DOCUMENTACIÓN DEL MANUAL DE PROCESOS PARA LA VALIDACIÓN DE USUARIOS Y PERFILES DEL ÁREA DE SEGURIDAD DE LA INFORMACION EN EL BANCO MUNDO MUJER

Universidad del Cauca

ASHLEY STEPHANY CUBIDES VALDERRAMA

INFORME FINAL PRÁCTICA PROFESIONAL

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS YADMINISTRATIVAS

PROGRAMA DE ADMINISTRACIÓN DE EMPRESAS

POPAYÁN

2019

DOCUMENTACIÓN DEL MANUAL DE PROCESOS PARA LA VALIDACIÓN DE USUARIOS Y PERFILES DEL ÁREA DE SEGURIDAD DE LA INFORMACION EN EL BANCO MUNDO MUJER

Universidad del Cauca

ASHLEY STEPHANY CUBIDES VALDERRAMA

INFORME FINAL PRÁCTICA PROFESIONAL

Asesor Académico

JORGE ENRIQUE BARRERA MORENO

Administrador de Empresas

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS CONTABLES ECONÓMICAS YADMINISTRATIVAS

ADMINISTRACIÓN DE EMPRESAS

POPAYÁN

2019

AGRADECIMIENTOS

Gracias a Dios y a la vida por todo lo aprendido,
Por las oportunidades y las bendiciones recibidas.
A mis padres y a mi hermana por su apoyo incondicional y por cada palabra de aliento.
A la Universidad del Cauca por convertirse en mi segundo hogar.
A mis profesores por el tiempo y los conocimientos compartidos.
A mis compañeros por todos los buenos momentos.
Al Banco Mundo Mujer por darme la oportunidad de hacer parte de su familia
Y poner en práctica todo lo aprendido.
Al profesor Jorge Enrique Barrera, mi asesor académico,
Por su acompañamiento durante mi práctica profesional.
Gracias a cada uno de ustedes, por hacer parte de este importante logro para mi vida,
Tanto en lo personal como en lo profesional.

CONTENIDO

Pág.

ÌNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La digitalización de la Banca y la incorporación de los sistemas informáticos en el mundo organizacional, hoy marcan la pauta de la competitividad y sostenibilidad de las organizaciones en el mercado. El Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia, destaca claramente la importancia de la información en las organizaciones, señalándola como uno de los recursos con mayor valor para cualquier organización. (MinTic, 2016:6)

Por lo anterior es fundamental velar por su protección y correcta administración. Para dichos efectos, el Banco Mundo Mujer, a través del área de Seguridad de la Información, ha implementado de manera transversal el Sistema de Gestión de Seguridad de la Información, dentro del cual se encuentra el proceso de Validación de usuarios y perfiles.

Para garantizar la eficiencia y efectividad del SGSI, la ley exige la documentación oficial de todas las políticas y procesos que lo conforman, por tal razón, se vuelve fundamental el documentar y estructurar formalmente el proceso a través de un manual en el cual se describa detalladamente el qué, cómo, cuándo y dónde se deben ejecutar las actividades que conforman el proceso y cada uno de los responsables.

El siguiente documento se encuentra dividido en cinco capítulos: El Capítulo I, hace referencia a la contextualización del trabajo: problematización, justificación y objetivos; el Capítulo II presenta la contextualización teórica: el marco teórico, los conceptos y la normatividad bajo las cuales se desarrolló el trabajo; en el Capítulo III se describe la metodología que se implementó; el Capítulo IV contiene la descripción del desarrollo de la práctica profesional y finalmente, el Capítulo V que contiene las conclusiones obtenidas de la realización del trabajo.

CAPÍTULO I.

1. CONTEXTUALIZACIÓN DEL TRABAJO

1.1. PROBLEMATIZACIÓN

1.1.1. Descripción del problema.

En búsqueda del logro de una correcta gestión de los activos informáticos, el Banco Mundo Mujer ha incorporado a sus operaciones: tecnologías, políticas y procesos, con el fin de fortalecer y promover tanto la protección, como el buen uso y la disponibilidad de la información, para el cumplimiento de los objetivos, la misión y la visión de la organización.

Desde el área de Seguridad de la Información, bajo el marco de la norma ISO 27001, se implementó el Sistema de Gestión de la Seguridad de la información (SGSI), que establece una guía sobre las políticas, procesos y procedimientos de seguridad, para la preservación de la confidencialidad, integridad y disponibilidad de los activos informáticos de la organización.

Así mismo, en contribución con la detección, prevención y reducción de los riesgos asociados a la seguridad de la información y la ciberseguridad, relacionados con el componente humano de la organización, el área de seguridad se encarga de ejercer el control sobre el acceso de los colaboradores a la información, según las funciones y necesidades de cada cargo. Para el seguimiento de la efectividad de este control se lleva a cabo el proceso de "Validación de usuarios y perfiles".

Este proceso es fundamental para corroborar que se esté dando un manejo eficiente y oportuno del acceso a los activos informáticos, ya que estos deben ser otorgados a los funcionarios conforme unas políticas y directrices establecidas en la organización y que están ligadas directamente con el flujo del personal del Banco.

Pese a la importancia de este proceso para la correcta implementación y mejora en el SGSI, aún no ha sido documentado formalmente, por lo que no se cuenta con una guía estándar para su operación eficiente y uniforme.

1.1.2. Definición del problema

El área de Seguridad de la información del Banco Mundo Mujer, actualmente no cuenta con un manual formalmente estructurado para el proceso de Validación de Usuarios y perfiles en el aplicativo Bantotal, a través del cual se establezca la guía para una correcta ejecución del proceso.

Por tal razón, se hace evidente la necesidad de elaborar la *Documentación del Manual de Procesos para la Validación de Usuarios y perfiles del área de Seguridad de la Información en el Banco Mundo Mujer*.

1.2. JUSTIFICACIÓN

Para una organización en etapa de crecimiento, como lo es el Banco Mundo Mujer, el documentar sus procesos es fundamental, ya que permite tener una mayor claridad sobre las actividades que se llevan a cabo al interior de la empresa, realizar la evaluación y mejora de los procesos, reducir el tiempo y los costos, incrementar la productividad y convertirse finalmente en un factor determinante de calidad tanto en el servicio como en la operación.

El proceso de Validación de usuarios y perfiles, hace parte del Sistema de Gestión de Seguridad de la Información implementado en el Banco, a través del cual, la organización busca propender por la confidencialidad, integridad, disponibilidad y confiabilidad de la información que dispone para el ejercicio de su actividad. El correcto desempeño de este proceso permite identificar incoherencias en la información confrontada, determinar puntos críticos en el proceso, emprender acciones correctivas y la mejora continua del mismo.

Por consiguiente, documentar este proceso es fundamental para que se realice de forma adecuada y que los resultados que se obtengan sean confiables. Al ser desarrollado correctamente, contribuye con el buen desempeño en la operatividad de las oficinas y facilita la toma de decisiones por parte de los directivos, promoviendo el mejoramiento del proceso y el logro de los objetivos organizacionales.

1.3. OBJETIVOS

1.3.1. Objetivo General

Realizar la documentación del Manual de Procesos para la Validación de usuarios y perfiles, en el área de Seguridad de la información del Banco Mundo Mujer.

1.3.2. Objetivos específicos

- Describir los elementos que conforman el proceso (objetivo, alcance y directrices)
- Identificar las actividades y los responsables implicados en el proceso de Validación de Usuarios y Perfiles.
- Realizar una descripción detallada del proceso.
- Elaborar el diagrama de flujo del proceso.
- Socializar el Manual del proceso de Validación de Usuarios y perfiles.

CAPÍTULO II.

2. CONTEXTUALIZACIÓN TEÓRICA

El siguiente capítulo comprende la dimensión teórica, conceptual, contextual y legal que enmarcaron el desarrollo de este trabajo práctico.

2.1. MARCO TEÓRICO

En la era de la información, las organizaciones modernas deben adaptarse rápidamente a los cambios y exigencias del mercado. Adoptar una cultura organizacional basada en el buen uso de la información, es indispensable para el incremento en la productividad y la calidad de los productos y servicios de una organización.

De tal manera, los desarrollos tecnológicos se convierten en herramientas poderosas para potenciar las operaciones y procesos corporativos, facilitando el flujo y tratamiento de los sistemas y activos informáticos en las organizaciones. Sin embargo, estas condiciones traen consigo nuevas amenazas para el mundo organizacional que están asociadas con la seguridad de la información, y por consiguiente demandan la implementación de medidas de control y protección de la misma.

Para Cruz; Fernández y Toval (2015:161) “La seguridad de la información es una condición que resulta de la creación y el mantenimiento de las medidas de protección que permiten a una empresa llevar a cabo sus funciones a pesar de los riesgos planteados por las amenazas a la disponibilidad de la información.”

“La seguridad de la información (S.I.) significa proteger la información y los sistemas de información del acceso no autorizado, el uso, la divulgación, la interrupción, la modificación o la destrucción. Se refiere a la confidencialidad, integridad y disponibilidad de datos, independientemente de la forma que tomen: electrónicos, impresos u otros formularios” (Newman, 2009: 317).

Los tres factores mencionados por Newman (2009:317), comprenden los principales objetivos de la seguridad de la información, que con los años se han convertido en los pilares fundamentales sobre los cuales las organizaciones han venido implementando estas medidas de seguridad. La Academia Nacional de Ciencia de los Estados Unidos (1991:49) los define de la siguiente manera:

- Confidencialidad: Garantizar que sólo quien esté autorizado tenga acceso a la información y a los sistemas informáticos.
- Integridad: Asegurar que no se realicen cambios o modificaciones sin autorización previa en la información y los sistemas informáticos.
- Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información en el momento en que lo requieran.

A medida que las organizaciones se han vuelto más dependientes de los sistemas de información, han tenido que mejorar muchos aspectos en la administración de la seguridad de su activos informáticos (Baskerville, Straub & Goodman, 2008:15). Así mismo, la S.I. ha pasado de orientarse simplemente en la protección física de los activos informáticos, a enfocarse en una gestión de alto nivel a través de políticas, procesos y procedimientos para una protección integral de la información (Nnolim, 2007) citado por (Universidad Industrial de Santander, 2016).

De esta manera, se reconoce la necesidad de contar con un marco orientador para la gestión eficiente de la seguridad de los activos informáticos en las organizaciones, el cual se concibe como una serie de estándares, políticas, controles y procesos documentados que a menudo se personalizan para resolver problemas específicos de seguridad de la información de cada organización (Granneman, 2013).

Actualmente, el enfoque que caracteriza la gestión de la información en las organizaciones está centrado en la detección, evaluación, prevención y control sobre los riesgos asociados a la S.I. (Syalim, Hori, & Sakurai, 2009). A su vez, implica aspectos tales como: el rol del personal y los altos directivos en el logro y mantenimiento de la S.I., la importancia de la alineación entre la cultura organizacional y la cultura de seguridad, el costo de la inversión

en la S.I., políticas de seguridad y los procesos asociados. (Universidad Industrial de Santander, 2016)

Todos los aspectos mencionados anteriormente constituyen lo que se conoce hoy como Sistema de Seguridad de la Información (SGSI). Este consiste en un agregado de políticas de administración de la información basadas en el diseño, implantación y mantenimiento de procesos para gestionar eficientemente los activos de información minimizando a la vez los riesgos de seguridad de la información asociados con las necesidades del negocio. (Pacheco, 2010)

Ahora bien, como uno de los principales componentes de un SGSI, la política de seguridad según Höne y Eloff se define de la siguiente manera:

"Consiste en un documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar en la consecución de la misión y visión de la organización. En esencia se documenta para explicar la necesidad de seguridad de la información (y sus principios) a todos los usuarios de los recursos de información." (Höne & Eloff, 2002)

Por otro lado, los procesos se caracterizan por implicar acciones repetitivas, que se realizan siempre de la misma manera. Según Zaratiegui (1999):

"Son secuencias ordenadas y lógicas de actividades de transformación, que parten de unas entradas (información e un sentido amplio – pedidos, materias primas, consumibles, etcétera). Para alcanzar unos resultados programados, que se entregan a quienes los han solicitado, los clientes de cada proceso" (Zaratiegui, 1999:82).

Para garantizar una correcta implementación, mantenimiento, control y mejora del SGSI, es imprescindible tener la documentación oficial de los procesos, como soporte en detalle de cada uno de los componentes del SGSI. En el caso de los procesos, debe contarse con los manuales respectivos de cada uno. Según Franklin (2009):

"Estos constituyen un documento técnico que incluye información sobre la sucesión cronológica y secuencial de operaciones concatenadas entre sí, que se constituye en una unidad para la realización de una función, actividad o tarea específica en una organización" (Franklin, 2009:245).

Es importante considerar los beneficios que representa la documentación de los procesos, dado que como herramienta en la administración de las organizaciones, facilita la comprensión del funcionamiento y orden en las actividades del proceso, además describe al detalle los elementos que lo componen: Etapas, actividades, responsables, estradas, salidas, clientes y usuarios, lo cual favorece la disminución de deficiencias o inconsistencias y el incremento de la productividad. (Franklin, 2009)

Así mismo, Gómez Cardona (2012:40) resalta también la importancia de contar con procesos ágiles, simples y eficientes en cualquier organización en proceso de crecimiento y desarrollo. Para lo cual destaca claramente la pertinencia de un manual como guía en la ejecución, seguimiento, control y mejora de los procesos para el cumplimiento de los objetivos corporativos.

2.2. MARCO LEGAL

La normatividad que enmarca la actividad del Banco Mundo Mujer, en relación con el tratamiento y la protección de los datos y la gestión de riesgos asociados a la seguridad de la información es la siguiente:

- Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia.
- Circular Externa 029 de 2014 de la Superintendencia Financiera de Colombia.
- ISO 27001 de 2013– Norma técnica sobre los requisitos estándares relacionados a tecnología de la información, técnicas de seguridad y sistemas de gestión de la seguridad de la Información (SGSI).
- Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia
- Ley Estatutaria 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1273 del 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- Ley 663 de 1993 - Estatuto Orgánico del Sistema Financiero

2.3. MARCO CONTEXTUAL

La práctica profesional fue desarrollada en el área de Seguridad de la Información del Banco Mundo Mujer en la ciudad de Popayán.[1]

- *Descripción de la organización.*

El Banco Mundo Mujer es una organización Caucana, que nace el año 1985 en la capital del departamento. En sus inicios, operaba como Fundación Mundo Mujer, una compañía dedicada al fomento y desarrollo de las comunidades de estratos 1,2 y 3 de la ciudad de Popayán, que otorgaba productos de crédito de fácil acceso para estas comunidades.

Posteriormente, con su fortalecimiento en el sector y su desarrollo y crecimiento organizacional, se consolidó como Banco e inició oficialmente a operar como tal en el año 2015 con el aval de la Superintendencia Financiera de Colombia.

Actualmente, es una de las organizaciones más reconocidas a nivel nacional, manteniendo desde sus raíces una filosofía empresarial centrada en promover el empoderamiento de la mujer y el desarrollo integral de la comunidad. Con sus 30 años de experiencia en el sector, hoy cuenta con 106 Agencias y 63 Puntos de Atención (PDA´s) en todo el país, promoviendo el crecimiento y desarrollo en aproximadamente 22 departamentos de Colombia.

- *Direccionamiento Estratégico.*

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

[1] La información general de la organización, su direccionamiento estratégico y su portafolio de productos, fueron extraídos del sitio web del Banco Mundo Mujer. (https://www.bmm.com.co)

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: Para aceptarnos como somos y reconocer nuestras debilidades para mejorar.
- Integridad: Actuar con honestidad para generar confianza.
- Liderazgo: Responsabilidad que entraña conducir personas y cumplir objetivos.
- Excelencia: Constancia, efectividad y responsabilidad.
- Respeto: para influir, generar afiliación y ser admirado.

Productos

- Crédito para negocio
- Crédito agropecuario
- Crédito para pequeña empresa
- Crédito de libre inversión
- Cuenta de Ahorro gratis
- Cuenta tu meta
- Cuenta de ahorro con tarjeta débito
- Cuenta de ahorro Chikiteens
- CDT progrese
- Seguro de deuda
- Seguro familia protegida

- *Descripción del área de desarrollo de la práctica profesional.*

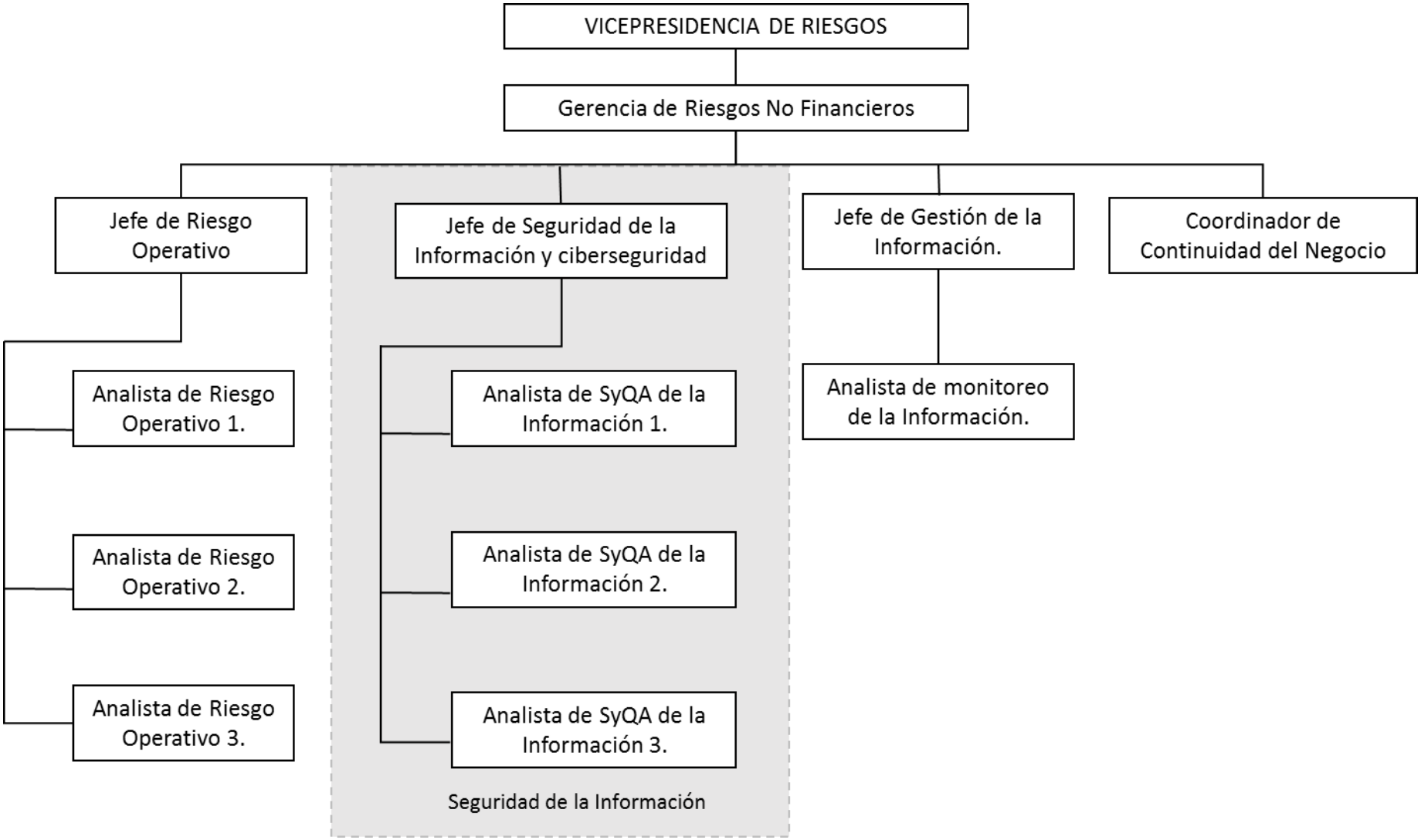
El área de Seguridad de la Información del Banco Mundo Mujer es la encargada de promover y velar por la protección y el buen uso de los activos y sistemas informáticos de la organización, propendiendo por el logro y mantenimiento de la confidencialidad, integridad y disponibilidad de los activos informáticos, además de trabajar constantemente por la mejora de los aspectos relacionados con la S.I. sin afectar la productividad y operatividad de la compañía. Las principales funciones de esta área son las siguientes[2]:

- Elaborar difundir las políticas de seguridad de la información para fomentar la protección y buen uso de los activos informáticos en toda la organización.
- Diseñar campañas de sensibilización sobre la seguridad de la información y la ciberseguridad.
- Establecer los controles que permitan monitorear los riesgos e incidentes de seguridad de la información a los que se expone el Banco.
- Creación y administración de perfiles en los aplicativos del Core Bancario.
- Revisar, analizar y autorizar las modificaciones y actualizaciones que se realicen en los sistemas informáticos y aplicativos del banco en la resolución de los incidentes de seguridad y en la operatividad diaria de la organización.
- Mantener actualizada a la organización en las medidas de protección de datos y seguridad informática.
- Demás actividades afines a la seguridad de los activos informáticos del Banco conforme a los requerimientos normativos en la protección y tratamiento de datos.

El área de seguridad de la información hace parte de una división más grande en la organización, que es el área de Riesgos No Financieros. A continuación se tiene la estructura de esta área funcional[3]:

[2] Cursos de Capacitación sobre Seguridad de la Información BMM 2018.
[3] Documentación del área de Seguridad de la Información, Banco Mundo Mujer.

Figura 1 Estructura del área de Seguridad de la Información



CAPÍTULO III.

3. CONTEXTUALIZACIÓN METODOLÓGICA

En este capítulo se presenta el aporte que representa el desarrollo de este trabajo para la organización, los resultados esperados y el marco metodológico sobre el cuál se orientó el trabajo práctico, para la el logro de los objetivos planteados sobre el estudio.

3.1. CONTRIBUCIÓN DEL TRABAJO

El producto resultado de la práctica profesional tiene como fin contribuir con el mejoramiento continuo en los procesos vinculados al SGSI del Banco Mundo Mujer y a la prevención y mitigación de los riesgos de seguridad de la información. A través de la documentación del Manual del proceso de Validación de Usuarios y Perfiles se establecieron los lineamientos que orientan la correcta ejecución del proceso para facilitar la toma de decisiones y la implementación de acciones correctivas y de mejora, a fin de promover una cultura de protección y buen uso de la información dentro y fuera de la organización.

3.2. RESULTADOS ESPERADOS

Con el desarrollo del presente trabajo, se pretende generar un aporte a la organización, específicamente al área de Seguridad de la Información, en términos de efectividad y eficiencia en la operatividad y desempeño de las funciones y demás elementos relacionados con el proceso de Validación de Usuarios y Perfiles. Con la identificación, análisis y documentación de cada una de las actividades, responsables, salidas y entradas de este proceso, se busca establecer un panorama más claro del cómo se debe ejecutar cada actividad.

De esta manera, el Banco Mundo Mujer contará en adelante con una herramienta importante para su desempeño en el marco de la gestión de la seguridad de la información, ya que este proceso como tal tiene como fin velar por el cumplimiento de las directrices que

orientan la correcta administración de los permisos y privilegios sobre la información conforme a los flujos del personal de la organización.

3.3. METODOLOGÍA

El enfoque de investigación predominante del estudio es no experimental ya que se basó esencialmente en la observación. Este estudio está constituido por dos momentos metodológicos: Inicialmente, la investigación adopto un carácter exploratorio en el que se realizó un análisis y evaluación de los problemas y necesidades que se presentan en el área de S.I. en materia de políticas y procesos para sugerir las soluciones pertinentes.

Esta etapa del estudio va desde la vinculación formal a la organización, la introducción y capacitación en los aspectos generales de la organización, el análisis de las necesidades del área, hasta la detección del problema.

Así mismo, una vez identificada la problemática se realizó en segunda instancia una investigación descriptiva ya que el principal objetivo de este trabajo es el análisis y la descripción detallada del proceso objeto de estudio.

De acuerdo con las características del objeto de la práctica profesional, en la investigación se implementaron técnicas de carácter cualitativo y cuantitativo. Los datos obtenidos a través de métodos como la observación directa, el análisis documental y las consultas a los asesores de la práctica profesional constituyen el factor cualitativo del estudio.

Sin embargo, en el desarrollo de la misma se construyeron indicadores de evaluación del proceso para monitorear el comportamiento de este durante un periodo de tres meses, estos constituyen el factor cuantitativo de este trabajo, estos resultados se presentaron a través de informes dirigidos a los jefes de las áreas relacionadas.

Para efectos de la documentación del proceso se aplicó la metodología planteada por Gómez (2012) para la construcción de manuales de procesos que consta de los siguientes pasos:

1. Identificación del tipo de proceso: gerencial, administrativo o general.

2. Análisis e inventario documental: levantamiento y estudio de los documentos sobre políticas y procesos que se aplican al interior del área de S.I.
3. Enlace documental: Establecer las correlaciones entre los documentos implicados en el proceso.
4. Levantamiento de la información de campo: Recopilación de información acerca del proceso de Validación aplicando un formulario de identificación de procesos. (Anexo 1)
5. Construcción del proceso conforme a la información recopilada en el formulario de construcción de procesos (Anexo 2).
6. Elaboración del diagrama de flujo de proceso.
7. Descripción detallada de cada una de las actividades en la secuencia del proceso.

Para efectos del desarrollo de la práctica profesional fue necesario recurrir a fuentes de información primaria y secundaria como apoyo a la consecución de los objetivos del estudio. Las fuentes primarias de información en este caso hacen referencia a datos obtenidos a través de la observación sobre la ejecución del proceso por parte del colaborador encargado, entrevistas personales y consultas a los asesores académico, empresarial y los analistas de seguridad de la información que son los principales interesados en documentar y estandarizar el proceso.

Las fuentes secundarias consultadas en el proceso de la práctica profesional comprenden la documentación formal interna sobre las políticas y procesos de seguridad de la información, informes y registros históricos sobre el comportamiento del proceso de validación de usuarios y perfiles, documentación sobre la norma ISO 27001, libros, artículos y documentación en la web sobre seguridad informática, manuales de procesos, indicadores de gestión y demás temáticas relacionadas tanto con el papel del área como con el objetivo del estudio.

3.4. CRONOGRAMA DE ACTIVIDADES

Etapa 1. Identificación del problema.

1. Vinculación laboral a la organización.

2. Realización de los cursos generales obligatorios de inducción al Banco Mundo Mujer.
3. Capacitación sobre las actividades y funciones a realizar en el área de Seguridad de la Información. (S.I.)
4. Análisis documental de las políticas, procesos y demás formatos del área de S.I.
5. Análisis documental y consultas externas a la norma ISO 27001 y temas relacionados a la gestión de la seguridad de la información.
6. Reunión con el Gerente de área y analistas de seguridad para obtener información de las necesidades y problemáticas del área de S.I.
7. Análisis y evaluación de las necesidades del área conforme a la norma y las posibles soluciones.

   Etapa 2. Construcción del manual para el proceso de Validación de Usuarios y perfiles.
8. Entrevista al funcionario ejecutor del proceso.
9. Observación del paso a paso de la ejecución del proceso objeto de estudio.
10. Identificación del tipo de proceso y los elementos que lo componen
11. Análisis e inventario documental de los documentos relacionados con el proceso.
12. Construcción del proceso conforme a la información recopilada.
13. Descripción detallada de cada una de las actividades en la secuencia del proceso.
14. Elaboración del diagrama de flujo de proceso.
15. Revisión y entrega del Manual del proceso de validación de usuarios y perfiles al Jefe del área de Seguridad de la Información.

Tabla 1Cronograma de actividades de la práctica profesional.

ACTIVIDADES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Etapa 1. Identificación del problema.																				
1. Vinculación laboral a la organización.																				
2.Cursos generales de inducción																				
3. Capacitación sobre las actividades a realizar																				
4.Análisis de las políticas y procesos del área de S.I.																				
5. Análisis documental sobre la ISO 27001 y temas relacionados.																				
6.Reunión con el Gerente de área y analistas de seguridad.																				
7. Análisis y evaluación de las necesidades del área y las posibles soluciones.																				
Etapa 2. Construcción del manual.																				
8. Entrevista al funcionario ejecutor del proceso.																				
9. Observación del paso a paso de la ejecución del proceso objeto de estudio.																				
10. Identificación del tipo de proceso y los elementos que lo componen																				
11. Análisis e inventario documental de los documentos relacionados con el proceso.																				
12. Construcción del proceso conforme a la información recopilada.																				
13. Descripción detallada de las actividades del proceso.																				
14. Elaboración del diagrama de flujo de proceso.																				
15. Revisión y entrega del Manual del proceso.																				

Fuente: Elaboración propia.

CAPÍTULO IV.

4. DESARROLLO DEL TRABAJO DE PRÁCTICA PROFESIONAL

4.1. Proceso de vinculación, inducción y contextualización.

- *Vinculación*

El Banco Mundo Mujer es una organización que por la esencia de su negocio y los riesgos asociados a este, ha establecido políticas estrictas sobre la información que otorga tanto al cliente interno como al cliente externo, conforme con los intereses de cada uno sobre la organización.

Por tal motivo, para el desarrollo de la práctica profesional en la organización, debió llevarse a cabo una vinculación formal por medio de un contrato de aprendizaje, en el cual se establecieron las obligaciones contractuales de las partes por un periodo de cinco meses para desempeñar las actividades del estudio en el área de Seguridad de la Información.

- Inducción

Como parte de esta etapa de acoplamiento y contextualización con la realidad organizacional, se realizaron efectivamente los cursos y capacitaciones sobre los componentes más importantes del Banco Mundo Mujer, con el fin de obtener un conocimiento a grandes rasgos acerca de aspectos como el direccionamiento estratégico, las áreas funcionales y su cultura organizacional. (Anexo 3.)

- Contextualización Área de Seguridad de la Información.

Se realizó un análisis documental del área de Seguridad de la Información para conocer y comprender cada uno de los procesos que se llevan a cabo, cómo se hacen, para qué se hacen, quién los ejecuta y por qué. Además, se realizó un análisis de las políticas de Seguridad de la Información que se han elaborado en el área e implementado en el Banco, lo cual permitió

identificar las bases principales del funcionamiento de esta división. En este análisis documental se estudiaron los siguientes elementos[4]:

- PR 017 Manual del proceso de Administración de Usuarios y Perfiles.
- PR 105 Manual del proceso de Control de Pasos entre Ambientes.
- PT 007 Políticas de Seguridad de la Información
- PT 042 Política de Seguridad de la Información y Ciberseguridad.

Conforme al análisis anterior, se identificó la norma sobre la cual se han implementado estas políticas y procesos, la ISO 27001 de 2013, norma conforme a la cual se realizó el diagnóstico de la situación del área de Seguridad que se evidencia en el siguiente apartado.

4.2. Diagnóstico del área de Seguridad de la Información

Para efectos del diagnóstico de la situación del área de trabajo, se realizó un análisis del cumplimiento por parte de la organización de los requisitos generales que señala la norma ISO 27001 a través del área de Seguridad de la Información, que es la encargada de definir las metodologías, políticas, procedimientos y tecnologías para proteger los activos informáticos del Banco Mundo Mujer.

La ISO/IEC 27001 (2013) es la norma que enmarca el "establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI) adaptado a las necesidades de las organizaciones individuales o a partes de ellas."

- Enfoque basado en procesos.

Esta norma adopta un enfoque basado en procesos señalando que para funcionar eficientemente, una organización debe identificar y gestionar muchas actividades, considerando

[4] Inventario documental del Banco Mundo Mujer.

una actividad como una operación que implica la transformación de entradas en salidas es decir, un proceso. (ISO/IEC 27001, 2013)

De esta manera, aplica el modelo de procesos "PHVA" (Planificar – Hacer- Verificar y Actuar) para estructurar los procesos que van a conformar el SGSI teniendo como entradas los requisitos de seguridad de la información que a través de los procesos del SGSI generan uso resultados que están relacionados con el cumplimiento de esos requisitos. Gráficamente se expresa así[5]:

Figura 2 Aplicación del modelo PHVA en el SGSI

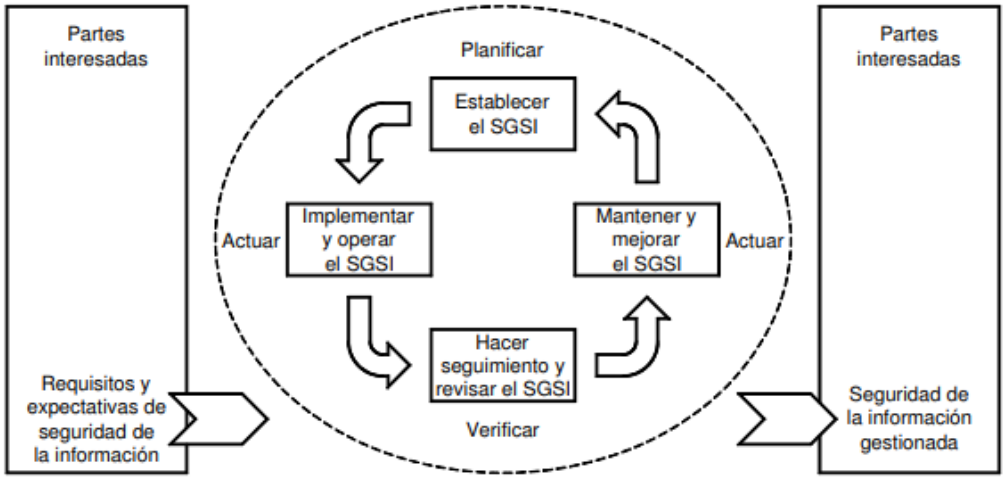


Tabla 2 Aplicación del modelo PHVA en el SGSI

ETAPA	DESCRIPCIÓN
Planificar: Establecer el SGSI	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer: Implementar y Operar el SGSI	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar: Hacer seguimiento y revisar el SGSI	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar: Mantener y mejorar el SGSI	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente: ISO/IEC 27001 de 2013

[5] Enfoque de procesos ISO/IEC 27001 de 2013

Cada organización conforme a su tamaño y actividad debe identificar los requisitos de seguridad que se adaptan a sus necesidades para de esa manera establecer las políticas, procesos y controles que conformarán su SGSI. El Banco Mundo Mujer, ha adaptado este modelo de procesos en su organización, implementado un SGSI alineado con sus objetivos corporativos y dentro del marco de los riesgos de seguridad de la información a los que se encuentra expuesto.

Ahora bien, se realizó un análisis de la organización conforme al nivel de cumplimiento de los requisitos de documentación señalados por la norma para la gestión de la seguridad de la información:

La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI **documentado**, entendiendo por documentado que el procedimiento está establecido, documentado, implementado y mantenido**;** para lo cual debe cumplir con los siguientes requisitos:

Tabla 3 Requerimientos de documentación según la norma ISO/IEC 27001

REQUISITOS DE DOCUMENTACIÓN	VALORACIÓN	DETALLE
Declaraciones documentadas de la política y objetivos del SGSI	Bueno	El área de seguridad cuenta con la documentación formal de cada una de las políticas que conforman el SGSI de Banco Mundo Mujer.
El alcance del SGSI	Bueno	En la política general de Seguridad de la Información se determina el alcance de la SGSI en la organización
Procedimientos y controles que apoyan el SGSI	Regular	La mayoría de los procedimientos a cargo del área de S.I. están documentados. Sin embargo, con el tiempo se incluyeron actividades de control que no han sido documentadas.
Descripción de la metodología de valoración de riesgos	Bueno	La metodología está documentada y es implementada por el área de Riesgo Operativo en su respectivo Manual.
Informe de valoración de riesgos	Bueno	El área de Riesgo Operativo se encarga de entregar un informe de seguimiento de la efectividad de los controles de mitigación de riesgo en toda la organización.
Plan de tratamiento de riesgos	Bueno	El área de Seguridad de la Información determina los mecanismos para el tratamiento de los riesgos asociados a la Seguridad de la información.
Registros del desempeño del proceso	Bueno	El área de S.I. cuenta con un repositorio en el que se lleva el registro histórico documentado de los informes de desempeño de los procesos de S.I.

Fuente: Administración documental Banco Mundo Mujer. Elaboración propia.

Conforme a la evaluación anterior, sobre el cumplimiento de los requisitos mencionados se identificó un punto de deficiencia en la documentación de procesos y procedimientos del SGSI.

De manera detallada se evaluó el cumplimiento en los requisitos de documentación en cada uno de los elementos del SGSI del Banco Mundo Mujer donde se calificó como (B) Bueno (R) Regular y (D) Deficiente:

Tabla 4 Matriz de evaluación de la documentación del SGSI del Banco Mundo Mujer.

ELEMENTO	Establecido	Documentado	Implementado	Mantenido
Políticas de Seguridad de la Información				
Uso de contraseñas.	B	B	B	B
Uso del correo institucional.	B	B	B	B
Uso de internet.	B	B	B	B
Seguridad para uso de USB.	B	B	B	B
Uso y control de portátiles.	B	B	B	B
Escritorio limpio.	B	B	B	B
Uso del File Server.	B	B	B	B
Política general de Seguridad de la información y ciberseguridad	B	B	B	B
Procesos y procedimientos de Seguridad de la Información				
Administración de usuarios y perfiles	B	B	B	R
Control de pasos entre ambientes	B	B	B	R
Validación de Usuarios y perfiles	R	D	D	D
Otros componentes del SGSI				
Informes de desempeño de los procesos ejecutados por el área de S.I.	B	B	R	B
Campañas de sensibilización en Seguridad de la Información y Ciberseguridad	B	B	B	R
Cursos de Seguridad de la Información para la inducción y capacitación del personal del Banco	B	B	B	B

Fuente: Adaptación Requisitos de documentación de la norma ISO/IEC 27001.

De acuerdo con la evaluación anterior, se pudo evidenciar que el proceso de validación de usuarios y perfiles no se encuentra documentado lo que ha afectado tanto su implementación como su mantenimiento. Lo anterior se debe a que al no contar con la guía de realización del

proceso, este no se ejecuta de manera uniforme y los resultados que arroja no generan la confianza necesaria en los directivos para poder ejercer las debidas acciones correctivas.

Este proceso está relacionado con el de administración de usuarios y perfiles, ya que hace las veces de control para el seguimiento del desempeño y correcta ejecución de las modificaciones en los accesos a la información conforme a las novedades de nómina, permitiendo identificar y mitigar posibles situaciones de riesgo para la seguridad de la información en toda la organización. Es fundamental para el área de seguridad que este proceso se lleve a cabo de forma eficiente, de tal manera que logre generar información útil para la toma de decisiones por parte de las áreas implicadas.

Conforme al análisis que se realizó de esta evaluación, y de acuerdo con los funcionarios y jefes del área relacionada, se comprobó la necesidad de establecer una guía orientadora para que la validación como control, se ejecute uniformemente y genere la información necesaria para evidenciar posibles problemas en el proceso principal. De esta manera, se decidió realizar la documentación formal de la validación de usuarios y perfiles a través de un manual de procesos.

4.3. Construcción del manual de procesos.

La construcción del manual se realizó de acuerdo con el proceso planteado por Gómez (2012) que consta de 7 etapas:

1. Identificación del tipo de proceso: gerencial, administrativo o general.

   La Validación de Usuarios y Perfiles se clasificó como un proceso gerencial ya que proporciona medios de seguimiento y control a jerarquías superiores sobre una actividad importante en la organización, como es el caso de la administración de los privilegios sobre los activos informáticos.

2. Análisis e inventario documental: En este paso se llevó a cabo el levantamiento y estudio de los documentos sobre políticas y procesos que se aplican al interior del área de S.I. donde se obtuvo lo siguiente:

N°	*INVENTARIO DOCUMENTAL S.I*
1	Estadístico de pasos
2	FRM 036 - Solicitud de modificación de perfil
3	Informe Indicador de Pasos entre ambientes
4	Informe Indicador de reporte y cumplimiento de novedades de nómina.
5	Matriz de perfiles por cargo.
6	Matriz de validación de novedades
7	PR 0105 Manual para el Control de pasos entre ambientes
8	PR 017 Manual para la Administración de Usuarios y Perfiles
9	PT 007 Políticas de Seguridad de la Información
10	PT 042 Política de seguridad de la información y la ciberseguridad
11	Registro histórico de modificaciones en Bantotal con cédula
12	Reporte 4151A de Modificación de usuarios en Bantotal
13	Reporte de Cambios de cargo
14	Reporte de cambios de segmento
15	Reporte de Egresados
16	Reporte de Licencias e incapacidades
17	Reporte de Modificaciones pendientes en Bantotal
18	Reporte de traslados de agencia
19	Reporte de Usuarios inactivos > 90 días
20	Reporte de vacaciones
21	Soporte control de Pasos entre ambientes

Tabla 5 Inventario documental

Fuente: Servidor de archivos Banco Mundo Mujer - Elaboración propia

3. Enlace documental: Correlaciones entre todos los documentos que se aplican al interior del área.

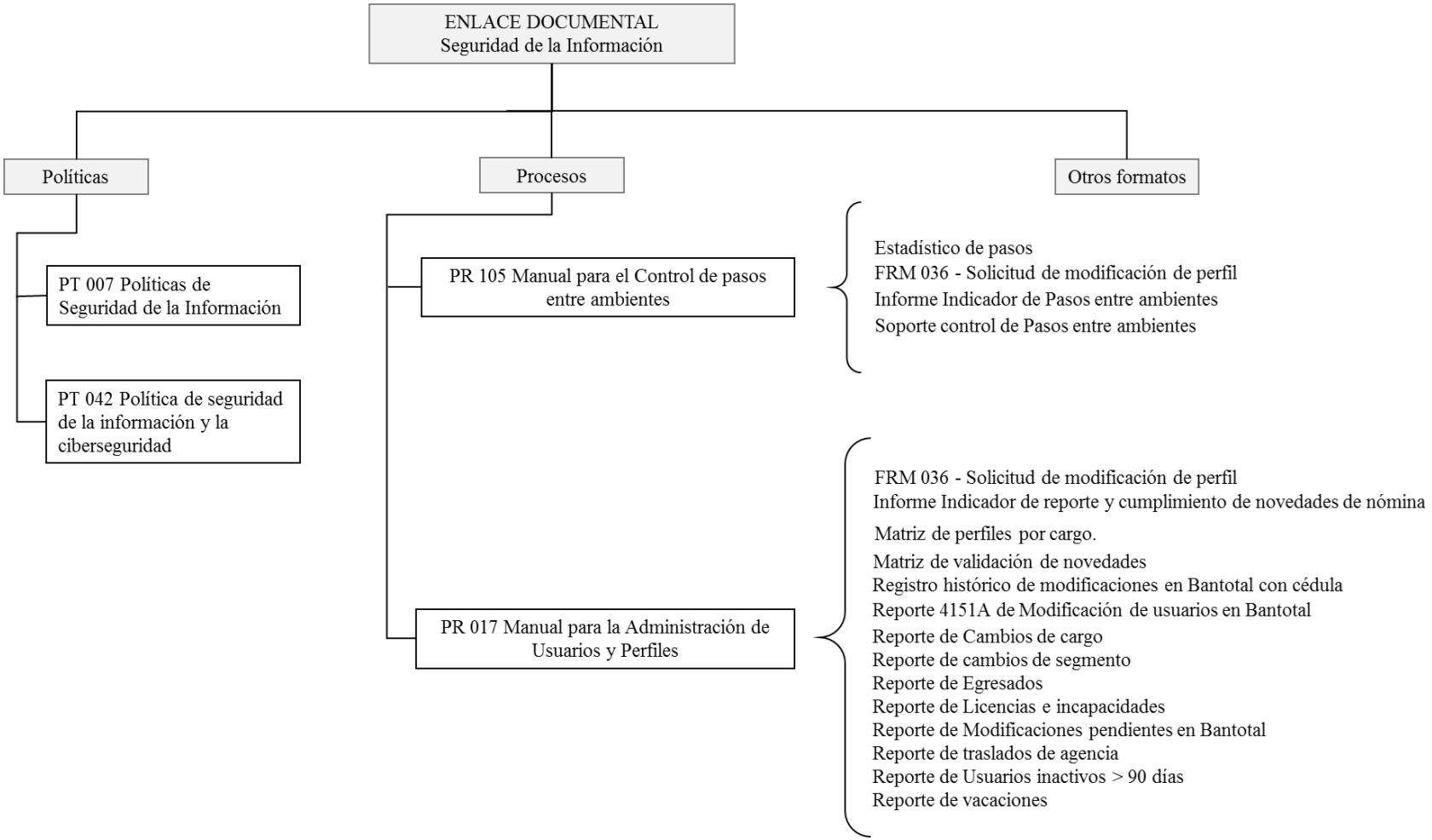


Figura 3 Enlace documental

4. Levantamiento de la información de campo.

Con el fin de recopilar la información sobre las actividades y demás elementos del proceso, se aplicó el formulario diseñado por el autor (Anexo 1), para la identificación de las actividades y demás elemento relacionados con la Validación de usuarios y perfiles.

En este caso, el formulario se aplicó a la persona encargada de ejecutar directamente el proceso, quien se encargó de describir detallada y concretamente cada una de las actividades que realiza y el cómo lo hace. Los resultados obtenidos son los siguientes:

FORMULARIO PARA LA IDENTIFICACIÓN DE PROCESOS Y PROCEDIMIENTOS

Área	Seguridad de la Información	**Fecha:**	08/10/2018	**N°**	1
Empleado	Ashley Stephany Cubides	**Cargo:**	Pasante Universitario		

1. Procedimiento: Validación de Usuarios y Perfiles en Bantotal

   1.1.Qué hace:

- Revisión y registro de los reportes diarios de las novedades de nómina: Vacaciones, egresos, cambios de cargo, licencias, traslados de agencia y cambios de segmento.
- Descarga y registro diario de los reportes por modificación de perfiles a usuarios del aplicativo Bantotal.
- Depuración de los reportes consolidados de las novedades que se validan para el informe mensual de cumplimiento y ejecución. Se eliminan registros repetidos, usuarios sin perfil en Bantotal y se realizan las modificaciones en los registros por cambios de fecha reportados.
- Validación semanal de los usuarios reportados e las novedades de Vacaciones, egresos, y cambios de cargo con respecto a las modificaciones evidenciadas en los registros consolidados del reporte 4151ª de Bantotal.
- Notificar al analista de seguridad de manera semanal la cantidad de usuario con novedad efectiva a los que aún no se les modifica el perfil correspondiente en Bantotal.

- Elaborar mensualmente el informe sobre Reporte y ejecución oportuna de las novedades de nómina que comprende el cálculo y medición a través de los indicadores de eficiencia y efectividad del proceso, demora y cumplimiento en el reporte de las novedades, desviación ANS y comparativos trimestrales de mejora del proceso junto con observaciones detalladas obtenidas de la validación.

1.2. Cómo lo hace:

- Desde el correo institucional asignado, se descarga el reporte diario de las novedades de nómina enviado por los analistas de Talento Humano. Este reporte se guarda por fecha en la carpeta correspondiente al histórico de cada novedad y en el consolidado de los registros mensuales que se lleva en una matriz de Excel.

- Además de guardar el registro en el Excel, se lleva un respaldo del correo enviado con el reporte para mantener la evidencia de que si se ha recibido el reporte de novedades por parte de TH.

- Por otro lado, el reporte sobre las modificaciones de los usuarios y perfiles se descarga directamente del aplicativo Bantotal, al que se tiene permiso de consulta. Para este reporte también se cuenta con una carpeta de evidencia y registro histórico en el cual se archivan diariamente estos reportes para la realización de las validaciones semanales.

- Para la validación de los usuarios, se deben depurar de los reportes de las novedades a aquellos usuarios que no tienen perfil en Bantotal, estos se identifican por sus cargos, es decir, conforme a la matriz de perfiles se identifican aquellos cargos que NO cuentan con permisos de acceso al aplicativo para no tenerlos en cuenta en la validación. También deben descartarse los reportes repetidos teniendo en cuenta el detalle de la novedad, es decir: Cancelación o modificación de fechas, para dejar un solo registro por cada usuario.

- Una vez depurados los reportados por novedades de nómina, se procede a realizar el rastreo en el reporte consolidado 4151ª de la última modificación de su perfil en Bantotal, para confirmar si se ha realizado el cambio y que este corresponda a la novedad reportada y se haya efectuado en las fechas señaladas.

- En el archivo de validación deben clasificarse y contarse los cambios realizados, los cambios que se encuentran endientes y los que nunca se hicieron. También es fundamental tener en cuenta tanto la demora del reporte desde Talento Humano como la demora en la modificación del perfil desde la fecha de inicio de la novedad.

- La validación se hace semanalmente, para informar al analista de seguridad sobre los usuarios que se encuentran con demora en la modificación de sus perfiles, para que estos den notificación al CIS y posteriormente se dé la debida gestión de estos cambios en un tiempo prudente. Con lo anterior se busca prevenir interrupciones y deficiencias en las labores diarias de los funcionarios involucrados y posibles riesgos por ineficiencias en la administración de los accesos a los sistemas informáticos.

- Con la información obtenida de las validaciones, se elaboran mensualmente los indicadores de gestión y cumplimiento con las observaciones detalladas sobre los hallazgos obtenidos de este proceso, lo anterior con el fin de contribuir con la mejora del proceso identificando factores críticos que puedan estar afectando su eficiencia, eficacia y efectividad.

- Finalmente, este informe es revisado en conjunto con los analistas de seguridad y el gerente de área para posteriormente ser enviado a las dos áreas relacionadas con el proceso que son Talento Humano y el Centro Integral de Servicios CIS. Este informe se convierte en una herramienta de comunicación que busca a través de una forma clara evidenciar el comportamiento del proceso y contribuir con mejoras para mayor agilidad en la gestión y administración de los perfiles.

1.3.Frecuencia

Actividad	Frecuencia
Registro de reporte de Novedades de Nómina	Diario
Registro de Reporte 4151ª de Modificación de Perfiles en Bantotal	Diario
Depuración de los reportes de novedades	Semanal
Validación de Usuarios en Bantotal	Semanal
Notificación de modificaciones pendientes por ejecutar.	Semanal
Elaboración del informe de Reporte y ejecución oportuna de las Novedades de Nómina	Mensual

1.4.Responsabilidades:

La responsabilidad en la realización de este proceso es compartida ya que para efectos de la eficiencia en el desarrollo del mismo se requiere de insumos obtenidos de otras áreas y del apoyo de los analistas de seguridad de la información.

1.5.Trámite: Una vez finalizado el proceso de validación, el CIS es el encargado de realizar las acciones correctivas correspondientes a los hallazgos resultados de la medición obtenida a través de este proceso.

2. Elaboración y trámite documental.

- Documentos generados: Tablas de registro mensuales y consolidados por novedad de nómina, Informe de Indicadores, Reportes se modificaciones pendientes en Bantotal.
- Documentos electrónicos: Reporte de Novedades de Nómina t Reporte 4151ª de modificación de usuarios y perfiles en Bantotal.

3. Observaciones: Este proceso es fundamental para identificar posibles factores de riesgo de seguridad de la información, ya que permite evidenciar desempeño deficiente de las áreas relacionadas con respecto a la ejecución de las novedades de nómina.

Tramitado por: Ashley Stephany Cubides Valderrama

Fecha de elaboración: 01/10/2018

Firma: _____

5. Construcción del proceso.

Conforme a la información recopilada en el formulario de construcción de procesos (Anexo 2), de acuerdo con lo descrito por la persona encargada de ejecutar el proceso se realizó la construcción del proceso como se evidencia a continuación:

FORMULARIO DE CONTRUCCIÓN DE PROCESOS Y PROCEDIMIENTOS

BANCO MUNDO MUJER S.A.

31/10/2018

Proceso: Validación de Usuarios y perfiles en Bantotal

Área/División: Seguridad de la Información

1. Describir concretamente las actividades en secuencia del proceso y el responsable.

N°	Descripción	Detalle	Responsables	Salidas
1	Revisión, descarga y registro del reporte de Modificación de usuarios y perfiles en Bantotal (4151A).	Desde el aplicativo Bantotal, se descarga el reporte 4151A sobre Modificaciones de Usuarios y Perfiles, que se hayan realizado en el día anterior. Este reporte se descarga y se guarda en los formatos PDF y Excel sin que se realice ninguna modificación sobre esta información.	Pasante Universitario Seguridad de la Información	Evidencias y registros históricos de los reportes.
2	Registro del reporte en el consolidado histórico 4151A con cédula.	Se registra el reporte 4151A que se descarga diariamente en un histórico consolidado que se lleva en Excel, en este reporte en especial se trae la cédula de los usuarios reportados desde el archivo del Directorio Activo para efectos de la validación.	Pasante Universitario Seguridad de la Información	Reporte consolidado con Cédula
3	Reporte de Novedades de Nomina.	Por medio del correo electrónico se envía al área de Seguridad de la Información y al CIS, en formato el reporte de los usuarios notificados por cada novedad de	Analista de Talento Humano	Reporte de Novedades

		nómina: Egresos, cambios de cargo, vacaciones, traslados de agencia, licencias.		
4	Revisión, descarga y registro del reporte de novedades de nómina.	Desde el correo electrónico, se revisan y descargan los reportes de cada novedad. Estos se guardan por fecha en la carpeta correspondiente al histórico de cada novedad y en el consolidado de los registros mensuales que se lleva en una matriz de Excel.	Pasante Universitario Seguridad de la Información	Evidencia e histórico de los reportes de cada novedad.
5	Depuración del reporte consolidado mensual de las novedades.	Se crea una copia del consolidado mensual de cada novedad a validar (vacaciones, egresos y cambios de cargo), se eliminan registros repetidos, usuarios sin perfil en Bantotal y las modificaciones en los registros por cambios de fecha reportados.	Pasante Universitario Seguridad de la Información	Matriz de validación de perfiles.
6	Validación de Novedades de Nómina (Vacaciones, egresos y cambios de cargo)	En la matriz base para la validación, se insertan los registros a validar de cada novedad ya depurados. Posteriormente, en el consolidado 4151A con cédula, se realiza un rastreo del usuario para verificar si efectivamente se le modificó el perfil de acuerdo con la novedad trayendo el último perfil que se le asignó y la fecha en que se hizo.	Pasante Universitario Seguridad de la Información	Reporte de modificaciones pendientes por ejecutar. Indicador de cumplimiento y ejecución de las novedades de nómina
7	Medición de demora en reporte de novedades.	Para cada usuario reportado, se calcula la diferencia entre la fecha efectiva de la novedad y la fecha en que fue reportado por Talento Humano para medir, individualmente y en promedio, el tiempo que se demoró TH en reportar la novedad.	Pasante Universitario Seguridad de la Información	Indicador de demora en reporte de Novedades.
8	Medición de demora en ejecución de novedades.	Para cada usuario reportado, se calcula la diferencia entre la fecha efectiva de la novedad y la fecha en que se le modificó el perfil en Bantotal para medir, individualmente y en promedio, el tiempo que se demoró	Pasante Universitario Seguridad de la Información	Indicador de demora en ejecución de novedades

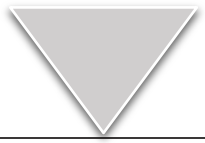
		el CIS en cambiarle el perfil al usuario conforme a la novedad.		
9	Reporte de modificaciones pendientes en Bantotal	Los usuarios reportados por TH cuya fecha de inicio de la novedad sea efectiva a la fecha de la validación y aún no se les haya modificado el perfil en Bantotal, deben reportarse como pendientes al analista de seguridad de la información para que este notifique al CIS y los cambios sean ejecutados de manera inmediata.	Pasante Universitario y Analista de seguridad de la información	Reporte de cambios pendientes por novedad.
10	Elaboración del Informe mensual sobre reporte y ejecución oportuna de las novedades de nómina.	Realizar el cálculo y medición a través de los indicadores de eficiencia y efectividad del proceso, demora y cumplimiento en el reporte de las novedades, desviación ANS y comparativos trimestrales de mejora del proceso junto con observaciones detalladas obtenidas de la validación.	Pasante Universitario Seguridad de la Información	Informe mensual sobre el reporte y ejecución oportuna de las novedades de nómina.
10.1	Revisión del informe	Se revisa que el informe esté elaborado correctamente: cifras, fechas, ortografía y redacción. Si está bien se pasa al punto 10.3. De lo contrario se pasa al punto 10.2.	Analista de Seguridad de la información	
10.2	Correcciones y modificaciones	Conforme a las recomendaciones y correcciones señaladas en la revisión, se realizan los cambios sugeridos y se vuelve a revisar el informe. (Paso 10.1.)	Pasante Universitario y Analista de seguridad de la información	
11	Envío a las áreas relacionadas	El informe debe enviarse en formato PDF a las áreas correspondientes: Talento Humano y Centro Integral de Servicios para que logren identificar las fallas y situaciones críticas en sus procesos.	Jefe de seguridad de la Información / Analista de Seguridad de la Información	Evidencia del envío en formato PDF

Tabla 6 Descripción detallada del proceso

6. Elaboración del diagrama de flujo de proceso.

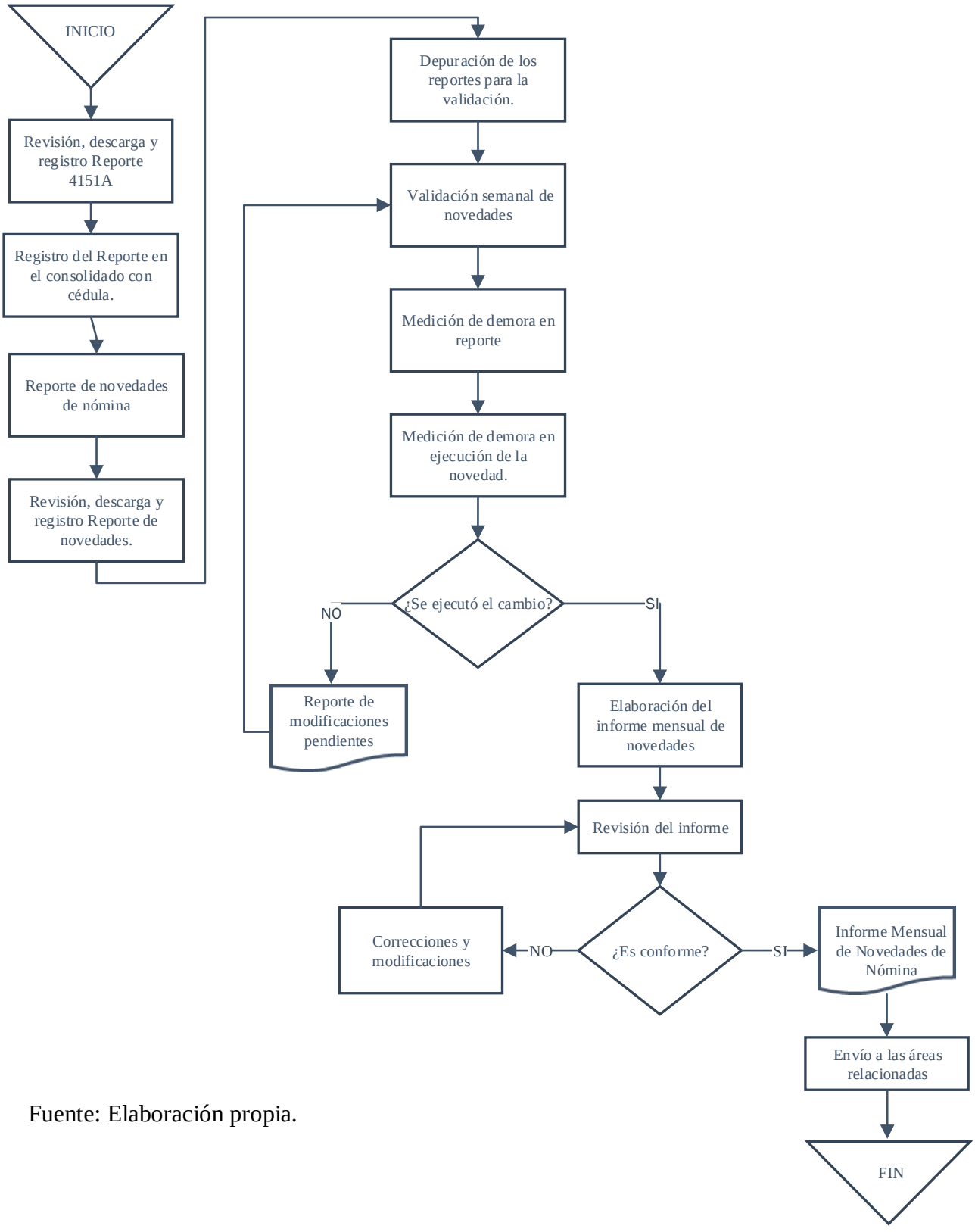
Para la elaboración del diagrama de flujo se consideró la simbología señalada por Gómez (2012), que es la siguiente:

Símbolo- dibujo- nombre	Descripción: finalidad y uso
 Procedimiento	Describe la tarea básica al inicio o en cualquier parte del proceso que se considere genérica.
 Procedimiento alterno	Identifica u procedimiento que, por su similitud o finalidad, puede reemplazar a otro son alterar el resultado del proceso
 Decisión	Permite tomar determinación sobre la orientación que se le debe dar al proceso o a la alternativa de ejecutar simultánea o previamente otro procedimiento.
 Datos	Proporciona información sobre los datos que se deben consultar, necesarios para continuar con el procedimiento siguiente.
 Datos almacenados	Proporciona información sobre datos prestablecidos, almacenados en cualquier medio, necesarios para continuar con el procedimiento siguiente.
 Documento	Muestra un documento propio del procedimiento o documento alternativo que se correlaciona, soporta y/o complementa. Puede ser físico o digital.

 Multi-documento	Corresponde a un conjunto de documentos propios de un procedimiento específico. Pueden ser sobre una misma operación o actividades correlacionadas.
 Disco magnético	Identifica el elemento físico magnético y/o electrónico, de donde se requiere obtener información para aplicar el procedimiento.
 Almacena interno	Muestra la fuente interna donde se debe disponer la información o documentos propios del procedimiento.
 Preparación	Determina la tarea manual o por medios electrónicos que se debe realizar con respecto al procedimiento. Por lo general es de ordenamiento.
 Operación manual	Identifica una labor que, por sus características, debe ejecutarse de manera manual con documentos o elementos físicos.
 Pantalla	Permite visualizar o ejecutar una actividad propia del procedimiento. Por lo general es de ayuda y/o consulta.
 Terminador - inicio	Muestra la culminación o inicio del conjunto de un proceso o de un bloque del mismo, cuando la secuencia debe tomar otra ruta.

Fuente: Gómez, Cardona, William Darío. Prácticas empresariales, Ecoe Ediciones, 2012.

Figura 4 Diagrama de flujo de proceso.



Fuente: Elaboración propia.

5. MANUAL DE PROCESOS

PR. VALIDACIÓN DE USUARIOS Y PERFILES EN BANTOTAL.

VERSIÓN 01

Vicepresidencia de riesgos

Gerencia de riesgos no financieros

Seguridad de la información

2019

MANUAL DE PROCESOS – PR VALIDACIÓN DE USUARIOS Y PERFILES EN BANTOTAL

	ELABORADO POR	REVISADO POR	APROBADO POR
Cargo	Pasante Universitario Seguridad de la Información	Pasante Universitario Seguridad de la Información	Gerente de Riesgos No Financieros
Nombre	Ashley Stephany Cubides Valderrama	Ashley Stephany Cubides Valderrama	Juan Pablo Rodríguez Calvache
Firma			

CONTROL DE CAMBIOS

VERSIÓN	**FECHA**	**DESCRIPCIÓN**
01	01/2019	Creación del Manual de procesos para la Validación de Usuarios y Perfiles en Bantotal.

Introducción

En el camino al fortalecimiento y crecimiento empresarial, es fundamental para toda organización determinar y aplicar procesos ágiles, simples y eficientes. Para lo cual, se hace indispensable el uso de herramientas, tales como los manuales de procesos y procedimientos, que sirven como guía en su ejecución, seguimiento, control y mejora. (Gómez 2012:40)

La estandarización de los procesos y procedimientos a través de los manuales, facilita la correcta operatividad y desempeño eficiente de las actividades fundamentales de la organización, contribuyendo así con el logro de los objetivos de la empresa.

El siguiente documento, contiene el Manual del Proceso de Validación de Usuarios y Perfiles en el aplicativo Bantotal, del área de Seguridad de la Información del Banco Mundo Mujer. En el cual, se describen cada uno de los elementos que componen este proceso: objetivo, alcance, directrices, actividades, responsables y las salidas.

1. *Objetivo*

Contribuir desde el área de seguridad de la Información, con el monitoreo y seguimiento de la eficiencia y eficacia en la modificación y actualización de los perfiles en Bantotal por parte del CIS, de los usuarios reportados por el área de Talento Humano en las novedades de nómina: Egresos, Vacaciones y Cambios de Cargo.

2. *Alcance*

Este proceso tiene aplicación desde la descarga, revisión y registro permanente de los reportes de Modificación de Usuarios en Bantotal (4151A) y de Novedades de Nómina; hasta la validación, seguimiento y control de la eficiencia y eficacia tanto en el reporte como en la modificación de los perfiles.

3. *Referencias normativas*

Este proceso hace parte del Sistema de Gestión de la Seguridad de la Información que se ha implementado en el Banco, por lo tanto está enmarcado en las normas ISO 27001 – La norma general sobre los Sistemas de Gestión de la Seguridad de la Información en las organizaciones.

4. *Términos y definiciones*

- Activos informáticos: Tangibles e intangibles; personas, bases de datos, sistemas y recursos que se traducen en información clave y confidencial de la organización.
- ANS: Acuerdo de Nivel de Servicio

- Bantotal: Es el principal aplicativo del Core bancario, en el cual se realizan todas las operaciones.
- Core Bancario: Consiste en la plataforma software encargada de administrar y potenciar las operaciones del negocio del Banco: préstamos, depósitos y transferencias. Así como realizar la gestión de la información de los clientes del banco.
- CIS: Centro Integral de Servicios.
- Indicador: Es una herramienta de medición cuantitativa que sirve para valorar y evaluar el desempeño de un proceso en un determinado periodo de tiempo.
- Novedad de nómina programada: Consiste en un evento que afecta las funciones de un colaborador pero que ha sido comunicado con anticipación. En este caso son: Las vacaciones, cambios de cargo, traslado de agencia y licencias remuneradas.
- Novedad de nómina no programada: Es un evento que se presenta de manera extraordinaria y que afecta las funciones y desempeño de un funcionario. Hace referencia a eventos tales como retiros, incapacidades, suspensiones, entre otros.
- Política de seguridad de la información: Son las directrices que enmarcan el tratamiento y administración de los recursos informáticos en la organización que permitan el logro de una operatividad continua y segura.
- Perfil: Nivel de acceso a determinada información, ya sea a modo de consulta, modificación o administración de un activo informático.
- Privilegio: Es el permiso de acceso que se otorga a determinada información. Cada cargo tiene unos privilegios de acceso distintos conforme a los requerimientos de su función en la organización.

- Recursos informáticos: Hardware (equipos) y software (programas) requeridos para el funcionamiento de los sistemas de información.
- Seguridad de la información: Es la acción de velar y propender por la confidencialidad, integridad y disponibilidad de la información y del desarrollo de buenas prácticas en el uso y tratamiento de los activos informáticos.
- Sistema de información: Conjunto de elementos organizados para el tratamiento y administración de la data, a través del cual se busca generar información acorde con las necesidades y objetivos de la organización.
- Sistema de Gestión de Seguridad de la Información SGSI: Consiste en un conjunto de políticas, procesos y procedimientos estructurados y definidos al interior de la organización, implementados con el fin de garantizar la eficiencia en la gestión de la seguridad de la información en el Banco.
- Servidor de archivos: Es un equipo que almacena de forma centralizada toda la información y los datos que obtiene y genera la organización y a través del cual se tiene la disponibilidad y acceso rápido y seguro a tal información para cliente interno.
- Usuario: Identificación que se otorga a cada uno de los funcionarios dentro de los sistemas de información, al ingresar a la organización.

5. Directrices

En el desarrollo del proceso se deben tener en cuenta las siguientes directrices:

- El área de Talento Humano debe reportar de forma oportuna al área de Seguridad de la Información y al CIS, mediante el correo institucional, las novedades de nómina cuando

estas se presenten y las modificaciones sobre las novedades reportadas para su actualización en los registros respectivos que maneje cada área.

- El acuerdo de nivel de servicio, que corresponde al tiempo máximo definido para realizar el reporte de las novedades por parte de Talento Humano es de 1 día, demoras superiores serán consideradas como reportes extemporáneos.
- El área de Seguridad de la Información debe llevar registro de todos los reportes de las Novedades, estos se deben guardar y clasificar por fecha y tipo de novedad en los formatos definidos (Excel y PDF).
- De igual forma, se debe llevar diariamente el registro del reporte 4151A, sobre las modificaciones de Usuarios y perfiles en el aplicativo Bantotal. Este debe guardarse por fecha y en los formatos definidos.
- Desde el Centro Integral de Servicios CIS, se deben efectuar las modificaciones de los perfiles, de acuerdo con el reporte de las novedades que emite Talento Humano diariamente.
- Del total de novedades reportadas por Talento Humano, se validan únicamente las correspondientes a Egresos, Vacaciones y Cambios de cargo.
- El tiempo máximo en que se deben efectuar los cambios sobre las novedades es de 1 día para Egresos y Vacaciones y 2 días para los cambios de cargo.
- El área de Seguridad de la Información debe realizar semanalmente la validación de los usuarios y perfiles en Bantotal para identificar demoras en modificación de perfiles y posteriormente notificar al CIS para hacer efectivos los cambios pendientes.
- En el proceso de validación se depuran de los reportes de TH a los usuarios que no tienen perfil en el aplicativo, los registros repetidos considerando cancelación de novedades o cambios de fecha.

- El área de Seguridad de la Información será la encargada de elaborar el informe mensual sobre el cumplimiento en el reporte y ejecución oportuna de las Novedades de Nómina, a través del cual se presentará información sobre el desempeño del proceso a través de indicadores de gestión y cumplimiento.

6. Proceso

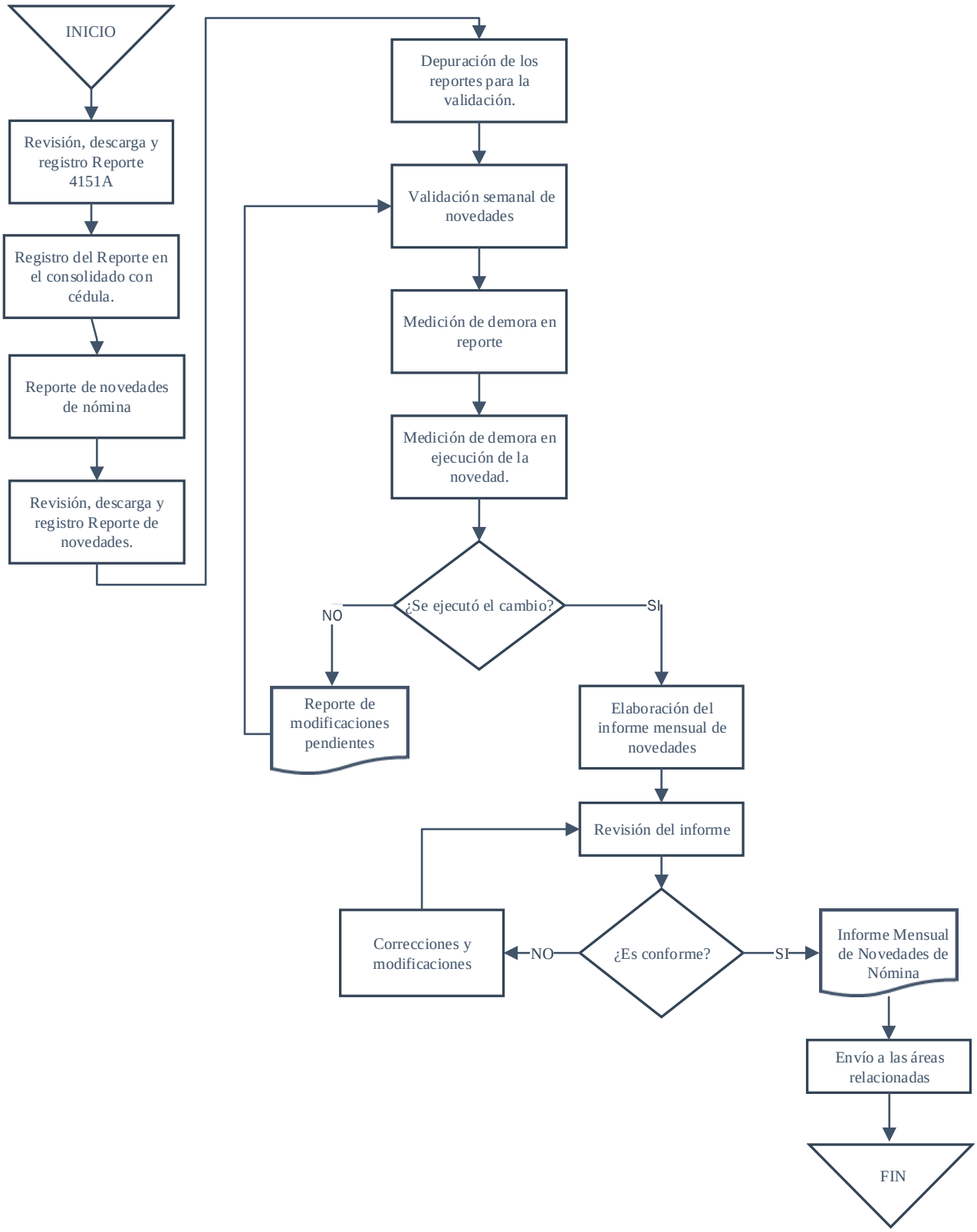
6.1.Descripción de las actividades y responsables.

N°	Descripción	Responsables	Salidas
1	Revisión, descarga y registro del reporte de Modificación de usuarios y perfiles en Bantotal (4151A).	Pasante Universitario Seguridad de la Información	Evidencias y registros históricos de los reportes.
2	Registro del reporte en el consolidado histórico 4151A con cédula.	Pasante Universitario Seguridad de la Información	Reporte consolidado con Cédula
3	Reporte de Novedades de Nomina.	Analista de Talento Humano	Reporte de Novedades
4	Revisión, descarga y registro del reporte de novedades de nómina.	Pasante Universitario Seguridad de la Información	Evidencia e histórico de los reportes de cada novedad.
5	Depuración del reporte consolidado mensual de las novedades.	Pasante Universitario Seguridad de la Información	Matriz de validación de perfiles.
6	Validación de Novedades de Nómina (Vacaciones, egresos y cambios de cargo)	Pasante Universitario Seguridad de la Información	Reporte de modificaciones pendientes por ejecutar. Indicador de cumplimiento y ejecución de las novedades de nómina
7	Medición de demora en reporte de novedades.	Pasante Universitario Seguridad de la Información	Indicador de demora en reporte de Novedades.

8	Medición de demora en ejecución de novedades.	Pasante Universitario Seguridad de la Información	Indicador de demora en ejecución de novedades
9	Reporte de modificaciones pendientes en Bantotal	Pasante Universitario y Analista de seguridad de la información	Reporte de cambios pendientes por novedad.
10	Elaboración del Informe mensual sobre reporte y ejecución oportuna de las novedades de nómina.	Pasante Universitario Seguridad de la Información	Informe mensual sobre el reporte y ejecución oportuna de las novedades de nómina.
10.1	Revisión del informe	Analista de Seguridad de la información	
10.2	Correcciones y modificaciones	Pasante Universitario y Analista de seguridad de la información	
11	Envío a las áreas relacionadas	Jefe de seguridad de la Información / Analista de Seguridad de la Información	

Fuente: Elaboración propia

6.2.Mapa de proceso



6.3.Descripción detallada del proceso

1. Revisión, descarga y registro del reporte de Modificación de usuarios y perfiles en Bantotal (4151A):

   Desde el aplicativo Bantotal, se descarga el reporte 4151A sobre Modificaciones de Usuarios y Perfiles que se hayan realizado en el día anterior. Este reporte se descarga y se guarda en los formatos PDF y Excel sin que se realice ninguna modificación sobre esta información.

2. Registro del reporte en el consolidado histórico 4151A con cédula:

   Se registra el reporte 4151A que se descarga diariamente en un archivo Excel que contiene el histórico consolidado que se lleva mensualmente por cada año. En este reporte en especial, se trae la cédula de los usuarios reportados desde el archivo del Directorio Activo para efectos de la validación.

3. Reporte de Novedades de Nomina:

   Por medio del correo electrónico el analista de Talento Humano se encarga de enviar al área de Seguridad de la Información y al CIS, en formato Excel el reporte de los usuarios notificados por cada novedad de nómina: Egresos, cambios de cargo, vacaciones, traslados de agencia, licencias, entre otros.

4. Revisión, descarga y registro del reporte de novedades de nómina:

   Desde el correo electrónico, se revisan y descargan los reportes de cada novedad. Estos se guardan por fecha en la carpeta correspondiente al histórico de cada novedad y en el consolidado de los registros mensuales que se lleva en una matriz de Excel.

5. Depuración del reporte consolidado mensual de las novedades:

   Se crea una copia del consolidado mensual de cada novedad a validar (vacaciones, egresos y cambios de cargo), se eliminan registros repetidos, usuarios sin perfil en Bantotal y las modificaciones en los registros por cambios de fecha reportados.

6. Validación de Novedades de Nómina (Vacaciones, egresos y cambios de cargo):

   En la matriz base para la validación, se insertan los registros a validar de cada novedad ya depurados. Posteriormente, en el consolidado 4151A con cédula, se realiza un rastreo del usuario para verificar si efectivamente se le modificó el perfil de acuerdo con la novedad trayendo el último perfil que se le asignó y la fecha en que se hizo.

7. Medición de demora en reporte de novedades:

   Para cada usuario reportado, se calcula la diferencia entre la fecha efectiva de la novedad y la fecha en que fue reportado por Talento Humano para medir, individualmente y en promedio, el tiempo que se demoró TH en reportar la novedad.

8. Medición de demora en ejecución de novedades:

   Para cada usuario reportado, se calcula la diferencia entre la fecha efectiva de la novedad y la fecha en que se le modificó el perfil en Bantotal para medir, individualmente y en promedio, el tiempo que se demoró el CIS en cambiarle el perfil al usuario conforme a la novedad.

9. Reporte de modificaciones pendientes en Bantotal:

   Los usuarios reportados por TH cuya fecha de inicio de la novedad sea efectiva a la fecha de la validación y aún no se les haya modificado el perfil en Bantotal, deben reportarse como pendientes al analista de seguridad de la información para que este notifique al CIS y los cambios sean ejecutados de manera inmediata.

10. Elaboración del Informe mensual sobre reporte y ejecución oportuna de las novedades de nómina:

    Realizar el cálculo y medición a través de los indicadores de eficiencia y efectividad del proceso, demora y cumplimiento en el reporte de las novedades, desviación ANS y comparativos trimestrales de mejora del proceso junto con observaciones detalladas obtenidas de la validación.

10.1. Revisión del informe: Se revisa que el informe esté elaborado correctamente: cifras, fechas, ortografía y redacción. Si está bien se pasa al punto 11 de lo contrario se pasa al punto 10.2.

10.2. Correcciones y modificaciones: Conforme a las recomendaciones y correcciones señaladas en la revisión, se realizan los cambios sugeridos y se vuelve a revisar el informe. (paso 10.1.)

11. Envío a las áreas relacionadas:

El informe debe enviarse en formato PDF a las áreas correspondientes: Talento Humano y Centro Integral de Servicios para que logren identificar las fallas y situaciones críticas en sus procesos. Además, Se lleva una evidencia de los informes y correos enviados relacionados con la el proceso de validación de usuarios y perfiles.

CONCLUSIONES

El Banco Mundo Mujer es una organización Caucana en crecimiento, que por las características de su actividad económica manipula y administra grandes volúmenes de información y se encuentra expuesta a importantes riesgos asociados a la protección de este intangible.

Por lo anterior, para minimizar la exposición al riesgo y garantizar una correcta y eficiente administración de la seguridad, el Banco, a través del área de Seguridad de la Información, ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI), compuesto por un conjunto de políticas y procesos asociados a la protección y buen uso de la información dentro de la organización.

La Validación de Usuarios y perfiles es un proceso incluido recientemente en el SGSI como mecanismo de control sobre un proceso principal. En vista de que la organización no contaba con la documentación formal de este proceso, se procedió a realizar la construcción del respectivo manual.

De manera exitosa se logró identificar cada uno de los componentes asociados a la Validación de Perfiles, es decir, el objetivo, alcance, la secuencia de actividades, los responsables y las directrices que enmarcan el desarrollo y ejecución de este proceso. Con lo anterior, se llevó a cabo la construcción, documentación y socialización del Manual de procesos para la Validación de Usuarios y Perfiles en el área de Seguridad de la Información del Banco Mundo Mujer

BIBLIOGRAFÍA

Academia Nacional de Ciencias de Estados Unidos. (1991). *Computers at Risk, Safe Computing In the Information Age.* Washington, D.C: National Academy Press. Obtenido de https://www.nap.edu/read/1581/chapter/1#ii

Baskerville, R., Straub, D., & Goodman, S. (2008). *Information Security: Policy, Processes and Practices.* Nueva York: M.E. Sharpe Inc. Obtenido de https://epdf.tips/information-security-policy-processes-and-practices-advances-in-management-infor.html

Banco Mundo Mujer. Obtenido de https://www.bmm.com.co/

Franklin, E. (2009). *Organización de Empresas 3ra Edición.* México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Gómez, W. (2012). *Prácticas Empresariales.* ECOE Ediciones.

Granneman, J. (2013). *IT security frameworks and standards: Choosing the right one.* Obtenido de Tech Target: http://searchsecurity.techtarget.com/tip/IT-securityframeworks-and-standards-Choosing-the-right-one

Höne, K., & Eloff, J. (2002). Política de seguridad de la información: ¿qué dicen las normas internacionales de seguridad de la información? *Computers & Security*, 402-409. Obtenido de https://doi.org/10.1016/S0167-4048(02)00504-7

ISO/IEC 27001. (2013). Tecnología De La Información - Técnicas De Seguridad - Sistemas De Gestión De Seguridad De La Información - Requisitos.

MinTic. (2016). *Guía de Seguridad y provacidad de la Información*. Obtenido de MinTic.gov.co:https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Newman, R. (2009). *Security and Access Control Using Biometric Technologies.* Cengage Learing.

Nnolim, A. (2007). *A framework and methodology for informatio security managemente.* Michigan, Lawrence Technological University, United States: ProQuest Dissertation & Theses. Obtenido de http://gradworks.umi.com/32/96/3296872.html

Pacheco, F. (2010). *La importancia de un SGSI*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

Syalim, A., Hori, Y., & Sakurai, K. (2009). *Comparación de métodos de análisis de riesgo: Mehari, Magerit, NIST800-30 y la Guía de administración de seguridad de Microsoft.* Obtenido de IEEE Xplore Digital Library: https://ieeexplore.ieee.org/document/5066554

Universidad Industrial de Santander. (2016). GESTÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Revisión bibliográfica. *El Profesional de la Información, 25*, 932.

Zapata, B. C., Fernández, A., & Toval, J. L. (2015). Security in cloud computing: A mapping study. *Cumputer Science and information systems, 112*, 161-184. Obtenido de https://doi.org/10.2298/CSIS140205086C

Zarateigui, J. (1999). La gestión por procesos: su papel e importancia en la empresa. *Economía Industrial*, 82. Obtenido de https://www.virtuniversidad.com/greenstone/collect/administracion/import/Cuatrimestre%20X/An%C3%A1lisis%20del%20Entorno%20y%20Estrategia%20Administrativa%20Empresarial/gesti%C3%B3nporprocesos.pdf

ANEXOS

Anexo 1. FORMULARIO PARA LA IDENTIFICACIÓN DE PROCESOS Y PROCEDIMIENTOS

Área _____ **Fecha:** ___/____/____ **N°** 1

Empleado _____ **Cargo:** _____

1. Procedimiento: Validación de Usuarios y Perfiles en Bantotal

1.1.Describa concretamente qué hace:_____

_____

_____

_____

_____

_____

1.2.Cómo lo hace: _____

_____

_____

_____

_____

1.3.Con qué frecuencia:_____

_____

_____

_____

_____

1.4.Responsabilidad del proceso:_____

_____
_____
_____
_____

1.5.Trámite y/o área donde continúa el proceso:

_____
_____

2. Elaboración y trámite documental: Documentos que sirven de enlace o soporte, cómo se elaboran y tramitan.

_____
_____
_____
_____

3. Observaciones:_____
_____
_____
_____

Tramitado por: Ashley Stephany Cubides Valderrama

Fecha de elaboración: 01/10/2018

Firma: _____

Anexo 2. FORMULARIO DE CONTRUCCIÓN DE PROCESOS Y PROCEDIMIENTOS

BANCO MUNDO MUJER S.A.

DD/MM/AA

Proceso: _____

Área/División: _____

2. Describir concretamente las actividades en secuencia del proceso y el responsable.

Cód. de sec	Descripción de la actividad	Responsable	Frecuencia	Salidas

- Cód. se secuencia: Código asignado por actividad secuencial.
- Descripción: Transcripción de cada actividad en la secuencia del proceso conforme a la información entregada por el funcionario ejecutor.
- Responsable: Denominación del cargo responsable de ejecutar cada actividad.
- Frecuencia: Frecuencia con la que debe ser realizada cada actividad: diario, semanal, mensual, etc.
- Salidas: Son los entregables que se generan como resultado de cada actividad.

Anexo 3. Cursos de Inducción al Banco Mundo Mujer

Nombre: CUBIDES VALDERRAMA ASHLEY STEPHANY
Usuario: 1083913513
Cargo:
Fecha de vinculación: Fecha por confirmar
Nivel de Organización: UNASSIGNED
Fecha de finalización: Todo

Título del curso	Fecha de Terminación	Créditos	Puntuación	Puntaje Post-evaluación	Estado
Curso Aprendamos en Familia - BMM	19/07/2018 06:03 PM COT	0.0	100		Terminado
Manual Riesgo Operativo V4	21/08/2018 08:54 AM COT	0.0			Terminado
CODIGO BUEN GOBIERNO	21/08/2018 08:55 AM COT	0.0			Terminado
CODIGO DE CONDUCTA	21/08/2018 08:56 AM COT	0.0			Terminado
REGLAMENTO INTERNO DE TRABAJO	21/08/2018 08:56 AM COT	0.0	100		Terminado
MANUAL SARLAFT V7	21/08/2018 08:57 AM COT	0.0			Terminado
Curso de Sarlaft Basico 2018	21/08/2018 08:59 AM COT	0.0			Terminado
CURSO DE RIESGO OPERATIVO	21/08/2018 09:07 AM COT	0.0	20		Terminado
BMM SAC 2016	21/08/2018 09:11 AM COT	0.0	100		Terminado
MANUAL SAC V6	21/08/2018 09:12 AM COT	0.0			Terminado
CURSO SEGURIDAD DE LA INFORMACIÓN 2016	21/08/2018 09:22 AM COT	0.0			Terminado
REGLAMENTO DE CONVIVENCIA LABORAL	4/10/2018 08:21 AM COT	0.0			Terminado
CURSO PQR MOD 00	4/10/2018 08:30 AM COT	0.0	100		Terminado
CURSO PQR MOD 01	4/10/2018 09:12 AM COT	0.0	100		Terminado
CURSO PQR MOD 02	4/10/2018 09:24 AM COT	0.0	100		Terminado
CONTINUIDAD DEL NEGOCIO	4/10/2018 10:15 AM COT	0.0	100		Terminado
Conflicto de Interés PT 012	4/10/2018 10:24 AM COT	0.0			Terminado
REGLAMENTO DE HIGIENE Y SEGURIDAD INDUSTRIAL	4/10/2018 10:29 AM COT	0.0			Terminado