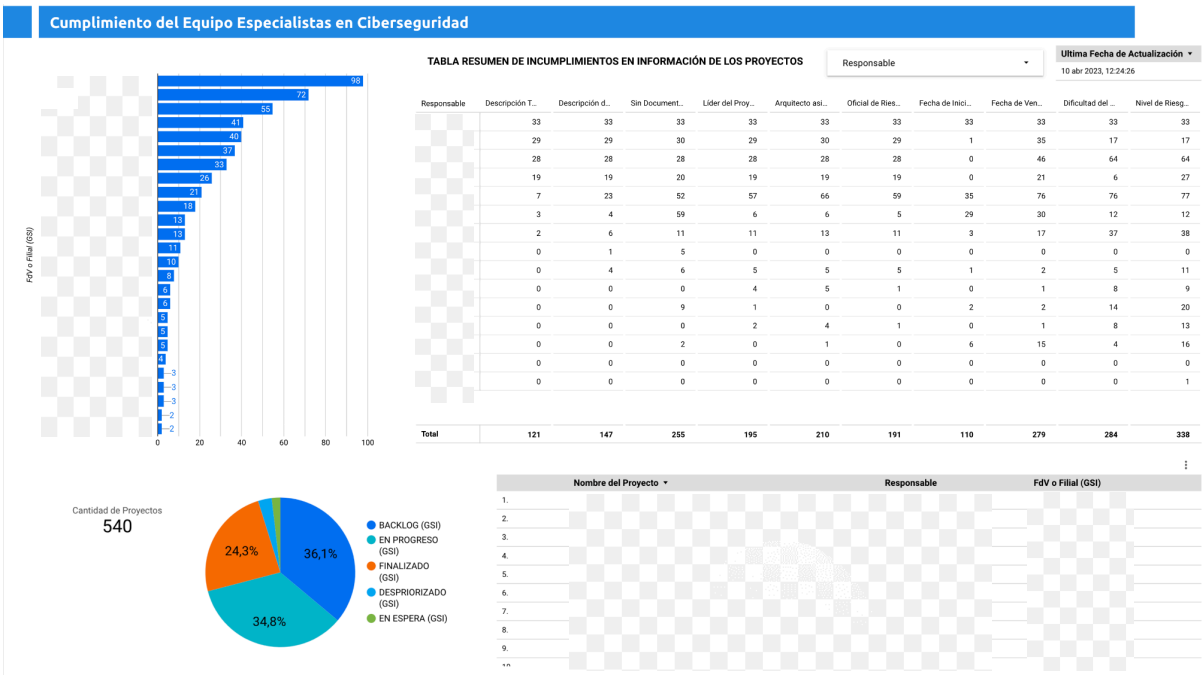


Figura 29: Visualización del Dashboard en Looker Studio

Se construyó un dashboard como panel de indicadores del equipo Especialistas en Ciberseguridad de la Gerencia de Seguridad Informática que considera tres vistas con sus respectivas visualizaciones agrupadas en 12 hojas temáticas, mencionadas a continuación:

1. **KPI del equipo**
    - Adherencia total de los proyectos a la ciberseguridad
    - Adherencia total a los puntos de control

2. **Vista general del equipo**
    - Adherencia de los proyectos a los puntos de control
    - Adherencia de los proyectos a los controles por unidad
    - Cantidad de proyectos
    - Cantidad de puntos de control
    - Porcentaje de estado de avance de los proyectos
    - Porcentaje de estado de avance de los puntos de control
    - Porcentaje de proyectos por categoría
    - Cantidad de proyectos por categoría

3. **Detalles del equipo**
    - Capacity del Equipo Especialistas basado en proyectos por año
    - Cumplimiento del Equipo Especialista para la ficha de un proyecto

- Filtro por Especialista en Ciberseguridad responsable
- Cantidad de proyectos por categoría
- Cantidad de proyectos por Especialista en Ciberseguridad
- Detalle de los proyectos atendidos
- Detalle del estado de avance de un proyecto
- Adherencia hacia los puntos de control por Especialista en Ciberseguridad
- Filtro por Unidad
- Detalle del Estado de avance de un punto de control por Especialista en Ciberseguridad

Finalmente este dashboard representa el resultado del trabajo realizado en esta tesis en torno al proceso realizado para la gestión interna en la interacción de ciberseguridad con proyectos tecnológicos, entregando un importante resumen que recopila los datos de las fuentes de datos en un solo sitio. Este a su vez los presenta de una manera digerible para que lo importante salte a la vista, acompañando a una toma de decisiones rápida y práctica.

6.7 Resultados de la Implementación

Los resultados se presentan en formato de una evaluación. Esta fue realizada para determinar el cumplimiento de los objetivos generados, así como los impactos y resultados de la implementación del nuevo proceso en conjunto con las herramientas que acompañan al proceso. Se abordaron dos puntos centrales, el primero hace referencia al análisis cualitativo de la solución basado en una encuesta y el segundo presenta algunos datos obtenidos a través de los dashboard generados, luego de una total visibilidad por parte del equipo Especialistas en Ciberseguridad.

6.7.1 Encuesta de Evaluación

Al no existir anteriormente un proceso, además de la complejidad de conseguir información histórica de los proyectos en los que los Especialistas en Ciberseguridad participaron, se dificulta la realización de una comparación de la situación anterior para contrastar con la situación luego de implementado el proceso y las mejoras a las que apunta este trabajo de tesis. Para este fin, se creó una encuesta que permite validar cualitativamente los resultados de la implementación de este trabajo y el cumplimiento de objetivos.

La encuesta fue dirigida al equipo Especialista en Ciberseguridad, quienes son las personas que utilizarán en su día a día este nuevo proceso y utilizarán las herramientas para dar seguimiento a este. El universo de encuestados fueron ocho personas, cada una de ellas con basta experiencia en Ciberseguridad e interactuando de manera directa y multidisciplinaria con los distintos proyectos vinculados en la Institución.

El medio utilizado para realizar esta encuesta y recolectar los datos fue Google Form, enviada por medio del chat del equipo. Las preguntas claves y las respuestas obtenidas se presentan a continuación:

Pregunta / Especialista	**¿Qué problemas visualizabas en la entrega de controles de seguridad, antes de la implementación de los puntos de control?**
Especialista (I.B)	Baja gestión en los proyectos, poca información para demostrar el rendimiento en el trabajo , pérdida de tiempo en coordinar actividades y repetición de actividades lo que se transformaba en trabajo tedioso. Esto es un framework que ha mejorado de manera significativamente el rendimiento y la salida con seguridad de los proyectos.
Especialista (S.C)	Que variaba el control en el tiempo para un mismo caso de uso, ya que muchas

	veces se entregaba bajo un juicio experto del momento y no a partir de una base estandarizada
Especialista (J.M)	Claridad del alcance
Especialista (P.M)	No se tenía un orden, ni se tenía una medición de estos.
Especialista (S.T)	No existía un único método de implementación utilizado.
Especialista (J.M)	Se presentaban múltiples formas de levantar, entregar, solicitar y recibir la información sobre los puntos de control de las unidades.
Especialista (M.U)	Que a veces los controles quedaban a criterio del especialista al no estar estandarizados en un proceso.
Especialista (E.P)	No tenía claridad total de qué controles debía aplicar
Pregunta / Especialista	**¿Consideras que la entrega de controles de ciberseguridad ha sido más precisa con los puntos de control? ¿Por qué?**
Especialista (I.B)	Sí, ya que existe un perfecto lineamiento de actividades que se deben seguir, y se definen los alcances de la seguridad en proyectos
Especialista (S.C)	Si, por que ya está definido que se va solicitar y con quienes se trabajará el control
Especialista (J.M)	Porque se entiende transversalmente el objetivo
Especialista (P.M)	Si, porque se le puede dar mayor seguimiento a través del jira
Especialista (S.T)	Si, ya que se puede dividir y dirigir mejor cada requerimiento a los equipos de trabajo
Especialista (J.M)	Si, pero es recomendable establecer el entregable deseado, acordado por cada unidad al equipo, o por unidad, ya que la idea del punto es recabar la evidencia del control de la mejor manera posible.
Especialista (M.U)	Si entrega más claridad a los proyectos al estar documentados en confluence y de alguna manera normados con un proceso
Especialista (E.P)	Sí, porque así está estandarizado
Pregunta / Especialista	**Con el nuevo proceso, ¿Cuál ha sido su experiencia utilizando las herramientas de Confluence y Jira para la entrega de controles a proyectos?**
Especialista (I.B)	Sí, gracias a Confluence queda todo documentado y con Jira podemos ver los tracks de los proyectos, lo cual agiliza mucho el trabajo
Especialista (S.C)	Experiencia más ordenada, menos retrabajo y mejor gestión del conocimiento
Especialista (J.M)	Siento que hacia el proyecto no influye. Si influye hacia lo que presentamos como

	equipo
Especialista (P.M)	Buena experiencia en los proyectos donde los he aplicado
Especialista (S.T)	Satisfactoria, más mejorable, puesto que podríamos avanzar a etiquetar y anexar todo directamente en Jira (equipos de la gerencia)
Especialista (J.M)	Fluido, se entiende y se ha aplicado, en todo caso, el tiempo para dedicarle al manejo de las herramientas colaborativas y llenar la información es un etapa en proceso.
Especialista (M.U)	A fluido totalmente Dada las experiencias de vidas anteriores dónde siempre había que documentar evidencias
Especialista (E.P)	Buena experiencia, permite trazabilidad y mantener orden en los controles
Pregunta / Especialista	**¿Cree usted que se ha cumplido con el objetivo de estandarizar la entrega de controles a los proyectos?**
Especialista (I.B)	Sí se ha cumplido con el objetivo a cabalidad
Especialista (S.C)	Si totalmente
Especialista (J.M)	Si
Especialista (P.M)	Si
Especialista (S.T)	En todos los casos, ya que se unifica la forma de pedir los distintos puntos de control a los distintos flujos de valor y equipos
Especialista (J.M)	Si, en cierto punto hay una manera más clara y precisa de presentar los puntos de control a las demás unidades fuera de la gerencia, lo importante sería como mencionaba establecer un formato del entregable esperado por unidad para los puntos de control, a manera de fijar las expectativas de las unidades
Especialista (M.U)	Si encuentro que es un proceso claro y eficiente
Especialista (E.P)	Si
Pregunta / Especialista	**Desde tu experiencia, ¿Cuál consideras que es el mayor aporte de la implementación de los puntos de control?**
Especialista (I.B)	Existen muchos beneficios, entre los cuales están: eficiencia, profesionalismo, orden en el trabajo, es una herramienta fundamental para dar la seguridad que corresponde a los proyectos del Banco
Especialista (S.C)	La estandarización de un trabajo multidisciplinario de toda la gerencia
Especialista (J.M)	El buscar un objetivo transversal de la gerencia en los proyectos
Especialista (P.M)	La estandarización para todos los especialistas y a parte se puede mostrar en qué está cada uno y en qué proyectos está involucrado.

Especialista (S.T)	Considero que el mayor aporte de los puntos de control es agregar la madurez necesaria al proceso de revisión de ciberseguridad, de forma que sea medible, mejorable y escalable en el tiempo, todo esto sin dejar fuera el hecho de mantener un estándar de revisión transversal para los especialistas de ciberseguridad.
Especialista (J.M)	Centralización, Organización y Distribución de la información que permite un retroalimentación entre los especialistas, y por qué no, más adelante de la gerencia cuando cada unidad cumpla con la revisión y cierre de sus puntos de control.
Especialista (M.U)	Más claridad en el análisis del especialista para decidir e implementar cada punto de control. También ha permitido más sensibilización y entendimiento de los puntos de control escritos en confluence hacia los proyectos
Especialista (E.P)	Estandarizar los requerimientos de ciberseguridad
Pregunta / Especialista	**Desde tu experiencia aplicando los puntos de control ¿Qué mejorarías del proceso y metodología?**
Especialista (I.B)	En base a estos puntos de control debe haber un perfecta sincronía con las diferentes áreas que apoyan ejecutando los puntos de control, por lo tanto la misión es generar más adherencia a los puntos de control
Especialista (S.C)	Del proceso, lo iniciaría a partir de alguna plataforma de autoatención donde los equipos de proyectos nos inicien un caso al cual se debe aplicar los puntos de control. Sobre la metodología mejoraría en considerar costos por puntos de control.
Especialista (J.M)	La asignación de las tareas a las unidades responsables del punto de control y el entregable por parte de la unidad responsable
Especialista (P.M)	Quizás alguna forma de automatización para ir agregando los proyectos cuando es una carga masiva para que no sea tan manual el proceso.
Especialista (S.T)	Dentro de muchas oportunidades de mejoras que tiene el proceso, destacaría la de avanzar con la integración de toda la gerencia, de forma que todo los requerimientos puedan ser canalizados a través de Jira. Esto se podría aplicar utilizando distintos formularios integrados a Jira, para generar tickets a los distintos tableros que maneje la gerencia de seguridad.
Especialista (J.M)	Establecer en forma clara, precisa y concisa el entregable esperado o definido por cada punto de control, de esta forma podemos más allá de medir la gestión por proyectos, referenciar todo lo relacionado a los soportes, bien sea por correo, un documento, un formato o hasta un formulario que permita recibir la información, de manera centralizada y homogénea. Todo proceso metodológico en desarrollo es perfectible, en búsqueda de la mejor estrategia para la gerencia y corporación.
Especialista (M.U)	Por ahora creo que la fase 2 sería empezar a subir al proceso a las áreas internas de nuestra gerencia, para así lograr la interacción con nuestro jira y de esta manera capacitarlos. La fase 3 empezar una puesta en marcha para que ya empiecen a asignarles tareas dentro de los proyectos

Especialista (E.P)	Un refinamiento de los controles que no aplican para proyectos

Además se realizaron las siguientes preguntas a las mismas ocho personas participantes, donde se solicitó responder basado en las siguientes afirmaciones, con las siguientes respuestas:

Muy de acuerdo, De acuerdo, Me es Indiferente, En desacuerdo, Muy en desacuerdo

1. He participado en reuniones donde he aplicado los puntos de control
   R: 8 Muy de acuerdo
2. He recibido la información suficiente para entender la metodología de puntos de control
   R: 6 Muy de acuerdo, 2 De acuerdo
3. He logrado implementar los puntos de control en los proyectos en los que me encuentro
   R: 5 Muy de acuerdo, 3 De acuerdo
4. La metodología de los puntos de control ha mejorado mi calidad de trabajo
   R: 7 Muy de acuerdo, 1 De acuerdo
5. Los puntos de control me han permitido mejorar la comunicación y colaboración con colegas
   R: 6 Muy de acuerdo, 2 De acuerdo
6. La metodología de los puntos de control, me ha permitido mostrar el avance de la seguridad en torno a un proyecto
   R: 6 Muy de acuerdo, 2 De acuerdo
7. Los puntos de control permitieron estandarizar mi entrega de controles de ciberseguridad hacia los proyectos
   R: 6 Muy de acuerdo, 2 De acuerdo
8. Las herramientas utilizadas en la metodología de los puntos de control (Jira y Confluence) me han permitido tener una mejor gestión de mis actividades
   R: 6 Muy de acuerdo, 2 De acuerdo
9. La disponibilidad de los controles de seguridad en confluence me ha permitido entregar los lineamientos con mayor claridad hacia los distintos equipos
   R: 7 Muy de acuerdo, 1 De acuerdo
10. He notado beneficios concretos en mi trabajo desde que se implementó la metodología de los puntos de control
    R: 6 Muy de acuerdo, 1 De acuerdo, 1 Me es indiferente
11. Los puntos de control han mejorado la eficiencia en mi trabajo
    R: 4 Muy de acuerdo, 4 De acuerdo
12. Me siento cómodo con la metodología de los puntos de control
    R: 6 Muy de acuerdo, 2 De acuerdo

13. Recomendaría la metodología de los puntos de control a otros equipos o compañías

R: 6 Muy de acuerdo, 2 De acuerdo

El resultado totalizado de las respuestas se refleja a continuación:

Respuesta	Cantidad	Porcentaje
Muy de acuerdo	79	75,96%
De acuerdo	24	23,08%
Me es Indiferente	1	0,96%
En desacuerdo	0	0%
Muy en desacuerdo	0	0%
Total	**104**	**100%**

La figura 30 muestra las 13 preguntas realizadas y el resultado de sus respuestas, reflejando una alta tendencia en las primeras 2 opciones (Muy de acuerdo y De acuerdo).

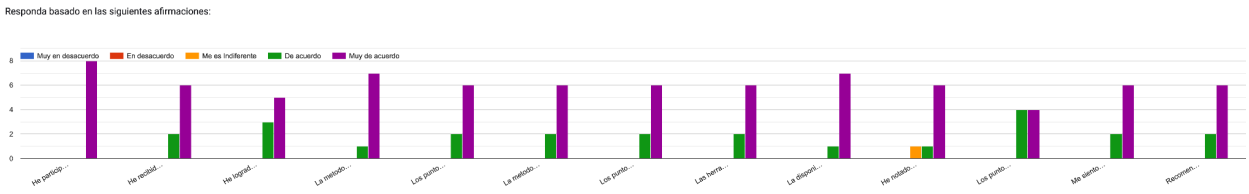


Figura 30: Resultado General de la Encuesta

Se puede apreciar que algunas respuestas reafirman los problemas planteados en un comienzo de este trabajo, no existía una forma estandarizada, había un bajo seguimiento en la gestión, no existía claridad en los controles para aplicar en los proyectos entre otros.

Las respuestas reflejan que en términos de experiencia este proceso ha mejorado el manejo de objetivos transversales y sus entregables en torno a los controles. Un punto a destacar sin duda y valorado por el equipo es que ahora existe un proceso claro, fluido y que permite un mayor entendimiento en torno a un punto de control. Esto con el apoyo de las herramientas, permiten un seguimiento de sus actividades para realizar gestión sobre ellas.

Es necesario destacar que las herramientas Jira y Confluence han permitido de manera útil implementar este nuevo proceso dentro del equipo. La gestión de actividades a través de los puntos de control, el registro de avances y la posibilidad de mostrar avances en torno a la seguridad de los proyectos sobresale en términos de la experiencia de los usuarios.

Sobre la encuesta de evaluación, se puede obtener que existen altas expectativas y sobre todo el interés de seguir mejorando este proceso implementado para ampliar su alcance, utilizándolo como punto de partida para el cumplimiento de nuevos objetivos plasmados en esta encuesta. Además, los usuarios ya plantean mejoras en su forma de trabajo y cumplimiento de sus objetivos.

6.7.2 Datos Obtenidos

Los siguientes datos son obtenidos directamente del dashboard generado para entregar visibilidad a los Líderes de equipos (Coordinadores, Jefaturas y Gerencias) dentro de la Gerencia de Seguridad Informática. La figura 31 corresponde a los valores de los KPI consolidados vinculados a la adherencia de la seguridad en los proyectos y hacia los puntos de control respectivamente.

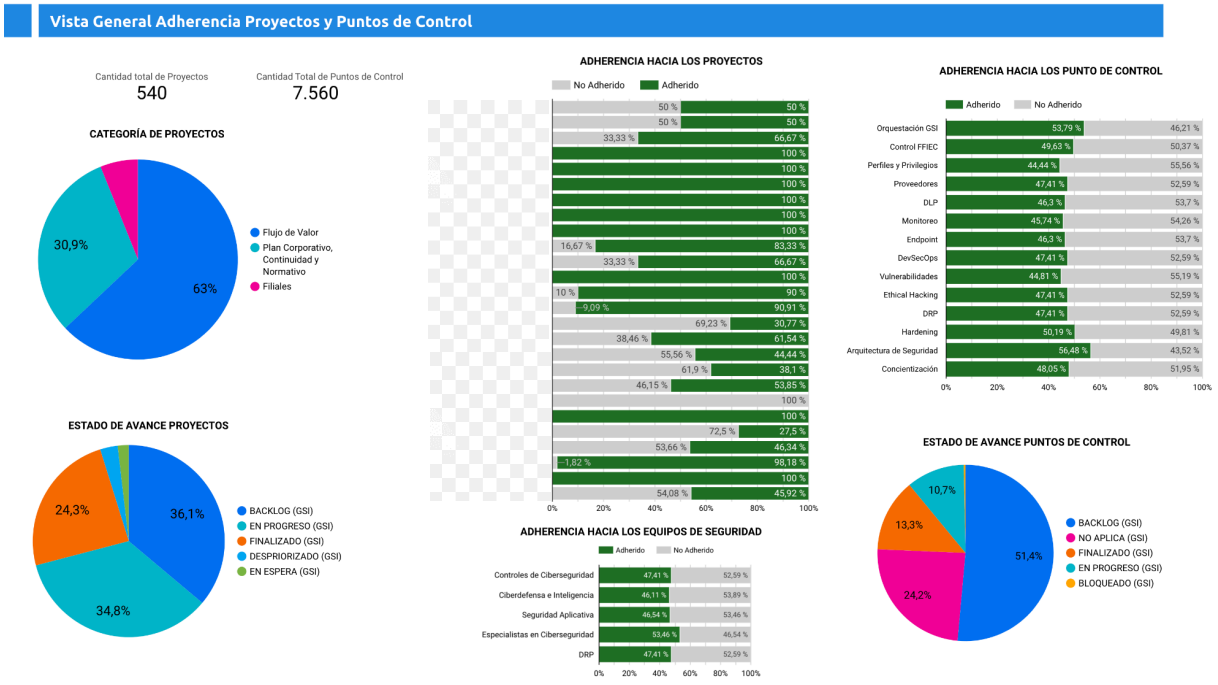


Figura 31: Vista General de la Adherencia

Dentro de esta vista, es posible apreciar la cantidad explícita de proyectos 540 y su respectiva cantidad de puntos de control 7560, cantidad que corresponde al multiplicar cada proyecto por sus 14 puntos de control, es decir 540*14=7560.

Desde el periodo de su implementación de Enero a Diciembre y entendiendo que la Corporación funciona por trimestres (Q1, Q2 , Q3 y Q4), cada proyecto ingresado a las plataformas refleja su estado de avance, además de su avance en torno a sus puntos de control. Todo evidenciado en los gráficos de torta inferiores. Estos estados se definen a través de los estados en el Jira definidos en los capítulos 6.4.2 y 6.4.3 respectivamente y explicados en la figura 22 y figura 23.

Volviendo a la figura 31, esta muestra un estado de avance de la seguridad en proyectos de 36,1% Backlog, 34,8% En Progreso, 24,3% Finalizado, 2,9% Despriorizado y 1,9% En Espera. Estos porcentajes se atribuyen a la creación y finalización de proyectos durante el año, dado el funcionamiento de trimestres en la Corporación, mostrando una diferencia significativa en los avances.

En torno a los puntos de control de seguridad en proyectos se muestra un estado de avance de 51,4% Backlog, 24,2% No Aplica, 13,3% Finalizado, 10,7% En Progreso y 0,4% Bloqueado. Estos porcentajes se atribuyen directamente al avance de los proyectos, pero también con avance el resultado de la interacción interna de la Gerencia de Seguridad Informática.

Sobre los datos de Adherencia hacia los proyectos y hacia los puntos de control se reflejan en detalle los porcentajes agrupados por categorías que en la Corporación son denominadas Flujos de Valor. Esta adherencia se encuentra vinculada a la próxima figura.

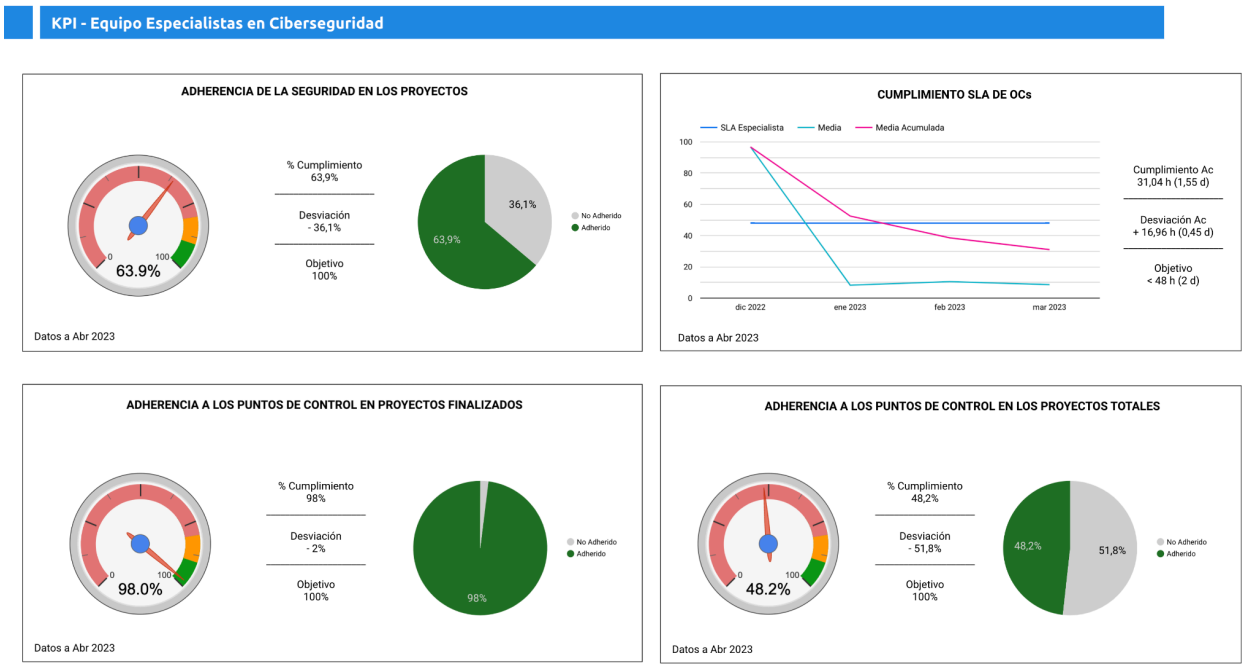


Figura 32: KPI Equipo Especialista en Ciberseguridad

Los datos de los gráficos de torta vinculados a la Adherencia de la figura 32, toman 3 definiciones para el cálculo de sus porcentajes, estos son:

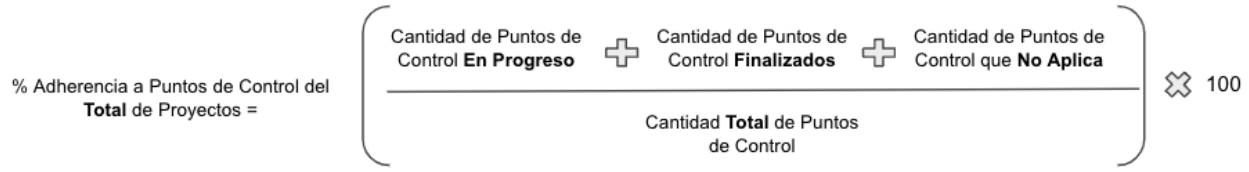
Adherencia a los Proyectos: El Especialista en Ciberseguridad se encuentra participando activamente o ha finalizado sus proyectos e iniciativas asignados.

$$\%\ \text{Adherencia a Proyectos} = \left(\frac{\text{Cantidad de proyectos atendidos}}{\text{Cantidad total de proyectos declarados}} \right) \times 100$$

Adherencia a los Puntos de Control de Proyectos Finalizados: El Especialista en Ciberseguridad garantiza y entrega conformidad al cumplimiento de los puntos de control en los proyectos e iniciativas finalizados.

$$\%\ \text{Adherencia a Puntos de Control en Proyectos } \mathbf{Finalizados} = \left(\frac{\text{Cantidad de Puntos de Control } \mathbf{Finalizados} + \text{Cantidad de Puntos de Control que } \mathbf{No\ Aplica}}{\text{Cantidad } \mathbf{Total} \text{ de Puntos de Control de Proyectos } \mathbf{Finalizados}} \right) \times 100$$

Adherencia a los Puntos de Control de Proyectos Totales: El Especialista en Ciberseguridad garantiza y entrega conformidad al cumplimiento de los puntos de control en los proyectos e iniciativas totales.



Todos los datos obtenidos y reflejados en el dashboard creado, muestran el avance que ha presentado el equipo de Especialistas en Ciberseguridad durante el año, evidenciando según el tiempo en que se observen los avances respectivos en torno a los proyectos cargados.

7. ANÁLISIS Y CONCLUSIONES

El desarrollo de este proyecto implicó la realización de tareas de investigación, de diseño e implementación de varias soluciones tecnológicas de apoyo al proceso, así como la integración de esas tecnologías. Además existió un levantamiento y coordinación entre los distintos equipos de la Gerencia de Seguridad Informática, equipos de implementación inicial y el equipo de Especialistas en Ciberseguridad, así como de los comités de proyecto y ejecutivo relevantes para el proyecto. Cabe mencionar que en el desarrollo y la implementación se realizaron algunos ajustes de tareas replanificadas, que no afectaron la planificación original del proyecto, lo que permitió cumplir con el cronograma trazado.

Teniendo en consideración que el equipo es relativamente nuevo y que no contaba con un proceso para la realización de las actividades de seguridad en proyectos, además de no contar con plataformas de apoyo para el seguimiento de actividades y su visualización, el resultado de este trabajo es satisfactorio, ya que ahora el equipo cuenta con una plataforma integrada para el seguimiento de sus actividades dentro del proceso y además cuenta con un dashboard que muestra la cantidad de proyectos (540) y sus puntos de control (7560) con sus respectivos cumplimientos (ver Figura 29), ambas operativas y en funcionamiento dentro de la Gerencia de Seguridad Informática.

7.1 Trabajo Realizado

Este trabajo de tesis abordó la creación de un proceso transversal para los proyectos, iniciativas o mejoras tecnológicas que se realizan en una Institución Financiera, agregando un proceso de gestión para la interacción de ciberseguridad con estos proyectos tecnológicos a través de 14 puntos de control.

Mediante la aplicación de la metodología de trabajo, que inició con un análisis de la situación actual, permitió determinar el punto de partida para la creación del proceso, buscar la combinación entre proceso y tecnologías, además de diseñar e implementar siempre con la mirada del equipo como usuario final y permitió crear un proceso a la medida que lleva a interactuar a ciberseguridad con proyectos tecnológicos.

Por otra parte, el trabajo de tesis desarrollado ha permitido generar el ambiente propicio para establecer una metodología de trabajo de fácil adopción. Además el hecho de establecer un gobierno formal de proyecto que permitió establecer definiciones claras de los roles y responsabilidades.

Destacar también que aplicar una metodología ágil para el levantamiento, diseño e implementación de este proyecto en torno a la creación de un proceso de gestión interna, permitió entre otros beneficios:

- La estandarización y documentación del proceso
- La implementación de mejoras (Quick Wins)
- Generar esfuerzos centralizados en los puntos de control como componentes del proceso
- Crear y documentar definiciones transversales para los proyectos
- Medir el cumplimiento de algo inexistente y necesario antes del desarrollo de este proyecto

7.2 Proceso e interacción de Ciberseguridad con Proyectos

Uno de los aspectos clave de este trabajo tiene relación con la gestión de la ciberseguridad con proyectos tecnológicos.

Los beneficios de contar con un proceso que tenga herramientas tecnológicas para su gestión, que permita dar seguimiento a proyectos aporta importantes ventajas tales como:

- Acceso rápido, en tiempo real y fiable a toda la información del avance de la ciberseguridad en los proyectos garantizando exactitud en lo declarado.

- Mejora de la precisión en las decisiones de ciberseguridad al poder contar con puntos de control estandarizados aplicables a los proyectos.

- Almacenamiento de la ficha del proyecto, de los datos de avance obtenidos y del documento evidencia del proyecto de manera centralizada. Esto permite su uso en estudios e investigaciones que mejorarán la gestión interna y definiciones en torno a los puntos de control.

También cabe señalar que para el Especialista en Ciberseguridad el uso de herramientas que faciliten el proceso de gestión en su ingreso, seguimiento y registro genera una serie de beneficios tales como:

- Reducción de errores de interpretación en controles, a través del uso de definiciones concretas y publicadas en Confluence.
- Incremento de la visibilidad para la revisión de ciberseguridad en proyectos, mediante el seguimiento en Jira.

- Reducción de incumplimientos por debilidad en gestión, evidenciado en Looker Studio.

7.3 Cumplimiento de Objetivos

Sin duda los objetivos propuestos en este trabajo de tesis fueron cumplidos en forma satisfactoria. Se ha conseguido el objetivo general, creando un proceso de gestión interna para la interacción de ciberseguridad con proyectos tecnológicos el cual permite aumentar los controles de seguridad y estandarizar la interacción realizada.

En lo que respecta a los objetivos específicos se puede indicar que se cumplieron satisfactoriamente cada uno de estos objetivos, destacando que actualmente cada objetivo fue adoptado en la práctica dentro de la Institución Financiera donde se aplicó este trabajo, siendo utilizados por la Gerencia de Seguridad Informática para interactuar con los distintos proyectos en los que participa, estos son:

- Definir y crear un proceso que permita dar seguimiento a los controles de seguridad elegidos para la implementación en los proyectos.
    - La creación del proceso de gestión interna ha mejorado algunas deficiencias en el seguimiento manual y bajo juicio experto que se realizaba, permitiendo actualmente en su implementación mostrar el estado real de un proyecto en torno al cumplimiento de seguridad a través del dashboard creado.
- Estandarizar la entrega de controles de ciberseguridad en los proyectos.
    - La estandarización de aplicabilidad de los 14 puntos de control permitió que todo proyecto tuviese una mirada de seguridad, medible y cuantificable, generando visibilidad en torno a su adherencia. Esta estandarización es evidenciada en el seguimiento actual que se realiza a nivel del equipo Especialistas en Ciberseguridad para un punto de control a través de Jira y sus distintos estados aplicados para los proyectos.
- Elegir un conjunto de herramientas que permitan dar prioridad, seguimiento y continuidad de los controles de ciberseguridad en los distintos proyectos tecnológicos.
    - La implementación realizada en la Gerencia de Seguridad Informática a través del conjunto de herramientas, ha permitido entregar la información

completa del proyecto en torno a la seguridad aplicada a través de los puntos de control, obteniendo responsables y corrigiendo actividades a tiempo. Esto se evidencia en el seguimiento Jira y en los tableros implementados en Looker Studio.

- Facilitar la disponibilidad de los controles de seguridad implementados en los proyectos de manera transversal para el equipo.
    - Los controles de seguridad se encuentran disponibles y son utilizados a nivel de la corporación, permitiendo mejorar su aplicabilidad, aclarando dudas en el proceso y definiendo claramente roles y responsabilidades.

7.4 Mejoras y Evolución

Todos los proyectos están abiertos a mejoras o ampliaciones y este es uno de ellos. Los proyectos tienen que tener una meta claramente delimitada y alcanzable dentro de un plazo establecido para ser considerados viables.

Este proyecto en particular tiene mucha proyección y sin duda evolucionará en nuevos requerimientos. En el futuro será precursor para nuevas integraciones, no solo para la interacción de la ciberseguridad con proyectos tecnológicos sino que también se le debe dar paso a la incorporación en la interacción de los riesgos vinculados a los distintos proyectos, identificando y estandarizando la interacción inter unidades. También se debe avanzar hacia la monitorización global del avance de la seguridad en un proyecto dando acceso a la integración con herramientas transversales que permitan a la unidades de proyectos apoyar el seguimiento conjunto.

Otro punto importante a escalar, visualizado y que despertó el interés dentro de la Gerencia de Seguridad Informática es la vinculación de los costos asociados por punto de control, permitiendo realizar los cobros de la seguridad a los proyectos por concepto de licenciamiento, integraciones y operación. Esto está vinculado al concepto de Seguridad como Servicio o Security as a Service (SECaaS) [20].

7.5 Conclusión

El trabajo de tesis efectuado cumplió ampliamente las expectativas, generando efectos positivos, como es la adopción de distintas herramientas tecnológicas para realizar gestión del proceso en la interacción de ciberseguridad con proyectos tecnológicos.

En lo que respecta a beneficios directos, se debe mencionar que antes de este trabajo no existía un proceso que registrara las actividades de acompañamiento en torno a la seguridad de los diversos proyectos tecnológicos de la Corporación. Actualmente todo lo implementado es utilizado por el equipo de Especialistas en Ciberseguridad y sus interacciones, además de encontrarse declarado como parte de los procesos formales internos de la Gerencia de Seguridad Informática. Por lo que su aporte se encuentra en la centralización de la participación de Seguridad, estandarización en los controles aplicados a los proyectos, disminución de errores de interpretación de un control, simplificación en la búsqueda de historia sobre un proyecto, Especialistas en Ciberseguridad con una visión unificada en torno a su participación dentro de un proyecto y visibilidad total en torno a métricas de estado de participación y de avance de la seguridad.

También mencionar que existen beneficios indirectos como es el aumento de visibilidad dentro de la Gerencia de Seguridad Informática en torno a los proyectos atendidos, incremento en la cantidad de indicadores posibles de obtener en torno a proyectos, apalancamiento de los resultados de la participación de Seguridad para obtención de presupuesto, incremento de la exactitud de la participación y la analítica que se desprende de los datos registrados para la toma de decisiones.

En torno a los beneficios de la implementación se pueden mencionar los siguientes:

- **Visibilidad:** Entrega una mirada integral a las distintas unidades de la Gerencia de Seguridad Informática de los proyectos.

- **Historia:** Permite que los equipos de la Gerencia de Seguridad Informática y sobre todo el equipo Especialista en Ciberseguridad conozca cómo se trabajó un proyecto

- **Gestión:** Permite una gestión ágil de los proyectos con mayor comunicación basada en objetivos.

- **Interacción:** Entrega una visión total de la participación de las unidades en los distintos equipos donde se encuentren realizando proyectos.

- **Cuantificar:** Permite dimensionar el esfuerzo y dedicación de la Gerencia de Seguridad Informática en los Proyectos

- **Datos:** Permite la toma de decisiones basada en datos con respaldo del equipo.

- **Aprendizaje:** Disminuye la curva de aprendizaje de los proyectos.

BIBLIOGRAFÍA

[1] NISTIR 7298, Glossary of key Information Security Terms Revisión 2, Mayo 2013, pág. 58
https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

[2] Ciberseguridad según Kaspersky: ¿Qué es la ciberseguridad?
https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[3] Michel Cukier, 2007, Estudio de la Escuela Clark de la Universidad de Maryland
https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

[4] IBM, 2022, Informe sobre el costo de una violación de datos
https://www.ibm.com/reports/data-breach

[5] CSIRT 2021, Noticia sobre Ciberataques en Chile
https://www.csirt.gob.cl/noticias/chile-recibe-410-millones-de-intentos-de-ciberataques-en-el-primer-trimestre-de-2021/

[6] Kaspersky, ¿Qué es la Deep Web y la Dark Web?
https://www.kaspersky.es/resource-center/threats/deep-web

[7] EY, 2021, Encuesta Global de Seguridad de la Información
https://assets.ey.com/content/dam/ey-sites/ey-com/es_cl/webcast/2021/08/ey-encuesta-global-de-la-seguridad-de-la-informacion-2021.pdf

[8] National Cyber Security Centre, UK, 2018, Secure by Default
https://www.ncsc.gov.uk/information/secure-default

[9] Ministry of Justice UK, Security Guidance, Security by Default
https://security-guidance.service.justice.gov.uk/secure-by-default/#secure-by-default

[10] Cybersecurity Guide, 2023, How to become a cybersecurity specialist
https://cybersecurityguide.org/careers/security-specialist/

[11] National Initiative for Cybersecurity Careers and Studies
https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/systems-architecture

[12] Atlassian, ¿Qué es ágil?
https://www.atlassian.com/es/agile

[13] Atlassian, ¿El manifiesto ágil sigue estando disponible?
https://www.atlassian.com/es/agile/manifesto

[14] Atlassian, Conceptos básicos de Confluence
https://www.atlassian.com/es/software/confluence/guides/get-started/confluence-overview

[15] Atlassian, Jira Work Management
https://www.atlassian.com/software/jira/work-management/product-guide/overview

[16] Slack, ¿Qué es Slack?
https://slack.com/intl/es-cl/what-is-slack

[17] Google, ¿Qué puedes hacer con Looker Studio?
https://support.google.com/looker-studio/answer/6283323?hl=ES

[18] Wikipedia, Tree (data structure)
https://en.wikipedia.org/wiki/Tree_(data_structure)

[19] Atlassian, Historias, epics e iniciativas
https://www.atlassian.com/es/agile/project-management/epics-stories-themes

[20] Zscaler, ¿Qué es la seguridad como servicio (SECaaS)?
https://www.zscaler.es/resources/security-terms-glossary/what-is-security-as-a-service