IMPLEMENTACIÓN DEL CICLO BPM EN EL PROCESO DESARROLLADO POR EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN DEL BANCO MUNDO MUJER

Práctica para Optar por el Título de:

Administradora de Empresas

Sustentado Por:

Claudia Vanessa Garcés Mazabuel

Facultad de Ciencias Contables, Económicas y Administrativas

Universidad del Cauca

Popayán – Cauca

2020

IMPLEMENTACIÓN DEL CICLO BPM EN EL PROCESO DESARROLLADO POR EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN DEL BANCO MUNDO MUJER

Práctica para Optar por el Título de:

Administradora de Empresas

Sustentado Por:

Claudia Vanessa Garcés Mazabuel

Asesor académico:

Henrry Ramirez Paruma

Empresarial:

Juan Pablo Rodríguez

Facultad de Ciencias Contables, Económicas y Administrativas

Universidad del Cauca

Popayán – Cauca

2020

Agradecimientos

Inicialmente agradezco a Dios por brindarme la oportunidad de realizar mi formación profesional en una gran institución como lo es la Universidad del Cauca, por haber estado conmigo en los momentos de mayor dificultad, por darme salud, fortaleza y ser mi guía durante este proceso.

A mi madre Claudia Garcés por ser el apoyo más grande durante mi educación universitaria, por su esfuerzo, por ser mi ejemplo a seguir y mi mayor motivación para culminar esta etapa.

A mi novio, por su amor y apoyo incondicional durante toda mi carrera.

Igualmente, agradezco el acompañamiento y apoyo recibido por mi Asesor académico PHD.Henrry Ramirez Paruma, quien estuvo al tanto de todas las actividades desarrolladas en base al cumplimento de los objetivos planteados.

Por último, agradezco a mis compañeros del área de Seguridad de la Información por todo lo que pude aprender en base a su experiencia y ser parte fundamental en la recolección de información, necesaria para el desarrollo del presente trabajo.

Tabla de Contenido

II. ÍNDICE DE TABLAS

III. ÍNDICE DE FIGURAS

IV. ÍNDICE DE ANEXOS

Introducción

La gestión de procesos es uno de los principios de gestión de la calidad es considerada como uno de los más grandes aportes que la gestión de la calidad cuando nació como evolución del aseguramiento de calidad. (Asociación Española para la Calidad [AEC] 2013).

La importancia de la gestión por procesos radica en los múltiples beneficios que proporciona**.** En primer lugar, una de las ventajas más importantes es que permite globalizar todos los sectores que forman parte de la empresa en este caso de un área. Esto lleva al trabajo de manera grupal y que el mismo se consiga fluidez en los procesos y mejora de comunicación entre los empleados. Anónimo. (2018). Gestión por procesos ¿Que la hace tan importante?

Underdahl (2013) define el ciclo BPM como: "El BPM es una forma de enfocar la gestión de la organización para satisfacer mejor las necesidades de los clientes. BPM permite que las organizaciones sean más eficientes y más capaces de cambiar. BPM es exactamente lo que necesita su organización para hacer frente a los desafíos del entorno empresarial moderno" (p.2). Teniendo en cuenta la influencia positiva de esta metodología en el Banco mundo mujer se quiere aplicar en el área de seguridad de la información que son los encargados de proteger y evitar distintos peligros que se presentan con la información tanto de usuarios como de colaboradores que influye en la realización de distintas actividades que se presentan en el área como la autorización en distintos aplicativos, control de pasos entre ambientes, campañas de e-mailing para alertar a los empleados y todo lo relacionado a las novedades de nómina. El área de seguridad de la información es uno de los principales canales, ya que sin de su debida autorización en el proceso que realiza se pueden retardar el cumplimiento de actividades por parte de otros empleados, pero también con la satisfacción del cliente en cuanto a las solicitudes que hacen respecto a desviaciones que se presentan.

Hoy en día existen muchas empresas que no tienen claridad de cuál debe ser el desarrollo adecuado, de sus procesos y de qué forma deben alinearse cada área de la empresa. Es por eso que el BPM es la herramienta idónea para las organizaciones que buscan reconocer los procesos que ejecutan, todo con el objetivo de medirlos y transformarlos de manera que sea posible implementar estrategias que cumplan las metas del negocio.

El presente proyecto contiene el desarrollo de la metodología BPM (Business Process Managment) que se quiere realizar con el objetivo de implementarlo en los procesos que se consideren críticos y de este modo se logre la mejora continua frente a los resultados que se obtengan. Su desarrollo es planeado a partir de cinco capítulos: el primer capítulo, describe la problemática que con la práctica se pretende resolver, contextualizando la situación y también se expone la formulación del problema en interrogatorio, se elabora la justificación de la trascendencia de la práctica y se expone el objetivo general y objetivos específicos de la práctica profesional los cuales manifiestan el propósito y lo que se pretende conseguir con estos; en el segundo capítulo se presenta el marco teórico, legal, de referencia y conceptual de la práctica profesional a realizar, con lo que se pretende dar una contextualización de lo que es un manual de gestión de indicadores, usando como metodología la citación de conceptos, enunciados, resoluciones y acuerdos que aportaran una idea más amplia de lo que se quiere llevar a cabo; el tercer capítulo, describe la contextualización metodológica en donde se justifica la metodología que se llevara a cabo en la práctica profesional; el cuarto capítulo, describe el desarrollo y ejecución de cada uno de los objetivos que se trabajaron en la práctica profesional, que metodología se implementó y cuáles fueron los resultados obtenidos. Finalmente, en el quinto capítulo se mencionan las conclusiones y sugerencia que se identificaron en el desarrollo de la práctica profesional, teniendo en cuenta cada uno de los objetivos que se trabajó.

1.Contextualización del trabajo

En este capítulo se desarrolla el problema, justificación y los objetivos necesarios para la realización del presente trabajo. inicialmente se abarca el problema en donde se pretende identificar las oportunidades que actualmente tienen los procesos del área de seguridad de la información del Banco Mundo Mujer, tomando cada cada una de las actividades que se realizan para unificarlas con controles que ayuden a visualizar las desviaciones del proceso. Por otra parte, la justificación abarca las oportunidades que trae consigo la realización de este en la organización. Finalmente, se plantean tanto el objetivo general como los objetivos específicos, los cuales orientarán el desarrollo de la implementación de BPM en el área, analizando los resultados que obtiene el área con lo que se pretende mejorar y retroalimentar continuamente en los procesos.

1.1 Problematización

1.1.1 Descripción del problema.

La adopción de estándares y metodologías de gestión de procesos de negocio muestra en las organizaciones su capacidad de adaptarse rápidamente a los cambios que se generan en el entorno, pero por otro lado se alinean todas las partes involucradas para lograr el objetivo propuesto~~o.~~ (Hitpass 2014). En una organización es importante adaptarse a los cambios para mostrar un buen desempeño, voluntad y aportar mejoras dentro del cargo que se ocupa.

Con el fin de que el área de Seguridad de la Información logre una mejora efectiva de sus procesos, nace la necesidad de implementar una herramienta que permita mejorar los procesos que se llevan a cabo dentro del área de Seguridad de la Información. Dentro de los procesos del área es necesaria su evaluación, ya que se generan muchos casos repetitivos que son rechazados por no cumplir ciertas pautas que solo generan pérdida de tiempo y reducción de efectividad en sus funciones.

El problema radica en que existen muchos procesos que el área debe registrar, validar, modificar e inhabilitar, pero se presentan diferentes inconsistencias que no permiten una buena gestión tanto para el área que administra estos procesos como para las personas que requieren de esto para su debido cargo.

1.2 Justificación

Lo que toda organización busca es la eficiencia en sus procesos, frente a esto se presentan diferentes inconsistencias que impiden el logro de la eficiencia dentro del área, por esto el ciclo BPM traerá grandes beneficios para ella, logrando la ejecución de alternativas de mejora en los procesos que se organizaran en una estructura cíclica que muestra sus estructuras lógicas(Marroquín 2015).

Así, se pretende reducir tiempo en ejecución, disminuir de fallas e inconsistencias, crear patrones y dar elementos que visualicen el estado del proceso. De este modo se crea un área con controles y evaluaciones que permite saber en todo momento qué, por qué y cómo ocurren las cosas**.** Es decir que en medio de cada proceso que se realice para autorización, creación, modificación, eliminación o inhabilitación de usuarios, sobres de usuarios sensitivos y Controller se logrará satisfacer a los colaboradores que requieren de ello pero también al realizar una buena implementación del nuevo proceso, las personas involucradas verán los cambios y las mejoras que traerá salir de su zona de confort donde viven en medio de situaciones que se pueden evitar o mejorar dentro de lo que se realiza. Sacando a flote su capacidad de adaptación que resulta siendo el factor que les impide acceder a nuevos retos que mejoren su trabajo individual como grupal.

En el campo profesional estas herramienta es muy utilizada por las ventajas que trae a la organización, al brindar un soporte en el desarrollo y el apoyo en la gestión de dicho proceso para realizar mejoras oportunas, administrar y optimizar de forma eficaz cada uno de los procesos.

A nivel personal esta implementación permitirá aplicar los conocimientos aprendidos como estudiante de administración de empresas, la observación de los patrones en que se trabajan, pero también va a fomentar la interacción con colaboradores que puedan aportar para crear beneficios y superar las deficiencias.

1.3 Objetivos

1.3.1 Objetivo General.

Aplicar BPM (Business Process Management) como metodología para garantizar la mejora continua del proceso seguridad de la información del Banco Mundo Mujer.

1.3.2 Objetivos Específicos.

- Descubrir y entender cada uno de los procesos que conforma el área de seguridad de la información.
- Diseñar los procesos de negocio de tal forma que el desempeño pueda ser medido y evaluado
- -Implantar el nuevo proceso en el área de seguridad de la información
- Realizar una prueba piloto de los procesos que se han definido y documentado
- Realizar la mejora continua sobre los resultados que se obtienen a través del nuevo proceso

2.Contextualización teórica

2.1 Marco Teórico

2.1.1 Antecedentes.

Los primeros antecedentes de BPM se pueden trazar en la llamada reingeniería de procesos de negocio (BPR) [Hammer, 1990; Zairi & Sinclair, 1995]. Al realizar un análisis profundo de ambas filosofías, es en este contexto que se da la primera diferenciación entre una reingeniería y una gestión por procesos: en el primer caso se habla de una iniciativa de corte radical, revolucionario y de un solo paso, mientras que en el segundo se considera como un proceso continuo y en constante evolución, de tal manera que se logra una mejora en el rendimiento empresarial. Algunos estudios [Davenport, 1993; Zairi & Sinclair, 1995] incluyen conceptos de Calidad Total (TQM) para ahondar esta diferenciación entre la reingeniería y la gestión por procesos.

Por lo tanto, se puede establecer, bajo este contexto histórico, que BPM surge de la aplicación de conceptos de reingeniería con los de calidad: “la meta primaria de BPM es para mejorar los procesos de negocio de tal forma que se garantice que las actividades críticas que influyen en la satisfacción del cliente se ejecuten tanto eficiente como eficazmente. Puede involucrar pequeños pasos de mejora, así como aprender continuamente de las mejores prácticas, resultando en un rediseño radical de procesos de negocio que logren un rendimiento superior” [Hammer, 1996; Zairi & Sinclair, 1995].

2.1.2 Marco contextual.

La gestión de procesos de negocio (BPM) es un método pensado para conseguir mejores procesos combinando la tecnología y la experiencia. BPM es una acción colaborativa de distintas unidades de negocios y del mundo de TI, y promueve un paradigma de procesos de negocios eficientes y lógicos. (Underdahl, 2013 p.13)

Los procesos de negocios pueden ser gestionados mejor en tiempo de ejecución si la monitorización presenta una respuesta eficaz para alertas sobre las condiciones. Esto permite a los usuarios del negocio detectar proactivamente las modificaciones e iniciar los procedimientos para resolverlas (Gartner 2012).

Las fases del ciclo de vida de BPM están relacionadas entre sí, organizadas en una estructura cíclica que muestra sus dependencias lógicas. Estas dependencias no implican un orden temporal estricto en el que las fases son ejecutadas. Muchas actividades de análisis y diseño/rediseño se llevan a cabo en cada una de estas fases (Smith, Fingar 2006) (Weske (2012).

En esta dimensión, Ovum desarrolla una serie de características y funcionalidades que diferencian las soluciones líderes en el mercado. Los grupos de criterios definidos para la gestión de procesos de negocio son (Ovum 2014):

- Descubrimiento de proceso y alcance del proyecto. El grado en que los procesos de negocio existentes pueden ser descubiertos y el subsecuente proyecto BPM puede ser creado utilizando la solución.
- Modelado y diseño de procesos. Desarrollo de modelos con la utilización de las aplicaciones/plantillas verticales pertinentes, según proceda.
- Simulación y pruebas. Asegurar que los diseños trabajan en el entorno del mundo real.
- Reglas de negocio. Cómo de bien soporta la solución las reglas de la organización en el diseño de procesos de negocio.
- Gestión de procesos en tiempo de ejecución. Asegurar que los procesos alcanzan los resultados deseados en el entorno del mundo real.
- Analíticas. Analizar dónde los procesos pueden requerir mejoras.

- Implementación especifica BPM. Como es implementada la solución en relación con BPM. Otros problemas de implementación son evaluados en la dimensión Ejecución.

En su libro Process Innovation Davenport (1993) define un proceso como sigue: Simplemente un conjunto de actividades estructurado y medible diseñado para producir una salida especificada para un cliente o mercado particular. Implica un énfasis fuerte en cómo se realiza el trabajo dentro de la empresa, en contraste a un énfasis enfocado en el producto a realizar.

En su libro BPM Hitpass (2017) define un proceso como el que debe cumplir un determinado fin en las ciencias económicas, destinado a producir bienes y servicios. Tambien que las actividades están encadenadas a través de una secuencia lógica que determina en su conjunto las condiciones de negocio.

Markides (2000) sostiene que el negocio se define según el producto, la función y el portafolio de capacidad básicas. La definición del negocio según su producto es la que se ha utilizado con más frecuencia.

Peter Drucker (1984) fue el primero en hablar del tema proponiendo que "un modelo de negocio se refiere a la forma en la que la empresa lleva a cabo su negocio". Propone un modelo que responda a quién es el cliente, ¿qué valora, ¿cuál es la lógica subyacente que explica cómo podemos aplicar dicho valor al cliente a un costo apropiado?

Eriksson y Penker (2000) postula que es una abstracción de cómo una empresa funciona, proporciona una vista simplificada de la estructura de negocios que actúa como la base para la comunicación, mejoras o innovación los requisitos de los sistemas de información que apoyan a la empresa.

La mayoría de los procesos fluyen a través de la empresa, pasan de departamento a departamento o de persona a persona, por tanto, no es extraño que, frecuentemente, los clientes

externos no reciban lo que han pedido. Esta situación es comparable con una carrera de relevos, donde el testigo pasa de persona a persona dentro de la empresa. Al igual que ocurre en la carrera, en la vida empresarial los problemas ocurren en el momento del cambio, cuando el testigo se cae al suelo. (Bendell, 1994)

(Zaratiegui 1999) Define un proceso como: “Secuencias ordenadas y lógicas de actividades de transformación, que parten de unas entradas (informaciones en un sentido amplio —pedidos, datos, especificaciones—, más medios materiales —máquinas, equipos, materias primas, consumibles, etcétera), para alcanzar unos resultados programados, que se entregan a quienes los han solicitado, los clientes de cada proceso.”

Según Karl Von Clausewitz(1900)la palabra gestión significa organizar los encuentros aislados con el fin de derrotar/destruir al enemigo: a sus fuerzas, a su voluntad y a su territorio, que es el objetivo ideal de la guerra.

Según expresan Claudia Villamayor y Ernesto Lamas, gestionar es una acción integral, entendida como un proceso de trabajo y organización en el que se coordinan diferentes miradas, perspectivas y esfuerzos, para avanzar eficazmente hacia objetivos asumidos institucionalmente y que desearíamos que fueran adoptados de manera participativa y democrática.

El proceso se vuelve a reiniciar y repetir, La mejora continua va ligada con la calidad, por lo que Deming define calidad como "un producto o servicio que tiene calidad si sirve de ayuda a alguien y disfruta de un mercado bueno y sostenido "(Deming: 1993).

A mayor calidad, mayor productividad, afirma Deming, lo que a su vez conduce un poder competitivo a largo plazo. Las mejoras en la calidad generan menores costos, ya que dan como resultado menos errores, menos retrasos y demoras, y evita la pérdida de tiempo y materias. Los

bajos costos llevan a mejoras en la productividad y esto origina una mayor penetración en el mercado, ventajas competitivas y por lo tanto la solución de posibles problemas que afectan el seguimiento de la empresa.

2.1.3 Definición de términos básicos internos.

Riesgos no financieros

Es necesario definir brevemente la temática de riesgos, para contextualizar mejor los diferentes aspectos de la naturaleza interna de la organización, relacionados con el área en la cual se desarrolla la práctica profesional.

El evidente crecimiento de la economía y del mercado financiero lo hace más dinámico y propenso a diferentes vulnerabilidades, obligando a las instituciones financieras a gestionar cada vez mejor el riesgo, entendido como "la posibilidad de sufrir un daño" (Banco Interamericano de Desarrollo, 1999, p.4).

Considerar lo anterior el Banco Mundo Mujer asume una serie de riesgos, los cuales debe gestionar eficientemente, convirtiéndose en la vicepresidencia de Riesgos en una de las más importantes dentro de la estructura general, ya que desde allí se gestionan todos los riesgos relacionados con las operaciones del banco.

Seguridad de la información

Esta área es la responsable de identificar la confiabilidad, integridad y disponibilidad de la información. Ahora bien, los diferentes riesgos del Banco Mundo Mujer se identifican y controlan desde el área de riesgo operativo, con base en el levantamiento de una matriz de Riesgo Operativo para cada área, en términos generales en esta matriz se identifican los riegos de los procesos, sus causas / s, se describen los controles y se seleccionan los planos de acción para mitigar estos riesgos.

Aplicativos del banco

Son los que permiten a los funcionarios del banco acceder a alguna de las plataformas en las que se llevan a cabo diferentes funciones, influye el área donde encuentre y el cargo que desempeñe.

2.2 Marco Legal

Circular Básica Jurídica - Reexpedida por la Circular Externa 029 de 2014

• Acceso e información al consumidor financiero

• Instancias de atención al consumidor en las entidades vigiladas

Ley 1748 del 26 de diciembre de 2014

"Por medio de la cual se establece la obligación de brindar información transparente a los consumidores de los servicios financieros y se dictan otras disposiciones". (se adiciona un inciso y un parágrafo al artículo 9° de la ley 1328 de 2009)

Ley 1480 de 2011 Estatuto del Consumidor

• Artículo 57 Facultades Jurisdiccionales a la Superintendencia Financiera de Colombia

• Decreto 710 de 2012 Delegatura para Funciones Jurisdiccionales en la SFC

• Ley 1328 de 2009 - Decreto 2555 de 2010

• Artículos 2.34.2.1.1 al 2.34.2.1.9 Régimen aplicable a la Defensoría del

Consumidor Financiero

• Artículo 11.2.1.4.11 (artículo 20 del Decreto 4327 de 2005 Dirección de Protección al Consumidor Financiero)

ISO/IEC 17799:2005 Es un estándar para la administración de la seguridad de la información

Implica la implementación de toda una estructura documental que debe contar con un fuerte apoyo de la alta dirección de cualquier organización. Este estándar fue publicado por la International Organization for Standardization (ISO) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Esta norma internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye la ISO 27001, donde dice que: La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (www.iso27000.es)

Ley 1266 de 2008: dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

Ley 1581 2012 Protección de datos personales: se dictan disposiciones generales para la protección de datos personales

2.3 Marco Conceptual

Para lograr una comprensión precisa del trabajo de práctica a desarrollar, es importante dominar de forma inequívoca diversos términos involucrados, que además se requiere sistematizar de forma correcta la realidad.

BMM: Siglas del Banco Mundo Mujer.

CIS: Área de Centro Integral de Servicios del Banco Mundo Mujer.

S.I: Siglas de Seguridad de la Información.

Área de Tecnología Informática: Área encargada de soportar, diseñar y mantener activos electrónicos y el hardware del banco.

Sistema de Gestión de Seguridad de la Información (SGSI): Se basa en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, que incluye estructura, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos de la Entidad.

Activo: Cualquier cosa que tenga valor para la organización.

Activos de información: Es todo activo que contenga información, la cualidad posee un valor y es necesario para realizar los procesos del negocio y soporte del banco. Se pueden clasificar en: Personas, Intangibles, Electrónicos, físicos y Servicios.

Información sensible: Es una categoría especial de datos de carácter personal especialmente protegido, que hacen parte del haber íntimo de la persona y pueden ser recolectados específicamente con el consentimiento expreso e informado de su titular y en los casos previstos en la ley: Salud, Sexo, Filiación política Raza u origen étnico.

Capacitación: Acción, que involucra un proceso sistemático, que tiene como fin desarrollar habilidades y competencias en el personal de una organización, para hacer más eficiente sus tareas y contribuir al logro de los objetivos organizacionales.

Sensibilización: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

SGSI: Hace referencia al Sistema de Gestión de Seguridad de la Información, elaborado por área de Seguridad de la información, el cual incluye varios elementos, como políticas, procedimientos, entre otros.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Backup: Copia de respaldo almacenada en el servidor en un dispositivo de almacenamiento externo.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no controlados.

Disponibilidad: es la garantía de los usuarios que tienen acceso a la información y a los activos asociados cuando lo requieren.

Integridad: es la protección de la exactitud y el estado completo de los activos.

Perfil: Nivel de acceso a determinada información como la consulta, modificación y administración.

Privilegios: Permiso de acceso a una plataforma o sistema de información.

Riesgo inherente: Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de este se haga a su interior

Riesgo residual: Es aquel riesgo que subsiste, después de haber implementado los controles.

2.4 Marco Situacional

Nombre de la Organización: Banco Mundo Mujer S.A.

Ubicación: Dirección General: Carrera 11 N° 5-56 Barrio Valencia - Popayán, Cauca-Colombia

Cultura Organizacional

Misión

Contribuimos al desarrollo económico de las comunidades trabajadoras del país, estimulando el ahorro y generando acceso fácil y oportuno al crédito y a los servicios financieros complementarios, mediante una metodología personalizada, que genera crecimiento y desarrollo del talento humano de la organización, rentabilidad para los accionistas y la entidad, garantizando su solidez y permanencia en el tiempo.

Visión

Seremos el Banco Líder de la Comunidad.

Valores

- Humildad Excelencia
- Integridad Respeto
- Liderazgo

Marca: Mundo Mujer El Banco de la Comunidad

Logotipo:

Mundo Mujer
El Banco de la Comunidad

3.Contextualización metodológica

3.1 Diseño de la investigación

Para iniciar es importante definir el término diseño que según Kerlinger (2002) sostiene que generalmente se llama diseño de investigación al plan y a la estructura de un estudio. Es el plan y estructura de una investigación concebidas para obtener respuestas a las preguntas de un estudio. El diseño de investigación señala la forma de conceptuar un problema de investigación y la manera de colocarlo dentro de una estructura que sea guía para la experimentación (en el caso de los diseños experimentales) y de recopilación y análisis de datos.

Dentro del desarrollo del trabajo se utilizará por un lado el tipo de investigación cuantitativa que es la que se genera por medio de los indicadores que se pretenden implementar con el fin de sacar datos para analizar y evaluar los comportamientos en los procesos. Y por otro lado la investigación se desarrollará de manera cualitativa que es la de mayor importancia ya que de una manera acertada se alcanzara los objetivos propuestos al identificar los procesos que se realizan en el área de Seguridad de la información el respectivo análisis y propuestas en los procesos que se puedan implementar mejoras.

3.2 Metodología de la investigación

La metodología de investigación se realizará a través de BPM (Business Process Management) o Proceso de negocio, será desarrollado a través del ciclo planteado teóricamente que será muy útil para lograr la mejora continua en los procesos, agilidad, y rapidez en procesos que resultan complejos por no haber sido evaluados y rediseñados. El ciclo de vida que conforma esta metodología según el libro Gestión de procesos de negocio para DUMMIES es el siguiente:

-Descubrimiento: Es aquí donde se busca identificar y entender los procesos de negocio que están dentro del área de seguridad de la información. Esta fase es de vital importancia para realizar

una especificación de cada uno de las funciones que son realizadas por los funcionarios involucrados El debido desarrollo de esta fase puede ser afectada por la claridad de los obstáculos que deben ser modificados y alineados con lo que se pretende lograr.

-Diseño: en esta etapa es necesario analizar las deficiencias que se están presentando en el proceso para crear el plan de implementación

-Ejecución: para que se pueda realizar la ejecución del proceso es necesario que los participantes tengan conocimiento de lo que se quiere implantar en el nuevo proceso, de esta manera se podrá realizar una simulación para su buen entendimiento. De esta manera se asegura que los participantes tendrán sus funciones de acuerdo al nuevo proceso.

-**Operación y mantenimiento:** Después de la ejecución del nuevo proceso, se debe realizar un seguimiento en donde se evalúe como está funcionando, medir el rendimiento de los procesos, analizar si se está cumpliendo con el objetivo del BPM. El mantenimiento se dará en los procesos que no han cumplido con lo que se quiere lograr, es por esto que deben ser transformados de acuerdo a las fases anteriores en donde se debería realizar el ciclo de nuevo, pero en una forma más general que permita la mejora continua en los procesos en los que aún no se llega a la meta. Es así como el desarrollo del ciclo BPM traerá beneficios al área de Seguridad de la información que se basa en un proceso efectivo, ágil y trasparente.

3.3 Fuentes de información

Las fuentes de recolección de datos, de las cuales se va a obtener la información necesaria para la implementación del modelo BPM son los datos primaros o directos y los datos secundarios.

Al respecto Santesmases (2009:75) expresa, que los datos primarios son los más idóneos para que se puedan adaptar a los propósitos de la investigación, sin embargo, tienen un costo elevado, superior al de los secundarios.

Agrega además que la encuesta es la obtención de información por medio de la comunicación ya que se efectúan preguntas contenidas en un cuestionario sobre el objeto de la investigación a la población de interés o a una muestra de ella, a través de entrevista personal, por correo, teléfono, correo electrónico, página web, etc.

Como datos primarios se tendrán la reunión con los analistas del área para conocer los procesos que realiza cada uno y así mismo si se presentan dudas que sean ellos quienes las aclaren para tener una buena definición de cada proceso, la documentación física y digital para tener un mejor conocimiento de cómo se manejan las solicitudes que realizan los funcionarios.

Un dato secundario expresan Grande y Abascal (2009:60) se obtiene de una información que ya existe, puede haber sido creada en el pasado por los investigadores o puede haber sido generada por terceros ajenos a ellos. En estos casos se habla, respectivamente de información secundaria interna o externa; esta información ahorra mucho tiempo y esfuerzos de todo tipo en la investigación y su costo de obtención es inferior al de la información primaria y muchas veces proporcionan al investigador la única información que puede emplear para alcanzar sus objetivos.

Los datos secundarios están constituidos por esos documentos y / o información que sirven de referencia para la elaboración del presente trabajo, como investigaciones, artículos y referencias bibliográficas.

3.4 Instrumentos de análisis

Los instrumentos de análisis que se utilizaran para el desarrollo del trabajo son entrevistas, información secundaria y la observación directa

-Entrevistas: Esta técnica será utilizada para realizar entrevistas no estructuradas que permitan obtener datos relevantes en los procesos para implementar mejoras en los que tengan inconsistencias.

-Información secundaria: Se revisarán las matrices de novedades de nómina, los diferentes formatos que son guardados de forma física o digital y los correos que llegan diariamente a Infoseguridad para conocer las posibles vulnerabilidades que se presenten.

-Observación directa: Este se dará a medida de cada jornada laboral e donde pueda observar y escuchar lo que se vaya presentando lo cual será muy útil para realizar correctamente las mejoras.

4.Desarrollo del trabajo de práctica empresarial

En este capítulo se va a especificar como se desarrolló la práctica empresarial en base a los objetivos planteados y su respectiva ejecución.

Es necesario tener en cuenta que el modelo BPM se divide en 4 fases que son: descubrimiento, diseño, ejecución, operación y mantenimiento.

4.1 Fase I: Descubrimiento

En la primera fase que es el descubrimiento se identificaron los procesos de negocio dentro del área de seguridad de la información. Teniendo en cuenta las actividades programadas se realizó esta fase de la siguiente forma:

4.1.1 Identificación de cada una de las solicitudes.

Durante la primera semana se identificó cada uno de los formatos que se manejan en el área para las solicitudes de accesos en aplicativos, plataformas y url que no se encuentran habilitadas para todo el personal. Así mismo se observa que se manejan otros procesos a nivel interno que permiten tener un control sobre los funcionarios e información explícita que facilita deshabilitar usuarios en caso de que se presente alguna inconsistencia.

Las tareas realizadas por los funcionarios dentro del área son:

- Solicitud de accesos a terceros
- Solicitud de usuarios y autorizaciones entre ambientes
- Definición de usuarios sensitivos
- Solicitud de usuarios de sobres sensitivos
- Solicitud de intercambio de información
- Solicitud de creación, modificación y cambio de perfil
- Solicitud de control de requerimientos de pasos entre ambientes

- Controller
- Directorio activo
- Inactividad de usuarios
- Pulse Score
- Validación de novedades de nómina
- Reporte de modificación de usuarios
- SOC y vigilancia Mnemo
- E-mailings

4.1.2 Documentación de la información según el requerimiento

Las solicitudes que son escaneadas se conservan de manera digital y se clasificaron según el tipo de tipo de solicitud.

Existe una carpeta llamada Autorizaciones en la cual se encuentran las solicitudes de acceso a terceros y solicitud de usuarios y autorizaciones entre ambientes. Lo realizado con estas solicitudes fue dividirlos por carpetas una que se le asignó el nombre de Acceso a terceros y Usuarios con Acceso Producción. Por otro lado, el formato FM-036 de Solicitud de creación, modificación o eliminación de perfil es quitado de autorizaciones para guardarlo en la carpeta de pasos a producción, ya que estos tienen una relación directa al ser este formato necesario para el control de requerimientos y pasos en lo relacionado a habilitar un reporte, transacciones, programas y parametrizaciones.

El formato de control de requerimientos y pasos entre ambientes: es escaneado y guardado según el aplicativo como lo es BANTOTAL,Neon, AZ7, Midas, Cartera digital, PQR, Riesgo y Liquidez, DWH, INFOR, SARA, File Server, Journal, Correo electrónico para tener un mejor orden y facilidad de búsqueda teniendo en cuenta que se guarda con el nombre del paso.

Solicitud de apertura de sobres: en donde son guardados los correos enviados por los solicitantes, de igual forma en un Excel se adiciona esta información para tener un control anual de cuantos sobres son pedidos y cuales en diferentes ocasiones.

Control de usuarios sensitivos: se guardan en una capeta con el mismo nombre en donde se le adicionan subcarpetas para que sean guardados según los servicios como: servicio web, PQR. QIKTOTAL, Red Box, Infor CPM, Autoriza 7, Portal de integración, Cero y riesgo de liquidez.

4.1.3 Especificación detallada de los procesos y sus respectivos requisitos para ser válidos

Con los analistas del área de Seguridad de la información se realizó una reunión para conocer más a fondo los procesos que realizan, de los cuales se mencionaron los siguientes:

-Solicitud De Accesos A Terceros

Este formato está dividido en 5 partes, en la primera se diligencian los datos del solicitante que debe ser de alguna de las áreas de dirección general, especificando su cargo, cédula y extensión la cual es necesaria para notificar que la solicitud es realizada.

En segundo lugar, se encuentran los datos del tercero o proveedor como lo son: su nombre, cédula, cargo, empresa y descripción del servicio que presta al banco.

En la tercera parte se especifican las plataformas a las cuales se necesita el ingreso algunas de ellas son: Juniper, Directorio activo, Webservices, las actividades a realizar en los sistemas de información en los que se requiere un permiso como lo es una autenticación y su fecha de inicio y fecha fin.

En la cuarta parte, se establece un horario de acceso de lunes a domingo en donde se establecen horarios de inicio y fin.

Por último, debe estar firmada esta solicitud por el gerente o jefe solicitante y por el gerente de riesgos no financieros que es la persona que autoriza que la solicitud sea llevada a cabo.

-Solicitud De Usuarios Y Autorizaciones Entre Ambientes

Este tipo de solicitud está dividido en dos partes que son: El diligenciamiento de Solicitud en donde se deben llenar los datos del solicitante: nombre, área, proveedor, cargo, correo, si es contratista o empleado. Aquí mismo se colocan las propiedades del usuario que son el nombre completo, usuario Windows, IP, reserva de DHCP, vigencia de acceso y ambiente.

Accesos a los sistemas de información y / o aplicaciones requeridas, el permiso que requiere ya sea para lectura, escritura, admon, propietario u otro. Después de esto se especifica el trabajo que necesita realizar.

En la segunda parte que es la de aprobaciones debe pasar por el coordinador del proyecto, responsable del ambiente, gerente de tecnología informática y Gerente de riesgos no financieros el cual firma después de que un analista de seguridad de la información verifique los datos requeridos, su validez y correspondan sobre todo al permiso que se solicita, de lo contrario no es aprobado.

-Definición De Usuarios Sensitivos

Este es un formato que como su nombre lo indica tiene la definición de cada usuario que tienen acceso a conexiones que se esté revisando, Ejemplo: Usuario “elaguado” es un usuario que tiene privilegios en la base de datos.

En este formato se describe los usuarios sensitivos de cada uno de los servicios que aplica, muchas veces no es necesario pedirlo en físico porque puede ser enviado por correo, al no realizarse esta acción se devuelve a Goany Where porque se olvida de imprimirla o pasarla. Es necesario que el formato siempre sea pasado en preproducción porque puede ocurrir que en el momento de ser llevado a producción un paso el formato no haya sido recibido y se perdería la evidencia.

-Solicitud De Usuarios De Sobres Sensitivos

En este proceso se debe realizar la solicitud por correo por parte del funcionario que requiere el sobre, especificando el número de sobre, servicio, actividad a desarrollar, tiempo de uso y devolución.

Con la solicitud realizada en el área de Seguridad de la Información por uno de los analistas que tiene la custodia de todos los usuarios que son necesarios para la configuración de los aplicativos. En este proceso lo que se hace en primer lugar, es el envío de un correo electrónico por parte de usuario solicitante donde informe que número de sobre necesita, el servicio y los días que lo requiere.

Ahora bien, para ser autorizado es importante tener en cuenta que otra área involucrada en este proceso es la de Tecnología Informática que son los encargados de identificar a los usuarios sensitivos y tienen en su poder la mitad de la contraseña de las aplicaciones del banco, como lo es comunicaciones, usuarios administradores de todas las aplicaciones del banco que son los más delicados porque tienen todos los permisos que les permite hacer cualquier cosa.

Después de ser autorizado, el analista con la custodia es el encargado de dirigirse al área de TI para hacer la unificación de las contraseñas requeridas para acceder al aplicativo que se desea configurar.

-Solicitud De Intercambio De Información

Esta solicitud se encuentra en el formato FM-484, lo que se hace en este proceso es intercambiar información entre un funcionario del banco y un funcionario de otra empresa.

En donde toda la información que se vaya a enviar a terceros o internamente, es sensible y manejada en una matriz de envío y recepción de información. Para cumplir adecuadamente con los requisitos:

- Se evalúa con qué frecuencia va a ser enviada la información.

-Si la información utilizada es crítica, aquí se tiene en cuenta una de las características del área de Seguridad de la Información que es la confidencialidad que se ve reflejada en el cuidado de la información entregada al usuario solicitante.

-Se evalúa si el uso es diario o mensual, para que se puedan definir las llaves de encriptación necesarias en la interpretación de la información y no solo esto, si no evitar que otros hagan uso de ella. Por esto sin la llave solo aparecerán códigos de programación.

- A este formato se le asignan responsables, el tipo de información que se va a prestar, se verifica de donde viene la información y el tipo de proceso, es decir, manual o técnico.

Por último, cuando se acaba la vigencia de los formatos, lo que se hace en caso de que el intercambio de información haya sido un largo plazo es llamar al interesado para saber si va a continuar con ello, para que pueda modificar su formato y así poder seguir contando con el acceso vigente.

-Solicitud De Creación, Modificación Y Cambio De Perfil

Es utilizado como soporte para crear una transacción, una parametrización, reportes, controles y programas, siempre debe estar como adjunto el formato FM-036 es la solicitud del requerimiento específica a quien se la van asignar. Debido a que muchas veces en la documentación no dice, por eso es necesario saber su asignación para realizar la habilitación respectiva.

-Solicitud De Control De Requerimientos De Pasos Entre Ambientes

Dependiendo del tipo de solicitud de Tecnología Informática ya sea para autorizar o evitar restricciones, parametrización, programas y reportes. El área de Seguridad de la Información lee lo que dice el paso para tener en cuenta si debe llevar algún formato. Lo que se hace normalmente es buscar el paso en una base de datos en donde se encuentra el manual técnico que define lo que

se debe hacer con el paso y si concuerda con lo dicho en el que se trae en físico, en caso de no concordar la descripción y solución de ambos se devuelve.

Cuando el paso va para el ambiente de producción se verifica que la fecha en la que se le dio el VoBo en preproducción sea superior a la fecha de elaboración del manual técnico, ya que esto indica que no se modificó en el área de TI.

En el paso existe una parte que es llamada objetos del paso que se tiene en cuenta el tipo de objeto y su descripción. Ya que si es un Save File es devuelto porque ya en su interior puede traer varios tipos de objeto que no se tiene conocimiento desde el área, viene encriptado. No se firma para no correr con responsabilidades de las cuales no se sabe.

-Controller

Es un aplicativo que tiene que ver con la herramienta AZ7, Bantotal, AS400 y DWH. Es una réplica en línea del ambiente productivo, en el cual no hay muchos usuarios, son muy pocos. Todos los usuarios del banco ingresan sobre todo para que Bantotal no se coloque lento. Aquí se ve toda la información relacionada con el ambiente de producción como lo son las cuentas de ahorro y CDT. Siempre se empieza a consultar aquí y no en Bantotal. Teniendo en cuenta que es en línea la diferencia son 5 minutos de réplica, lo hacen con el fin de no colapsar el sistema y mejorar la disponibilidad en DWH.

Diariamente llegan al correo de infoseguridad los controles de AZ7, BMM, DWH, que son almacenados en una carpeta para que el analista al que corresponda haga la verificación respectiva en cuanto a cada aplicativo.

-Directorio Activo

El control que se tiene desde Seguridad de la Información es validar los usuarios que tienen actualmente perfil Egresado, no se encuentre en el directorio activo ya que de esta manera es deshabilitado su permiso a un equipo del banco.

Lo que se encarga el analista de seguridad de la información es de validar que se haya realizado el cambio al usuario reportado por talento humano como egresado.

-Inactividad De Usuarios

En la política 007 se estipula que después de 90 días que un usuario no ingrese a Bantotal o autoriza su perfil se convierte en inactivo, esto pasa cuando solicitan un usuario, pero nunca fue necesario entonces para llevar un control sobre esto, pasan a un perfil que no tiene ninguna funcionalidad. Pero si más adelante el usuario requiere que este perfil se active se tiene que hacer una solicitud para que el CIS le asigne el perfil correspondiente. Desde el área de SI es sobretodo un control para que los usuarios no se queden activos innecesariamente.

-Pulse Score (Ingresos A Juniper)

Diariamente el SOC envía al correo de Seguridad de la Información un informe Pulse Score con el fin de llevar a cabo el control de los usuarios que acceden a esta plataforma.

Desde Seguridad de la Información se le hace seguimiento a los usuarios que están autorizados para conectarse, pero por otro lado por medio del reporte enviado por el SOC se verifica que las personas conectadas estén autorizadas para ello, es decir que la fecha de vencimiento sea superior a la del día que se revisa el reporte. Por otro lado, el reporte se descarga en PDF Pulse Score en donde muestra las personas que ingresaron el día anterior a la plataforma y también los ingresos fallidos.

Con este informe lo que se hace es llevar a cabo un registro en Excel de los datos donde están todos los usuarios tanto de BMM y otras empresas.

Se señala en el día correspondiente a los usuarios y así mismo se verifica si su permiso está vigente, en caso de que no esté, se debe llamar al área encargada de quitar el permiso hasta que la solicitud sea actualizada por el funcionario implicado.

Cabe aclarar que estas solicitudes solo se llevan a cabo en la dirección general, en las agencias no es necesario todo está centralizado acá, lo que se requiere en las agencias se solicita directamente en la dirección general dependiendo de quién los tenga a su cargo que son los funcionarios de operaciones y comercial.

-Validación De Novedades De Nómina

Desde el área de seguridad de la información se lleva un control sobre los usuarios que tienen perfil Bantotal con el fin de vigilar las actividades que realizan dentro de la plataforma.

La de mayor impacto en las diferentes novedades de nómina son los egresos de personal que representan un riesgo extremo, seguido por los cambios de cargo (riesgo alto), ingresos y vacaciones (riesgo moderado) y cambios de segmentos y traslados (riesgo bajo). Estas novedades de nómina representan riesgo en diferentes niveles, ya que dependiendo del cargo tienen acceso a información de clientes que es muy importante que se mantenga en confidencialidad. Diariamente llegan informes de cada novedad reportada por talento humano, las cuales son colocadas en libro de Excel según sea la novedad, con el fin de cruzar esta información con los reportes del CIS (Centro Integral de Servicios) que son los encargados de activación o deshabilitación de un perfil. Es aquí donde el área de Seguridad de la Información se encarga de verificar que cada usuario se encuentre en el perfil correspondiente y en caso de presentar alguna inconsistencia se debe informar al CIS, el usuario que debe ser modificado o esperar respuesta del porqué realizó el cambio.

Por otro lado, hay funcionarios que son enviados en el informe pero que no tienen perfil Bantotal el cual debe ser verificado en la matriz de cargos y perfiles que está en dominio del área para filtrar el cargo y así mismo observar si cuenta o no con perfil Bantotal. En caso de que deba tener perfil según la matriz, pero en el reporte 4151A dado por el CIS no se encuentre lo dicho, se debe informar para su creación y control en las diferentes validaciones de nómina existentes.

-Reporte De Modificación De Usuarios

Diariamente desde Bantotal se descarga el informe 4151A para ser guardado tanto en PDF como en Excel, en este reporte se ven todos los cambios relacionados con las novedades de nómina de cada usuario, es importante su descarga diaria ya que a partir de este se generan cambios en las matrices que existen por cada novedad, que por medio de fórmulas en Excel se actualiza la información que permite dejar un usuario con visto bueno o pendiente, teniendo en cuenta la novedad como por ejemplo si está en vacaciones su perfil actual sea este y no el del cargo al que corresponde durante sus días laborales. Este es un reporte muy completo que nos permite ver que funcionario reporta cambios a un usuario para comunicarse con el caso de que no sea lo que se requiere, contiene todo lo que se necesita para que se actualicen las matrices en el caso que se requiera y permite validar información que se necesita de diferentes años si se presenta alguna inconsistencia.

-SOC

Alertas que saca cada dispositivo o servicio que está configurado para enviar los diferentes Logs(registros) al sistema.

Un ejemplo particular para entender mejor este tipo de alerta es Windows, cada vez que un usuario se conecta se registra lo que hizo, qué eliminó, o donde ingresó, Si cambió la contraseña, es decir que todo lo guarda en el registro que tenga habilitado Windows. Con el SOC se llegó a configurar todo lo que se hace en el ingreso a las máquinas, viendo los ataques de los cuales son sacados los temas para realizar las campañas.

-Vigilancia Mnemo

Es la misma empresa que se encarga del SOC se llama Mnemo, la diferencia es que en los correos que envían hay alertas o informes en donde aparece la imagen, el nombre de banco, la presidenta, y los parámetros que ya están configurados, todas estas alertas salen en base a las redes

sociales con las que cuenta el banco como Facebook, LinkedIn y YouTube. Esto se lleva a cabo por medio del directorio activo que se tiene en el área Seguridad de la Información que es controlado por un analista de la misma, en donde se puede ver que está haciendo el usuario. Por ejemplo, escribir en el buscador: como hackear un banco es aquí donde este reporte le llega al jefe de SI y se busca respuesta al porque está interesado en esta información o simplemente menciona al banco en una de sus publicaciones lo cual se le denomina falso positivo.

-E-Mailings

La elaboración e-mailings en el área de seguridad de la información son creadas en base a las diferentes amenazas que se presentan durante las jornadas laborales o alertas SOC, ya que se hacen en base a la confidencialidad de la información de clientes, en precaución como usuarios de tarjetas de crédito, correos sospechosos que contienen malware, entre otros. Con el fin de concientizar a los empleados de la importancia de ser precavidos o de evitar ciertas situaciones al no tener conocimiento de los riesgos a los que están expuestos.

Por eso el jefe de Seguridad de la Información se encarga de esta labor que es creada con la herramienta power point y examinada por el Gerente de riesgos no financieros que es el encargado de dar el visto bueno o pedir que se hagan correcciones al e-mailing que se está elaborando.

4.2 Fase II: Diseño

En esta fase se realizó el análisis de debilidades de cada uno de los procesos para buscar mejoras que puedan ser implementadas en el área. Por otro lado, se diseñan los procesos en un programa llamado Bizagi que permite la creación de diagramas de flujo para hacer más entendibles los procesos.

4.2.1 Diagramas de flujo.

A continuación, se muestran los diseños realizados para cada uno de los 15 procesos mencionados en la anterior fase con su respectiva descripción de los elementos que los componen.

Solicitud de accesos a terceros

 Inicio

 Solicita por medio del formato FM - 022, diligenciando solo la primera sección en los campos aplicables, entregando el documento debidamente firmado al Gerente de Riesgos no Financieros o jefe de seguridad de la información.

 Recibe la solicitud y asigna al Analista de Seguridad de la información para que evalúe la petición.

 Revisa la solicitud de acceso a terceros, garantizando que no se incumplan los parámetros de seguridad para el acceso al ambiente de producción y no se afecte la continuidad del servicio.

 ¿El acceso del usuario es viable?

 Informa al Gerente de Riesgos no Financieros el rechazo de la solicitud, explicando los motivos que soportan la decisión y notifica al Gerente, director o Jefe de área solicitante que su solicitud no puede ser tramitada.

 Recibe el formato físico FM022 por parte del Analista de Seguridad de la Información para que gestione la aprobación con TI.

 FIN

 Gerencia, Director de área o jefe de área


Gerente de Riesgos No financieros o Jefe de Seguridad de la Información

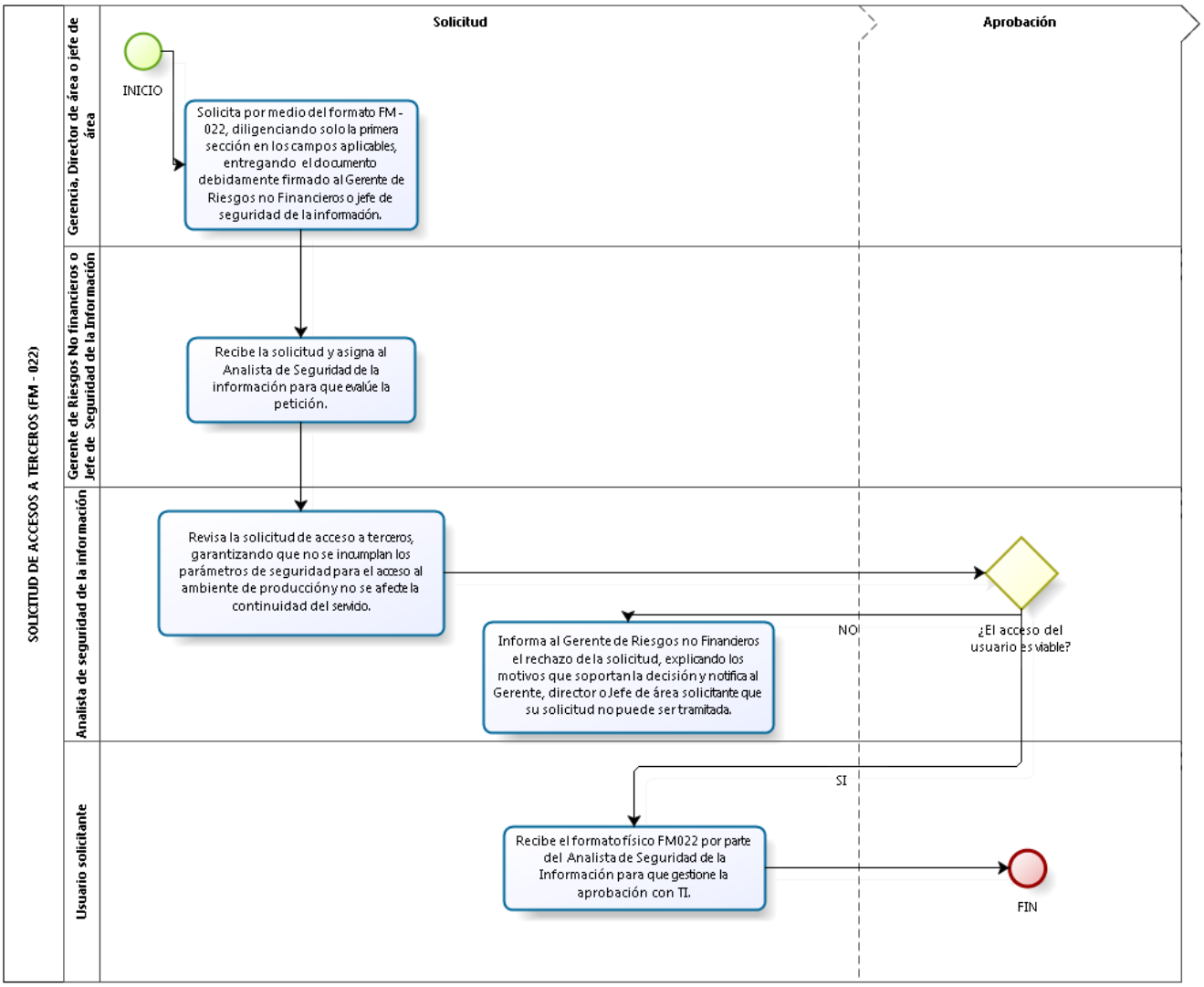

Analista de seguridad de la información


Usuario solicitante


Solicitud


Aprobación

Figura 1. Solicitud de accesos a terceros



Fuente: Elaboración propia

Solicitud de usuarios y autorizaciones entre ambientes

 INICIO

 Solicita por medio del formato FM-170, diligenciando solo la primeria sección en los campos aplicables; entrega el documento debidamente firmado al gerente de Riesgos no Financieros o Jefe de seguridad de la información

 Recibe la solicitud y asigna al Analista de seguridad de la información para que evalúe la petición.

 Revisa la solicitud de acceso a los ambientes, garantizando que no se incumplan los parámetros de seguridad para el acceso al ambiente de producción y no se afecte la continuidad del servicio.

 ¿El acceso al ambiente de producción es viable?

 Informa al Gerente de Riesgos No Financieros o Jefe de Seguridad de la Información y Ciberseguridad el rechazo de la solicitud, explicando los motivos que soportan la decisión.

 Notifica al Gerente, director o jefe de área solicitante que su solicitud no puede ser tramitada

 FIN

 Entrega el formato en físico FM-170 al solicitante para que gestione la aprobación con TI.

 Entrega el formato FM-170 a tecnología para la respectiva autorización y asignación de privilegios de acceso a terceros.

 Revisa la solicitud respecto a lo autorizado por seguridad de la información para la adecuada asignación de privilegios de acceso a terceros.

 ¿El acceso del usuario es viable?

 Informa al Gerente, Director o Jefe de área solicitante.

 FIN

 Recibe notificación al correo electrónico por parte del Gerente de Tecnología con copia a seguridad de la información que los privilegios ya fueron concedidos

 FIN

 Gerente de tecnología

 Gerencia, Director de área o Jefe de área

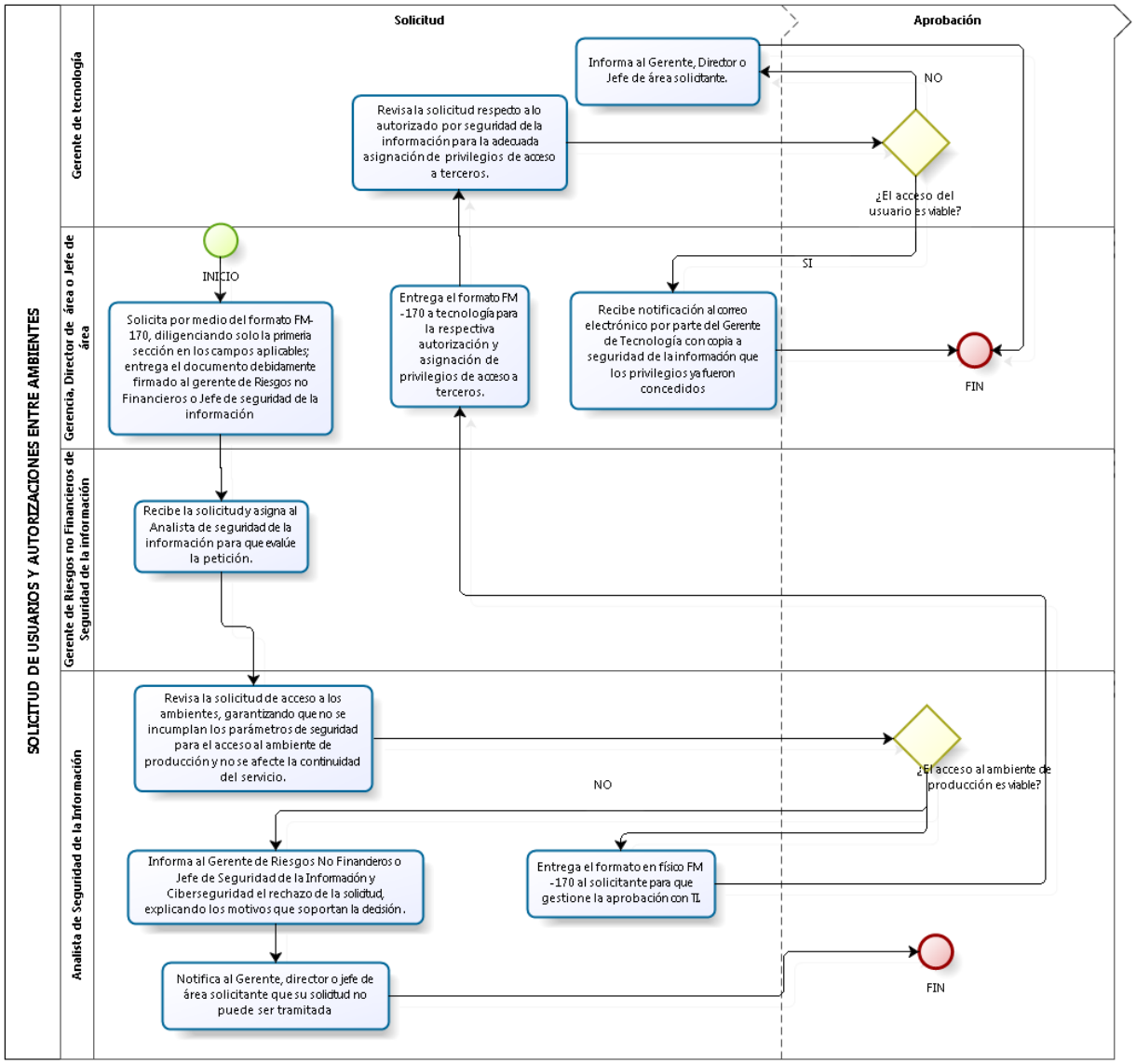
 Gerente de Riesgos no Financieros de Seguridad de la información

 Analista de Seguridad de la Información

 Solicitud

 Aprobación

Figura 2. Solicitud de usuarios y autorizaciones entre ambientes



Fuente: Elaboración propia

Definición de usuarios sensitivos

 Inicio

 Solicita por medio del formato FM-080, diligenciando solo la primera sección en los campos aplicables, entregando el documento debidamente firmado al Gerente de Riesgos No Financieros o Jefe de seguridad de la información.

 Recibe la solicitud y asigna al Analista de Seguridad de la Información para que evalúe la petición

 Revisa la solicitud de definición de usuarios sensitivos, garantizando que no se incumplan los parámetros de seguridad para tener conexión IP y no se afecte la continuidad del servicio.

 ¿El acceso del usuario es viable?

 Recibe la notificación del rechazo de la solicitud, donde se le explican los motivos que soportan la decisión

 Notifica al Gerente, director o Jefe de área solicitando que su solicitud no puede ser tramitada

 FIN

 Gerente, Director o Jefe del área

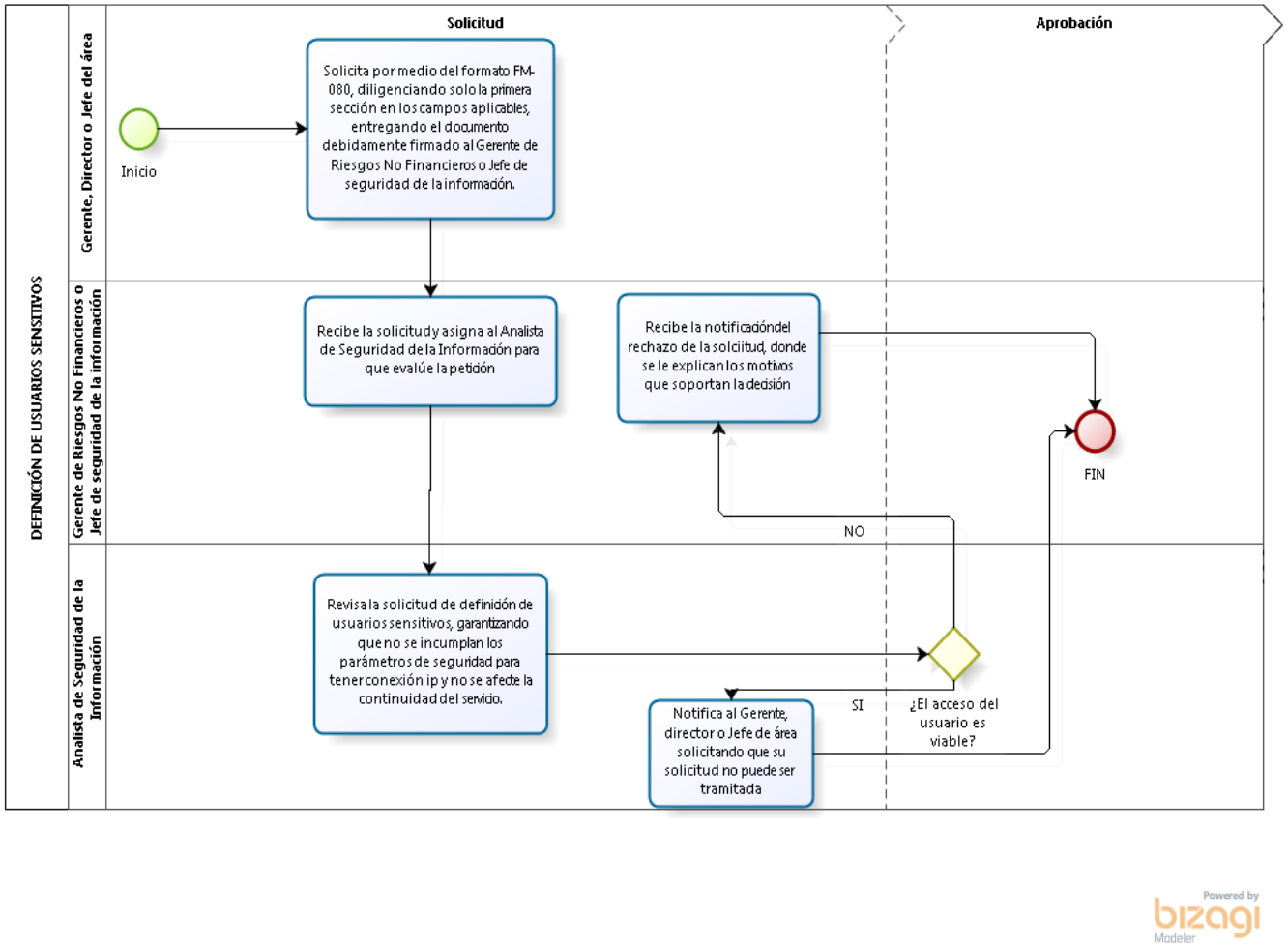
 Gerente de Riesgos No Financieros o Jefe de seguridad de la información

 Analista de Seguridad de la Información

 Solicitud

 Aprobación

Figura 3. Definición de usuarios sensitivos



Fuente: Elaboración propia

Solicitud de usuarios de sobres sensitivos

 INICIO

 Solicita por correo electrónico el sobre que necesito, junto con la actividad a desarrollar y fecha de utilización y entrega.

 Recibe la solicitud del sobre.

 ¿El acceso al sobre por parte del usuario es viable?

 Informa al usuario el rechazo de la solicitud, explicando los motivos que soportan la situación

 Se reúne con el encargado del área de tecnología informática para unificar la contraseña del sobre solicitado.

 Entrega al usuario la contraseña del sobre solicitado.

 FIN

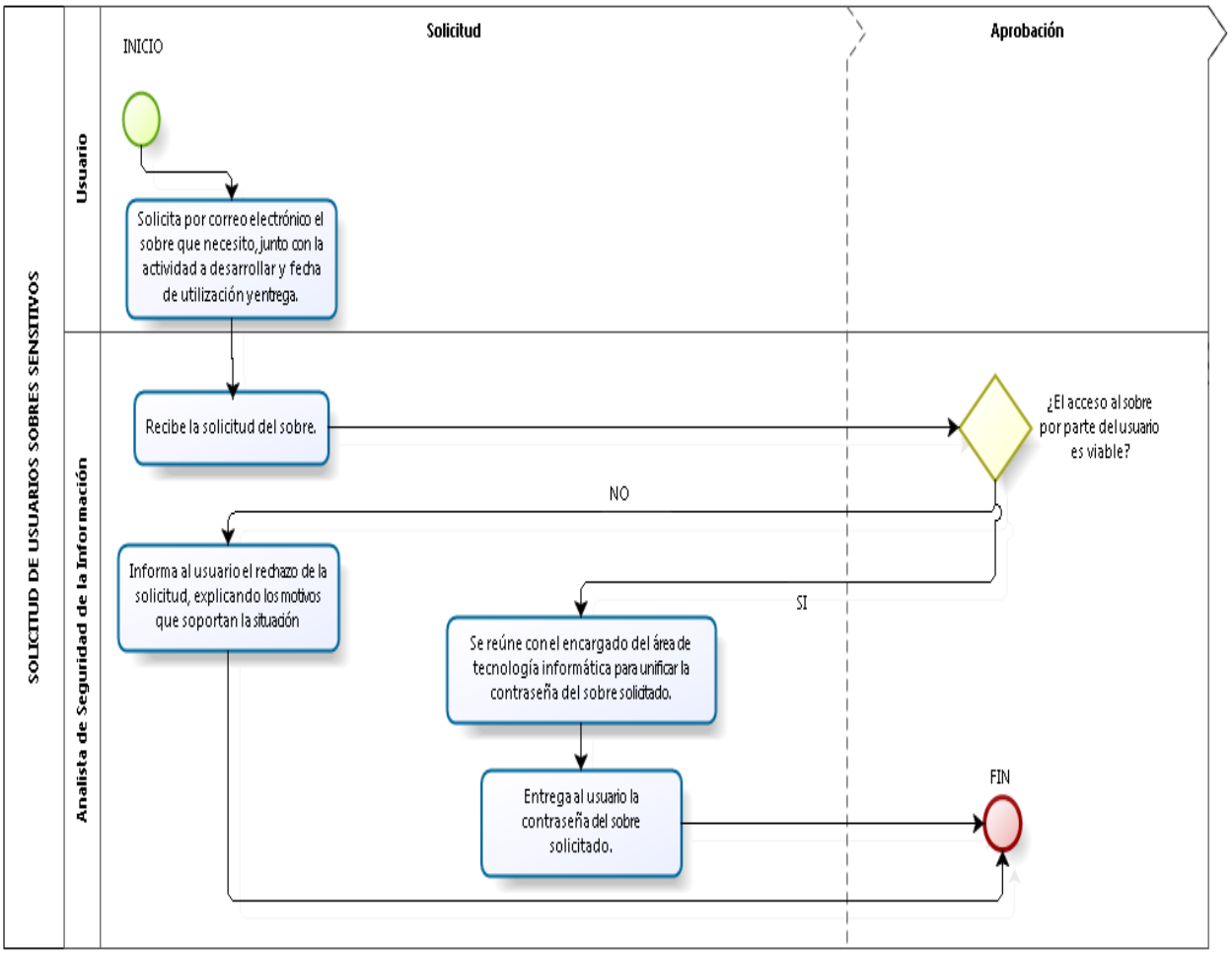
 Usuario

 Analista de Seguridad de la Información

 Solicitud

 Aprobación

Figura 4. Solicitud de usuarios de sobres sensitivos



Fuente: Elaboración propia

Solicitud de intercambio de información

 Inicio

 Solicita por medio del formato FM-484, diligenciando solo la primera sección en los campos aplicables, entregando el documento debidamente firmado al Gerente de Riesgos No Financieros o Jefe de seguridad de la información.

 Recibe la solicitud y asigna al Analista de Seguridad de la Información para que evalúe la petición

 Revisa la solicitud de intercambio de información, garantizando que no se incumplan los parámetros de confidencialidad y que su uso sea el adecuado

 ¿El acceso es viable?

 Se le notifica que la solicitud no puede ser tramitada

 Recibe el formato físico FM-484 por parte del analista de Seguridad de la Información con la respectiva descripción de la trasmisión y recepción de información que requiere para realizar su proceso.

 Se le notifica que la solicitud no puede ser tramitada

 FIN

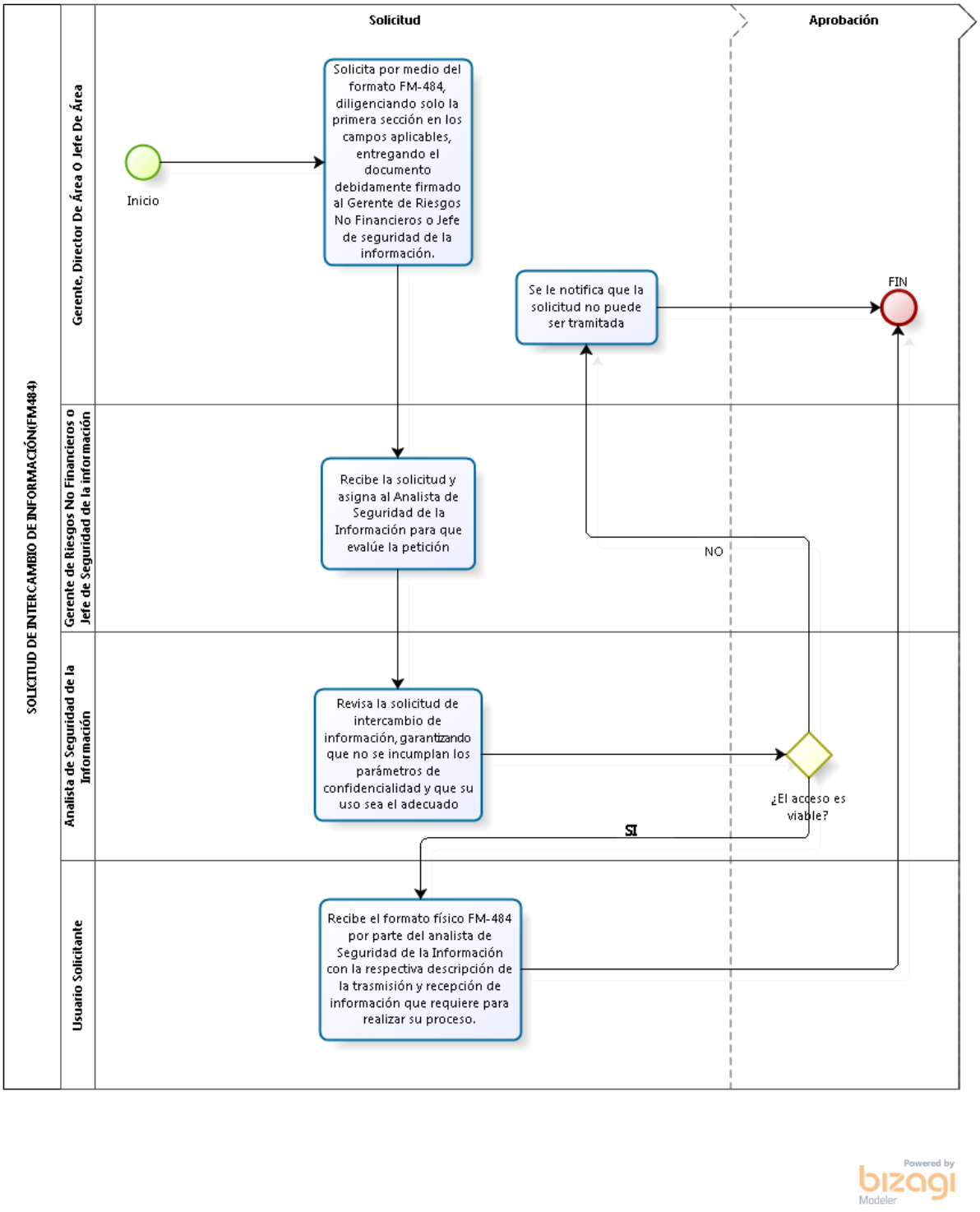
 Gerente, Director De Área O Jefe De Área

 Gerente de Riesgos No Financieros o Jefe de Seguridad de la información

 Analista de Seguridad de la Información  Usuario Solicitante

 Solicitud  Aprobación

Figura 5. Solicitud de intercambio de información



Fuente: Elaboración propia

Creación, modificación o eliminación de perfil

 INICIO

 Diligencia formato FM-036 con el fin de solicitar la modificación, creación o eliminación de perfil en los sistemas de información

 Entrega en forma física el formato FM-036 debidamente diligenciado al área de Seguridad de la información

 Evalúa la solicitud de acuerdo con los parámetros de seguridad establecidos y determina si la modificación es viable

 ¿La modificación es viable?

 Informa al solicitante que la solicitud no es viable

 Realiza las modificaciones requeridas dentro del ambiente de preproducción y confirma al área solicitante

 Informa al funcionario para que realice el proceso de capacitación y adaptación a la nueva funcionalidad

 Informa al analista de Seguridad de la información que el proceso de capacitación ha finalizado con el fin de que se aplique la funcionalidad en el ambiente

 FIN

 Gerencia, Director de área o Jefe de área  Solicitud

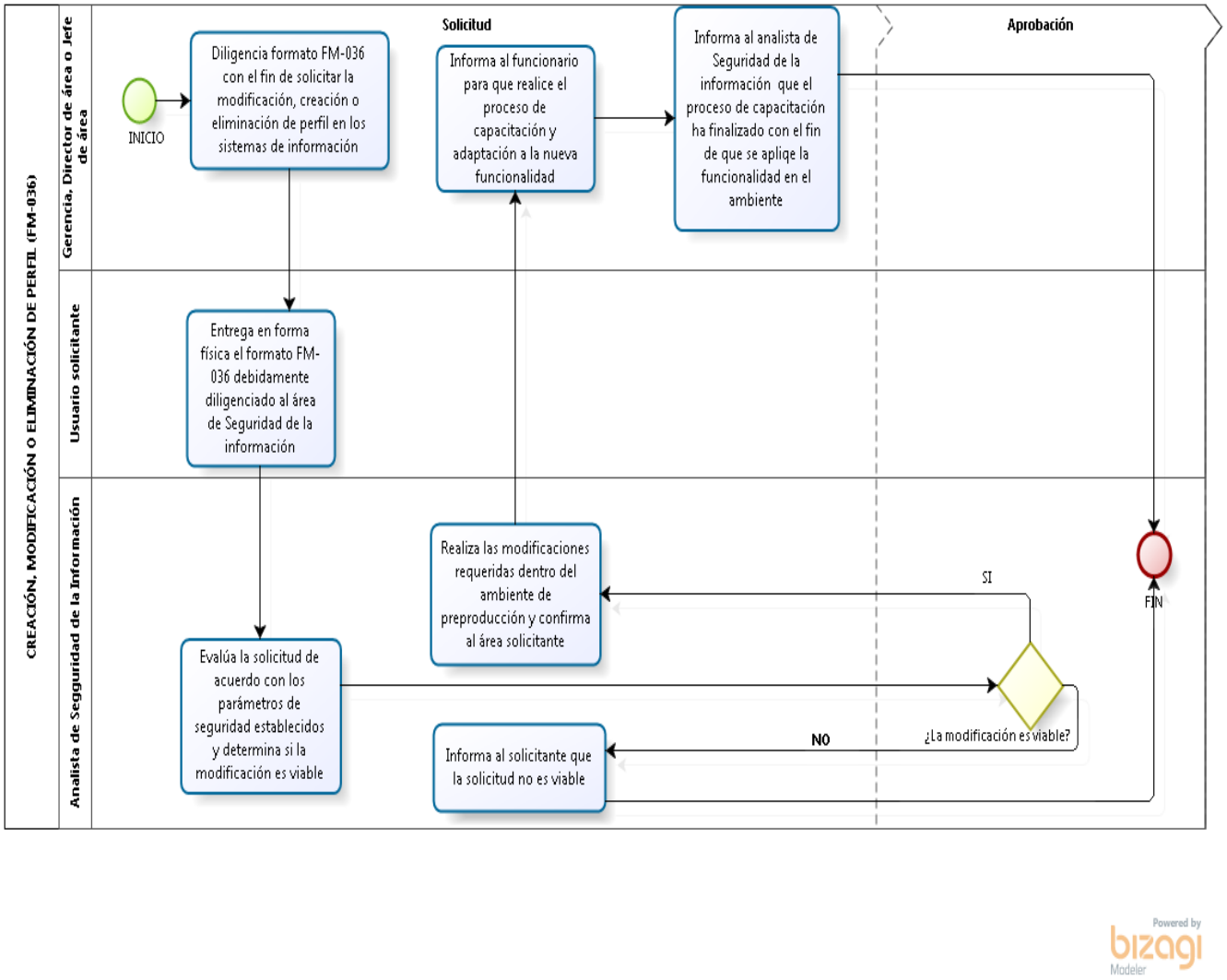
Usuario solicitante

Solicitud

Aprobación

Analista de Seguridad de la Información

Figura 6. Creación, modificación o eliminación de perfil



Fuente: Elaboración propia

Solicitud de control de requerimientos y pasos entre ambientes preproducción

 INICIO

 Entrega el paso al Analista de Seguridad de la información.

 Registra el paso en el control de requerimientos de paso y firma la hoja de control de analista de TI

 Verifica que el paso tenga todas las firmas correspondientes y formatos anexos

 ¿Se puede realizar la solicitud?

 Autoriza la solicitud realizada y firma respectivamente en producción

 Recibe el formato debidamente autorizado y llevado al área de gestión de la demanda para que continúe con el proceso.

 Se informa y devuelve el paso al analista de TI ya que no puede aprobado por la falta de algún formato o inconsistencia en los tipos de objeto.

 FIN

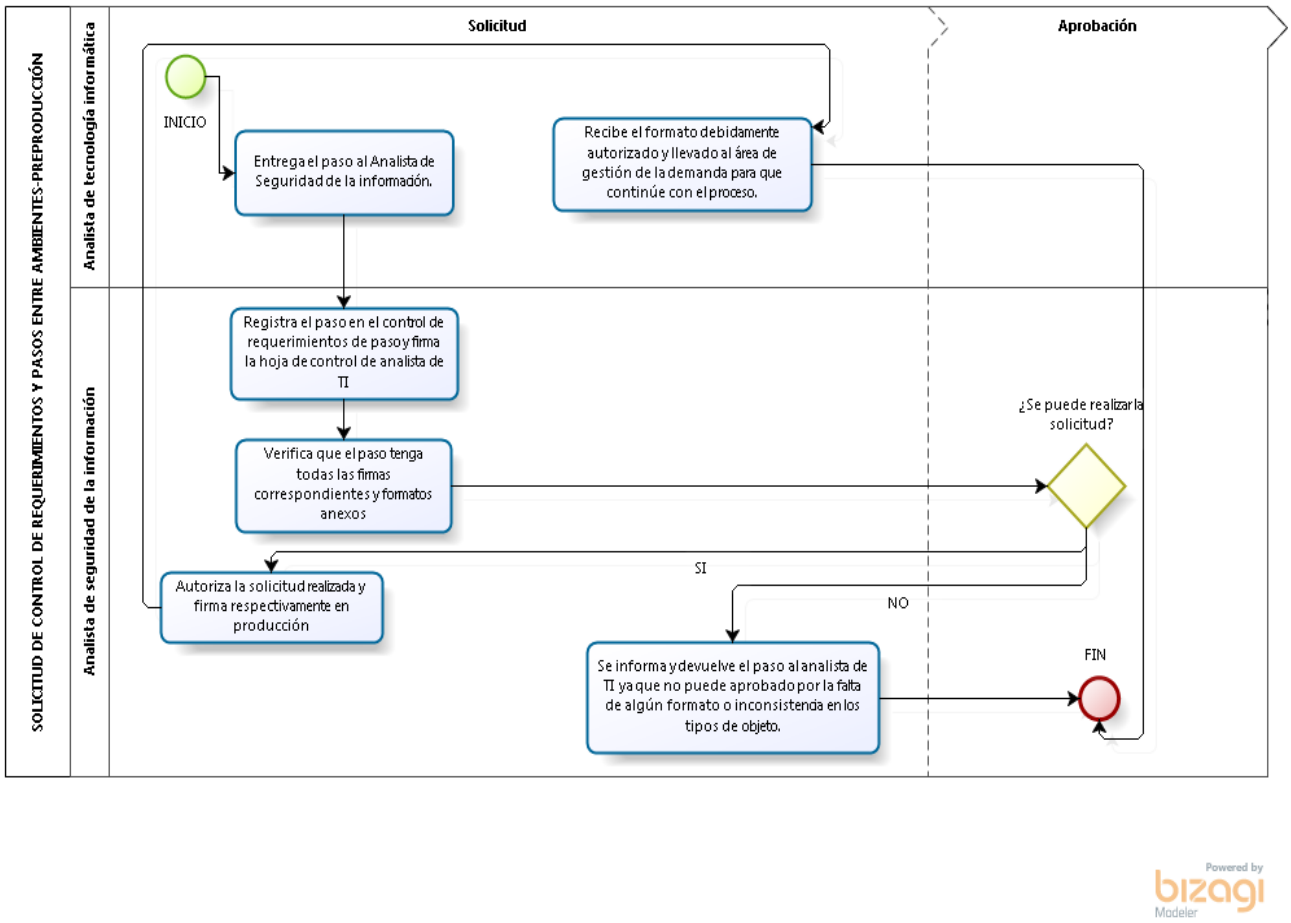
 Analista de tecnología informática

 Analista de seguridad de la información

 Solicitud

 Aprobación

Figura 7. Solicitud de control de requerimientos y pasos entre ambientes – preproducción



Fuente: Elaboración propia

Solicitud de control de requerimientos y pasos entre ambientes producción

 INICIO

 Entrega el paso al Analista de Seguridad de la Información.

 Registra el paso en el control de requerimientos de paso y firma la hoja de control de analista de TI

 Verifica que el paso cuente con la aprobación en producción y tenga el VoBo en el mismo.

 ¿Se puede realizar la solicitud?

 Autoriza la solicitud realizada y firma respectivamente en producción.

 Firma en el ambiente de producción aprobando la autorización del mismo.

 Recibe el formato debidamente autorizado.

 Se informa y devuelve el paso al analista de TI que no se puede aprobar el paso ya sea por algún formato o inconsistencia en los tipos de objeto

 FIN

 Analista de tecnología informática

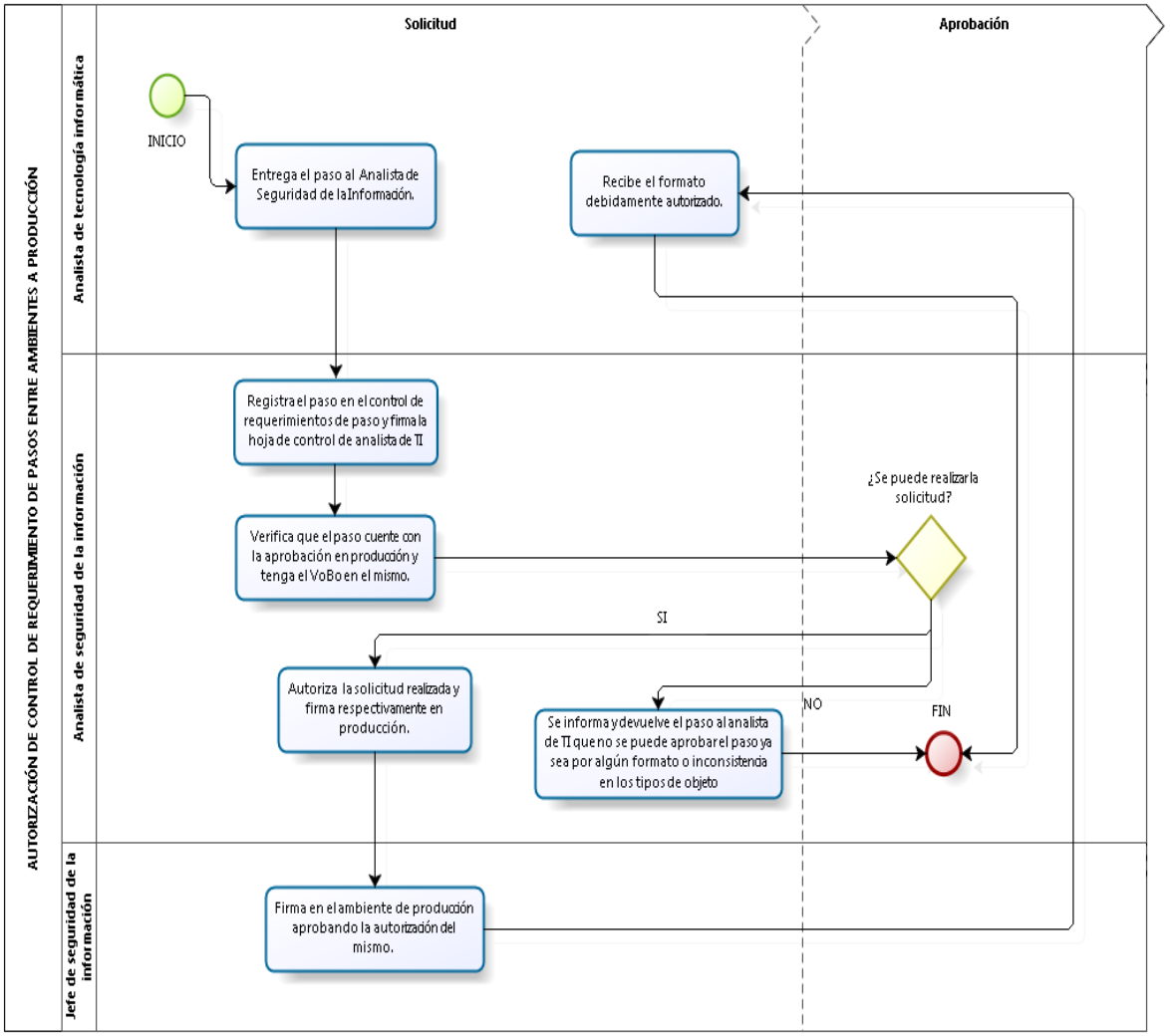
 Analista de seguridad de la información

 Jefe de seguridad de la información

 Solicitud

 Aprobación

Figura 8. Solicitud de control de requerimientos y pasos entre ambientes – producción



Fuente: Elaboración propia

CONTROLLER

 INICIO

 Recibe diariamente por correo electrónico los Controller de Autoriza 7(AZ7), Bantotal (BT) Y Datawherehouse (DWH) y lo guarda en su carpeta respectiva

 Revisa las direcciones de usuarios IP los cual no deben tener conexión desde ninguna máquina

 ¿Los usuarios revisados tienen conexión sobre alguna máquina?

 Se pregunta si fue solicitado por el encargado de conexiones IP

 Revisa las modificaciones sobre las tablas Bantotal o DWH, Solo deben aparecer aquellos scripts que fueron autorizados por el área de Seguridad

 FIN

 Revisa las consultas de información que realizaron y si hubo alguna sentencia

 Deshabilita el acceso a los aplicativos Controller y pregunta al usuario sobre su conexión

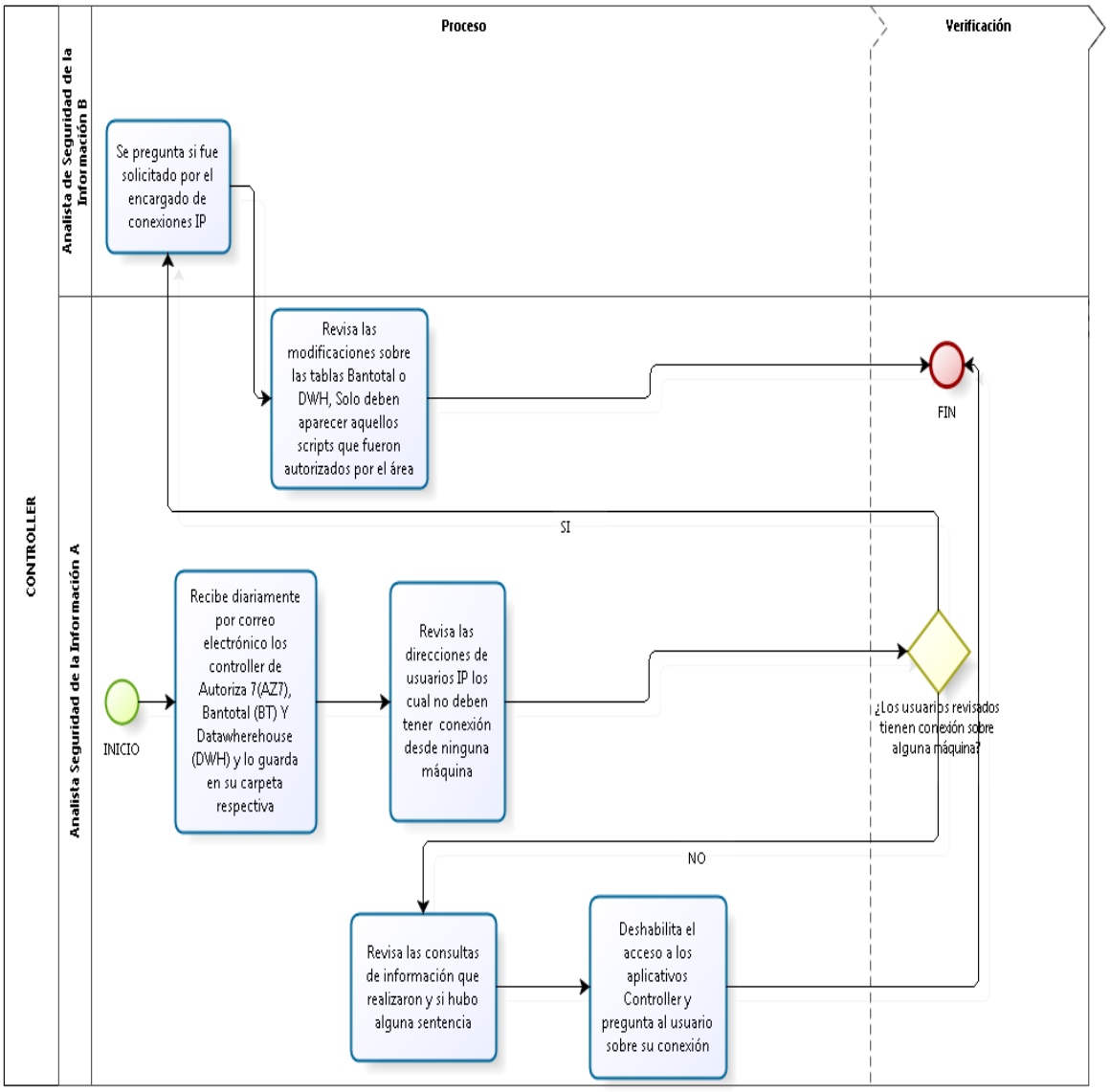
 Analista de Seguridad de la Información B

 Analista Seguridad de la Información A

 Proceso

 Verificación

Figura 9. Controller



Fuente: Elaboración propia

Directorio activo

 INICIO

 Revisa los retiros de personal reportados y diligencia el formato FM-035. Reporta diariamente por correo a Seguridad de la Información, al CIS y funcionarios autorizados el formato con la información del personal desvinculado.

 Crea y asigna la solicitud del área de soporte tecnológico informando los funcionarios a inhabilitar en los sistemas de información a su cargo.

 Inhabilita los usuarios correspondientes en los sistemas de información a su cargo

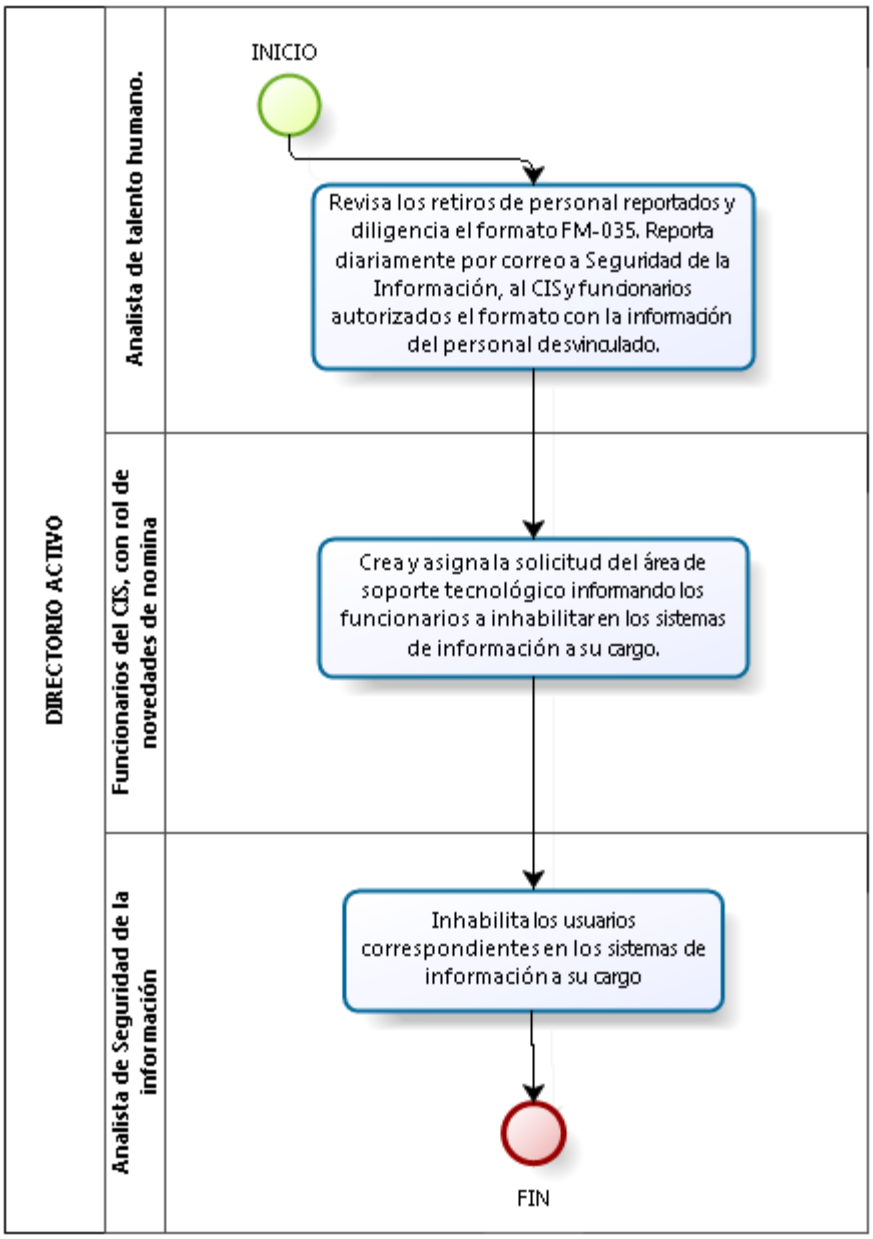
 FIN

 Analista de talento humano.

 Funcionarios del CIS, con rol de novedades de nomina

 Analista de Seguridad de la información

Figura 10. Directorio activo



Fuente: Elaboración propia

Inactividad de usuarios

 INICIO

 Se revisa en la base de datos los usuarios que llevan más de 90 días inactivo

 Informa al CIS que debe ser inactivado un usuario.

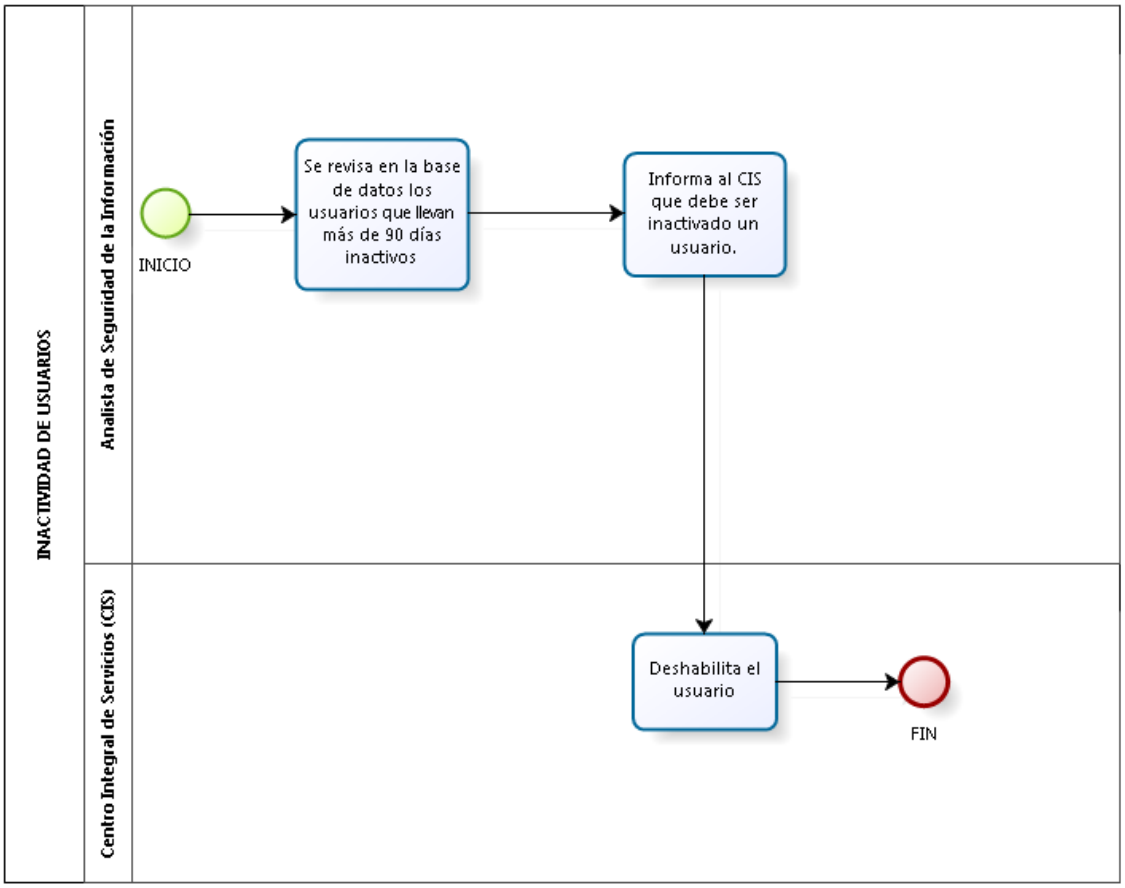
 Deshabilita el usuario

 FIN

 Analista de Seguridad de la Información

 Centro Integral de Servicios (CIS)

Figura 11. Inactividad de usuarios



Fuente: Elaboración propia

Pulse score

 INICIO

 Envía al área de Seguridad de la Información el reporte de usuarios conectado a Juniper

 Guarda diariamente el informe en PDF y Excel

 Verifica que los usuarios tengan fecha de acceso vigente

 ¿Los usuarios cuentan con acceso vigente?

 Guarda la evidencia y se envía al área de tecnología informática con copia al área de Seguridad de la Información

 FIN

 Se informa al usuario que un acceso no está vigente y será deshabilitado por el CIS , Si no trae el formato en el transcurso de la jornada

 FIN

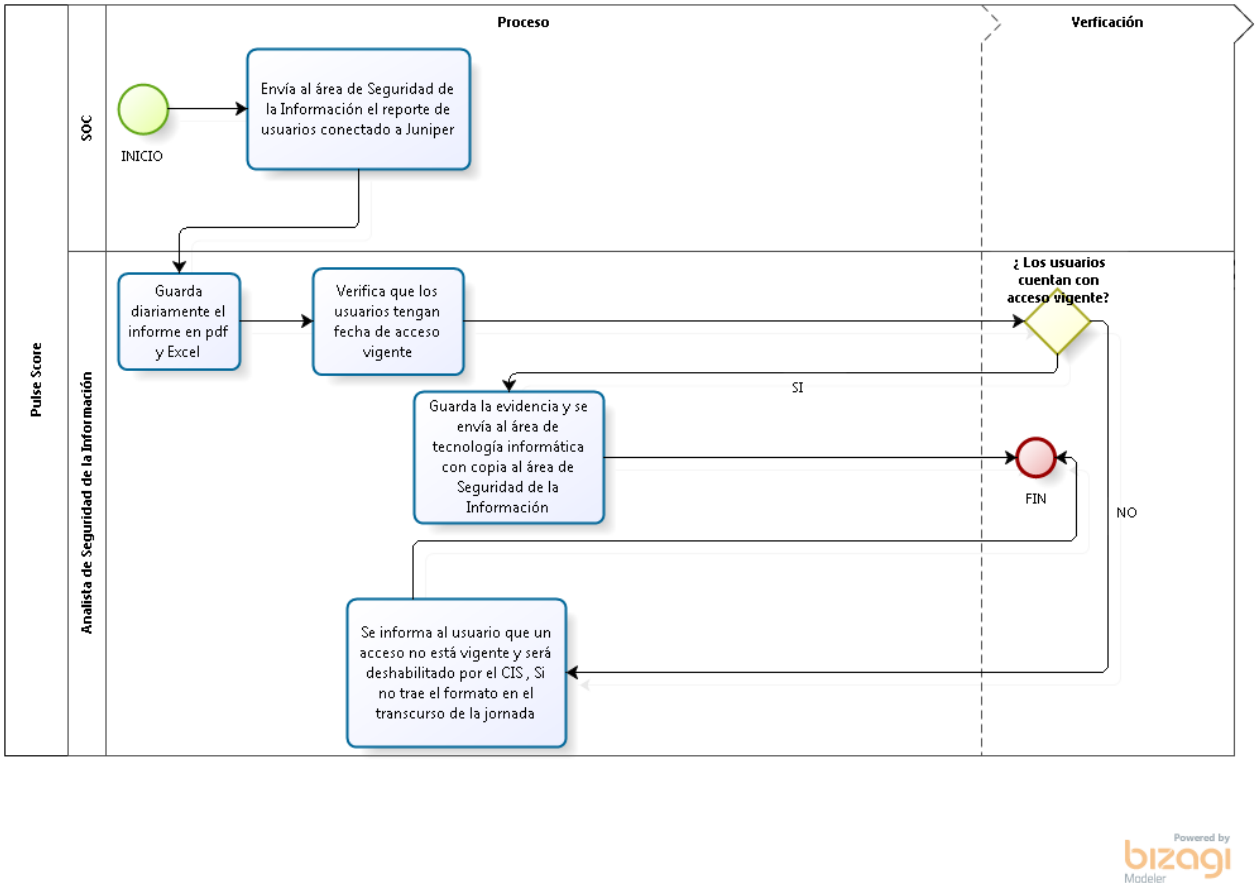
 SOC

 Analista de Seguridad de la Información

 Proceso

 Verificación

Figura 12. Pulse score



Fuente: Elaboración propia

Validación de novedades de nómina

 INICIO

 Revisa las novedades de personal reportado y diligencia el formato FM-035. Reporta diariamente por correo a Seguridad de la Información, al CIS y funcionarios autorizados el formato con la información del personal desvinculado.

 Diariamente guarda las novedades de nómina reportadas en su respectivo Excel donde se analiza el perfil BT que debe corresponder a la novedad reportada.

 ¿Coincide el reporte de perfil BT con el reportado por Talento Humano?

 Guarda sin reportar al CIS ninguna validación

 Reporta al encargado de las novedades de nómina en el CIS que el cambio no se ha realizado, se pide hacerlo o que notifiquen si se presenta alguna inconsistencia.

 Realiza el cambio de perfil.

 FIN

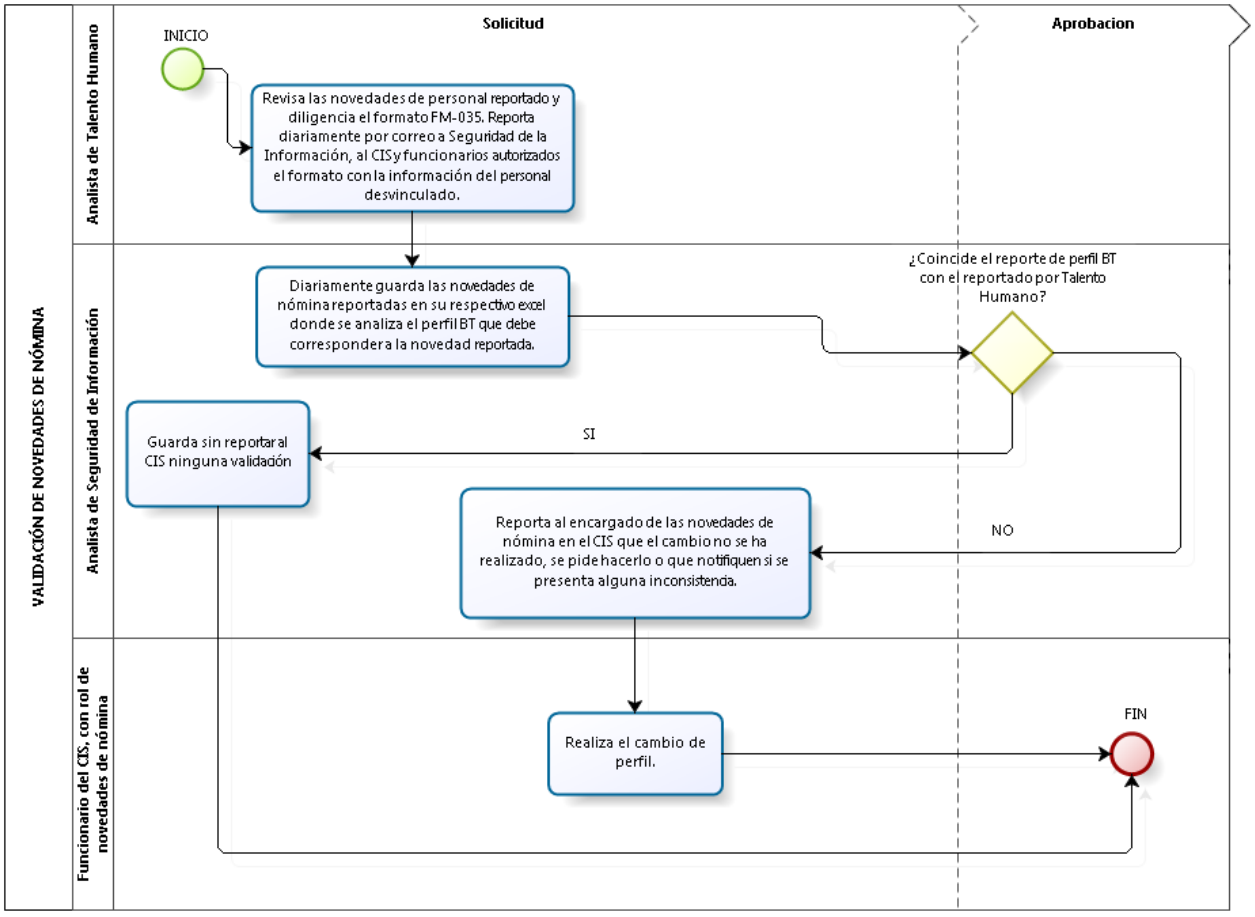
 Analista de Talento Humano

 Analista de Seguridad de la Información

 Funcionario del CIS, con rol de novedades de nómina

 Solicitud  Aprobación

Figura 13. Validación de novedades de nómina



Fuente: Elaboración propia

Reporte de modificación de usuarios

 INICIO

 Ingresa a Bantotal para descargar el reporte 4151A, lo guarda en su respectiva carpeta tanto en Excel como en PDF

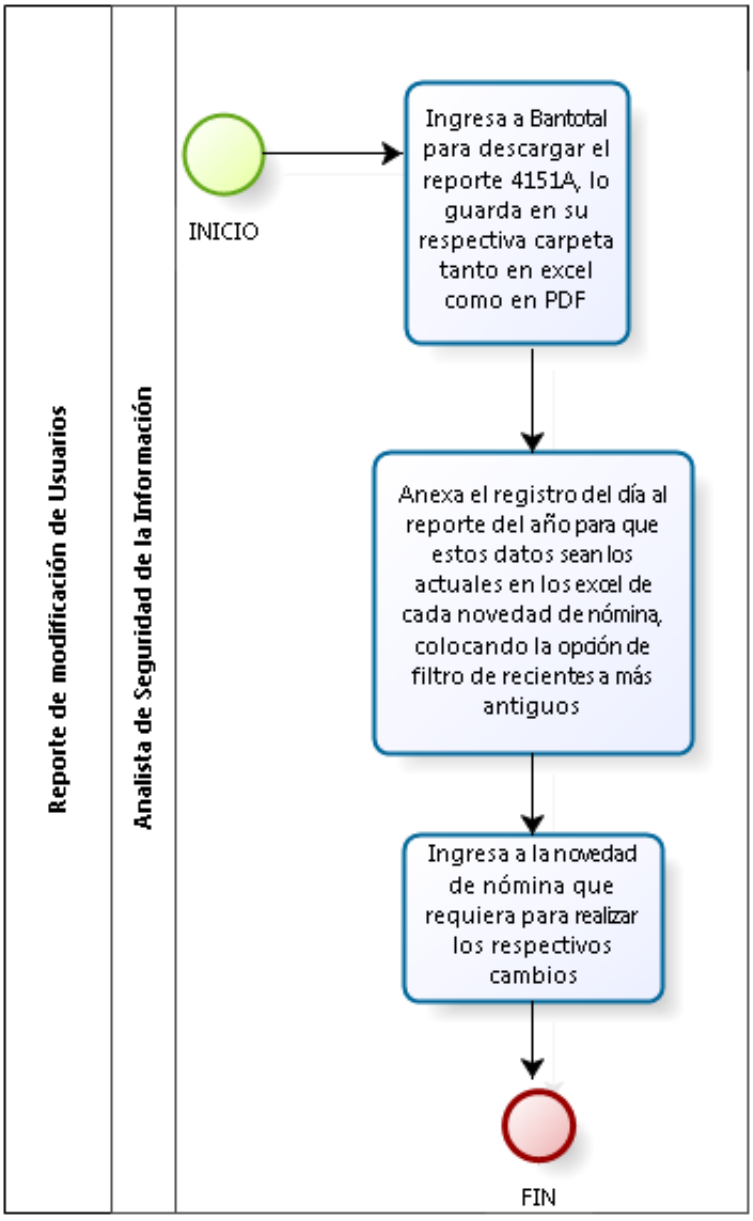
 Anexa el registro del día al reporte del año para que estos datos sean los actuales en los Excel de cada novedad de nómina, colocando la opción de filtro de recientes a más antiguos

 Ingresa a la novedad de nómina que requiera para realizar los respectivos cambios

 FIN

 Analista de Seguridad de la Información

Figura 14. Reporte de modificación de usuarios



Fuente: Elaboración propia

SOC

 INICIO

 Envía las alertas que genera cada dispositivo o servicio que está siendo monitoreado por el SOC

 Gestiona las alertas reportadas por el SOC, descartando los falsos positivos

 ¿Es un falso positivo?

 FIN

 Se encarga de la vulnerabilidad y su respectiva solución

 Revisa las alertas reportadas por el SOC para emitir campañas de sensibilización sobre los nuevos ataques o vulnerabilidades, asignando al pasante universitario la realización de campaña en base a lo requerido

 FIN

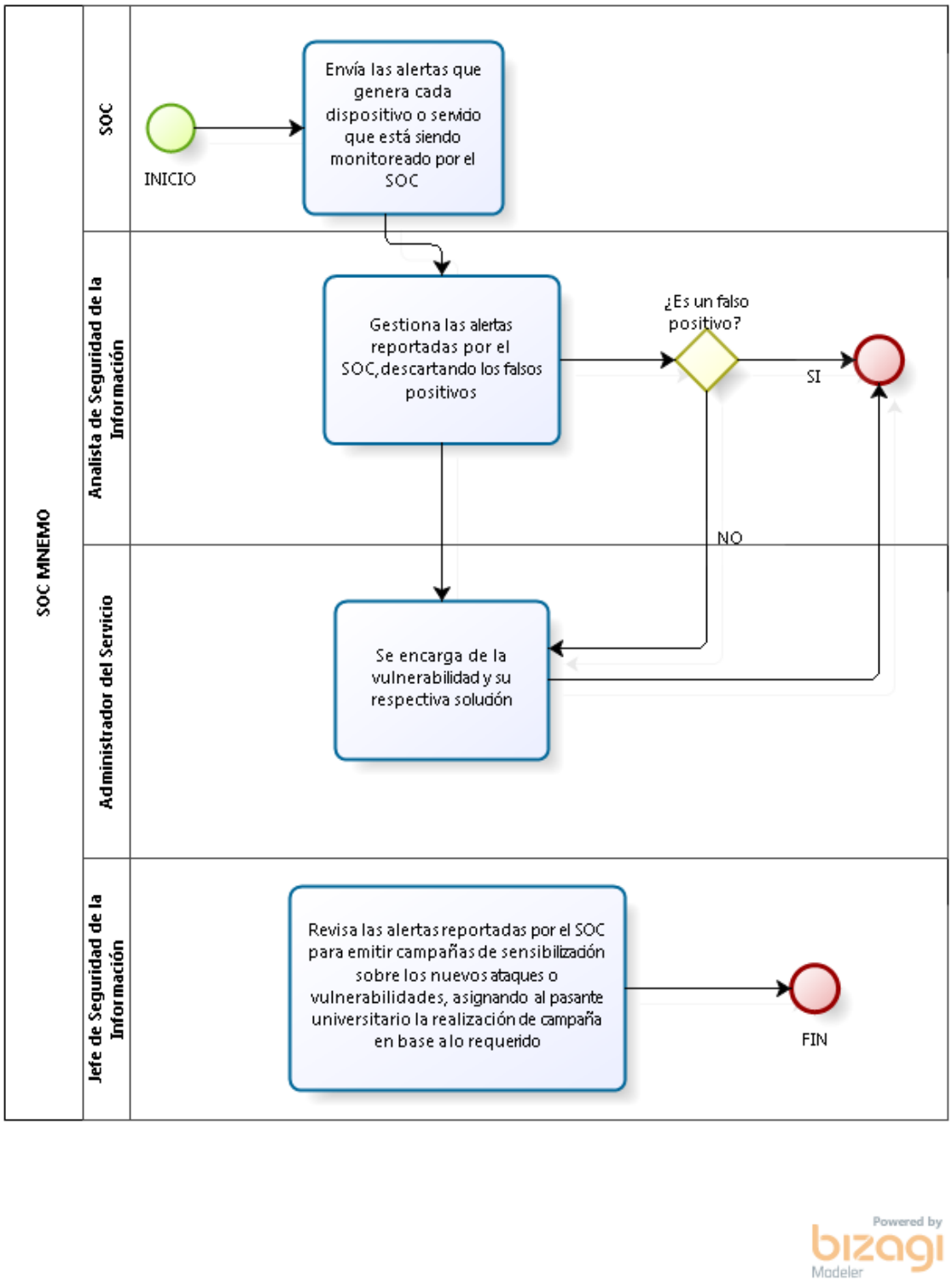
 SOC

 Analista de Seguridad de la Información

 Administrador Del Servicio

 Jefe de Seguridad de la Información

Figura 15. SOC



Fuente: Elaboración propia

Vigilancia MNEMO

 Inicio

 Envía las alertas de búsqueda avanzada en las redes sociales del Banco al área de Seguridad de la información

 Analiza la información recaudada en base a las alertas reportadas en las redes sociales que llevan a una mala imagen de la organización

 Analiza la información recaudada en base a las alertas reportadas en las redes sociales que llevan a una mala imagen de la organización

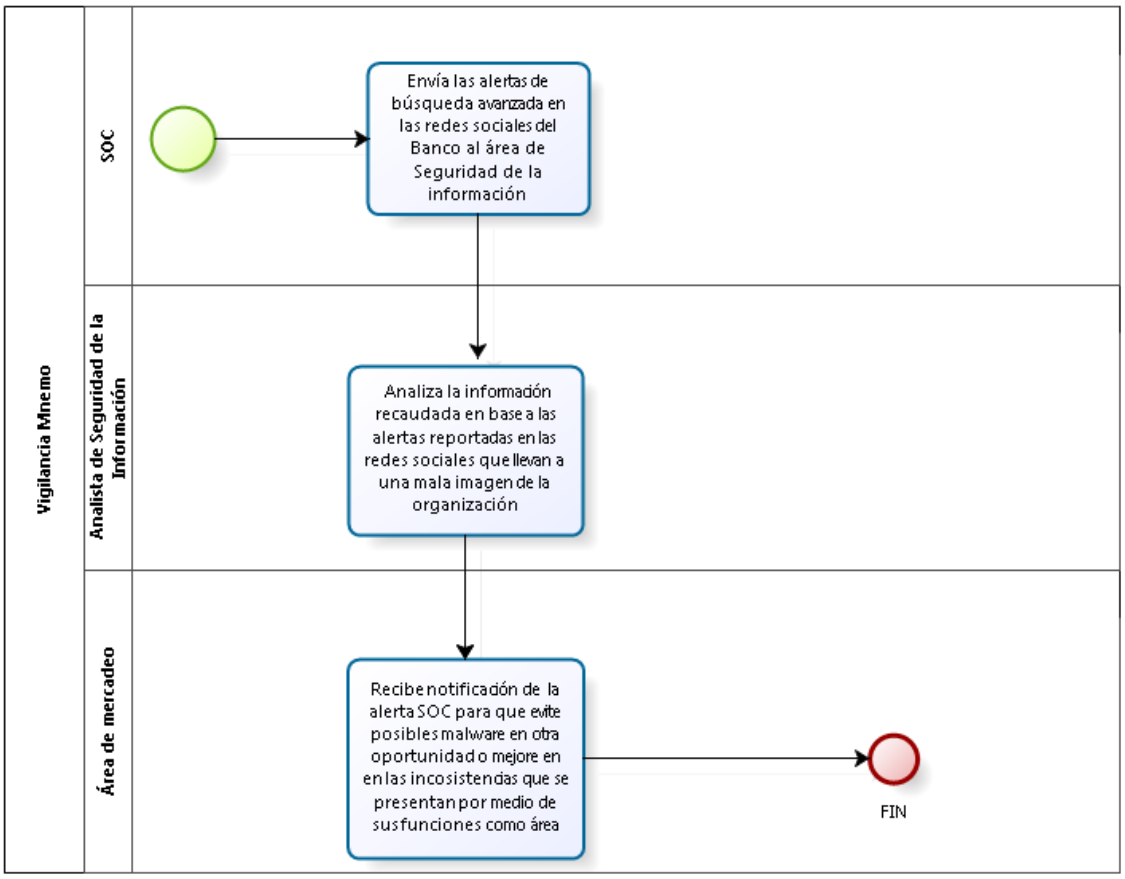
 FIN

 SOC

 Analista de Seguridad de la Información

 Área de mercadeo

Figura 16. Vigilancia MNEMO



Fuente: Elaboración propia

CAMPAÑA

 Inicio

 Analiza las vulnerabilidades que se presentan para asignar al pasante universitario la realización de la campaña de sensibilización

 Investiga sobre el tema asignado y realiza la campaña en power point

 Revisa el E-mailing realizado por la pasante y hace las debidas sugerencias para que sean corregida, si es necesario

 ¿Es necesario realizar correcciones?

 Realiza las modificaciones respectivas

 Revisa la campaña y la envía por correo electrónico a todos los funcionarios del Banco Mundo Mujer a nivel nacional

 FIN

 Jefe de Seguridad de la Información

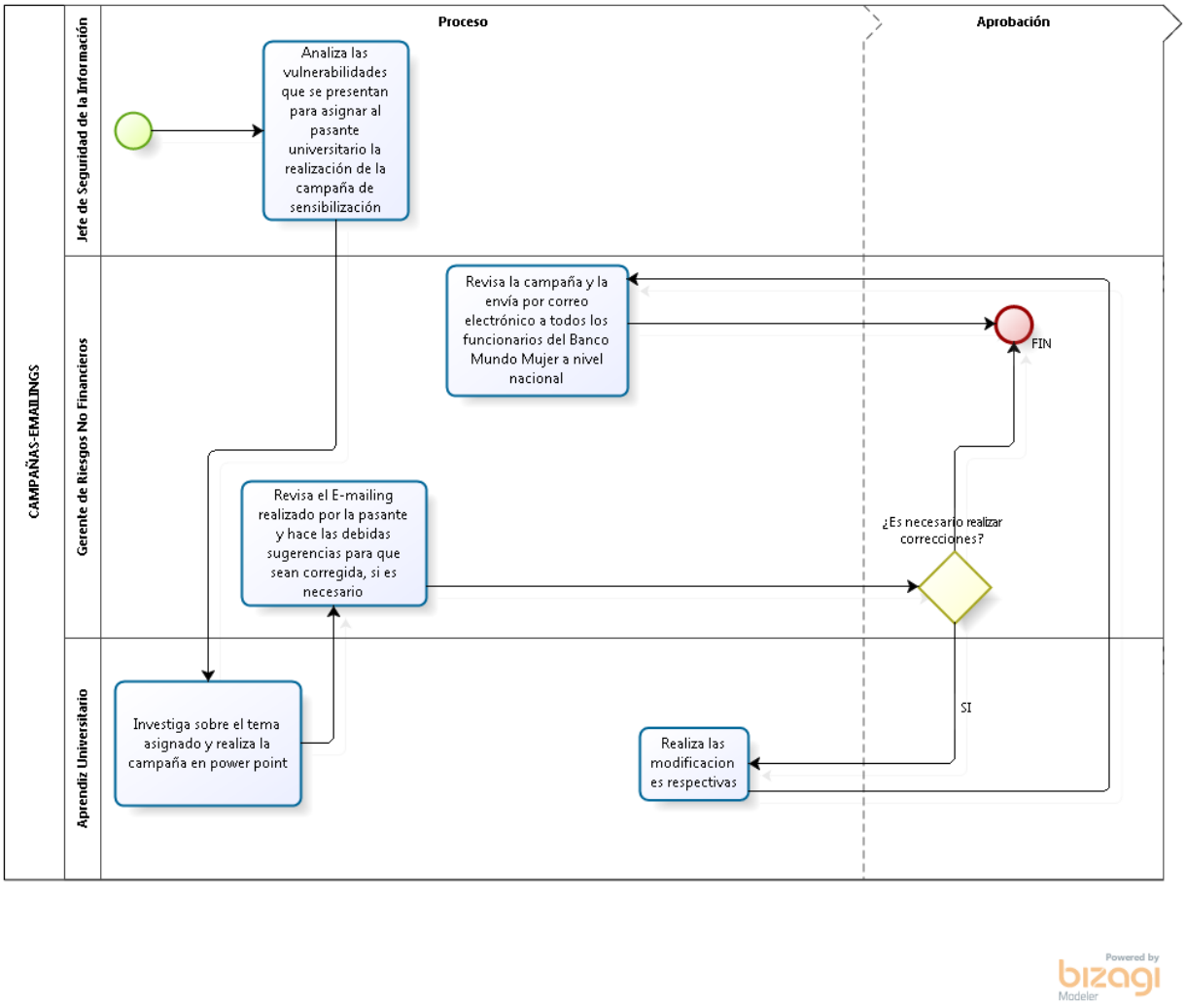
 Gerente de Riesgos No Financieros

 Aprendiz Universitario

 Proceso

 Aprobación

Figura 17. Campaña



Fuente: Elaboración propia

4.2.2 Observación y evaluación de la realización de los procesos.

Teniendo en cuenta la recopilación de datos efectuada para conocer los procesos, es necesario la creación de una matriz que permita observar y evaluar las debilidades de cada proceso para que de este modo se puedan crear oportunidades de mejora en los procesos que lo requieran.

Tabla 1. Matriz de oportunidades de mejora

TAREA	DEBILIDADES	OPORTUNIDADES DE MEJORA
Solicitud de acceso a terceros	Los formatos tienen una vigencia de acceso, lo que implica su actualización en dicho momento. Pero hay usuario que siguen ingresando a las plataformas sin tener ese acceso, lo que implica un riesgo de acceso a la información.	Se cuenta con un Excel que registra la fecha de vencimiento de acceso, lo que se debe hacer con ello es llevar a cabo un control y filtrar por mes las personas a las cuales se les vence su vigencia para así comunicarse con el funcionario encargado del proveedor o tercero, para que presente su actualización y sea llevada al área de Seguridad de la información antes del vencimiento, de lo contrario será enviado un correo para deshabilitar el usuario al área de tecnología informática el mismo día de su último acceso con el fin de evitar accesos sin permiso.
Solicitud de usuarios y autorizaciones entre ambientes	Los formatos tienen una vigencia de acceso, lo que implica la actualización del formato en dicho momento. Pero hay usuarios que siguen ingresando a las plataformas sin tener ese acceso, lo que significa un riesgo de información.	Se cuenta con un Excel que registra la fecha de vencimiento de acceso, lo que se debe hacer con esto es llevar a cabo un control y filtro por mes las personas a las cuales se les vence su vigencia para así comunicarse con ellos y si es necesario su actualización la traigan al área de Seguridad de la información antes del vencimiento, de lo contrario que pueda enviar un correo para deshabilitar el acceso a la plataforma o ambiente de preproducción y producción por medio del área de tecnología informática el mismo día de su último acceso con el fin de evitar accesos sin permiso.
Definición de usuarios sensitivos	NO APLICA	NO APLICA
Solicitud de usuarios de sobres sensitivos: La solicitud es realizada por un funcionario por medio del correo electrónico.	Llegan al buzón de entrada diariamente diferentes correos que impiden la respuesta rápida y eficiente para esta solicitud.	Es necesario que esta información sea enviada con copia no solo al analista con custodia del área, sino también a otro de los analistas para que haya comunicación y se presente la debida atención de la solicitud que se realiza teniendo en cuenta que se trabaja en conjunto con el área de tecnología informática.

Solicitud de intercambio de información	NO APLICA	NO APLICA
Solicitud de creación, modificación y cambio de perfil.	Los formatos muchas veces llegan incompletos, lo que dificulta la asignación en la creación de un transacción, parametrización, etc.	Se debe verificar antes de permitir que el usuario se retire del área, que este formato se encuentre completo o esté dentro del paso cuando es llevado al área para evitar inconvenientes y pérdida de tiempo al no poder realizar lo solicitado
Solicitud de control de requerimientos de pasos entre ambientes	Hay pasos que son devueltos porque no cumplen con las condiciones necesarias para ser autorizados en el área y deben ser analizados desde el inicio.	Capacitar correctamente al funcionario encargado de traer el paso al área con el fin de evitar inconsistencias en el proceso.
Controller	Dentro de los aplicativos que se manejan en Controller muchas veces ingresan desde IP que no están autorizadas.	Lo que se debe hacer es pedir inmediatamente el bloqueo de esta acción y así mismo preguntar el porqué del ingreso a la plataforma sin permiso, o pedir el formato donde se evidencie que tiene acceso pero no ha sido reportado.
Directorio activo	Se presentan demoras por parte de talento humano que impiden una acción a seguir a tiempo en la activación de usuario en base a las novedades de nómina.	Crear un indicador que mida el tiempo de notificación por parte de Th con el fin de mejorar en base a las demoras que se presentan en los ingresos
Inactividad de usuarios	Esto se da debido a que muchas personas piden un usuario Bantotal o Autoriza7 pero no lo usan durante 90 días o quizás nunca.	Analizar si realmente el usuario ingresará a la plataforma para evitarse el proceso de inactividad de un usuario, en caso de que nunca lo utilice.
Pulse score	Permite el acceso de usuarios que actualmente no cuentan con permiso.	Es necesario informar al usuario cuando finaliza su vigencia y así mismo al encargado en el área de tecnología informática de su gestión en caso de no presentar tiempo el formato FM-170

Validación de novedades de nómina	Reporte inoportuno de novedades importantes y de alto riesgo como vacaciones, egresados y cambios de cargo que hacen que por parte del CIS no se puedan realizar cambio de perfiles.	Realizar un informe en el que se le pueda mostrar mensualmente a Th los retrasos y así mismo mejoren para poder generar los cambios correspondientes.
Reporte de modificación de usuarios	Este reporte es cruzado con las matrices de novedades de nómina teniendo en cuenta la última fecha de modificación, lo que hace que se presenten inconsistencias en los perfiles ya que se pudo realizar el cambio pero días siguientes se modifica el perfil y el que se muestra como actual puede crear alteración en el indicador, al no coincidir con lo anteriormente reportado	Lo que se debe hacer es un monitoreo que permita fijar los valores cada vez que se genera el cambio, con el fin de evitar la alteración del indicador y por estos datos erróneos en los informes que se entregan al CIS.
SOC y vigilancia MNEMO	NO APLICA	NO APLICA
E-mailings	Como se menciona en la realización de cada campaña se debe pasar por 2 vistos buenos de los cuales el Gerente de riesgos no financieros pausa la publicación de las campañas debido a que no siempre está disponible para verificar la campaña y hacer correcciones si es necesario.	Al perderse más o menos 20 días entre modificación y publicación, se establecerá un horario de una hora de 9 a 10am los días sábados que es donde hay menos posibilidad de que el gerente esté con mucho trabajo por realizar, de esta manera logrando modificaciones y pronta publicación logrando también que por parte de auditoria sea bien calificado al realizar las publicaciones que se requieren mensualmente

Fuente: Elaboración propia

4.2.3Validación de los procesos en indicadores de desempeño.

Para la creación de los indicadores de desempeño es de vital importancia tener en cuenta las alternativas de mejora que se pretender implementar, con el fin de que en medio de ellas se lleve una medición que es generada por medio de indicadores de desempeño. Para esto las actividades se convierten en objetivos estratégicos a los cuales se le identifican los factores relevantes a medir y de aquí obtendremos el indicador en cada caso.

Tabla 2. Validación de los procesos en indicadores de desempeño

OBJETIVO ESTRATEGICO	FACTOR RELEVANTE	INDICADOR
Disminuir en los usuario el acceso de usuarios sin autorización, informándoles por medio de llamada telefónica acerca del vencimiento de su autorización 5 días antes de que caduque.	Acceso sin autorización	Porcentaje de disminución de usuarios que acceden sin autorización.
	Llamada telefónica	Número de llamadas realizadas mensualmente para evitar accesos o autorizados
Mejorar la recepción en las solicitudes de sobres usuarios sensitivos pedidos por los usuarios por medio del envío de la información a todos los analistas del área para ser vistos y evaluados prontamente.	Recepción de sobres de usuarios sensitivos	Cantidad de sobres pedidos en el mes
	Información vista y comunicada al analista de de custodia	Porcentaje de solicitudes atendidas
Verificar que la información y formatos del paso o formato estén completas para evitar inconvenientes y pérdida de tiempo al no poder realizar lo solicitado	Evitar inconvenientes y pérdida de tiempo en las solicitudes	Número de errores e inconsistencias en los pasos
Realizar capacitación al funcionario encargado de control de requerimiento de pasos entre ambientes con un énfasis especial en las firmas y formatos que debe adjuntar para llevar un paso al		

área de Seguridad de la información		
Proteger los scripts que se encuentran en cada aplicativo, para evitar posibles daños al sistema sin un usuario con acceso autorizado	Evitar ingresos a los aplicativos que generen daños	Cantidad de usuarios que ingresan sin autorización a los aplicativos
Mejorar el envío de la novedad de nómina Ingresos por parte de talento humano por medio de un indicador que les exija y muestren agilidad en la notificación deseada	Agilidad en el reporte de ingresos	Reportes oportunos
		Reportes fuera de tiempo
Determinar si un usuario necesita realmente la autorización de usuario Windows en Bantotal o Autoriza 7 por medio de 3 preguntas que se realizarán para tomar control	Preguntas realizadas para dar una autorización en Bantotal o Autoriza7	Número de personas con acceso
Monitorear los valores dados por el CIS frente a los de Talento humano por medio de la fijación de fórmula que permita mantener un dato verídico	Fijación de fórmula en datos reportados por el CIS	Cantidad de reportes fijados en cada novedad en el indicador del CIS
Fijar un horario con el Gerente de riesgos no financieros que permita el cumplimiento de los E-mailings realizadas por mes.	Cumplimiento de E-mailings	Número de campañas realizadas por mes

Fuente: Elaboración propia

4.3 FASE III: EJECUCIÓN

4.3.1 Explicación y simulación del nuevo proceso que se pretende implantar.

Teniendo en cuenta las mejoras propuestas en la matriz de oportunidades y mejora se procede a ejecutarlas en el área de seguridad de la información, con el fin de buscar mejoras que son necesarias en la mayoría de los procesos. Con la disposición de mis compañeros y mostrándole a cada uno las mejoras que se pretenden realizar en sus procesos respectivamente, se inicia una simulación en la que evidencien la creación de procesos con mejores tiempos de ejecución y de

respuesta en ellos. Esta simulación sirve para retroalimentar las mejoras de alternativa ya creadas, pero en este caso los funcionarios se sintieron a gusto con lo propuesto y no se presentaron nuevos escenarios para ser añadidos a los ya existentes.

4.3.2 Creación de controles que permitan medir el desempeño y la transformación del proceso.

En la Tabla 3, Se puede evidenciar la actividad desarrollada

Tabla 3. Matriz de controles y evaluación de transformación

PROCESO	VARIABLE	SUPERVISIÓN	ALTERNATIVA DE MEJORA SIGUE		
			CAMBIOS +	CAMBIOS-	IGUAL
Solicitud de acceso a terceros	Accesos sin permiso	Disminuyó en un 60%, ya que al estar pendiente del Excel y las fechas de vencimiento se evitó el ingreso de varios funcionarios, pero también la actualización del formato de otros. Este cambio se vio muy reflejado sobre todo a finales de diciembre en donde un 25% de los usuarios perdían el 31/12/2019 el acceso a los sistemas de información.	X		
Solicitud de usuarios y autorizaciones entre ambientes		Disminuyó en un 40% ya que con algunos funcionarios se esperó unos días más, debido a que a diferencia de las otras solicitudes, aquí se tiene acceso a preproducción y producción que se encuentran datos sensibles pero necesarios para las actividades diarias de los funcionarios.			X
Solicitud de usuarios de sobres sensitivos: La solicitud es realizada por un funcionario	Respuesta a solicitud	Fue de gran ayuda que se implementara este cambio ya que en varias ocasiones mis compañeros le hacían acuerdo a la analista que tiene en custodia los usuarios sensitivos de verificar el correo.	X		

por medio del correo electrónico.					
Solicitud de creación, modificación y cambio de perfil. (FM-036)	Verificación de formatos	Haciendo un promedio de 10 pasos que necesitan el formato FM-036, tres de ellos fueron devueltos al verificar y no contar con dicho requerimiento. Disminuyendo el tiempo tanto para el solicitante como para el analista de verificar y dar respuesta al paso.	X		
Solicitud de control de requerimientos de pasos entre ambientes	Capacitación	Realicé una capacitación al funcionario encargado de llevar el control de requerimientos de pasos con el fin de focalizarse en las firmas que debe recolectar en cada ambiente y que con un check list pueda estar seguro que el paso debe ser llevado al área de Seguridad de la información.	X		
Controller	Accesos sin permiso	Se siguen realizando las restricciones correspondientes, se ha presentado acciones como las de un usuario que quería ejecutar una sentencia para consultar información sobre la base de datos. Lo cual representa un riesgo si dicho usuario no tiene el permiso de realizarlo			X
Directorio activo	Indicador de ingresos	Desde el mes de diciembre se creó el indicador que nos permite evaluar a talento humano en la novedad de Ingreso de personal, este indicador es dividido en dos partes una es los reportes oportunos es decir los menores a 1 y los reportes fuera de tiempo que son los mayores a 1.	X		

Inactividad de usuarios	Encuesta	Esta fue realizada para ver con qué frecuencia un usuario va a utilizar la plataforma evitando así activación en ellas sin que sea necesario. Es importante que por parte de los usuarios exista cierto compromiso para evitar que esto suceda.	X		
Pulse score	Usuarios informados	Dentro de mi pasantía he tenido que llamar por extensión a 20 personas para que lleven el formato pero 4 de ellas lo omitieron por lo cual tuve que recurrir a pedir que se deshabilitara el usuario por parte de Tecnología Informática	X		
Validación de novedades de nómina	Informe	Se realizó un informe basado en las novedades de nómina más importantes como lo son las vacaciones cambios de cargo y egresos. Con el fin de medir a talento humano en sus reportes para de este modo poder exigir agilidad en las acciones que debe realizar el CIS.	X		
Reporte de modificación de usuarios	Fijación de resultados	El funcionario encargado lo que hace después de descargar el reporte 4151A es entrar a cada novedad y fijar los valores que están en formulas sobre todo si son de cambios temporales con el fin de no alterar los indicadores que se fijaron.	X		
E-mailings	Cantidad de campañas	Desde enero se ha realizado oportunamente las campañas ya que al fijar este tiempo el gerente brinda el tiempo necesario para mostrarle lo que se realiza para que pueda ser aprobado y de tal modo publicado a nivel nacional.	X		

Fuente: Elaboración propia

4.4 FASE IV: OPERACIÓN

En esta fase es muy importante medir el rendimiento de lo que se implementó, analizar la operación de los funcionarios en sus nuevos procesos su coordinación y comunicación para definir un rendimiento óptimo.

4.4.1 Realización de prueba piloto.

En la ejecución de la prueba piloto participaron en total 4 funcionarios que son los que pertenecen al área de Seguridad de la información del Banco Mundo Mujer con cargo de analista de Seguridad de la información: Marcela Solano, Duvan Tombe y Andrés Pardo. Por otro lado, la Aprendiz Universitaria Vanessa Garcés quien se encargó de realizar el debido empalme con la nueva pasante, ya que es de vital importancia que en ciertas tareas se siga prestando atención para no caer en procesos antiguos que generan retrocesos.

El tiempo de implementación de BPM y sus respectivas mejoras se llevó a cabo durante dos meses y medio, ya que los 2 anteriores se utilizaron para todo lo relacionado con el diseño del mismo

4.4.2 Supervisión del rendimiento frente a lo que se busca.

Esta actividad fue fundamental realizarla en la prueba piloto ya que la supervisión permite evaluar la realidad de ejecutar un nuevo proceso, como el desempeño de cada funcionario con lleva a medir en cantidad y porcentaje los indicadores establecidos.

Tabla 4. Indicadores de rendimiento

INDICADOR	SUPERVISIÓN	
	ENERO	FEBRERO
Porcentaje de disminución de usuarios que acceden sin autorización.	55%	45%
Número de llamadas realizadas mensualmente para evitar accesos o autorizados	25	19
Cantidad de sobres pedidos en el mes	11	14
Porcentaje de solicitudes atendidas a tiempo	80%	98%
Número de errores e inconsistencias en los pasos	4	6
Cantidad de usuarios que ingresan sin autorización a los aplicativos	5	3
Reportes oportunos(%)	75%	87%
Reportes fuera de tiempo (%)	15%	13%
Número de personas con acceso	88	93
Cantidad de reportes fijados en novedad cambios de cargo y traslados en el indicador del CIS	48	56
Número de campañas realizadas por mes	2	2

Fuente: Elaboración propia

4.4.3 Análisis de la coordinación y comunicación en el nuevo proceso.

Se realizó un análisis dentro del área referente a la coordinación y la comunicación que son actividades que conllevan a satisfacer a los clientes en este caso los clientes internos con lo que se genera una relación en el área de Seguridad de la Información.

La coordinación en el área se lleva a cabo con la implementación del nuevo proceso de una buena forma ya que según la evaluación que se realizó en los procesos se están alcanzando las metas propuestas siendo este el principal objetivo.

Al tener una coordinación donde los funcionarios trabajan en equipo e individualmente facilitaron el buen funcionamiento y el éxito de lo propuesto. Aunque existen mejoras por realizar ya que esto permitió realizar ajustes en algunas de las alternativas de mejora que solo se pudo

analizar más a fondo gracias a la ejecución de los nuevos procesos que se muestran en la matriz de oportunidades de mejora.

La comunicación se emplea en esta actividad como un mecanismo de coordinación en el área de seguridad de la información para que en conjunto los funcionarios logren cumplir con los objetivos, como lo es informar acerca de una actividad a otro analista en caso de que no esté enterado de una labor pendiente enviada por correo o haga omisa por sus múltiples ocupaciones en referencia a los clientes internos. En el área existe una comunicación informal que Henry Mintzberg la denomina “adaptación mutua” la comunicación facilita la cooperación, la dirección de actividades, reduce la incertidumbre y permite en este análisis enfrentar las contingencias que se presentan.

4.5 Fase V: Mantenimiento

4.5.1 Análisis de la adaptación de los participantes frente a los cambios.

Teniendo en cuenta los valores de la tabla de indicadores de desempeño se procede a realizar un análisis de los participantes frente a los cambios y como implementan lo sugerido para mejorar los procesos.

Los indicadores representan una buena adaptación de las partes implicadas, pero esto también se ve relejado en el cumplimiento de las actividades por cada funcionario, la responsabilidad en la ejecución de sus funciones, eficiencia en el mismo y el servicio al cliente interno mejora gracias a las nuevas medidas que dan mayor agilidad a lo que se quiere lograr con la implementación del BPM.

Los ajustes realizados han sido acoplados de la mejor manera para los funcionarios que están dispuestos a mejorar en su área y salir de su zona de confort.

4.5.2 Detección de errores que siguen siendo consistentes.

En los formatos de solicitud de accesos a terceros y autorizaciones entre ambientes se siguen presentando fallas debido a que hay usuarios que hacen omisa la llamada que se les realiza para que traigan al área de Seguridad de la Información el formato actualizado.

Por otro lado, en Controller aunque son pocos los casos se se siguen conectando para realizar cambios en tablas que son importantes y sin una autorización pueden generarse eliminaciones las cuales no tendrán un responsable de ello.

Por ultimo en los sobres de usuarios sensitivos es necesario implementar también un rediseño ya que se da la comunicación entre los dos funcionarios, pero igual no se cumple en 100% la eficacia de resolver la petición de un cliente interno.

4.5.3 Realización de rediseños en los procesos requeridos

Solicitud De Accesos A Terceros

Se seguirá informando al usuario de su vigencia de acceso, pero ahora a su jefe también se le informará para que tome las medidas correctivas necesarias en caso de que no lleven el formato y necesiten el uso de los sistemas de información.

Controller

Es necesario crear campañas de sensibilización para los usuarios de estas aplicaciones en donde se evidencie la importancia de no realizar cambios en las talas y no ingresar sin pedir la debida autorización.

Sobres De Usuarios Sensitivos

Asignar en la jornada la labora 10 minutos para este tipo de solicitudes que son importantes realizarlas pronto para que los usuarios puedan realizar sus actividades.

4.5.4 Evaluación de manera global la efectividad del proceso

Se realizó un aporte al área de seguridad de la información en términos de mejoramiento en los procesos. Este puede ser comprobado en la Fase de ejecución y operación donde se encuentran las matrices con sus respectivos análisis que dan a conocer los diferentes cambios que se proporcionaron y en cuales no fue necesario implementar el modelo.

A continuación, en la Tabla 5, se mostrará una síntesis de la versión actual del proceso y su versión mejorada.

Tabla 5. Evaluación efectividad del proceso

INDICADOR	SUPERVISIÓN	
	MEJORA	META
Porcentaje de disminución de usuarios que acceden sin autorización.	45%	20%
Número de llamadas realizadas mensualmente para evitar accesos o autorizados	19	5
Porcentaje de solicitudes atendidas a tiempo	98%	100%
Número de errores e inconsistencias en los pasos	6	1
Cantidad de usuarios que ingresan sin autorización a los aplicativos	3	0
Reportes oportunos(%)	87%	97%
Reportes fuera de tiempo (%)	13%	2%
Cantidad de reportes fijados en novedad cambios de cargo y traslados en el indicador del CIS	56	15
Número de campañas realizadas por mes	2	2

Fuente: Elaboración propia

Estos datos son estimados en base a los análisis, observaciones y supervisiones realizadas en la caracterización del proceso y el debido levantamiento de la información.

Los mejores resultados se obtuvieron en la información dada a los usuarios en su vigencia de acceso, las solicitudes de sobres atendidas a tiempo que son de vital importancia para la satisfacción del cliente interno y las demás se encuentran en el proceso de ser lo suficientemente eficientes

porque si han representado grandes cambios, pero con el tiempo se logrará que sea totalmente pulcras en los procesos que se encuentran.

La implementación de BPM se vio reflejada en la ejecución de tareas adicionales que debían implementarse para mejorar en los diferentes procesos que presentaban repetitivamente inconsistencias por falta de atención en vigencias, en informes o correos electrónicos.

El tiempo de los procesos no fue un factor relevante porque los procesos deben realizarse diariamente y la jornada laboral se considera adecuada para cumplir con las tareas diarias a realizar.

Por ultimo en términos cualitativos, el principal aporte es la visibilidad de mejora en los procesos que quizás no se habían realizado por permanecer en una zona de confort, pero gracias al modelo BPM y su ejecución se mejora la comunicación en el área y los distintos procesos en donde el cliente interno se ve beneficiado.

5. Conclusiones

Dentro del desarrollo del trabajo fue de gran importancia el descubrir y entender cada uno de los procesos que conforma el área de seguridad de la información, esto permitió tener una visión más clara de lo que se realiza en el área y como por medio de cada uno de los procesos se pueden generar cambios.

El diseño de los procesos de negocio fue muy útil para que el desempeño en cada proceso pudiera ser medido y evaluado, de tal forma se pudo realizar la validación de los procesos por medio de factores relevantes que llevaron a la creación de indicadores.

Para la implementación del nuevo proceso en el área de seguridad de la información se contó con funcionarios dispuestos al cambio, lo que facilitó la explicación y simulación del mismo, que permitieron la creación de controles para medir el avance de la oportunidad de mejora.

En la realización de la prueba piloto de los procesos que se han definido y documentado, se evidenció una buena coordinación y comunicación entre las partes lo cual se evaluó como una transformación positiva en la operación del nuevo proceso.

La metodología BPM lleva a los procesos a la mejora continua, dentro de los procesos analizados se encontraron tres que fue necesario realizarles un rediseño teniendo en cuenta que los resultados obtenidos no fueron los esperados y con sus cambios se espera que tengan cambios significativos.

Referencias Bibliográficas

AEC. (2013). Gestión por procesos. Obtenido de https://www.aec.es/web/guest/centro-conocimiento/gestion-por-procesos

Anónimo. (2018). Gestión por procesos, ¿qué la hace tan importante? Obtenido de https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/gestion-por-procesos-que-la-hace-tan-importante

Anónimo (2010)Lineamientos metodológicos para la construcción de indicadores de desempeño, Obtenido de https://www.cepal.org/ilpes/noticias/paginas/5/39255/INDICADORES_METODOLOGIA_AECID_MARMIJO.pdf

Davenport; Zairi & SinclairBPM (1993): el nacimiento de SemanticWebBuilder Process http://www.semanticwebbuilder.org.mx/es_mx/swb/BPM_el_nacimiento_de_SemanticWebBuilder_Process

García(2009) Mecanismos de coordinación en empresas, Obtenido de https://www.researchgate.net/publication/38290539_Mecanismos_de_coordinacion_en_empresas

Hitpass (2014) Bernhard Hitpass, Jakob Freund, Bernd Rucke. " BPMN 2.0 Manual de referencia y Guía Práctica ". 4ta edición, 2011.

Hitpass (2017) “BPM Business Process Management Fundamentos y Conceptos de Implementación” 3ra Edición Actualizada y Ampliada.p17

Kerlinger, F. (2002) Enfoque conceptual de la Investigación del comportamiento, p.83.

Santesmases (2009:75) Fuentes de información Fuentes de información. Obtenido de http://www.eumed.net/tesis-doctorales/2012/mirm/fuentes_informacion.html

Underdhal, (2013), Gestión de procesos de negocio para Dummies, New Jersey , 2da edición limitada de IBM

ANEXOS

Anexo 1. Capacitación a funcionaria del área de T.I

PARTICIPANTE: Fernanda García Pajoy

PARTICIPANTE	
NOMBRE	**FIRMA**
Fernanda García Pajoy	Fernanda García

Cuestionario

Evalué de 1 a 5 los siguientes aspectos, teniendo en cuenta que:

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

ASPECTOS A EVALUAR	1	2	3	4	5
1.Eficacia de la metodología				X	
2.Dominio del tema por parte del capacitador					X
3.Pertenencia del horario					X
4.Pertenencia del lugar					X

1.Antes de recibir esta capacitación, mi nivel de conocimientos o habilidades para el objetivo de este curso eran:

EXCELENTE	BUENO	REGULAR	MALO
		X	

2. Después de recibir esa capacitación, mi nivel de conocimientos o habilidades para el objetivo de este curso fue:

EXCELENTE	BUENO	REGULAR	MALO
	X		

3.Teniendo en cuenta la capacitación recibida de lo aprendido, que porcentaje podrá aplicar en su trabajo.

☐ **25%** ☐ **50%** ☐ **75** ☐ **100%** X

4.Para mejorar futuras capacitaciones le pedimos deja su recomendación en que se puede adicionar, suprimir o dar menos énfasis.

Me parece que es importante adicionar en una futura capacitación, un material mas amplio que permita evidenciar los diferentes casos que se pueden presentar. Para que de esta manera no se deje por fuera ningun contenido del formato control de requerimiental y pasos entre ambientes.

Anexo 2. Indicador novedad de nómina ingresos

Este indicador se obtuvo en base a la medición del tiempo de notificación por parte de talento humano en enviar ingresos de funcionarios. Para poder ser medido hace una comparación entre a fecha de ingreso y la fecha que reporta talento humano sacando de este modo el indicador que mide los reportes oportunos y reportes fuera de tiempo. Un ejemplo de lo que se le añadió al Excel que por confidencialidad no podré mostrar dentro de mis evidencias es el siguiente:

NOMBRE DE USUARIO	FECHA DE INGRESOS	FECHA DE REPORTE DE TH
Usuario A	02/01/2020	05/01/2020

Esto se realiza con cada usuario y como lo es en este caso son 3 días de reporte fuera de tiempo de talento humano o puede darse el caso de un reporto oportuno si notificado el mismo día que ingresa el funcionario. Este indicador, fue enviado en el mes de diciembre y enero a talento humano para mejorar en ello y ha funcionado al no presentarse mucho tiempo de notificación en esta novedad de ingresos que genera demoras en la activación de usuarios por parte del CIS

DICIEMBRE

NOVEDAD	**REPORTES OPORTUNOS**	**REPORTES FUERA DE TIEMPO**	**REPORTES OPORTUNOS (%)**	**REPORTES FUERA DE TIEMPO(%)**
INGRESOS	108	78	58,06%	41,93%
TOTAL DE INGRESOS	186			

ENERO

NOVEDAD	**REPORTE OPORTUNO**	**REPORTE FUERA DE TIEMPO**	**% REPORTE OPORTUNO**	**% REPORTE FUERA DE TIEMPO**
INGRESOS	182	34	84.25%	15.74%
TOTAL DE INGRESOS	216			

Se presentó un cambio positivo ya que disminuyeron los reportes fuera de tiempo en un 26% aproximadamente. Con este indicador se pretende realizar un cuadro comparativo trimestral para ver cómo se va transformando y anualmente ver sus mejoras, teniendo en cuenta que solo en estos dos meses hubo un cambio significativo.

Anexo 3. Formato para evaluar inactividad de usuarios

1.Con qué frecuencia va a utilizar su usuario en el mes

_____

2. Qué importancia tiene la inactividad de su usuario

Es indiferente	Irrelevante	Relevando

3.Si deja de utilizar su usuario, ¿nos podríamos como con usted después de los 90 días de inactividad?

SI__ NO__

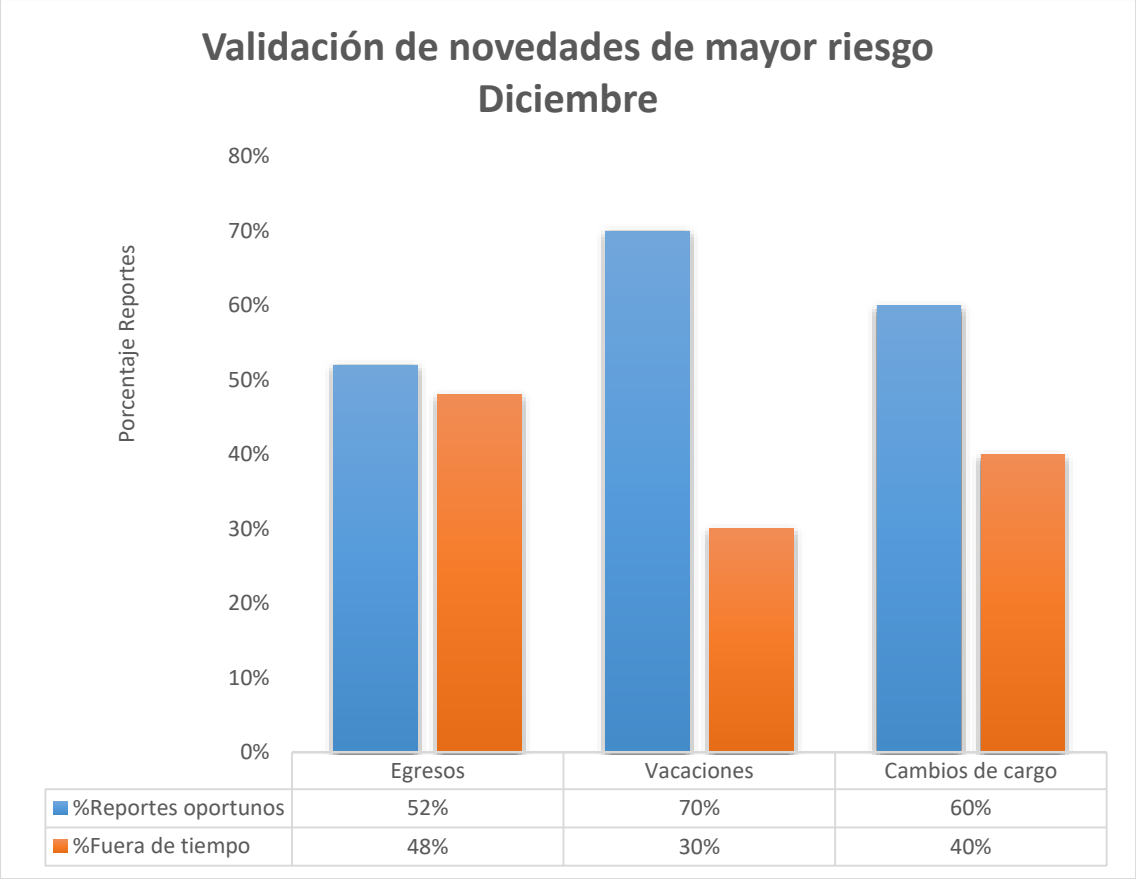
Anexo 4. Informe de validación de novedades de nómina

Indicador: reporte y ejecución oportuna de las novedades de nómina de mayor riesgo

Para esta validación se tienen en cuenta las novedades que generan mayor riesgo al no ser reportadas a tiempo por el área de Talento Humano, los datos se obtienen del perfil actual de cada usuario, y se valida si el cambio ha sido realizado o si existen cambios pendientes o cambios no realizados. A continuación, se muestra la tabla que contiene esta información, seguida de una gráfica y por último el análisis correspondiente a cada novedad.

VALIDACIÓN DE NOVEDADES DE MAYOR RIESGO DICIEMBRE

NOVEDADES	Reportes Oportunos	Reportes fuera de tiempo	Total	%Reportes oportunos	%Fuera de tiempo
Egresos	69	64	133	52%	48%
Vacaciones	327	139	466	70%	30%
Cambios de cargo	127	83	210	60%	40%
Total de novedades	523	286	809	65%	35%

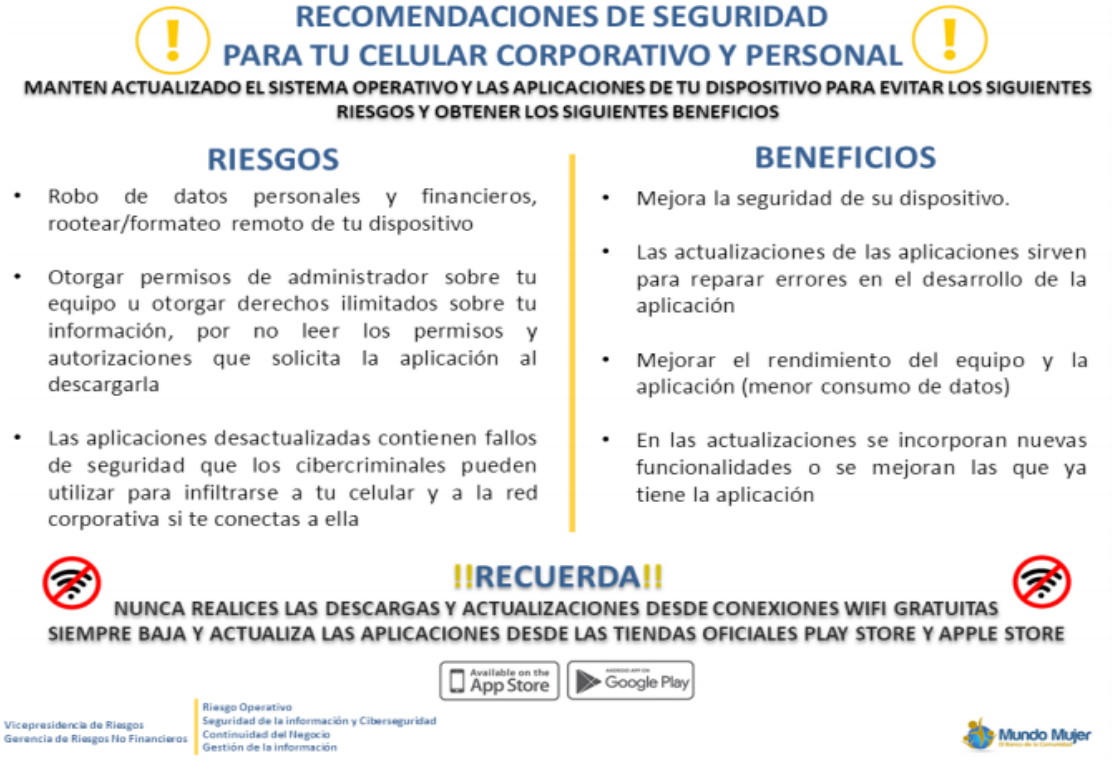


Como se puede visualizar en la gráfica el reporte oportuno de novedades de nómina por parte de Talento humano tiene un mayor porcentaje que demuestra eficiencia frente a los de fuera de tiempo. Para el área de Seguridad de la información es de suma importancia que los reportes fuera de tiempo disminuyan su porcentaje, con el fin de no retrasar al área del CIS en los reportes que deben proporcionar al área.

Anexo 5. Campañas mensuales

Publicación mes de Noviembre

Publicación mes de Diciembre



Publicaciones mes de enero

¡¡¡ATENCIÓN!!!

TENGA CUIDADO, están llegando a los correos del Banco, mensajes maliciosos suplantando empleados o directivos del Banco con el fin de robar información, tomar control de las cuentas de correo y cometer otros tipos de fraude

Para que el banco no sea víctima de este tipo de ataques y/o robo
TENGA SIEMPRE PRESENTE Y SIGA LAS SIGUIENTES RECOMENDACIONES

1. Evite abrir los adjuntos o dar click en los links de correos desconocidos o que no ha solicitado

2. Evite descargar adjuntos de tipo ejecutable como .EXE, .BAT, .COM, .BIN, .RAR, de ser necesario solicite apoyo del área de soporte

3. No inscriba el correo corporativo a redes sociales, blogs, tiendas en línea y/o supermercados en línea

4. Informe inmediatamente al área de seguridad de la información o al área de soporte si sospecha de un correo, ***en especial si provienen de correos externos o directivos del banco y manifiestan que quieren hablar temas confidenciales o delicados. Confirme en persona la instrucción del correo antes de ejecutarla***

5. Nunca reenvíe los correos SPAM/PROMOCIONES desde y hacia los correos del banco

Vicepresidencia de Riesgos
Gerencia de Riesgos No Financieros

Riesgo Operativo
Seguridad de la información y Ciberseguridad
Continuidad del Negocio
Gestión de la información

Mundo Mujer

ENCRIPTACIÓN DE DE DATOS

Es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamete ilegibles gracias a un algoritmo que desordena sus componentes.

BENEFICIOS

- Si encriptas un dispositivo nadie podrá ver lo que contiene.
- Incluso si te roban el terminal, no podrán acceder a su contenido sin la contraseña. Yen caso de lograr extraerlo, lo que podrá ver será un montón de caracteres que no podrá entender.
- Tus datos personales van a estar a salvo de caso cualquier ataque malintencionado. Puedes tener la tranquilidad de que tu información la verás sólo tú y además decidirás quién los verá y quién no.

RIESGOS

- Nuevos tipos de ataque::

Cuando las empresas comienzan a utilizar la encriptacion de forma masiva, los hackers se adaptan al nuevo escenario.

- Dificultades para compartir información:

Dentro del entorno corporativo, si la encriptacion de datos alcanza determinados limites, podría suceder que se viese perjudicado el rendimiento de los procesos que se encontrarían con los limites del cifrado de la información y la dificultad para compartir datos críticos del negocio.

Vicepresidencia de Riesgos
Gerencia de Riesgos No Financieros

Riesgo Operativo
Seguridad de la información y Ciberseguridad
Continuidad del Negocio
Gestión de la información

Mundo Mujer

Publicaciones mes de febrero

¡ALERTA! SIMJACKER

La nueva falla de la tarjeta SIM permite a los hackers secuestrar cualquier teléfono con solo enviar SMS.

PERMITE...

Recopilar información de la tarjeta SIM como **nuestra ubicación o el número IMEI** para posteriormente, mandarlo como SMS al atacante	Reproducir sonido, apagar la tarjeta, lanzar el navegador, enviar datos, enviar mensajes multimedia o SMS	Realizar diferentes fraudes y suplantación de identidad hasta espionaje, por medio de las vulnerabilidades que se presentan

Vicepresidencia de Riesgos
Gerencia de Riesgos No Financieros

Riesgo operativo
Seguridad de la información y Ciberseguridad
Continuidad del negocio
Gestión de la información

Mundo Mujer

USO ADECUADO DEL ESCANER E IMPRESORAS

Protege la información del cliente y del Banco

DOCUMENTOS IMPRESOS

- Una vez imprima sus documentos retírelos de la impresora, ¡no los descuide! esto puede generar fuga de información.
- Recuerde que el uso de impresoras es exclusivo para los documentos laborales.
- Imprima estrictamente lo necesario, en lo posible use el servidor de archivos para transferir información. Si debe imprimir, utilice las dos caras del papel, con esto contribuira a la proteccion del medio ambiente.

ESCANER

A diario se evidencia que no se está cumpliendo la oplitica establecida para el buen uso de escaneos, dejando información confidencial a disposición de todos los funcionarios.

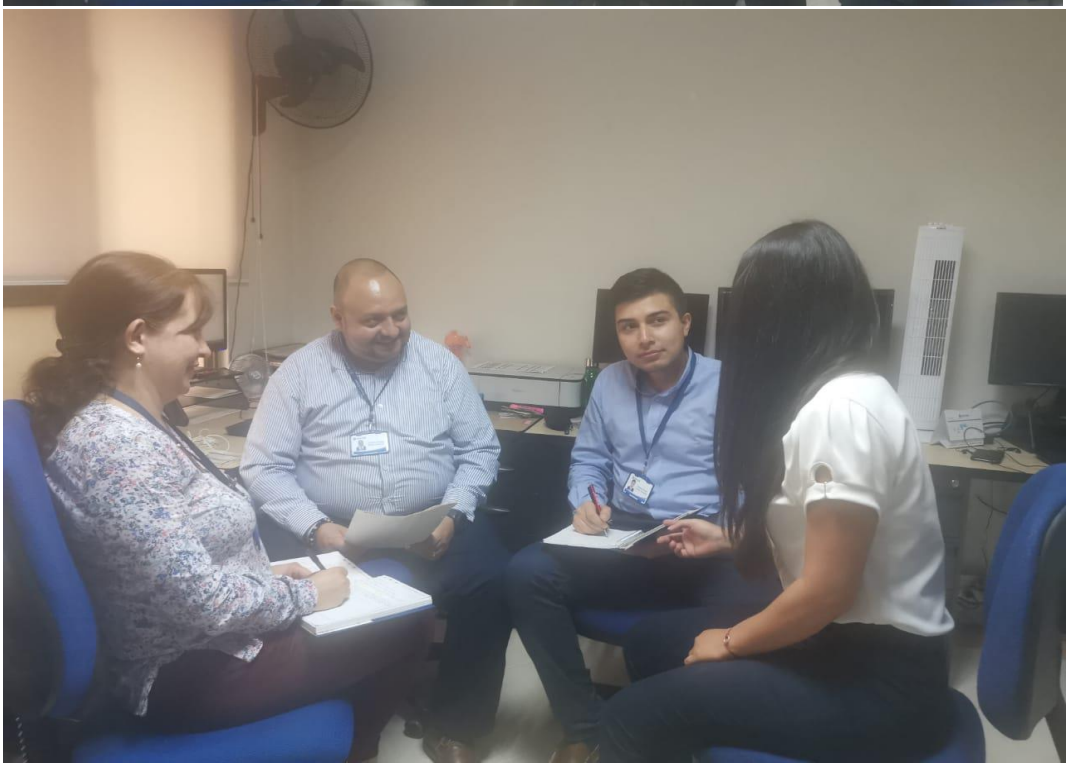
- Una vez haya sido escaneado un documento se deberá copiar el archivo en su equipo y eliminar inmediatamente el archivo de la carpeta públicada.
- Proteja con contraseña toda información que sea transeferida a través de la carpeta publica.
- Recuerde.! El mal uso del escáner conlleva a incumplir sus deberes como funcionario al no proteger los datos de sus clientes.

Vicepresidencia de Riesgos
Gerencia de Riesgos No Financieros

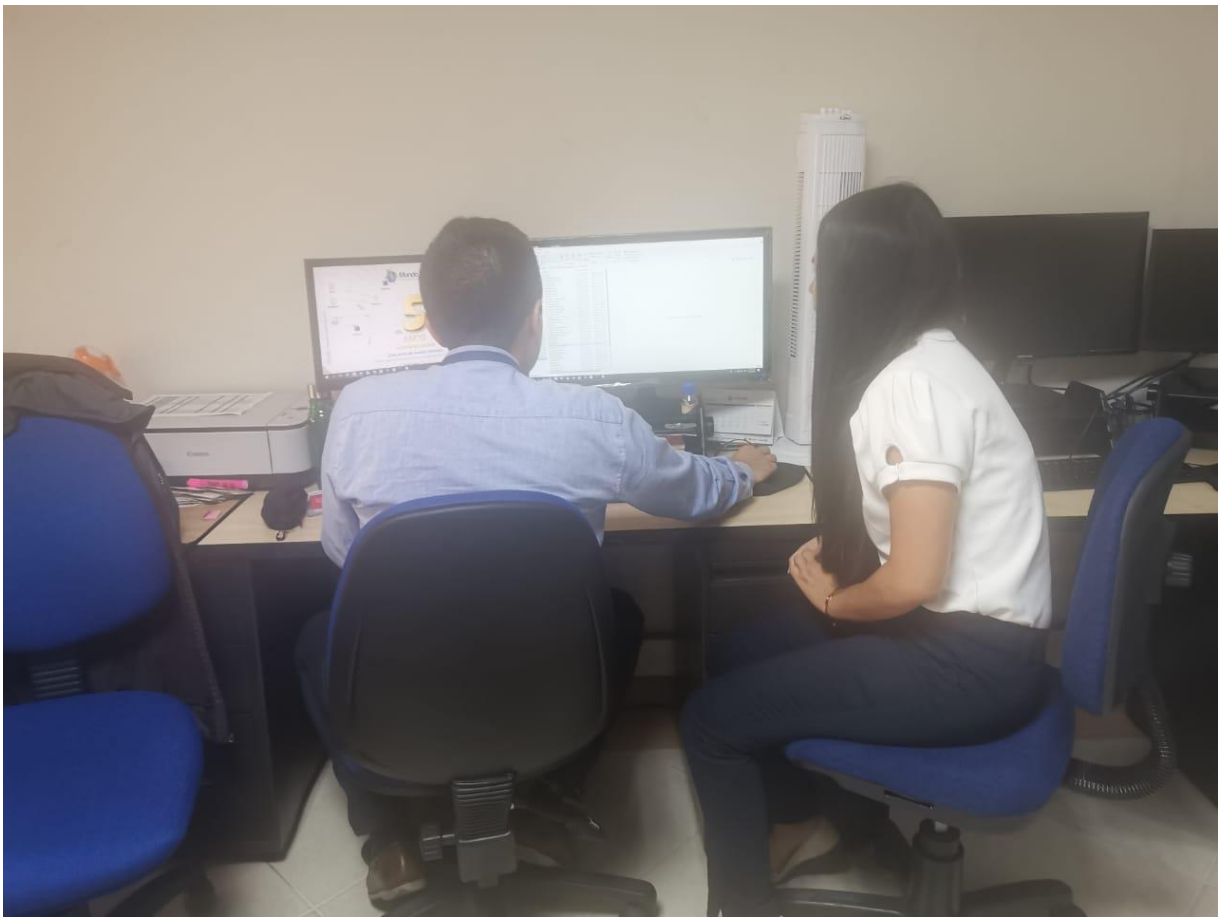
Riesgo Operativo
Seguridad de la información y Ciberseguridad
Continuidad del Negocio
Gestión de la información

Mundo Mujer

Anexo 6. Conocimiento de los procesos llevados a cabo en el área de Seguridad de la Información



Anexo 7. Evidencia reunión de verificación de novedades de nómina



Anexo 8. Acta reunión: Conocimiento de los procesos llevados a cabo en el área de Seguridad de la Información

BANCO MUNDO MUJER

ACTA DE REUNIÓN DE TRABAJO

ACTA No. 001

Fecha: 11 de noviembre del 2019 **Hora:** 08:00am

Tema: Conocimiento de los procesos llevados a cabo en el área de Seguridad de la Información

Responsable de la reunión	
Nombre	**Cargo**
Claudia Vanessa Garcés Mazabuel	Aprendiz universitaria
Participantes	
Nombre	**Firma**
Marcela Patricia Solano	
Norbey Duvan Tombe	
Andrés Pardo	
Objetivos de la reunión	
- Conocer los procesos realizados por los analistas del área de Seguridad de la información - Mencionar inconsistencias en los procesos que realizan - Aclarar dudas sobre los procesos que tienen actividades minuciosas	
Agenda de trabajo	
- Explicación de lo que se pretende con la reunión - Preguntar por cada proceso que se ha identificado	
Desarrollo de la reunión	
En esta reunión se dió a conocer cada uno de los procesos realizados por los participantes, con el paso a paso, así mismo se mencionan las incidencias que se presentan en algunos de ellos con el fin de buscar mejoras por medio de la herramienta BPM(Business Process Management). Se menciona la importancia del área de Seguridad de la información para el Banco Mundo Mujer, ya que el debido cumplimiento de las actividades permite que la entidad pueda sentirse segura en términos de las principales características que representa al área como lo son la integridad, disponibilidad y confidencialidad. Por último según los procesos mencionados por los funcionarios se hacen preguntas que aclaren mejor el desarrollo de ciertos procesos que se han respondido a grandes rasgos con el fin de poder hacer un mejor análisis de cada de uno e identificar las falencias que se puedan presentar.	

Anexo 9. Acta reunión: Evidencia reunión de verificación de novedades de nómina

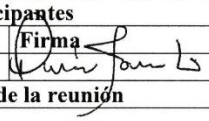
BANCO MUNDO MUJER

ACTA DE REUNIÓN DE TRABAJO

ACTA No. 002

Fecha:8 de enero del 2020 **Hora:** 09:00am

Tema: Verificación de informe de novedades de nómina

Responsable de la reunión	
Nombre	**Cargo**
Claudia Vanessa Garcés Mazabuel	Aprendiz universitaria
Participantes	
Nombre	**Firma**
Norbey Duvan Tombe	
Objetivos de la reunión	
- Comparar la información de las novedades dado por talento humano y el CIS frente a las dadas por el documento Excel de datos estadísticos - Verificar la veracidad de los valores que asigna el reporte 4151ª en el indicador del CIS - Mejorar el informe	
Agenda de trabajo	
- Verificación de cada uno de los valores que se colocan en el informe - Leer y modificar los datos que sean necesarios para dar una mejor redacción al informe	
Desarrollo de la reunión	
Esta reunión se dio con el fin de mejorar las inconsistencias que se estaban presentando en el indicador del CIS (Centro integral de servicios) en el que habían valores que no concordaban con lo que esta área afirmaba de su realización a tiempo. En el informe se eliminó una parte en donde la información era repetitiva y poco entendible en su interpretación. La verificación y modificación de las novedades de nómina es importante para que en próximos informes se tenga la certeza en la medición que se le hace al área de talento humano y al CIS por medio de los indicadores, para que coincida y cada una busque mejoras frente a los reportes que generan.	