



Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Centro de Investigación en Sistemas de Información

**Desarrollo de una Guía de Implementación
para un Sistema de Gestión de la Seguridad
de la Información Mediante el Uso de la
ISO 27001 y la Gestión de Procesos de Negocio**

Trabajo Especial de Grado
presentado ante la Ilustre
Universidad Central de Venezuela
por los Bachilleres
José Gabriel Castro Lazo C.I. 24635905
Joaquín Miguel Molina Waldrop C.I. 25156295
para optar al título de
Licenciados en Computación

Prof(a). Mercy Ospina
Prof. Franky Uzcategui

Caracas, 17 / 05 / 2017

UNIVERSIDAD CENTRAL DE VENEZUELA

FACULTAD DE CIENCIAS

ESCUELA DE COMPUTACIÓN

ACTA

Quienes suscriben, miembros del jurado designado por el Consejo de la Escuela de Computación, para examinar el Trabajo Especial de Grado titulado **"Desarrollo de una guía de implementación para un SGSI mediante el uso de la ISO 27001 y la gestión de procesos de negocio"** y presentado por los bachilleres: Br. José Castro Lazo y Br. Joaquin Molina, a los fines de optar al título de **Licenciado en Computación**, dejamos constancia de lo siguiente:

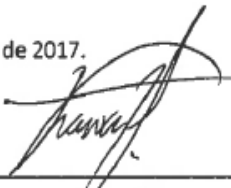
Leído como fue dicho trabajo, por cada uno de los miembros del jurado, se fijó el día 17 de Mayo de 2017, a las 11:00 horas, para que los autores lo defendieran en forma pública, lo que estos hicieron en la Sala PBIII de la Escuela de Computación, mediante una presentación oral de su contenido, luego de lo cual respondieron a las preguntas formuladas. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobar con la nota de 20 puntos.

En fe de lo cual se levanta la presente Acta, en Caracas el día 17 de Mayo de 2017.



Profa. Mercy Ospina

(Tutora)



Prof. Franky Uzcategui

(Tutor)



Prof. Franklin Sandoval

(Jurado)



Prof. José Mirabal

(Jurado)

AGRADECIMIENTOS

A Dios Nuestro Señor, por habernos dado la vida, por ser nuestra guía, por darnos la fortaleza para seguir adelante y permitirnos llegar hasta este momento tan importante de nuestra formación profesional.

A nuestros padres por ser nuestro apoyo durante estos largos años de formación profesional.

A nuestros colegas y compañeros de la Universidad. Gracias a ellos esta etapa estuvo llena de buenos y divertidos momentos.

A nuestros Tutores, Franky y Mercy, por confiar y creer en nosotros para la realización de este proyecto. Por todo su tiempo dedicado, por sus palabras y consejos.

Y por último, pero no menos importante, a nuestra Universidad, la UCV, por brindarnos la oportunidad de poder vivir esta etapa de crecimiento personal y profesional dentro de sus aulas de clase y por ser testigo y escenario de vernos convertidos en Licenciados en Computación.

Universidad Central de Venezuela.
Facultad de Ciencias
Escuela de Computación
Centro de Investigación de Sistemas de Información

Desarrollo de una guía de implementación para un Sistema de Gestión de la Seguridad de la Información mediante el uso de la ISO 27001 y la Gestión de Procesos de Negocio

Autor(es): José Castro Lazo.
Joaquin Molina.

Tutores: Prof(a). .
Prof. Franky Uzcategui.

Fecha: Mayo de 2017.

RESUMEN

El presente Trabajo Especial de Grado tiene como finalidad la realización de una guía basada en buenas prácticas y normas especializadas en la seguridad de la información, que permita la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de cualquier organización, haciendo uso de la Gestión de Procesos de Negocios para visualizar, orquestar e implementar esta metodología. Esta propuesta está sustentada por el estudio e investigación de las Instituciones Normalizadoras Internacionales más reconocidas y las normas y estándares más utilizados por las organizaciones a nivel mundial, fundamentando de esta forma, la utilización de la ISO 27001 como la mejor opción entre dichas normas y estándares. Este documento hace énfasis en el dominio de control de acceso (uno de los catorce dominios que define la ISO 27001), identificando a los sistemas de información de las organizaciones como uno de sus mayores activos y basándose en el hecho de que el control de acceso es el aspecto más penetrante y omnipresente en la seguridad de la información, y por lo tanto no puede ser ignorado a la hora de implementar un SGSI. La aplicación que se desarrolló usando la herramienta Bonita BPM, hace uso de posiciones funcionales, con el fin de que los usuarios seleccionen “lo que son” y no lo que desean, lo que hace al sistema más intuitivo y rápido de usar, además de cumplir con los objetivos del control de acceso. Se emplea un marco de trabajo basado en las mejores prácticas del ciclo de vida BPM propuesta por (Smith & Fingar, 2003) la cual contempla las fases de descubrimiento, modelado, ejecución, despliegue, monitoreo y optimización. Del trabajo se concluyó que al acoplar un estándar como lo es ISO 27001 y la Gestión de Procesos de Negocio para ayudar a la organización en la Gestión de la Seguridad de la Información, brinda numerosos beneficios tanto en etapas tempranas del proyecto como en la planificación, así como en la ejecución y optimización ya que el enfoque de BPM y la ISO 27001 (siguiendo PDCA Plan-Do-Check-Act) conducen hacia la mejora continua. En el caso específico del control de acceso se logra un control eficiente en todas las partes del proceso, identificación de los participantes, procedimentación de sus actividades, cumplimientos de los acuerdos de nivel de servicio y las mejoras continuas.

Palabras Claves: ISO 27001, Sistema de Gestión de la Seguridad de la Información, Procesos, Gestión de Procesos de Negocio, Seguridad de la Información, Control de Acceso, Bonita BPM

Índice de Contenido

Introduccióni

CAPÍTULO 1 PROBLEMA DE INVESTIGACIÓN1

1.1. Planteamiento del problema1

1.2. Objetivos del TEG2

1.2.1. Objetivo General2

1.2.2. Objetivos Específicos2

1.3. Solución propuesta y alcance3

1.4. Justificación4

Capítulo 2 Marco Conceptual7

2.1. Información7

2.2. Seguridad de la información8

2.2.1. Confidencialidad, Integridad y Disponibilidad8

2.2.2. Impacto de un incidente de seguridad9

2.3. Gestión de la seguridad de la información10

2.3.1. Beneficios de gestionar la seguridad de la información12

2.4. Instituciones Normalizadoras Internacionales12

2.4.1. ITU-T12

2.4.2. ISO/IEC13

2.4.3. CEN/CENELEC13

2.5. Normas Internacionales de Evaluación y Certificación14

2.5.1. TCSEC (Libro naranja)14

2.5.2. ITSEC16

2.5.3. ISO/IEC 2700017

2.6. ISO 2700118

2.6.1. Dominios19

2.6.2. Beneficios de implementar la ISO 2700121

2.6.3. Como adaptarse a la ISO 2700121

2.7. Procesos de Control de Acceso29

2.7.1. Proceso29

2.7.2. Actividad30

2.7.3. El proceso y el procedimiento31

2.7.4. Características de los procesos31

2.7.5. Componentes de los procesos31

2.7.6. Tipos de procesos32

2.8. Gestión por procesos33

2.8.1. Diferencias entre gestión por funciones y gestión por procesos34

2.8.2. Objetivos de la gestión por procesos34

2.8.3. Beneficios de la gestión por procesos35

2.9. Gestión de Procesos de Negocio (BPM)35

2.9.1. Consideraciones de BPM	35
2.9.2. Historia y evaluación de BPM	36
2.9.3. Principales funcionalidades	36
2.9.4. Principales beneficios de BPM	37
2.9.5. BPMN	37
2.9.6. Herramientas BPM (Business Process Management Suites)	44
2.10. Proceso de control de acceso lógico	45
2.10.1. Dominio de control de acceso	46
2.10.2. Control de acceso lógico	46
2.10.3. Proceso de control de acceso	47
2.10.4. Política de control de acceso	48
2.10.5. Retos del proceso de control de acceso	48
2.10.6. Ventajas del proceso de control de acceso	49
2.10.7. Elementos del proceso de control de acceso	49
2.11. Estado del arte	50
2.11.1. Descripción del proceso de solicitudes de accesos de la plataforma Ultimus	50
2.11.2. Descripción del proceso de solicitudes de accesos de la plataforma Bizagi	53
2.12. Modelo propuesto	53
2.12.1. Doble participación	54
2.12.2. Posición Funcional	54
2.12.3. Perfilamiento Corporativo	54
Capítulo 3 Marco Metodológico	57
3.1. Metodología de desarrollo	57
3.1.1. Descubrimiento	58
3.1.2. Modelado	58
3.1.3. Despliegue	59
3.1.4. Ejecución	59
3.1.5. Monitoreo	59
3.1.6. Optimización	60
Capítulo 4 Marco Aplicativo	61
4.1. Sistema de solicitudes de acceso	61
4.2. Herramientas tecnológicas	61
4.2.1. Bonita BPM	61
4.2.2. Servicios Web	64
4.2.3. MySQL	65
4.3. Etapas del proyecto	66
4.3.1. Descubrimiento	66
4.3.2. Modelado	69
4.3.3. Despliegue	106
4.3.4. Ejecución	109

Conclusiones	121
4.4. Recomendaciones	121
Bibliografía	123

Índice de Figuras

Ilustración 1 Arquitectura de la solución	4
Ilustración 2 Los tres pilares de la Seguridad de Información	9
Ilustración 3 Impacto de un incidente de Seguridad	10
Ilustración 4 Dominios de la Seguridad de la Información	11
Ilustración 5 Alcance de la ISO 27001 con respecto a otras normas y regulaciones	19
Ilustración 6 Circulo de mejora continua para la implementación de un SGSI	22
Ilustración 7 Arranque del proyecto	23
Ilustración 8 Planificar	25
Ilustración 9 Implementar	26
Ilustración 10 Seguimiento	27
Ilustración 11 Mejora continua	28
Ilustración 12 Adaptación del SGSI en BPMN	28
Ilustración 13 Adaptación del SGSI en BPMN - Seguimiento	29
Ilustración 14 ¿Qué es un proceso?	30
Ilustración 15 Tipos de procesos	33
Ilustración 16 Orquestación	38
Ilustración 17 Coreografía	39
Ilustración 18 Colaboración	40
Ilustración 19 Formulario de solicitud de Perfiles de Acceso de Ultimus	51
Ilustración 20 Estatus del Incidente	52
Ilustración 21 Gráfico del Estatus del Incidente	52
Ilustración 22 Flujo de Solicitud de Accesos propuesto por Bizagi	53
Ilustración 23 Proceso de control de acceso propuesto (Flujo básico)	56
Ilustración 24 Proceso de control de acceso propuesto (Cancelación)	56
Ilustración 25 Ciclo de vida BPM	58
Ilustración 26 Bonita BPM Studio	63
Ilustración 27 Bonita BPM Portal	63
Ilustración 28 Diagrama de arquitectura de un cliente REST integrado con Bonita BPM (Bonitasoft, 2017)	64
Ilustración 29 Interoperabilidad de los Servicios Web (W3C)	65
Ilustración 30 Estructura de la base de datos para el control de acceso	70
Ilustración 31 Servicios web con endpoints	71
Ilustración 32 Canales del proceso de control de acceso	72
Ilustración 33 Modelos de datos de negocio	73

Ilustración 34 Variables de negocio73

Ilustración 35 contrato de instanciación del proceso74

Ilustración 36 Inicialización de las variables del contrato de instanciación74

Ilustración 37 Creación de actividades para el formulario de inicio75

Ilustración 38 Formulario para generar solicitud de acceso desde UI Designer75

Ilustración 39 Envelope para la generación de una nueva solicitud de accesos76

Ilustración 40 Script para generar cuerpo de correo electrónico a solicitante76

Ilustración 41 Script que retorna los datos del endpoint *obtenerMAtrizPorSolicitud*77

Ilustración 42 Revisión de formulario78

Ilustración 43 Condición de temporizador para enviar recordatorio al aprobador78

Ilustración 44 Habilidad del flujo de delegado de aprobación79

Ilustración 45 Formulario de la tarea “Revisar solicitud” y “Revisar solicitud (Delegado)”80

Ilustración 46 Flujo del proceso según la revisión del aprobador80

Ilustración 47 Expresión de condición de ¿Solicitud aprobada?81

Ilustración 48 Envelope para actualizar la solicitud rechazada82

Ilustración 49 Script cuerpo de correo de rechazo de solicitud82

Ilustración 50 Envelope para actualizar la solicitud aprobada83

Ilustración 51 Script cuerpo de correo de aprobación de solicitud para el solicitante83

Ilustración 52 Flujo del administrador84

Ilustración 53 Script para buscar correos de los Administradores85

Ilustración 54 Contrato de la actividad “Administrar accesos”85

Ilustración 55 Operaciones en la actividad “Administrar accesos”86

Ilustración 56 Script que actualiza la matriz de control de acceso de una solicitud86

Ilustración 57 Formulario de la tarea “Administrar accesos”87

Ilustración 58 Elementos ocultos en el UI Designer87

Ilustración 59 Expresión de iteración de la actividad “Guardar accesos administrados”88

Ilustración 60 Envelope para gestionar los accesos en la matriz de control de acceso89

Ilustración 61 Script que actualiza el estado de la solicitud en el carril del Administrador89

Ilustración 62 Expresión de condición de ¿Quedan accesos por administrar?90

Ilustración 63 Flujo al finalizar la gestión por parte del administrador91

Ilustración 64 Envelope para gestionar la solicitud por parte del administrador91

Ilustración 65 Flujo del verificador92

Ilustración 66 Script para buscar correos de los Verificadores92

Ilustración 67 Contrato de la actividad “Verificar accesos”93

Ilustración 68 Operaciones de la actividad “Verificar accesos”93

Ilustración 69 Script que actualiza la matriz de control de acceso de una solicitud verificada94

Ilustración 70 Formulario de la tarea “Verificar accesos”95

Ilustración 71 Flujo de devolución de solicitud95

Ilustración 72 Cuerpo de correo de devolución de solicitud96

Ilustración 73 Expresión de iteración de la actividad “Guardar accesos verificados”97

Ilustración 74 Envelope para verificar los accesos en la matriz de control de acceso97

Ilustración 75 Script que actualiza el estado de la solicitud en el carril del Verificador97

Ilustración 76 Expresión de condición de ¿Quedan accesos por verificar?98

Ilustración 77 Flujo al finalizar la verificación por parte del verificador99

Ilustración 78 Envelope para finalizar una solicitud99

Ilustración 79 Flujo del proceso de cancelación de solicitud100

Ilustración 80 Query para obtener la información de una solicitud por su id100

Ilustración 81 Contrato de instanciación del proceso de cancelación101

Ilustración 82 Inicialización del contrato101

Ilustración 83 Información obtenida del servicio web para realizar la cancelación102

Ilustración 84 Expresión de la condición de ¿Solicitud aprobada?103

Ilustración 85 Flujo de cancelación si la solicitud tiene estado “Pendiente”103

Ilustración 86 Mensaje a enviar al otro Pool104

Ilustración 87 Correlación entre las dos instancias104

Ilustración 88 Captura de mensaje y correlación en el “proceso de solicitud de acceso”105

Ilustración 89 Envelope para cancelar una solicitud105

Ilustración 90 Script que genera cuerpo de correo de cancelación al aprobador106

Ilustración 91 Exportar página “ControlAccesoHome”106

Ilustración 92 Agregar página como un recurso en el portal107

Ilustración 93 Formulario de creación de una aplicación en el portal108

Ilustración 94 Formulario para añadir una página a una aplicación108

Ilustración 95 “ControlAccesoHome” como página de inicio de la aplicación109

Ilustración 96 Página de inicio (solicitante)109

Ilustración 97 formulario de solicitud110

Ilustración 98 lista de usuarios desplegada en el formulario de solicitud110

Ilustración 99 correo electrónico enviado al solicitante111

Ilustración 100 correo electrónico enviado al supervisor del solicitante111

Ilustración 101 listado de solicitudes pendientes112

Ilustración 102 listado de solicitudes completadas112

Ilustración 103 listado de solicitudes por aprobar113

Ilustración 104 formulario de aprobación113

Ilustración 105 Correo electrónico enviado a los administradores114

Ilustración 106 listado de solicitudes por gestionar114

Ilustración 107 Formulario de administración115

Ilustración 108 listado de solicitudes por gestionar (previo guardado)115

Ilustración 109 formulario de administración (previo guardado)116

Ilustración 110 listado de solicitudes por verificar116

Ilustración 111 formulario de verificación117

Ilustración 112 Correo Electrónico de devolución117

Ilustración 113 listado de solicitudes por gestionar (previa devolución)117

Ilustración 114 formulario de administración de una solicitud devuelta118

Ilustración 115 formulario de verificación de la solicitud devuelta118

Ilustración 116 solicitudes completadas (incluida la solicitud finalizada)119

Ilustración 117 listado de solicitudes por gestionar (solicitud de remoción)119

Ilustración 118 listado de solicitudes completadas con los 3 posibles estados120

Ilustración 119 Correo electrónico de rechazo de solicitud120

Índice de Tablas

Tabla 1 Cantidad de certificaciones ISO 27001 por región5

Tabla 2 Referencia entre criterios ITSEC y claves TCSEC.17

Tabla 3 Diferencias entre gestión funcional y gestión por procesos34

Tabla 4 Elementos básicos de modelado41

Tabla 5 Comparación entre BPMS's Open Source45

Tabla	6	Flujo	diseñado	en	la	fase	de	descubrimiento	67
-------	---	-------	----------	----	----	------	----	----------------	----

INTRODUCCIÓN

Las organizaciones cada vez son mas competitivas, el mercado padece cambios continuamente y el cliente es cada vez mas exigente. Es por ello que la sostenibilidad de las mismas se ha hecho mucho mas compleja y ahora se enfrentan a demandas de rentabilidad, calidad y seguridad de un mayor nivel. La norma internacional ISO 27001 ayuda a establecer un SGSI (Sistema de Gestión de Seguridad de la Información) eficiente que permite convertir estas demandas en una ventaja competitiva frente a otras organizaciones con misiones parecidas.

Para poder enfrentar todos los retos que se presentan, las organizaciones deben desarrollar procesos y estándares que midan y cumplan con dichos estándares, además de integrar todos los principios de negocio en los Sistemas de Gestión. Actualmente, la ISO 27001 es la norma más popular y utilizada por las organizaciones para implementar su Sistema de Gestión de Seguridad de la Información, de hecho, con solo 27.536 organizaciones certificadas en el año 2015 (Datos de la encuesta realizada por ISO anualmente, o, *Survey data*¹), está entre los tres estándares ISO más famosos. (ISO, 2017)

Implementar un SGSI mediante la metodología propuesta en ISO 27001 permite la mejora continua de los departamentos de la organización, relacionadas con la información de mayor importancia para la alta gerencia de la misma. Un Sistema eficaz de Gestión de Seguridad de la Información según ISO 27001, tiene como finalidad, generar valor añadido a las organizaciones, ya que les permiten realizar sus procesos de una forma mucho más económica y rápida.

La ISO 27001 no es una norma aislada, puede ser combinada con otras normas, metodologías y mejores prácticas para aprovechar aún más sus bondades, como es el caso de la ISO 9000 que hace referencia a la Gestión de Calidad o con otros conceptos como la Gestión de procesos de negocio.

En esta investigación se aprovecharon las ventajas y el auge que ha tomado la gestión por procesos, la cual se basa en una serie de procesos que interfieren y/o interactúan entre otros con la misma finalidad, alcanzar los objetivos planteados por la organización, y generar de esta forma, mejoras en la eficiencia y la eficacia de la gestión empresarial.

La Gestión de Procesos de Negocio o BPM (Business Process Management) nace como un marco de trabajo dentro de la ciencia de la computacion y es un enfoque empresarial operativo basado en la coordinación de las actividades y decisiones que deben realizar todas las partes involucradas durante un proceso de negocio, con el objetivo de convertirse en una organización altamente eficiente, agil, innovadora y adaptable.

¹ ISO Survey data (ISO, 2017)

El objetivo de este trabajo de investigación es plantear los lineamientos necesarios para poder implementar un Sistema de Gestión de la Seguridad de la Información apoyándose en la metodología BPM para representar cada uno de los procesos que complementan al mismo.

El presente documento está compuesto por cuatro capítulos que se describen a continuación:

Capítulo 1: Se describe el Problema de Investigación, donde se detalla la situación actual de como algunas organizaciones llevan a cabo una mala gestión de los procesos y controles necesarios para el correcto funcionamiento de un SGSI, como por ejemplo, su proceso de control de acceso lógico y los problemas que presentan, y a su vez se detalla la propuesta que busca solventar dichos problemas. Además, se desarrollan el objetivo general y los objetivos específicos del presente trabajo de investigación, junto con la Justificación de la solución propuesta.

Capítulo 2: En este capítulo se definen los conceptos y conocimientos que fueron utilizados para llevar a cabo la solución propuesta. Se describe que es la seguridad de la información, los conceptos ligados a la misma, así como los riesgos y las ventajas de implementar o no un SGSI. Se detallan algunas de las Normas Internacionales más reconocidas a nivel de seguridad de la información, entrando a fondo con la norma ISO 27001. Se definen otros conceptos como procesos, como estos se gestionan y sus características; más adelante se profundiza en lo que respecta a la Gestión de Procesos de Negocio (BPM), definición, notación BPMN, su ciclo de vida y beneficios; luego se introduce Bonita BPM, la cual es la plataforma utilizada para el desarrollo de la aplicación.

Capítulo 3: Comprende el Marco Metodológico de la investigación. En el mismo se explica la metodología utilizada en el desarrollo del trabajo.

Capítulo 4: En este último capítulo se presenta el Marco Aplicativo, donde se detalla el diseño de la solución propuesta para responder así al objetivo general y a los objetivos específicos planteados.

Por último, se exhiben las conclusiones y las referencias bibliográficas utilizadas para el desarrollo del Trabajo Especial de Grado.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

El presente capítulo tiene como finalidad desarrollar el contexto del problema, explicando como algunas de las organizaciones de hoy en día, no gestionan bien sus procesos, más específicamente, los procesos ligados a la seguridad de la información, como el control de acceso, gestión de riesgos, políticas de seguridad, entre otros. Esto trae como consecuencia que las vulnerabilidades que presenten los activos sean explotadas por una o más amenazas que se presenten y se transformen en daños al sistema o a la organización a nivel operacional, de reputación o financiero. Con la exposición del problema se quiere plantear el uso de un SGSI para garantizar de esta forma la seguridad de la información haciendo uso de una herramienta que sirva como guía para dicha implementación.

Adicionalmente se describe el objetivo general de la investigación y el camino que hay que seguir para conseguir dicho objetivo a través de los objetivos específicos. Por último, se relata la justificación del por qué se ha de implementar un SGSI siguiendo la metodología propuesta por la ISO 27001 y apoyándose sobre la gestión de procesos de negocios para el descubrimiento, modelado y ejecución de los procesos necesarios para solucionar el problema planteado, también se justifica el por qué se utiliza la herramienta Bonita BPMS, especializada en la automatización y modelado de procesos que apoya la metodología BPM.

1.1. Planteamiento del problema

Para muchas organizaciones, la información es el activo más importante y decisivo para su viabilidad. La información puede adoptar diferentes formas, puede estar impresa, escrita en papel, digital, transmitida por correo, mostrada en videos o hablada en conversaciones.

Debido a la alta disponibilidad que esta presenta en ambientes cada vez más interconectados, se ve más expuesta a amenazas y vulnerabilidades que la puedan destruir, modificar, perder, o darle un uso indebido que perjudique a la organización ya sea a nivel financiero o de reputación.

Las personas juegan un papel primordial para las organizaciones ya que son estas las encargadas de dar significado a dicha información. Sin las personas no se podría dar forma a símbolos y datos, ni procesarlos o tomar decisiones a partir de ellos. Es por esto que, aunque sean otro activo importante, también representan un riesgo fundamental para las organizaciones.

Entonces, las organizaciones se ven en la necesidad de aumentar el control sobre las actividades que realizan las personas diariamente. Sin embargo, surge otro problema que puede ser representado con la siguiente interrogativa: ¿Es posible controlar las intenciones de las personas? La respuesta es no, y por ello se requiere ir más allá.

Otro problema que se tiene actualmente, es debido a que las organizaciones se precipitan a lanzar o adquirir productos y servicios sin tomar en cuenta los aspectos de seguridad tratando de escapar de

la obsolescencia tecnológica o debido a temas de competitividad con otras empresas, muchas veces con la promesa de que en el camino se mejoraran dichos aspectos de seguridad.

Es muy común que, en las organizaciones, la alta gerencia y los encargados de la seguridad de la información no estén alineados, ya sea porque los oficiales de seguridad no le hacen entender los riesgos que corre la organización en temas de seguridad a nivel del negocio, o simplemente la alta gerencia no le da la importancia que el tema amerita. Una de las causas de esto es que la seguridad de la información depende en gran parte de la prevención, y las empresas consideran este tópico cuando se genera algún incidente potencial y no antes de su ocurrencia.

Por ejemplo, se pueden dar situaciones donde se esté desarrollando un sistema para uso interno de la organización, donde el área de seguridad se percata de algunas brechas o vulnerabilidades, sin embargo, para la alta gerencia la usabilidad es más importante que la seguridad y deciden aceptar dichos riesgos. Es aquí donde entran al juego los hackers o cualquiera de sus derivaciones, los cuales tienen distintas motivaciones dependiendo de su caso particular como lo son: demostrar su dominio, hacer alarde de sus habilidades, venganza (muy común en los ataques internos), creatividad mal enfocada, malversación de fondo o la codicia.

Existen otras razones por las cuales la seguridad es ignorada o pasa a un segundo plano como:

- La cuota de mercado es más importante que la seguridad
- El diseño de la interfaz es más importante que la seguridad
- Los nuevos diseños de características son más importantes que la seguridad
- La usabilidad es más importante que la seguridad

Por todo lo anterior, se generó en las organizaciones la necesidad, en poca o gran medida, de una forma de gestionar la seguridad de la información. Es aquí donde surgen las normas y recomendaciones internacionales y locales que promueven y estandarizan formas de realizar dicha gestión. Las organizaciones pueden escoger cuál de estas seguir basándose en la que mejor se adapte a las necesidades y requisitos de la misma. Sin embargo, algunas de estas normas necesitan de personal especializado y de auditorías muy costosas que certifiquen que están cumpliendo con todas las especificaciones de una norma. De este punto, surge la problemática que se busca atacar en este trabajo de investigación, la cual es la necesidad de tener una herramienta que sirva de guía rápida y eficiente en la implementación de un SGSI dictada por una norma dentro de una organización.

1.2. Objetivos del TEG

1.2.1. Objetivo General

Desarrollar una guía de implementación para un SGSI mediante el uso de la ISO 27001 y la gestión de procesos de negocio.

1.2.2. Objetivos Específicos

- Recolectar información acerca de los estándares, normas y mejores prácticas de la gestión de la seguridad de la información en una organización.

- Describir los pasos a seguir para llevar a cabo la implementación de un SGSI.
- Modelar el proceso de control de acceso lógico a través de la herramienta Bonita, utilizando el estándar BPMN.
- Diseñar las pantallas y formularios que servirán de interacción entre los participantes y el proceso.
- Definir y configurar las reglas de negocio asociadas al proceso de control de acceso lógico.
- Configurar y ejecutar el proceso modelado en el portal de aplicaciones de la herramienta Bonita.

1.3. Solución propuesta y alcance

Como ya se mencionó, la ISO 27001 describe las buenas prácticas para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), esta norma es avalada mundialmente y al ser promovida por la ISO da valor agregado a organizaciones que pueden demostrar dentro de sus procesos la aplicación de estas buenas prácticas a través de los catorce dominios que define la ISO 27000. Cubrir en su totalidad los catorce dominios de la seguridad de la información dentro de la organización requiere de un trabajo arduo de definición, implementación, ejecución y mejora de los procesos que soporten cada uno de ellos. Entendiendo esto, se decidió implementar el proceso de solicitudes de accesos de los activos de una organización, como parte del dominio de control de acceso, siguiendo los lineamientos descritos en la ISO 27001 y utilizando una plataforma de Gestión de Procesos de Negocio (BPM), y con el respaldo de una metodología que permite definir, modelar, implementar, automatizar y mejorar el proceso continuamente.

¿Por qué empezar con el Dominio de control de acceso?

A pesar de que una organización pudiese dar motivos suficientes para no implementar uno o más dominios del SGSI, esto no ocurre con el dominio de control de acceso, ya que el mismo es un aspecto omnipresente dentro del área de la seguridad de la información. El dominio de control de acceso es transversal al resto de los dominios, y se debe contar con él para realizar una implementación correcta y eficiente.

Ejemplos claros de esto se pueden ver en la relación directa que tiene con otros dominios como las Políticas de Seguridad de la Información, donde se tiene un documento que puede especificar los métodos por los cuales un empleado dentro de una organización obtiene accesos a los distintos componentes. Otro caso, se da en el dominio de Seguridad de los Recursos Humanos, donde se plantea que los empleados que sean trasladados de departamento o abandonen a la organización por cualquier motivo, se les debe realizar una evaluación de sus accesos para adaptarlos a la nueva posición funcional o removerlos en su totalidad de ser necesario.

La ilustración 1 describe la estructura de la solución propuesta, la cual tiene como núcleo al motor de ejecución de Bonita BPM que se encarga de gestionar el proceso, las tareas, los usuarios, eventos, entre otros. Esta se comunica a entes como el servidor SMTP (para el envío de las notificaciones dentro del proceso) y servicios web (donde se encuentra información de la organización como las

posiciones funcionales, perfiles, tipos de solicitud y la matriz de control de acceso) mediante los conectores de Bonita. Finalmente, se tiene la aplicación que utiliza las APIs REST de Bonita para mostrarles a los usuarios de forma más usable y centralizada sus solicitudes de acceso pendientes y completadas dentro del sistema. La aplicación también permite a los usuarios con perfil de aprobador, administrador o verificador ver y disparar las tareas que se encuentren pendientes dentro de su bandeja de entrada.

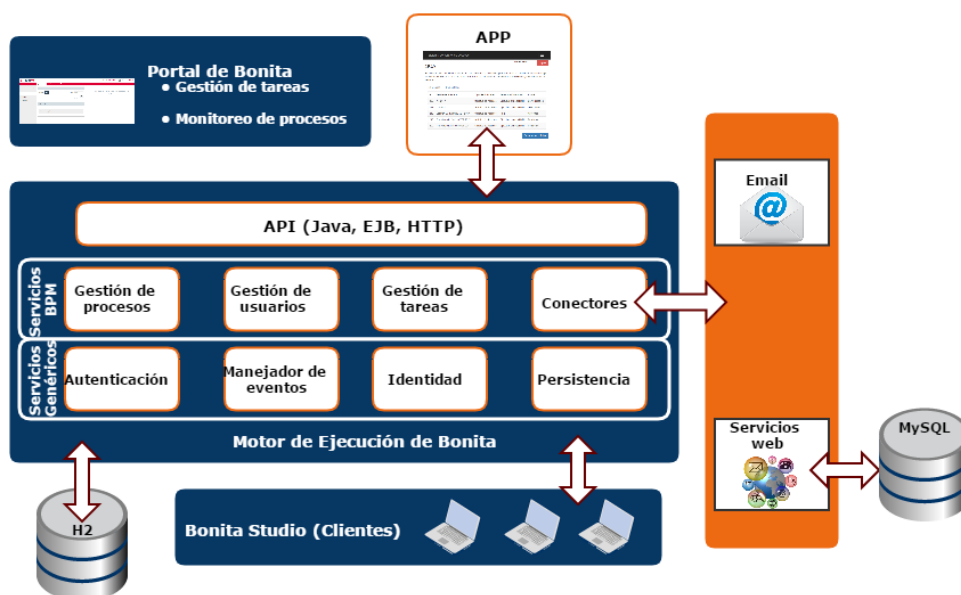


ILUSTRACIÓN 1 ARQUITECTURA DE LA SOLUCIÓN

Las herramientas tecnológicas utilizadas para llevar a cabo esta propuesta son:

- Bonita BPM Studio
- Portal Bonita BPM
- Base de datos de prueba H2
- Servicios web sobre Java
- Servidor Glassfish para los servicios web
- Base de datos MySQL para los servicios web

1.4. Justificación

Según (Baldecchi Q., 2014), La seguridad de información es proteger la información de un amplio rango de amenazas para garantizar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de las inversiones en las oportunidades de negocio.

La protección de la información se va logrando mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos, organización, controles, hardware y software y, lo más importante, mediante comportamientos éticos de las personas.

Todos estos puntos pueden unificarse a través de un sistema de gestión. Por ello, se plantea el uso de la metodología de la gestión de la seguridad de la información propuesta por la ISO, ISO 27001, la cual a través de sus catorce dominios provee una serie de normas y controles que ayudan en el cumplimiento de los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

La norma ISO 27001 acoge un proceso que está enfocado en establecer, implementar, revisar, mantener y mejorar un SGSI en la organización y actualmente es el estándar más utilizado para la certificación. (ISOTools Excellence, 2015)

La Tabla 1, muestra el crecimiento progresivo de la cantidad de empresas certificadas en ISO 27001 en los últimos 4 años encuestados por (ISO, 2017).

TABLA 1 CANTIDAD DE CERTIFICACIONES ISO 27001 POR REGIÓN

Año	2012	2013	2014	2015
TOTAL	19620	21604	23005	27536
África	64	99	79	129
América Central y del Sur	203	272	273	347
Norte América	552	712	814	1445
Europa	6379	7952	8663	10446
Asia Oriental y el Pacífico	10422	10116	10414	11994
Asia Central y del Sur	1668	2002	2251	2569
Oriente Medio	332	451	511	606

FUENTE: (ISO, 2017)

BPM se ha convertido en una herramienta de confianza para las organizaciones a la hora de buscar soluciones a diversos problemas que surgen a partir de un mercado altamente congestionado y competitivo. BPM, es la combinación de estrategias, procesos, métodos y tecnologías que una organización implementa como solución para el desarrollo de procesos.

Una herramienta BPM da soporte completo al ciclo de vida de un proceso de negocio, desde su análisis hasta la mejora continua producto de la fase de optimización, permitiendo a las organizaciones definir de manera más formal y completa sus procesos, replantearlos de forma más rápida y efectivamente, reducir las tareas humanas pudiendo ejecutar procesos de manera automática, analizar tiempos de ejecución, detectar actividades redundantes, entre otros beneficios.

Por tanto, se planteó el uso de la metodología BPM a través de Bonita para ayudar con la guía de implantación de un SGSI en cualquier organización. Bonita es una herramienta BPM bastante

completa, y que tiene un crecimiento importante actualmente en el mercado. Proporciona una documentación muy completa y, además, tiene una comunidad muy activa de la cual se puede sacar mucho provecho en sus foros.

CAPÍTULO 2

MARCO CONCEPTUAL

El propósito de este capítulo es presentar los conocimientos utilizados como base teórica para el desarrollo del Trabajo Especial de Grado. De esta forma, el capítulo comienza con la definición de información desde la perspectiva de activo en las organizaciones. Seguidamente se desarrolla como tal la Seguridad de la información, lo que esta busca preservar y que impacto puede causar un incidente de seguridad.

Luego, se describe la gestión de la seguridad de la información junto con los beneficios que se desprenden de su realización. A su vez, se detallan las Instituciones Normalizadoras Internacionales y las Normas Internacionales de Certificación más reconocidas y utilizadas por las organizaciones. Esto, para poder dar introducción al tema central de la investigación la cual es la utilización de la norma ISO 27001 como metodología para la implementación de un SGSI basado en buenas practicas.

Adicionalmente, se define el término proceso y los elementos que interactúan con este para obtener un resultado. Por otra parte, se hace referencia a fondo del proceso de control de acceso, el cual es uno de los catorce dominios que presenta la ISO 27001 como requerimientos para la implementación del SGSI.

En la siguiente sección se introduce el concepto de gestión por procesos, se visualizan los objetivos que este persigue y los beneficios de esta forma de gestión en contraste con la gestión tradicional.

Luego, se explica el concepto de Gestión de Procesos de Negocio (BPM) y el origen y evolución del mismo. Se detallan sus beneficios y los entandares en los que se sustenta el desarrollo de una aplicación BPM. Se establece un cuadro comparativo entre algunas plataformas tecnológicas y se explica la seleccionada para el desarrollo de la solución, describiendo sus componentes y principales características.

Para finalizar, se muestra la complicación de resultados de otras investigaciones y soluciones, así como el modelo que propuso este trabajo de investigación.

2.1. Información

Es un activo que, como otros activos importantes del negocio, tiene valor para una organización y por lo tanto necesita ser protegido adecuadamente. (ISO, 2005)

La información puede ser:

- Creada
- Almacenada
- Destruída
- Procesada

- Transmitida
- Usada para fines correctos e incorrectos
- Perdida
- Sustraída
- Impresa o escrita en papel
- Transmitida por correo postal o electrónico
- Mostrada en videos
- Mostrada/publicada por la web
- Verbal

2.2. Seguridad de la información

La seguridad de la información es la preservación de la Confidencialidad, la Integridad y la Disponibilidad (BS Grupo, 2014). Esto se va logrando mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos, organización, controles, hardware y software y, lo más importante, mediante comportamientos éticos de las personas. (Baldecchi Q., 2014)

El propósito de la Seguridad de la Información es proteger los recursos valiosos de una organización, como la información, el hardware y el software contra una amplia gama de amenazas; para minimizar los daños, ampliar las oportunidades del negocio, maximizar el retorno de la inversión y garantizar la continuidad del negocio. A través de la selección y aplicación de las medidas apropiadas, la seguridad de la información ayuda a la misión de la organización mediante la protección de sus recursos físicos y financieros, la reputación, la posición legal, empleados y otros bienes tangibles e intangibles.

2.2.1. Confidencialidad, Integridad y Disponibilidad

De acuerdo (Hernandez, 2012), lo que tienen en común los objetivos de la seguridad de la información es que se dirigen al menos a uno de los principios básicos de seguridad: confidencialidad, integridad y disponibilidad, mejor conocido como CIA (*Confidentiality, Integrity, Availability*). En la Ilustración 2 se puede ver como estos tres principios forman la base de la Seguridad de la Información

- Confidencialidad: se refiere al esfuerzo empleado en evitar la divulgación no autorizada de la información a quienes no la necesitan, o el derecho para verla.
- Integridad: se refiere al esfuerzo empleado en evitar la modificación no autorizada o incorrecta de los sistemas y la información. También se refiere a la cantidad de confianza que puede ser colocado en un sistema y la precisión de la información dentro de ese sistema.
- Disponibilidad: se refiere al esfuerzo empleado para evitar la ruptura del servicio y la productividad.

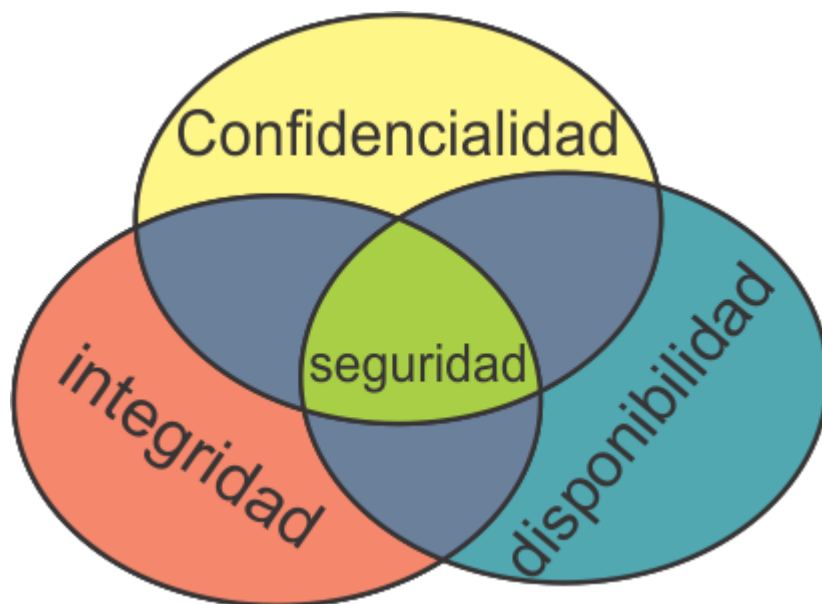


ILUSTRACIÓN 2 LOS TRES PILARES DE LA SEGURIDAD DE INFORMACIÓN

FUENTE: (ALONSO LÓPEZ, Y OTROS, 2015)

2.2.2. Impacto de un incidente de seguridad

Según (BS Grupo, 2014), un incidente de seguridad de información es indicado por una a varias series de incidentes inesperados y no deseados que tiene una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. En la Ilustración 3 se muestra un gráfico que representa un escenario donde ocurre un incidente de seguridad, rompiendo de esta forma con la confidencialidad, la integridad y la disponibilidad.

Algunas de las consecuencias que puede ocasionar un incidente de seguridad de información son:

- Desventaja competitiva
- Perdidas en el negocio
- Daños en la reputación
- Fraude
- Falla en la toma de decisiones
- Responsabilidad Legal
- Moral escasa
- Interrupción operacional
- La seguridad en sí
- Violación de la privacidad

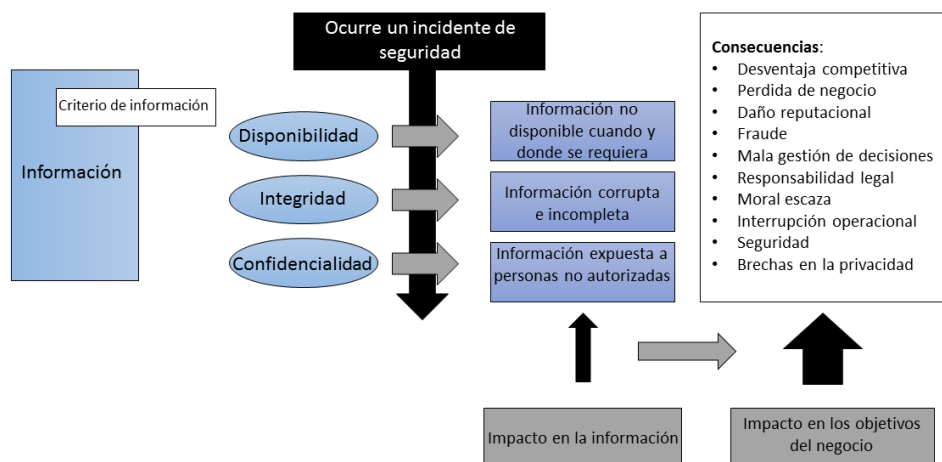


ILUSTRACIÓN 3 IMPACTO DE UN INCIDENTE DE SEGURIDAD

ADAPTACIÓN DE: (BS Grupo, 2014)

2.3. Gestión de la seguridad de la información

Para ISO (*International Organization for Standardization*) un sistema de gestión queda definido por un proceso de 4 etapas, creado por Walter Andrew Shewhart y popularizado por William Edwards Deming, Planificar (Plan), Implementar (Do), Medir (Check) y Mejorar (Act).

La Gestión de la Seguridad de la Información se puede dividir en varios dominios como se detalla en la Ilustración 4. Estos dominios se interrelacionan y son actualizados periódicamente por la familia ²ISO 27000, siendo la ISO/IEC 27001 el estándar más conocido. Dicho estándar especifica todos los requerimientos que debe tener un SGSI (Sistema de Gestión de la Seguridad de la Información).

De acuerdo a la (ISO, 2017), “un SGSI es un enfoque sistemático para la gestión de la información confidencial de una organización para que siga siendo seguro. Incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgos”. Puede ayudar a las pequeñas, medianas y grandes organizaciones en cualquier sector a mantener los activos de información seguros.

2

La ISO (*International Organization for Standardization*) es una organización que se encarga de desarrollar y publicar estándares internacionales <http://www.iso.org/iso/home/about.htm>



ILUSTRACIÓN 4 DOMINIOS DE LA SEGURIDAD DE LA INFORMACIÓN

FUENTE: (ECC INTERNATIONAL, 2015)

Para muchas organizaciones, la información es el activo más importante, pero para otras son las personas, ya que las segundas son las encargadas de dar significado a dicha información. Sin las personas no se podría dar forma a símbolos y datos, ni procesarlos o tomar decisiones a partir de ellos.

Sin embargo, las personas también son el mayor riesgo dentro de las organizaciones, ya que la información de las organizaciones está disponible en ambientes cada vez más interconectados, lo que la expone a amenazas y vulnerabilidades, y como se mencionó anteriormente, son las personas quienes manipulan la información. Entonces, se hace evidente la necesidad de aumentar el control sobre las actividades de las personas, ya que no es posible controlar las intenciones de las mismas, es por esto que se popularizaron los sistemas de gestión de la seguridad de la información.

Según (Hansche, Berti, & Hare, 2004), la gestión de la seguridad implica la identificación de los activos de información de una organización y el desarrollo, documentación e implementación de las políticas, normas, procedimientos y directrices, que aseguren su disponibilidad, integridad y confidencialidad.

2.3.1. Beneficios de gestionar la seguridad de la información

Existe una gran cantidad de beneficios que se desprenden de gestionar la seguridad de la información, estos comprenden desde el cuidado de la reputación de la organización hasta la prevención de grandes pérdidas monetarias. (BS Grupo, 2014) engloba dichos beneficios que provee la seguridad de la información en los siguientes puntos:

- Protege la información de un rango de amenazas
- Garantiza la continuidad del negocio
- Minimiza las pérdidas financieras
- Optimiza el retorno de la inversión
- Incrementa las oportunidades de negocio

En pocas palabras, la seguridad de la información garantiza la supervivencia del negocio.

2.4. Instituciones Normalizadoras Internacionales

Existen diversas organizaciones internacionales que se encuentran asociadas a la seguridad de la información. Dichas organizaciones promueven estándares y normas que ayudan a las empresas en el camino a la implementación de sistemas de gestión de la seguridad de la información.

Dentro de las instituciones normalizadoras internacionales más conocidas se encuentran: la ITU-T, ISO/IEC y CEN/CENELEC.

2.4.1. ITU-T

El Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T, por sus siglas en inglés) es el organismo especializado de la Organización de las Naciones Unidas para las TIC (Tecnologías de la Información y la Comunicación).

Se encargan de la elaboración de normas técnicas que garantizan la interconexión continua de las redes y las tecnologías, y tienen como objetivo la optimización en el acceso a las tecnologías de la información y la comunicación (TIC) de todo el mundo. (ITU-T, 2017)

Según (ITU-T, 2017), las Comisiones de Estudio del Sector de Normalización de las Telecomunicaciones de la ITU-T reúnen a expertos de todo el mundo para elaborar normas internacionales conocidas como Recomendaciones ITU, que actúan como elementos definitorios de la infraestructura mundial de las TIC. Las normas resultan indispensables para la interoperabilidad de las TIC, y cuando se intercambian mensajes de voz, vídeo o datos, las normas hacen posibles las comunicaciones globales asegurando que las redes y dispositivos de TIC de los distintos países utilizan un mismo lenguaje.

Desde su creación en 1865, el ITU-T ha impulsado un enfoque para la elaboración de normas basado en las contribuciones y el consenso, en el que todos los países y empresas, con independencia de su tamaño, disponen de idénticos derechos para influir en la elaboración de las Recomendaciones ITU-T. Desde sus inicios como organismo normalizador del intercambio telegráfico internacional, a través de

su papel formador en materia de telecomunicaciones, y en el actual ecosistema convergente de las TIC, el ITU-T ha proporcionado según (ITU-T, 2017) las mejores herramientas del mundo a la comunidad global de la normalización y se mantiene como el único organismo verdaderamente global de normalización de las TIC.

2.4.2. ISO/IEC

De acuerdo a (ISO, 2017), la Organización Internacional de Normalización (ISO, por sus siglas en inglés, *International Organization for Standardization*) es una organización internacional independiente y no gubernamental con una membresía de 162 organismos nacionales de normalización. Su secretaría central se encuentra en Ginebra, Suiza.

A través de sus miembros, reúne a expertos para compartir conocimientos y desarrollar estándares internacionales voluntarios, basados en el consenso y relevantes para el mercado, que apoyen la innovación y proporcionen soluciones a los retos globales.

2.4.2.1. Los estándares de la ISO

(ISO, 2017) dice que los estándares internacionales hacen que las cosas funcionen. Ofrecen especificaciones de clase mundial para productos, servicios y sistemas, para garantizar la calidad, la seguridad y la eficiencia, y que son fundamentales para facilitar el comercio internacional.

A la fecha de hoy, la ISO ha publicado veintiún mil quinientos cincuenta y cuatro (21554) estándares internacionales y documentos relacionados, que abarcan casi todas las industrias, desde la tecnología hasta la seguridad alimentaria, la agricultura y la sanidad. Los estándares internacionales de la ISO tienen impacto sobre todas las organizaciones en todas las regiones del mundo.

2.4.2.2. Historia

ISO tuvo sus inicios en 1946, cuando delegados de 25 países se reunieron en el Instituto de Ingenieros Civiles de Londres y decidieron crear una nueva organización internacional "para facilitar la coordinación internacional y la unificación de los estándares industriales". El 23 de febrero de 1947, la nueva organización, ISO, comenzó oficialmente sus operaciones. (ISO, 2017)

Desde entonces, la ISO ha publicado más de 21554 Estándares Internacionales que abarcan casi todos los aspectos de la tecnología y la fabricación. Hoy cuentan con miembros de 162 países y 3921 organismos técnicos encargados del desarrollo de estándares. Más de 135 personas trabajan a tiempo completo para la Secretaría Central de ISO en Ginebra, Suiza.

2.4.3. CEN/CENELEC

Todos los productos y servicios que compramos y usamos en nuestra vida cotidiana tienen que cumplir con ciertos estándares de seguridad y calidad. En Europa, estos estándares son elaborados y acordados por los tres organismos europeos de normalización oficialmente reconocidos: el CEN (Comité Europeo de Normalización), el CENELEC (Comité Europeo de Normalización Electrotécnica) y el ETSI (Instituto Europeo de Estándares de Telecomunicaciones).

Al establecer estándares comunes que se aplican en todo el mercado único europeo, el CEN y el CENELEC garantizan la protección de los consumidores, facilitan el comercio transfronterizo, garantizan la interoperabilidad de los productos, fomentan la innovación y el desarrollo tecnológico, incluyen la protección del medio ambiente y permiten a las empresas crecer. Los productos y servicios que cumplen estos Estándares Europeos pueden ser ofrecidos y vendidos en todos los países participantes. El CEN y el CENELEC reúnen a los organismos nacionales de normalización de 34 países. Su red involucra federaciones empresariales, organizaciones comerciales y de consumidores, grupos ambientalistas y otras partes interesadas de la sociedad. Más de 60.000 expertos técnicos de la industria, la investigación, la academia y otros antecedentes están directamente involucrados en su trabajo.

En conjunto, el CEN y el CENELEC ofrecen una plataforma para el desarrollo de Estándares Europeos y otras especificaciones técnicas en una amplia gama de sectores. Trabajan en estrecha colaboración con la Comisión Europea para garantizar que las normas se corresponden con cualquier legislación pertinente de la UE.

El CEN y el CENELEC también cooperan con la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI) para llegar a acuerdos sobre normas comunes que puedan aplicarse en todo el mundo, facilitando así el comercio internacional.

En 2016, se creó el Grupo enfocado CEN-CENELEC sobre ciberseguridad (CSCG, por sus siglas en inglés) para analizar los avances tecnológicos y su impacto en el mercado único digital, y así, evaluar la forma en que las normas pueden apoyar políticas y reglamentos sobre ciberseguridad y protección de datos y formular recomendaciones para el establecimiento de normas internacionales. (CENELEC, 2017)

2.5. Normas Internacionales de Evaluación y Certificación

A nivel internacional, existen una serie de normas que pueden ser utilizadas por las organizaciones como guía para gestionar su seguridad y su vez obtener una certificación que denote que cumplen con una serie de controles y estándares. Estas normas son la TCSEC, la ITSEC y la ISO 27000.

2.5.1. TCSEC (Libro naranja)

Según (Clemson School of Computing, n.d.), los Criterios de Evaluación del Sistema Informático Confiable (TCSEC, por sus siglas en inglés) (1983-1999), mejor conocido como el Libro Naranja (*Orange Book*), fue la primera metodología de evaluación de la seguridad informática. El Libro Naranja era parte de una serie de libros desarrollados por el departamento de la defensa de los Estados Unidos en los años 80 y los llamo Serie Arcoíris debido a las cubiertas coloridas del informe. La Serie Arcoíris documentó los requisitos de seguridad para contextos tales como redes, bases de datos, sistemas de auditoría, guía de contraseña y otros componentes de un sistema informático.

En la TCSEC se definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas

van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 el más elevado. Todas las clases incluyen requisitos tanto de funcionalidad como de confianza. (Universidad Nacional Autónoma de México, n.d.)

- Nivel D (Protección mínima)

Sin seguridad, está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.

- Nivel C1 (Protección Discrecional)

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, debido a que no hay forma de distinguir entre los cambios que hizo cada usuario.

- Nivel C2 (Protección de Acceso Controlado)

Este nivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.

- Nivel B1 (Seguridad Etiquetada)

Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

- Nivel B2 (Protección Estructurada)

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

- Nivel B3 (Dominios de seguridad)

Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones.

- Nivel A1 (Protección verificada)

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

2.5.2. ITSEC

Los Criterios de evaluación de la seguridad en la tecnología de la información (ITSEC, por sus siglas en inglés), conformado principalmente por Francia, Alemania y Reino Unido, crearon su propio estándar de seguridad a principio de los 90's, este se conoce como el Libro Blanco (*White Book*). (Universidad Autónoma de Mexico, n.d.)

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada. E1, el punto de entrada por debajo del cual no cabe la confianza útil, y E6 el nivel de confianza más elevado.

La correspondencia que se pretende entre los criterios ITSEC y las claves TCSEC es la siguiente mostrada por la Tabla 2:

TABLA 2 REFERENCIA ENTRE CRITERIOS ITSEC Y CLAVES TCSEC.

CRITERIOS ITSEC	CLAVES TCSEC
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-B3, E6	A1

FUENTE: (UNIVERSIDAD AUTÓNOMA DE MEXICO, N.D.)

2.5.3. ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (ISO2700.es)

2.5.3.1. Origen

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (*British*

Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- ✓ 1979 Publicación BS 5750 - ahora ISO 9001
- ✓ 1992 Publicación BS 7750 - ahora ISO 14001
- ✓ 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido, así como el año de publicación formal de la revisión.

En marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información. La última revisión y modificación realizada de la ISO 27001 fue en el año 2015.

2.5.3.2. La familia ISO 27000

Al igual que en otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. El presente trabajo de investigación solo hace énfasis en las normas ISO 27001 e ISO 27002.

ISO 27001

Publicada el 15 de octubre de 2005 y actualizada en el 2015. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

ISO 27002

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición y siendo la 2013 la versión más reciente. Es una guía de buenas prácticas que describe los objetivos y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2013.

2.6. ISO 27001

En la Ilustración 5 se muestra una representación de la ISO 27001, donde se refleja que el estándar abarca muchas de las normas que las organizaciones tienen que cumplir, es decir, que con la implementación de la ISO 27001 se asegura el cumplimiento de muchas otras normas y regulaciones.



ILUSTRACIÓN 5 ALCANCE DE LA ISO 27001 CON RESPECTO A OTRAS NORMAS Y REGULACIONES

FUENTE: (BS GRUPO, 2014)

2.6.1. Dominios

La actual versión del estándar (2015) describe catorce dominios que están graficados en la Ilustración 3 y que son explicados a continuación (ISOTools Excellence, 2016):

2.6.1.1. Políticas de Seguridad de la Información

Hace énfasis en la importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

2.6.1.2. Organización de la Seguridad de la Información

Busca estructurar un marco de seguridad eficiente tanto mediante la asignación de responsabilidades relacionadas a la seguridad de la información, segregación de funciones, contacto con las autoridades, contacto con grupos de interés especial y seguridad de la información en la gestión de proyectos.

2.6.1.3. Seguridad de los recursos humanos

Si se analizan los incidentes de seguridad que se producen en las organizaciones, se podrá notar que la gran mayoría de estos tienen su origen en un error humano. Sugiere investigar los antecedentes de los postulantes y la revisión de los términos y condiciones de los contratos antes de integrarlos. Durante la contratación se propone se traten los temas de responsabilidad de gestión, concienciación, educación y capacitación en seguridad de la información. Para el caso de despido o cambio de puesto de trabajo también deben tomarse medidas de seguridad, como lo es la remoción o actualización de privilegios o accesos.

2.6.1.4. Gestión de activos

Centra la atención en la información como activo, y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la seguridad y en la alteración no deseada. Se denotan responsables, se realiza una clasificación de la información y manejo de los soportes de almacenamiento.

2.6.1.5. Control de acceso

Intenta controlar quien accede a la información dentro de un aspecto relevante, tomando como premisa que no todas las personas de una organización necesitan acceder a toda la información para realizar sus actividades diarias, sino que existen roles que necesitan un mayor nivel de acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, entre otros. Siendo algunos de los controles que se incluyen en esta sección.

2.6.1.6. Criptografía

Habla sobre la utilización de técnicas criptográficas a la hora de tratar con información sensible o crítica para proteger y garantizar su autenticidad, confidencialidad e integridad.

2.6.1.7. Seguridad física y del entorno

La seguridad no es solo a nivel tecnológico sino también físico, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles por parte del personal externo. Los documentos con los que se están trabajando no sólo permitirán gestionar de forma adecuada la seguridad, sino que se acabarán convirtiendo en hábitos que aportarán eficiencia en la gestión.

2.6.1.8. Seguridad de las operaciones

Habla sobre procedimientos y responsabilidades; protección contra malware; resguardo; registro de actividad y monitorización; control del software operativo; gestión de las vulnerabilidades técnicas; coordinación de la auditoría de sistemas de información.

2.6.1.9. Seguridad de las comunicaciones

Busca garantizar la seguridad de la red y proteger de forma adecuada los medios de transmisión de información.

2.6.1.10. Adquisiciones, desarrollo y mantenimiento de los sistemas de información

Requisitos de seguridad de los sistemas de información; seguridad en los procesos de desarrollo y soporte; datos para pruebas.

2.6.1.11. Relación con los proveedores

Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben establecer medidas de seguridad pudiendo ser muy recomendable e incluso necesario en determinados casos.

2.6.1.12. Gestión de incidentes de seguridad de la información

Trata sobre estar preparado para cuando ocurran incidentes de seguridad, dando una respuesta rápida y eficiente y analizarlos para poder prevenirlos en el futuro.

2.6.1.13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio

Sufrir una pérdida de información relevante y no poder recuperarla de alguna forma puede poner en peligro la continuidad de negocio de la organización. Este punto trata la redundancia de la información.

2.6.1.14. Cumplimiento

Indica que se debe tener presente la legislación, las normas y políticas aplicables. Se quiere la conformidad con requisitos legales y contractuales; revisiones de la seguridad de la información.

2.6.2. Beneficios de implementar la ISO 27001

Según (ISO2700.es), implementar la ISO 27001 trae consigo los siguientes beneficios:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001L).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

2.6.3. Como adaptarse a la ISO 27001

Para poder adaptarse al estándar 27001 es recomendable utilizar una metodología PDCA (Plan-Do-Check-Act), la cual está atada a la especificación de la norma ISO 9001, donde aparece mencionado como un principio fundamental para la mejora continua de la calidad.

El nombre del Ciclo PDCA (o Ciclo PHVA) viene de las siglas Planificar, Hacer, Verificar y Actuar, del inglés “Plan, Do, Check, Act”. También es conocido como Ciclo de mejora continua o Círculo de Deming, por ser Edwards Deming su autor. Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales...). El círculo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para

incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para ser usada en empresas y organizaciones.

La Ilustración 6 muestra el detalle de los pasos a seguir para construir, implementar y mejorar un SGSI, siguiendo la metodología PDCA y adaptarse así a la norma 27001.

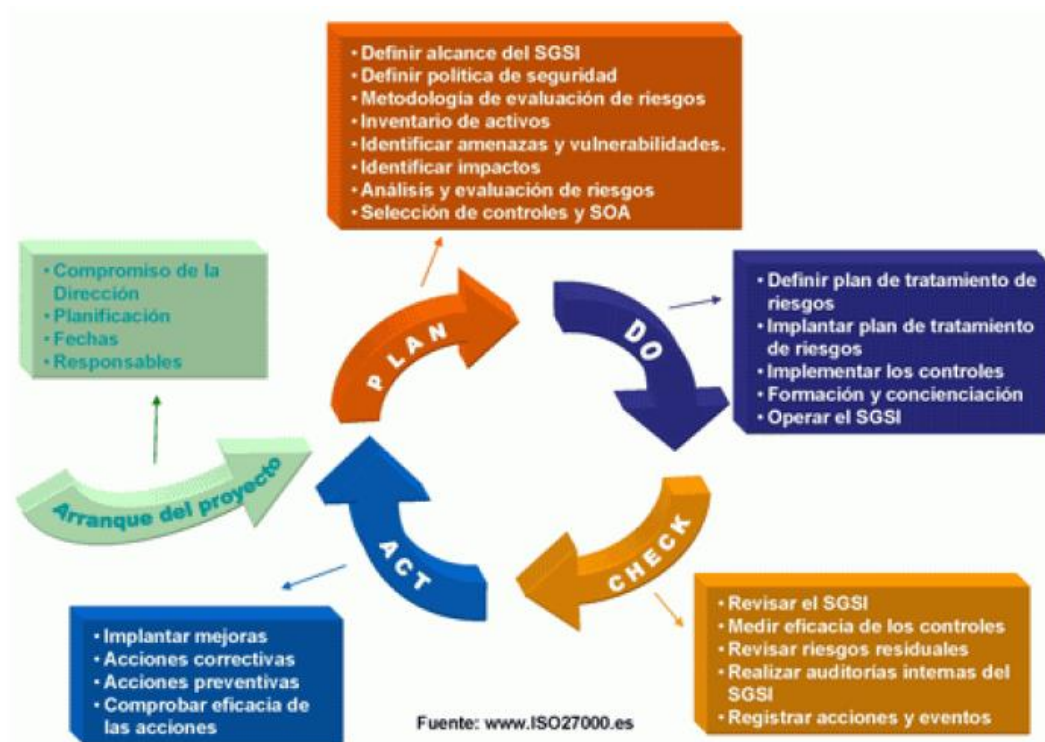


ILUSTRACIÓN 6 CIRCULO DE MEJO

CIÓN DE UN SGSI

FUENTE: (ISO27000.ES)

2.6.3.1. Arranque del proyecto

A continuación, se detallan las actividades a realizar en el arranque del proyecto que se muestran en la Ilustración 7.

1. Compromiso de la Dirección: El apoyo claro y decidido de la Dirección de la organización es una de las bases fundamentales sobre las que iniciar el proyecto. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.
2. Planificación, fechas, responsables: El tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre las siguientes fases.

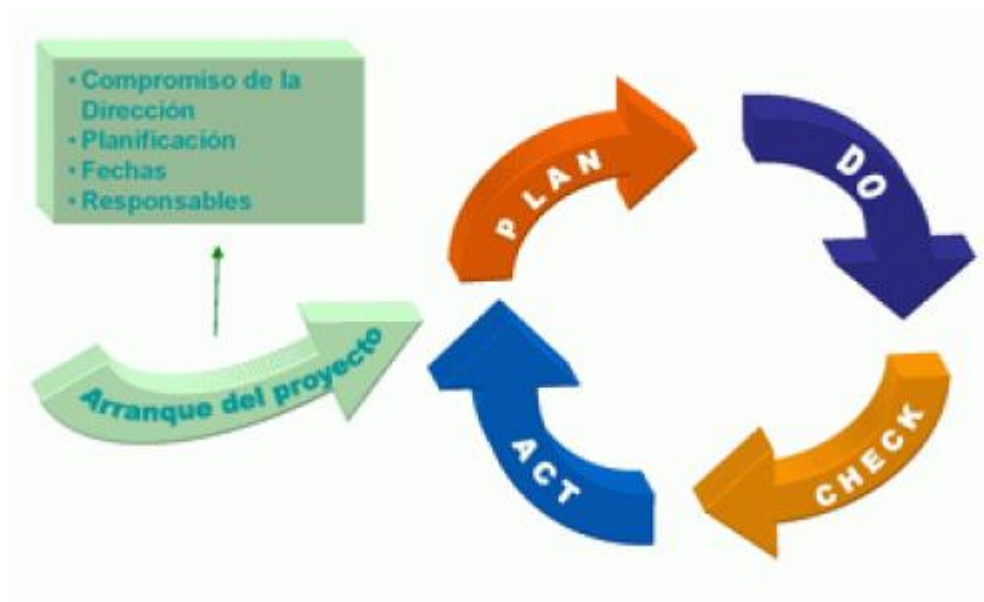


ILUSTRACIÓN 7 ARRANQUE DEL PROYECTO

FUENTE: (ISO2700.ES)

2.6.3.2. Planificación

Trata de establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes a la gestión de riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos generales de la organización.

A continuación, se especifican dichas pertinencias, y que son graficadas en la Ilustración 8:

1. Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
2. Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.
3. Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla. El riesgo nunca puede eliminarse por completo (ni sería rentable hacerlo), por lo que es necesario definir una estrategia de aceptación de riesgo.

4. Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
5. Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
6. Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
7. Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.
8. Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede ser reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).
9. Selección de controles: seleccionar controles para el tratamiento de los riesgos en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.
10. Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
11. Confeccionar una Declaración de Aplicabilidad: la llamada SOA (por sus siglas en inglés) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.



ILUSTRACIÓN 8 PLANIFICAR

FUENTE: (ISO2700.ES)

2.6.3.3. Implementación

Esta fase trata de implementar y operar la política, controles, procesos y procedimientos del SGSI a través de los puntos que se encuentran en la Ilustración 9.

1. Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
2. Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
3. Implementar los controles: todos los que se seleccionaron en la fase anterior.
4. Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
5. Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
6. Gestionar las operaciones del SGSI: y todos los recursos que se le asignen.
7. Implantar procedimientos y controles: de detección y respuesta a incidentes de seguridad.

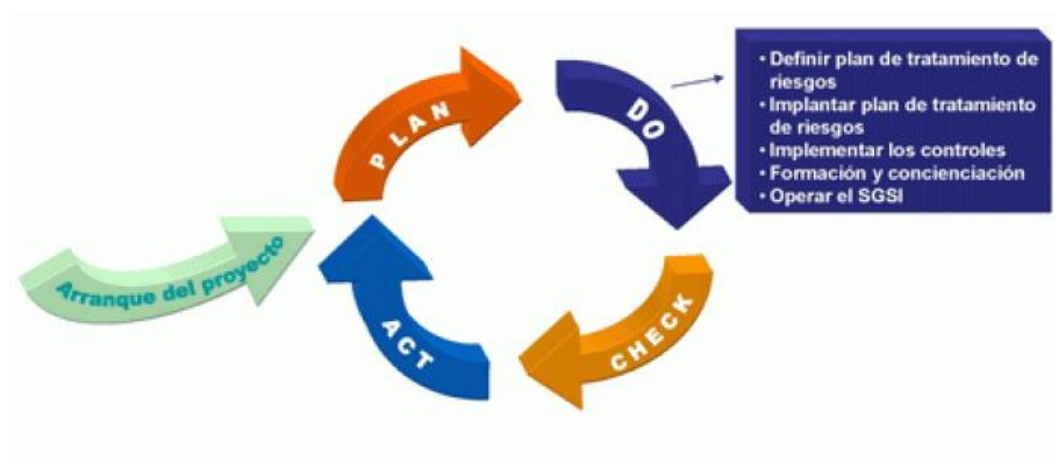


ILUSTRACIÓN 9 IMPLEMENTAR

FUENTE: (ISO2700.ES)

2.6.3.4. Seguimiento

El seguimiento o medición, busca evaluar, y donde sea aplicable, medir el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica, e informar los resultados para gestionar su revisión. Dichos puntos son mostrados gráficamente en la Ilustración 10 y explicados a continuación:

1. Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
2. Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y retroalimentación de todos los interesados.
3. Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.
4. Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.
5. Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
6. Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

7. Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
8. Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.



ILUST

FUENTE: (ISO2700.ES)

2.6.3.5. Mejora continua

La mejora continua u optimización es la fase de toma de acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr mejora continua del SGSI.

A continuación, se detallan las actividades a realizar en esta fase y se muestran gráficamente en la Ilustración 11.

1. Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
2. Acciones correctivas: para solucionar no conformidades detectadas.
3. Acciones preventivas: para prevenir potenciales no conformidades.
4. Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
5. Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

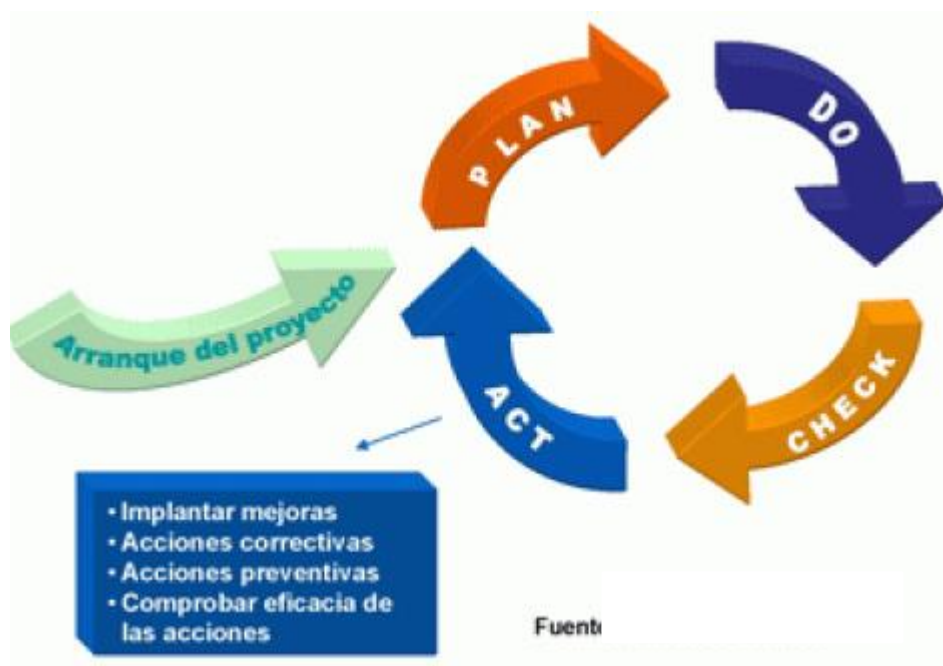


ILUSTRACIÓN 11 MEJORA CONTINUA

FUENTE: (ISO2700.ES)

Teniendo claro todas las actividades que en general deben llevarse a cabo para adaptar una organización a la normativa ISO 27001, se procesó toda la información de manera tal que se pudo crear un diagrama con la notación BPMN que muestra de forma ordenada y secuencial los pasos a seguir para lograr el mismo objetivo. En la Ilustración 12 se muestra el diagrama desde el inicio o arranque del proyecto, y se aprecian los cuatro pasos del PDCA en forma de un conjunto de actividades abstractas.

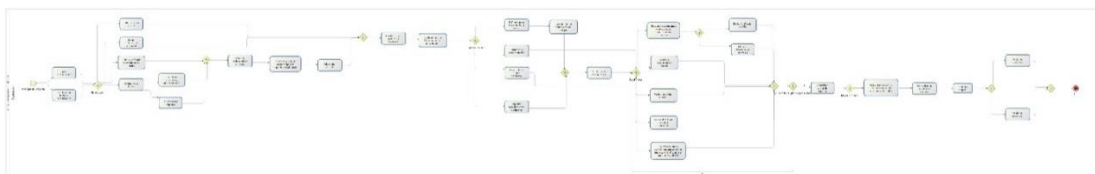


ILUSTRACIÓN 12 ADAPTACIÓN DEL SGSI EN BPMN

En la fase de seguimiento, que se muestra en la Ilustración 23, se puede notar que existe una iteración que se repite mientras no sean encontrados mejoras o errores a corregir en el proceso.

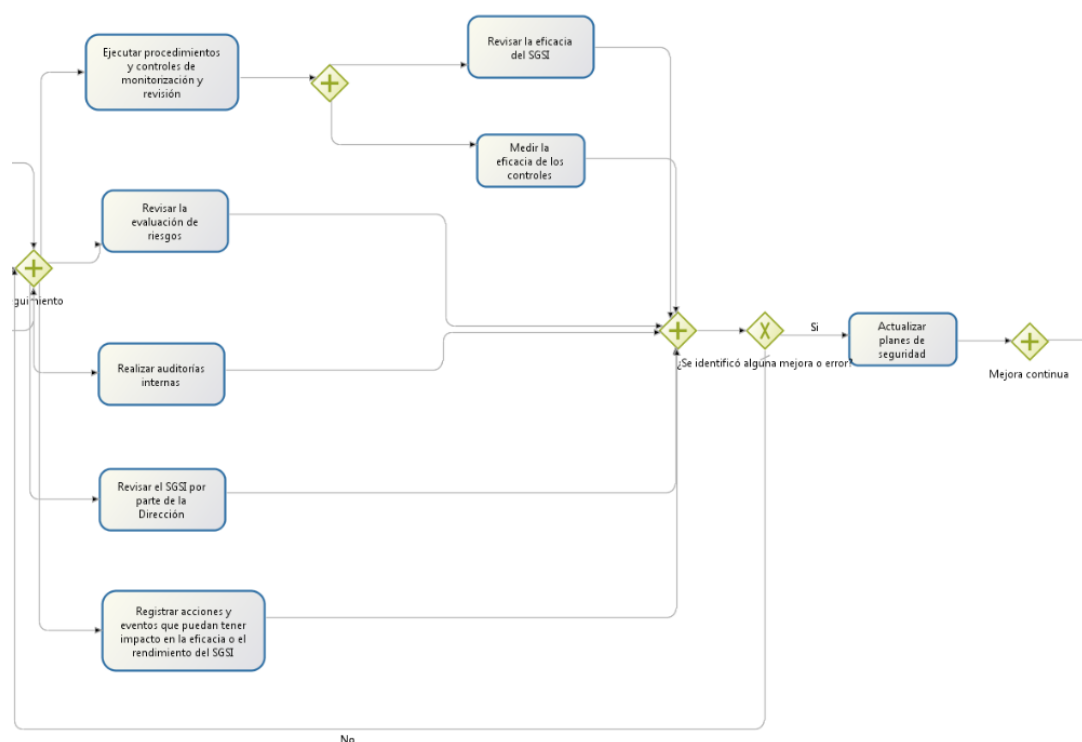


ILUSTRACIÓN 13 ADAPTACIÓN DEL SGSI EN BPMN - SEGUIMIENTO

Este diagrama permite expresar el proceso de implementación de un sistema de gestión de la seguridad de la información en un único lugar, además de que lo convierte en un elemento entendible tanto por el área de negocios, como por el área de tecnología logrando una comunicación mucho más clara y fluida entre ambas partes. Teniendo el proceso unificado en este diagrama, se pueden aprovechar las bondades de la gestión de procesos de negocio ya que normaliza el método de notación que sirve como ayuda en la automatización de los procesos y a la hora de cambios en el mismo, es mucho más fácil visualizarlo y adaptarlo.

Ya habiendo abarcado algunas de las normas internacionales más conocidas en lo que respecta a la seguridad de la información, y cubierto a fondo la ISO 27001, la cual es la metodología en la que finalmente se basó la implementación, se procederá a describir en detalle el proceso de control de acceso. Para esto, se definirá en primer lugar que es un proceso, sus componentes, importancia, la gestión de procesos y su notación.

1.1. Procesos de Control de Acceso

2.6.4. Proceso

Se puede definir como una serie de actividades o toma de decisiones que son sistemáticas, repetitivas e interrelacionadas. Orientadas a obtener un resultado específico como consecuencia del valor añadido aportado por cada una de las actividades o entradas y suministrando salidas a un cliente externo o interno. (Pérez Fernández de Velasco, 2004)

La Ilustración 14 muestra de forma gráfica la definición de proceso y los elementos con los que interactúa.

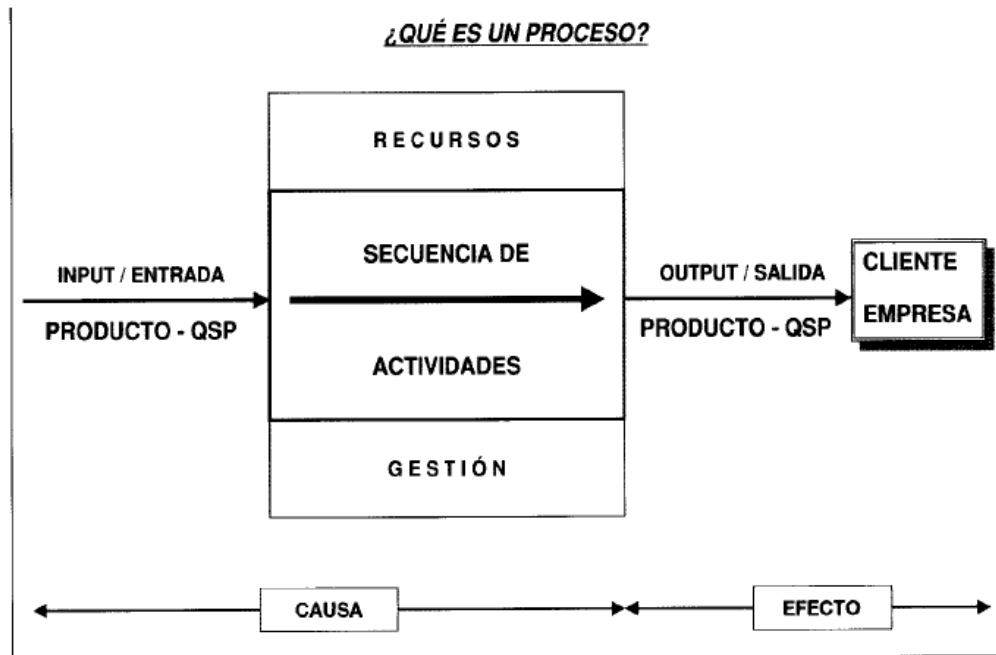


ILUSTRACIÓN 14 ¿QUÉ ES UN PROCESO?

FUENTE (PÉREZ FERNÁNDEZ DE VELASCO, 2004)

1.1.1. Actividad

Según (Pérez Fernández de Velasco, 2004), una actividad es el conjunto o la suma de tareas necesarias para la obtención de un resultado. Normalmente se agrupan en un procedimiento para facilitar su gestión. La secuencia ordenada de actividades da como resultado un subproceso o un proceso.

No todas las actividades que se realizan se traducen en procesos. Para determinar si una actividad realizada por una organización es un proceso, debe cumplir los siguientes criterios (Girón Arévalo & Quishpe Villafuerte, 2008):

- ✓ La actividad tiene una misión o propósito claro.
- ✓ La actividad contiene entradas y salidas, se pueden identificar los clientes, proveedores y producto final.
- ✓ La actividad debe ser susceptible de descomponerse en operaciones o tareas.
- ✓ La actividad puede ser estabilizada mediante la aplicación de la metodología de gestión por procesos (tiempo, recursos, costes).
- ✓ Se puede asignar la responsabilidad del proceso a una persona

1.1.2. El proceso y el procedimiento

En la gestión basada en procesos es fácil confundir el concepto “proceso” con el de “procedimiento”. Los procedimientos son el “cómo” se lleva a cabo una o varias actividades, centrándose en la forma de trabajar o realizar determinadas tareas. En cambio, el proceso, según la norma internacional (ISO, 2005) de sistemas de gestión de calidad, se entiende como una serie de actividades mutuamente relacionadas o que interactúan entre ellas, las cuales transforman elementos de entrada (necesidades de los clientes) en elementos de salida (necesidades ya gestionadas). Éstos últimos tienen que aportar un valor añadido a los elementos entrantes para considerar el proceso eficiente. Pongamos un ejemplo. Una organización quiere mejorar el proceso de gestión de control de acceso en las aplicaciones a sus empleados. Esto se consideraría el proceso a mejorar. ¿Cómo hará la organización para mejorar este proceso? Las acciones que se realicen para llevar a cabo esta mejora serán los procedimientos. En este caso, se podría tratar de poner más recursos que gestionen los accesos para disminuir el tiempo de ocio de los empleados sin permisos en las aplicaciones que necesitan para realizar sus actividades diarias, expandir la cantidad de personas que pueden aprobar o rechazar accesos mediante una delegación de funciones o implantar herramientas de gestión para facilitar y mejorar el seguimiento de la matriz de control de acceso de la organización. (Captio)

1.1.3. Características de los procesos

Las características de los procesos son (Girón Arévalo & Quishpe Villafuerte, 2008):

- ✓ Es definido por un verbo de acción en infinitivo que denota la cualidad de imperativo (terminaciones ar, er, ir).
- ✓ Tiene un principio y un fin (límites).
- ✓ La finalidad de un proceso es generar un producto o servicio.
- ✓ Existen para satisfacer la necesidad de un cliente.
- ✓ Todo proceso tiene un dueño.
- ✓ Transforma o complementan las entradas (valor agregado).
- ✓ Se representan en un diagrama.
- ✓ Debe ser evaluado.
- ✓ Debe ser mejorado.

1.1.4. Componentes de los procesos

Según (Girón Arévalo & Quishpe Villafuerte, 2008), un proceso está compuesto por cinco factores, los cuales son:

- ✓ Recursos humanos: es el conjunto de personas con conocimientos, habilidades y aptitudes que forman parte de una organización para resolver una necesidad o llevar a cabo una actividad dentro de esta.
- ✓ Medio ambiente: conjunto de condiciones bajo las cuales se realiza el trabajo.
- ✓ Insumos: son los bienes y servicios que se incorporan al proceso, que, con el trabajo de los empleados y el apoyo de equipo, son transformados en otros bienes y/o servicios con un valor agregado mayor.

- ✓ Equipo: instrumentos y aparatos que utiliza el capital humano para agilizar uno o varios procesos y así transformar los insumos en productos y/o servicios.
- ✓ Método: método de trabajo, procedimiento, Hoja de proceso, gama, instrucción técnica, instrucción de trabajo, etc. Es la descripción de la forma de utilizar los recursos, quien hace que cuando y ocasionalmente el cómo.

1.1.5. Tipos de procesos

No todos los procesos de una organización tienen la misma influencia en la satisfacción de los clientes, en los costes, en la estrategia, en la imagen corporativa o en la satisfacción del personal. Es conveniente clasificar los procesos, teniendo en consideración su impacto en estos ámbitos. Los procesos se suelen clasificar en tres tipos: estratégicos, clave u operativo o de soporte y (Ministerio de Fomento, 2015) los describe como:

- ✓ Procesos clave: Son los procesos que tienen contacto directo con el cliente (los procesos operativos necesarios para la realización del producto/servicio, a partir de los cuales el cliente percibirá y valorará la calidad: comercialización, planificación del servicio, prestación del servicio, entrega, facturación, entre otros).
- ✓ Procesos estratégicos: Son los procesos responsables de analizar las necesidades y condicionantes de la sociedad, del mercado y de los accionistas, para asegurar la respuesta a las mencionadas necesidades y condicionantes estratégicos (procesos de gestión responsabilidad de la Dirección: marketing, recursos humanos, gestión de la calidad, entre otros).
- ✓ Procesos de soporte: Son los procesos responsables de proveer a la organización de todos los recursos necesarios en cuanto a personas, maquinaria y materia prima, para poder generar el valor añadido deseado por los clientes (contabilidad, compras, nóminas, sistemas de información, entre otros).

A partir de aquí, se empiezan a identificar todos los procesos que irían incluidos en cada bloque y se puede construir un mapa de procesos como muestra la Ilustración 15, el cual no es más que un esquema o diagrama que presenta una visión global de la estructura de la empresa, donde se presentan todos los procesos que la forman, así como sus principales relaciones. (Captio)

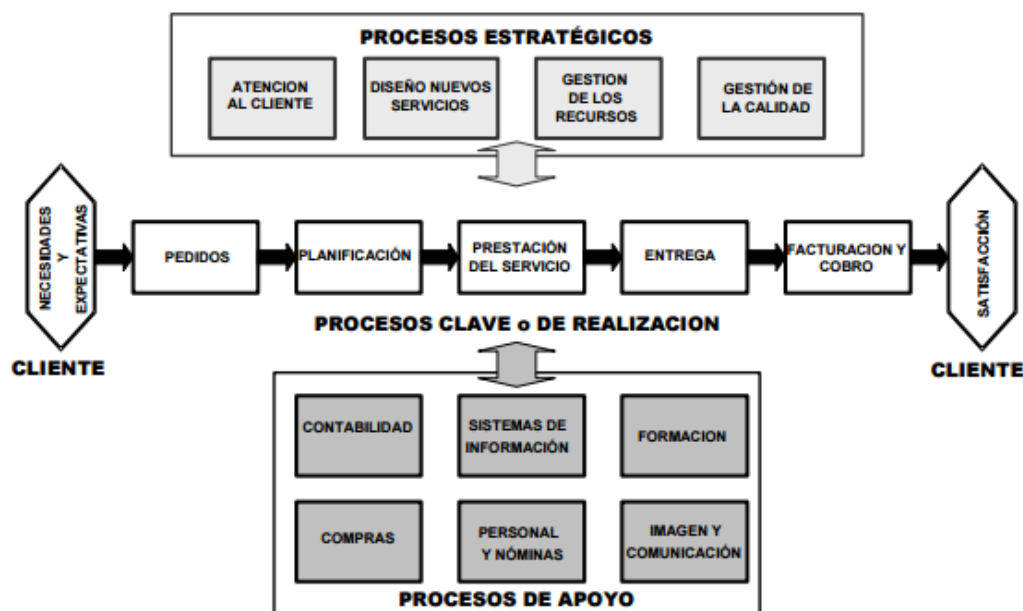


ILUSTRACIÓN 15 TIPOS DE PROCESOS

FUENTE: (MINISTERIO DE FOMENTO, 2015)

1.2. Gestión por procesos

Antes de definir la gestión de procesos, es necesario hablar sobre los sistemas de gestión, que (Araujo Sandoval, Mejía Pardo, Castrejon, & Salirrosas Cerna, 2014) los describe como el conjunto de responsabilidades, procedimientos, procesos y recursos que se aplican dentro de una organización para lograr una determinada política. Dentro de los sistemas de gestión podemos encontrar la gestión funcional o tradicional y la gestión basada en procesos.

Teniendo en cuenta estos dos tipos de gestión, puede surgir la pregunta ¿Cómo debo estructurar a mi organización para generar mayor valor a mis clientes?

Hoy en día, muchas organizaciones se rigen por una Gestión Funcional. Este tipo de gestión se basa en el funcionamiento de la organización de forma vertical, dividiendo la empresa en departamentos, lo que dificulta la interacción de unos con otros, además de la relación con los clientes.

Este tipo de gestión carece de efectividad al no lograr de forma eficaz la consecución de los objetivos empresariales, como sería satisfacer las necesidades de los clientes. En este tipo de gestión, la estructura organizativa se establece mediante un organigrama, que permite definir la estructura jerárquica entre los distintos cargos de la organización. Sin embargo, este tipo de estructura no refleja el funcionamiento de la empresa, las relaciones con los clientes, las responsabilidades de la organización ni los resultados y comporta fallos en distintos ámbitos de la organización, afectando a los objetivos iniciales.

Es aquí donde entra la gestión de procesos, la cual requiere que la organización se divida en procesos y no en departamentos. La gestión de procesos se centra en las actividades de la organización, separando las que generan mayor valor para el cliente con el fin de maximizarlas y minimizar aquellas que no estén aportando valor. La organización se considera como un sistema de procesos que se relacionan entre sí y se encuentran conectados, en que la estructura clásica vertical se orienta hacia una estructura horizontal, la cual favorece la participación de varias personas de distintos departamentos dentro de un mismo proceso.

La gestión basada en procesos fragmenta los problemas que puede tener una organización con sus actividades en problemas más pequeños y, mediante una serie de procesos adaptados a cada dificultad, se busca la solución para obtener los resultados deseados y que aporten un valor añadido a la organización. (Captio)

1.2.1. Diferencias entre gestión por funciones y gestión por procesos

La Tabla 3 muestra una comparativa de las características más resaltantes de la gestión funcional y la gestión por procesos.

TABLA 3 DIFERENCIAS ENTRE GESTIÓN FUNCIONAL Y GESTIÓN POR PROCESOS

Gestión funcional	Gestión por procesos
Organización por departamentos o áreas	Organización orientada a los procesos
Los departamentos condicionan la ejecución de las actividades	Los procesos de valor añadido condicional la ejecución de las actividades
Autoridad basada en jefes departamentales	Autoridad basada en los responsables del proceso
Principio de jerarquía y de control	Principio de autonomía y de autocontrol
Orientación interna de las actividades hacia el jefe o departamento	Orientación externa hacia el cliente interno o externo
Principios de burocracia, formalismo y centralización en la toma de decisiones	Principios de eficiencia, flexibilidad y descentralización en la toma de decisiones
Ejercicio del mando por control basado en la vigilancia	Ejercicio del mando por excepción basado en el apoyo o la supervisión
Principio de eficiencia: ser más productivo	Principio de eficacia: ser más competitivos
Como hacer mejor lo que venimos haciendo	Para quien lo hacemos y que debemos hacer
Las mejoras tienen un ámbito limitado: el departamento	Las mejoras tienen un ámbito transfuncional y generalizado: el proceso

FUENTE: (GIRÓN ARÉVALO & QUISHPE VILLAFUERTE, 2008)

1.2.2. Objetivos de la gestión por procesos

Los objetivos de la gestión por procesos están orientados a la satisfacción del cliente y al aumento de la productividad. Según (Araujo Sandoval, Mejia Pardo, Castrejon, & Salirrosas Cerna, 2014), los objetivos de la gestión por procesos son:

- ✓ Satisfacer a los clientes desde sistemas de gestión más eficaces
- ✓ Contar con una organización más eficiente desde el punto de vista de los costos y control de los ciclos de producción

- ✓ Tener una organización más flexible que constantemente se pueda adecuar a la organización y el sistema a la estrategia del negocio

1.2.3. Beneficios de la gestión por procesos

De acuerdo a (Captio), adicional a los beneficios que aporta a la organización el uso de indicadores para medir los resultados, existen otra gran variedad de beneficios que aporta esta metodología, los cuales se nombran a continuación:

- ✓ Homogeneización de la forma de trabajar
- ✓ Control de todas las acciones de los procesos
- ✓ Eliminación de actividades que no aportan ningún valor a la organización
- ✓ Mejora de la salida de información
- ✓ Reducción del tiempo de operación
- ✓ Focalización de los procesos en obtener la satisfacción del cliente
- ✓ Mejora de los servicios que ofrece la organización
- ✓ Conocimiento de los participantes en cada proceso
- ✓ Facilidad de identificar nuevas oportunidades de negocio
- ✓ Definición de una estructura sistémica alineada con la estrategia de la organización

1.3. Gestión de Procesos de Negocio (BPM)

La Gestión de Procesos de Negocio (BPM) es un marco de trabajo basado en la coordinación de las actividades y decisiones que todas las partes involucradas deben realizar durante un proceso de negocio, con el objetivo de convertirse en una organización altamente eficiente, ágil, innovadora y adaptable. BPM involucra cualquier combinación de modelado, automatización, ejecución, control, medición y optimización de flujos de actividad empresarial, en apoyo de objetivos empresariales, sistemas, empleados, clientes y socios tanto internos como externos a la organización. (Palmer, 2014)

1.3.1. Consideraciones de BPM

- ✓ BPM es una disciplina; es una práctica; es algo que haces.
- ✓ El negocio proviene del estado de estar ocupado, e implica un trabajo comercialmente viable y rentable. Una empresa existe para proporcionar valor a los clientes a cambio de algo más valioso.
- ✓ Una persona que hace BPM debe considerar un proceso en el ámbito de las actividades comerciales interrelacionadas que cooperan holísticamente para cumplir con un objetivo de negocio. Un profesional de BPM debe considerar las métricas de todo el sistema al evaluar un proceso específico.
- ✓ Se debe enfatizar que BPM debe hacerse en el contexto de los objetivos de la empresa, y no una pequeña parte de ella. Cualquier mejora de un proceso debe ser una mejora en términos de los objetivos de la empresa, cualquier otra cosa no se llamaría una mejora.
- ✓ Dentro y más allá de los límites de la organización se reconoce que la organización es parte de un sistema más grande. Los clientes forman parte del proceso empresarial. Su interacción,

junto con las de los empleados debe ser considerada como parte de la interacción de extremo a extremo. (Palmer, 2014)

1.3.2. Historia y evaluación de BPM

BPM no es un concepto nuevo, por el contrario, para comprender su evolución, podemos remontarnos a las llamadas “Eras de la Información” que se dividen en tres “olas” la cuales van desde la década del 70 a la actualidad.

Este tema fue abordado por Howard Smith and Peter Fingar en “Brief history of business process management” referenciándolo como el camino de éxitos y fracasos que siguieron las organizaciones en la lucha por lograr la mayor eficiencia enfocándose en los procesos de negocio. Es aquí donde empieza la primera ola (‘70- ‘80) donde los procesos se encontraban implícitos en la práctica del trabajo y no eran automatizados. Luego, sigue con la segunda (‘90) cuyo inicio fue marcado con la propuesta de Michael Hammer y James Champy de donde surge el concepto de reingeniería de los procesos, entendiendo esto como una herramienta orientada a la mejora de procesos, aplicándoles cambios radicales, replanteando y rediseñándolos por completo. Estos cambios originaron soluciones de software, como los ERPs y CRMs los cuales en cierta forma facilitaron la gestión de los datos e información en las organizaciones teniendo en cuenta la vista y experiencia del cliente, pero esto no era suficiente como para proporcionar a los actores del negocio el control total del ciclo de vida de los procesos.

La tercera ola BPM que tuvo su inicio en el 2000 y que continua en la actualidad, permite a las organizaciones crear y optimizar nuevos procesos de negocios sobre la marcha, no perdiendo de foco que el movilizador es siempre el constante “cambio” en el día a día de las organizaciones. De esta forma, a través de los procesos de negocio ágiles, la cadena de valor puede ser continuamente monitoreada y optimizada. (GlobalLogic, 2012)

1.3.3. Principales funcionalidades

Según (Club BPM, 2009) las principales funcionalidades que BPM provee, tenemos:

- ✓ Asignar actividades a las personas de forma automática y según cualquier criterio, o según cargas de trabajo.
- ✓ Recordar a las personas sus actividades.
- ✓ Optimizar la colaboración entre personas que comparten actividades.
- ✓ Automatizar y controlar el flujo de documentos, datos e imágenes.
- ✓ Asignarles proactivamente a las personas que deben ejecutar las actividades, todos los recursos necesarios (Documentos, información, Aplicaciones, etc.) en cada una de ellas.
- ✓ Definir y controlar “alertas” según criterios de tiempo, de evento o de condición, provocando así algún mensaje a un supervisor, un “escalado” de actividades a otras personas para que las resuelvan, y/o una resignación automática.
- ✓ Modificar los procesos y gestionar excepciones “en vivo”, o “al vuelo”, y desde cualquier lugar, es decir, permitir modificar cualquier instancia de proceso ya iniciada, sin necesidad

de volver a iniciarla y sin necesidad de meter mano informáticamente. Además, a través de cualquier navegador para que realmente se pueda realizar desde cualquier lugar.

- ✓ Proveer una vista “on-line” para supervisores del estado e histórico de cada instancia de proceso, de cada actividad, y del desempeño de las personas.
- ✓ Hacerles llegar a cada persona sus actividades y alertas, independientemente de su ubicación geográfica, a través de la WEB, Email, SMS, o cualquier otro dispositivo móvil.
- ✓ Proveer métricas para responsables de áreas, organizadores, gestores de procesos y calidad, tanto para efectos de Mejora Continua como de Indicadores de Calidad y de Gestión.
- ✓ Proveer un alto nivel de soporte para la interacción humana.

1.3.4. Principales beneficios de BPM

Según (Club BPM, 2009) los beneficios, tanto tangibles como intangibles, son numerosos. A continuación, se describen los más importantes:

- ✓ Mejora la atención y servicio al cliente.
- ✓ Incrementa el número de actividades ejecutadas en paralelo.
- ✓ Minimiza el tiempo requerido por los participantes para acceder a la documentación, aplicaciones y bases de datos.
- ✓ Disminuye “drásticamente” el tiempo de transferencia de trabajo, información y documentos entre actividades.
- ✓ Asegura la continua participación y colaboración de todo el personal en el proceso.
- ✓ Disminuye “drásticamente” el tiempo que los participantes, supervisores y administradores necesitan para conocer la situación de un ítem de trabajo (P.ej.: Orden de compra, participación de siniestro, pedido de cliente).
- ✓ Simplificación de salidas automáticas. Documentos Word, Faxes, e-mails, mensajes cortos a móviles, etc.
- ✓ Disponibilidad de mecanismos para una mejor gestión y optimización de procesos.

1.3.5. BPMN

La Notación de Modelado de Procesos de Negocio (BPMN, por sus siglas en inglés) es una notación gráfica que describe los pasos en un proceso de negocio. BPMN representa el flujo de extremo a extremo de un proceso de negocio. La notación ha sido diseñada específicamente para coordinar la secuencia de procesos y los mensajes que fluyen entre los diferentes participantes del proceso en un conjunto de actividades relacionadas. BPMN fue inicialmente desarrollada por la organización *Business Process Management Initiative* (BPMI), y es actualmente mantenida por el *Object Management Group* (OMG), después de la fusión de las dos organizaciones en el año 2005. Su versión actual, es la 2.0.2. (OMG, 2016)

Según (White & Miers, 2009), en BPMN, los “Procesos de Negocio” involucran la captura de una secuencia ordenada de las actividades e información de apoyo. Modelar un proceso de negocio implica representar como una organización realiza sus objetivos centrales; los objetivos por si mismos

son importantes, pero por el momento no son capturados por la notación. Con BPMN, solos los procesos son modelados.

En el modelado de BPMN, se pueden percibir distintos niveles de modelado de procesos:

- ✓ Mapas de Procesos: Simples diagramas de flujo de las actividades; un diagrama de flujo sin más detalle que el nombre de las actividades y tal vez las condiciones de decisión más generales.
- ✓ Descripción de Procesos: Proporcionan información más extensa acerca del proceso, como las personas involucradas en llevarlo a cabo (roles), los datos, información, etc.
- ✓ Modelos de Proceso: Diagramas de flujo detallados, con suficiente información como para poder analizar el proceso y simularlo. Además, esta clase de modelo más detallado permite ejecutar directamente el modelo o bien importarlo a herramientas que puedan ejecutar ese proceso (con trabajo adicional).

BPMN tiene la finalidad de servir como lenguaje común para cerrar la brecha de comunicación que frecuentemente se presenta entre el diseño de los procesos de negocio y su implementación, esto facilitará una mejor comprensión de lo que se realiza.

2.6.4.1. Categorías de los procesos

Desde su descripción, BPMN ha tratado de dar soporte a tres categorías principales de procesos:

Orquestación

En BPMN, los modelos de orquestación tienden a implicar una perspectiva única de coordinación, por ejemplo, representan una vista específica del negocio u organización del proceso. Como tal, un proceso de orquestación describe como una única entidad de negocio lleva a cabo las cosas. Como se muestra en la ilustración 16

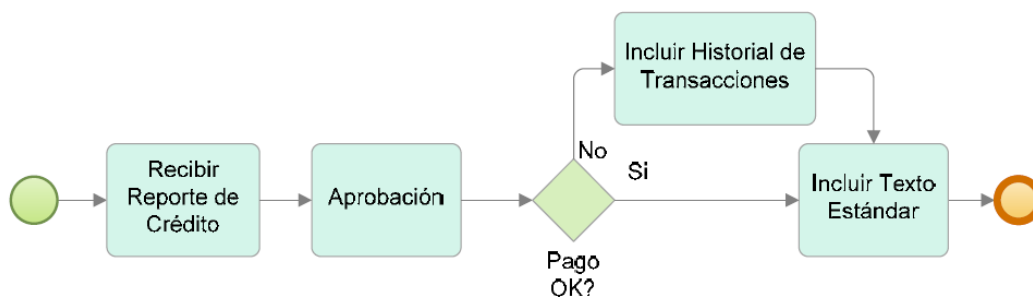


ILUSTRACIÓN 16 ORQUESTACIÓN

FUENTE: (WHITE & MIERS, 2009)

Un diagrama BPMN puede contener más de una orquestación. En tal caso, cada orquestación aparece dentro de su propio contenedor llamado Pool.

El hecho que los modelos de orquestación están contenidos en un Pool indica que consiste de elementos de procesos que coexisten dentro de un contexto bien definido, o centro de control. Un modelo de orquestación ejecutado por una BPMS cumple exactamente esta descripción, pero

también aplica a situaciones que no son parte de un sistema semiautomático. Una consecuencia del “contexto bien definido” en una orquestación es que cualquier dato está disponible para todos los elementos del modelo.

Coreografía

Un modelo de proceso de coreografía es una definición del comportamiento esperado (una clase de contrato procedimientos o protocolo) entre los participantes que interactúan. Esos participantes pueden ser roles de negocio generales (por ejemplo, un despachador) o una entidad específica de negocio (por ejemplo, FedEx como empresa de transporte).

Como en la definición de un ballet, en BPMN una coreografía describe las interacciones de los participantes. En BPMN, una coreografía define la secuencia de interacciones entre dos o más participantes, como se muestra en la Ilustración 17. En BPMN, las interacciones son la comunicación, a través de la cual se intercambia un mensaje entre dos participantes.

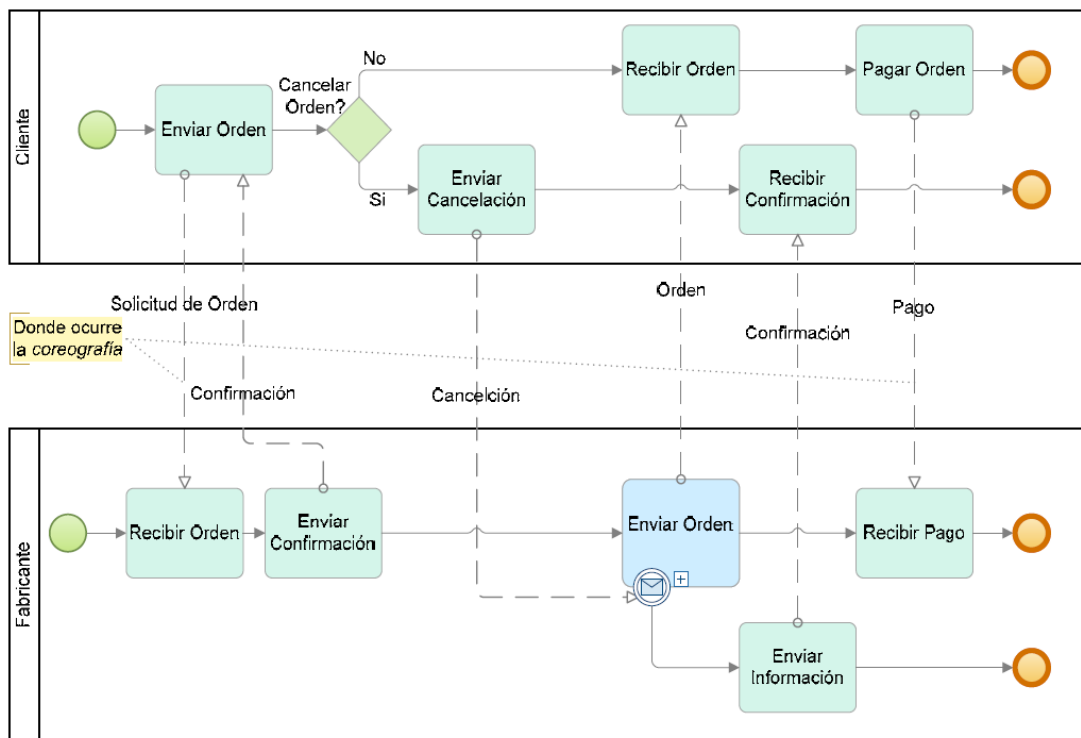


ILUSTRACIÓN 17 COREOGRAFÍA

FUENTE: (WHITE & MIERS, 2009)

Colaboración

La colaboración tiene un significado específico en BPMN. Mientras que la coreografía muestra el conjunto ordenado (protocolo) de interacciones entre los participantes. Una colaboración puede contener también una coreografía (cuando esté disponible en BPMN) y una o más orquestaciones.

Para ser más específicos, una colaboración es cualquier diagrama BPMN que contenga dos o más participantes como se muestra con los Pools, en el caso de la Ilustración 18, el Pool de Cliente colabora con el Pool de Fabricante y viceversa. Los Pools tienen Flujos de Mensajes entre ellos. Cualquiera de los Pools puede llegar a contener una orquestación (un proceso), pero no está requerido.

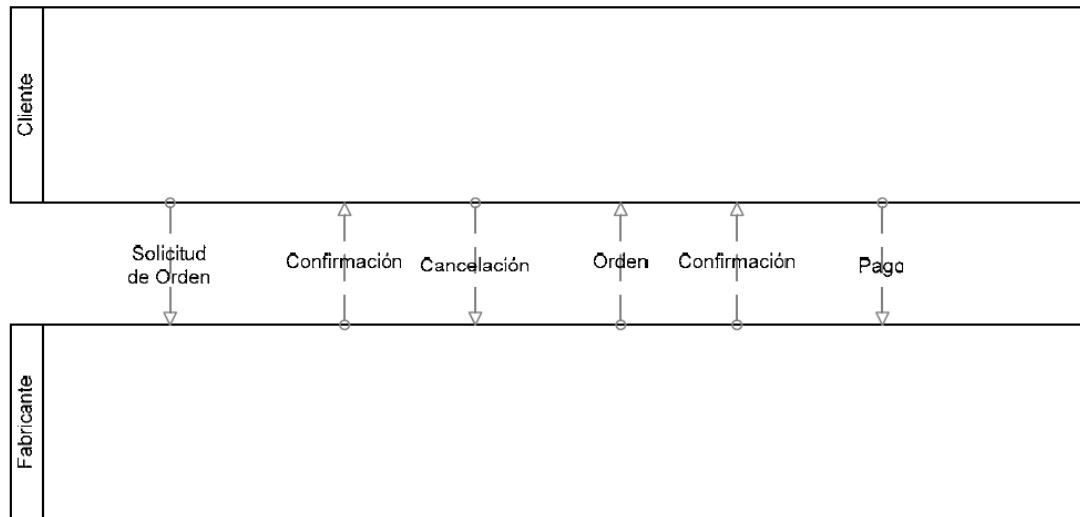


ILUSTRACIÓN 18 COLABORACIÓN

FUENTE: (WHITE & MIERS, 2009)

2.6.4.2. Elementos de BPMN

Cabe destacar que uno de los motores para el desarrollo de BPMN es crear un mecanismo simple y comprensible para crear modelos de procesos de negocio, mientras que al mismo tiempo es capaz de manejar la complejidad inherente de los procesos de negocio. El enfoque adoptado para manejar estos dos requisitos contradictorios fue organizar aspectos gráficos de la notación en categorías específicas. Esto proporciona un pequeño conjunto de categorías de notación para que el lector de un diagrama BPMN pueda reconocer fácilmente los tipos básicos de elementos y comprender el diagrama. Las cinco categorías básicas de elementos son:

- ✓ Objetos de flujo
- ✓ Datos
- ✓ Conexión de objetos
- ✓ Swimlanes o canales
- ✓ Artefactos

Los objetos de flujo son los elementos gráficos principales para definir el comportamiento de un proceso de negocio. Hay tres objetos de flujo

- ✓ Eventos
- ✓ Actividades

- ✓ Puertas de enlace

Los datos se representan con los cuatro elementos:

- ✓ Objetos de datos
- ✓ Entradas de datos
- ✓ Salidas de datos
- ✓ Tiendas de datos

Hay cuatro formas de conectar los objetos de flujo entre sí u otra información:

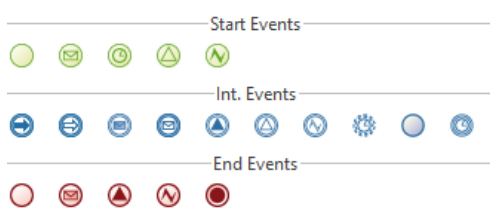
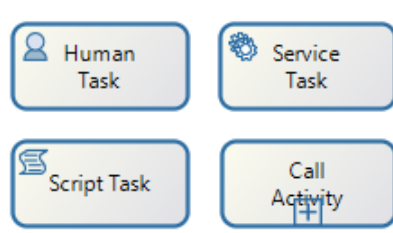
- ✓ Flujos de secuencia
- ✓ Flujos de mensajes
- ✓ Asociaciones
- ✓ Asociaciones de datos

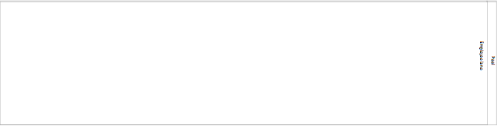
Hay dos formas de agrupar los elementos primarios de modelado a través de "Swimlanes:"

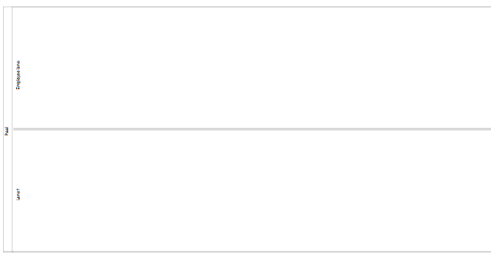
- ✓ Área funcional o Pool
- ✓ Carril o Lane

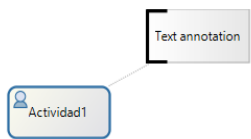
A continuación, se presenta en la Tabla 4 algunos de los elementos de BPMN más importantes:

TABLA 4 ELEMENTOS BÁSICOS DE MODELADO

Tipo	Descripción	Imagen
Evento	Un evento es algo que ocurre durante el curso de un proceso o una coreografía. Estos eventos afectan el flujo del modelo y suelen tener una causa (desencadenante) o un impacto (Resultado). Los eventos son círculos con centros abiertos para permitir que los marcadores internos diferencien diferentes Disparadores o Resultados. Hay tres tipos de eventos, en función de cuándo afectan al flujo: Inicio, Intermedio y Fin.	
Actividad	Una actividad es un término genérico para el trabajo que la empresa realiza en un proceso. Una actividad puede ser atómica o no atómica (compuesto). Los tipos de Actividades que forman parte de un modelo de proceso son: Subproceso y tarea, que son rectángulos redondeados. Las actividades se utilizan tanto en	

	Procesos estándar como en Coreografías.	
Decisión	se utiliza para controlar la divergencia y la convergencia de los flujos de secuencia en un proceso y en una coreografía. Por lo tanto, determinará ramificación, bifurcación, fusión y unión de rutas. Los marcadores internos indicarán el tipo de control de comportamiento.	 Paralelo (AND) Exclusivo (XOR) Inclusivo
Flujo de secuencia	Se utiliza un flujo de secuencia para mostrar el orden en que las actividades se realizarán en un proceso y en una coreografía.	
Flujo de mensaje	Se utiliza un flujo de mensajes para mostrar el flujo de mensajes entre dos participantes que están preparados para enviarlos y recibirlos. En BPMN, dos áreas funcionales separadas en un Diagrama de Colaboración representarán a los dos Participantes.	
Asociación	Una asociación se utiliza para vincular información y artefactos con elementos gráficos BPMN. Anotaciones y otros artefactos pueden asociarse con los elementos gráficos. Una punta de flecha en la Asociación indica una dirección de flujo, cuando corresponda.	
Área Funcional o Pool	Un área funcional es la representación gráfica de un participante en una colaboración. También actúa como un "swimlane o canales" y un contenedor gráfico para dividir un conjunto de Actividades de otras áreas funcionales. Un área funcional puede tener detalles internos en la forma del proceso que se ejecutará o puede no	

	tener detalles internos, es decir, puede ser una "caja negra".	
Carril o Lane	Un carril es una subpartición dentro de un proceso, a veces dentro de un área funcional y se extenderá en todo el proceso, ya sea vertical u horizontalmente. Los carriles se utilizan para organizar y clasificar las actividades.	
Objeto de datos	Los Objetos de Datos proporcionan información sobre qué Actividades requieren que se realicen y / o qué producen. Los Objetos de datos pueden representar un objeto singular o una colección de objetos. La entrada de datos y la salida de datos proporcionan la misma información para los procesos.	
Mensaje	Se utiliza un mensaje para representar el contenido de una comunicación entre dos Participantes.	
Grupo	Un grupo es un agrupamiento de elementos gráficos que están dentro de la misma categoría. Este tipo de agrupación no afecta a los flujos de secuencia dentro del grupo. El nombre de la categoría aparece en el diagrama como la etiqueta del grupo. Las categorías se pueden utilizar con fines de documentación o análisis. Los grupos son una forma en la que las categorías de objetos se pueden visualizar visualmente en el diagrama.	

Anotación	Las anotaciones son un mecanismo para que un modelador proporcione información de texto adicional para el lector de un Diagrama BPMN.	
-----------	---	---

FUENTE: (OMG, 2011)

1.3.6. Herramientas BPM (Business Process Management Suites)

Es una colección integrada de tecnologías de software que permiten control, manejo y mejoramiento continuo de los procesos a través de la automatización de cada una de las fases de su ciclo de vida: Descubrimiento, Modelado, Despliegue, Ejecución, Monitoreo y Optimización.

La eficiencia y la eficacia en los procesos de negocio representa un foco importante en todas las organizaciones debido a la competitividad que existe en la actualidad. Es por ello que es necesario que las organizaciones desarrollen ventajas competitivas en su forma de operar. Las herramientas BPM ayudan al desarrollo de dichas ventajas.

2.6.4.3. Aspectos funcionales provistos por los BPMS

- ✓ Obtener un gráfico que puede ser de utilidad para los dueños del negocio, como a los analistas para conocer el flujo de trabajo.
- ✓ Simular el proceso de negocio, pudiendo utilizarlo como prueba con datos actuales e históricos.
- ✓ Proporcionar la facilidad de crear automáticamente interfaces y reportes.
- ✓ Proporcionar la facilidad de crear reglas de negocio, pudiendo ser utilizadas para conducir el flujo del proceso y la toma de decisiones.
- ✓ La capacidad para la integración con otras herramientas externas, dado que muchas veces el BPMS no provee todo lo necesario para el ciclo de vida de los procesos de negocio.
- ✓ La capacidad de enviar o recibir mensajes de eventos del sistema o del negocio.
- ✓ La capacidad de reconocer indicadores de desempeño, que se pueden obtener de la ejecución de los procesos de negocio.
- ✓ (S. Rodríguez, Bazan, & Díaz, 2015)

2.6.4.4. Principales beneficios de un BPMS

Los principales beneficios que provee una herramienta BPM según (STATUM, 2014) son:

- ✓ Implementación de procesos horizontales de una forma ágil y efectiva.
- ✓ Integración de la información del negocio dispersa en diferentes sistemas.
- ✓ Participación de los usuarios en todas las fases del ciclo de vida de los procesos.
- ✓ Monitoreo del cumplimiento de los factores clave del negocio.
- ✓ Medio para el mejoramiento y eficiencia continua de los procesos de negocio.
- ✓ Mejora de los tiempos de respuesta de TI ante cambios y nuevos requerimientos:
 - Mayor rapidez en la incorporación de mejoras a los procesos de negocio.

- Reducción de tiempo a menos de la mitad en la incorporación de nuevas funcionalidades.

2.6.4.5. Cuadro comparativo

A continuación, en la Tabla 5 se muestra una comparación de las características básicas de algunos de los BPMS de software libre más utilizados.

TABLA 5 COMPARACIÓN ENTRE BPMS'S OPEN SOURCE

Herramienta	Versión actual	Estándares	Licencia	Tecnología base
Bonita	7.4.3	BPMN 2.0 XPDL	GPL v2	Java
Intalio	7.5.0	BPMN 2.0 Orientada a SOA	GPL + licencia de Intalio	Java
JBPM	6.5.0	BPMN 2.0 Orientada a SOA	Apache License 2.0	Java
ProcessMaker	3.0	BPMN 2.0 Orientada a SOA	AGPLv3	PHP
Activiti	5.23	BPMN 2.0	Apache License 2.0	Java

FUENTE: ELABORACIÓN PROPIA

La razón por la que se decidió el uso de la herramienta Bonita BPM fue debido a su alto nivel de documentación y por su activa comunidad. Bonita BPM provee las funcionalidades y características necesarias para llevar a cabo la implementación del proceso de control de acceso, como lo son:

- *UI Designer*, para la creación de páginas y formularios de interacción
- Conectores
- Fácil integración con las diferentes aplicaciones de una organización a través de la arquitectura orientada a servicios (SOA)
- Puede manejar un alto volumen de usuarios

2.7. Proceso de control de acceso lógico

El control de acceso es uno de los dominios que no pueden pasar desapercibidos y que es intrínseco a la seguridad de la información. Es el aspecto más penetrante y omnipresente de la seguridad de la información. Aunque las personas sean el mayor activo de las organizaciones, también son su mayor riesgo. Se gasta mucho dinero en controles y medidas de seguridad que al fin y al cabo son gestionadas por las personas, los cuales son el eslabón más débil en la cadena de la seguridad, de hecho, según (BS Grupo, 2014), el 70% de las amenazas son internas.

El objetivo de la seguridad de la información es asegurar la continuidad de CIA en los activos de una organización. El control de acceso juega un rol importante asegurando la confidencialidad de los sistemas y la información mediante la administración de los accesos de los activos para prevenir la exposición de los datos controlando quien puede ver, usar, modificar o destruir dichos activos.

El acto de controlar el acceso inherentemente ofrece características y beneficios que protegen la integridad de los activos de la empresa. Mediante la prevención de accesos no autorizados o inapropiados las organizaciones pueden conseguir una gran confianza en sus datos y la integridad de los sistemas.

Finalmente, los procesos de control de acceso van de la mano con los esfuerzos para garantizar la disponibilidad de recursos dentro de una organización. Una regla para que un recurso crítico pueda estar disponible para su uso durante periodos alargados de tiempo, es que sólo las personas que tengan la necesidad de utilizar ese activo en particular se les deben permitir el acceso. Adoptar esta posición asegura que el recurso no se bloquee o se congestionara por personas que no tienen razones para usarlo.

A continuación, se explicará el término de control de acceso y el proceso como tal, el cual es al que se le quiere aplicar la metodología BPM.

2.7.1. Dominio de control de acceso

El dominio de control de acceso describe diversas opciones de seguridad del sistema de información que controlan el acceso a los recursos de información y procesamiento de datos de una organización. Se basa en las cuestiones básicas tratadas en el Dominio de Seguridad de la Información, con énfasis en los diversos controles administrativos, físicos y técnicos.

El dominio de control de acceso cubre los mecanismos con los cuales un sistema otorga o revoca el derecho a acceder a los datos o ejecutar una acción en un sistema de información. Es importante tener claro algunos conceptos claves que forman la base para entender cómo funciona el control de acceso y el porqué es la clave de la disciplina de seguridad. (Hernandez, 2012, pág. 4)

El concepto más significativo y fundamental que se debe conocer es precisamente la definición de que se refiere el término “control de acceso”.

2.7.2. Control de acceso lógico

Según (Hernandez, 2012): “es el proceso de permitir solo a usuarios, programas u otros sistemas informáticos autorizados ver, modificar o cualquier otra posesión de los recursos de un sistema informático. Es también un mecanismo para limitar el uso de algunos recursos a usuarios autorizados”.

En conclusión, el control de acceso es un conjunto de mecanismos, procesos o técnicas que trabajan juntas para proteger los activos de una organización. Ayudan en la protección contra las amenazas y

mitigan las vulnerabilidades a medida que reducen la exposición de actividades no autorizadas y proveyendo acceso a la información y sistemas solo a las personas, procesos y sistemas autorizados.

Adicionalmente, casi todos los puntos de entrada de una organización y sus sistemas de información necesitan algún tipo de control de acceso. Dada la importancia del control de acceso a través de las prácticas de seguridad, es necesario entender los cuatro atributos clave del control de acceso que permiten una buena administración de la seguridad. Específicamente, el control de acceso permite:

- Especificar que usuarios pueden acceder a un sistema.
- Especificar a qué recursos pueden acceder estos usuarios.
- Especificar que operaciones pueden ejecutar estos usuarios.
- Hacer respetar las responsabilidades y las no responsabilidades de las acciones de dichos usuarios.

Cada una de estas cuatro áreas, aunque están interrelacionadas, representan un enfoque establecido e individual para definir una estrategia eficaz de control de acceso. (Hernandez, 2012, pág. 5)

2.7.3. Proceso de control de acceso

Existen muchos enfoques diferentes para implementar un esquema de control de acceso. Sin embargo, según (Hernandez, 2012), hay un enfoque general que es aplicable a casi cualquier situación y provee un marco de trabajo útil para el control de acceso. El proceso puede dividirse en tres actividades:

- Definir los recursos

La primera actividad para permitir una estrategia efectiva de control de acceso es específicamente definir los recursos o componentes que existen en el entorno para que los usuarios puedan acceder. Esencialmente, este paso responde la pregunta fundamental de seguridad, “¿Que se está intentando proteger?”.

- Determinar los usuarios

La siguiente actividad en la gestión de control de acceso es la definición de quien puede acceder a los recursos dados. El concepto de identificación de quien tiene permitido el acceso y proporcionar las credenciales necesarias para su rol es fundamental para la seguridad.

El acto de especificar que usuarios pueden tener acceso a un sistema es típicamente manejado por una demanda operacional. Las decisiones en el control de acceso usualmente se basan en consideraciones organizacionales, sociales o políticas. El estatus personal o funcional dentro de la organización puede dictar el tipo o el alcance del acceso a los activos de la organización que pueden ser asignados.

El aspecto más importante de determinar qué usuarios tendrán acceso es una clara comprensión de las necesidades del usuario y el nivel de confianza dado a esa persona o entidad. Debe existir

un proceso de identificación, el cual toma en consideración la validez de la necesidad de acceso a la luz de las necesidades del negocio, política de la organización, los requisitos legales, información sensible, y riesgo para la seguridad. Es importante comprender que, con cada nuevo usuario o comunidad, el perfil de riesgo de una organización cambia.

- Especificar el uso de los usuarios hacia los recursos

Finalmente, en el proceso de control de acceso es para especificar el nivel de utilización de un recurso dado y las acciones de los usuarios permitidos para ese recurso.

Por último, una vez que un usuario se identifica y autentica, un sistema de control de acceso debe ser sensible al nivel de autorización para dicho usuario a utilizar los recursos identificados. Por lo tanto, no es suficiente simplemente con identificar y autenticar a un usuario con el fin de acceder a los recursos. También es necesario controlar que acciones son permitidas para un recurso determinado en base a la función del usuario.

2.7.4. Política de control de acceso

“El primer elemento de un programa de control de acceso efectivo es establecer una política de control de acceso y asociar estándares y procedimientos. Una política de control de acceso especifica los lineamientos de cómo los usuarios son identificados y autenticados y el nivel de acceso concedido a los recursos” (Hernandez, 2012). La existencia de una política de control de acceso asegura que las decisiones que rigen el acceso a los activos de la empresa se basan en una directriz institucional formalizada. La ausencia de una política dará lugar a inconsistencias en el aprovisionamiento, la gestión y administración de los controles de acceso. La política proveerá el marco de trabajo para la definición de los procedimientos necesarios, lineamientos, estándares y las mejores prácticas en relación con la supervisión de la gestión de accesos.

2.7.5. Retos del proceso de control de acceso

De acuerdo con (Osiatis), aplicar el proceso de control de acceso en una organización trae consigo una lista de retos a considerar, los principales retos a que se enfrenta habitualmente la gestión de acceso son:

- ✓ Verificar la identidad de los usuarios.
- ✓ Verificar la identidad de la persona u organismo que autoriza la asignación de permisos.
- ✓ Integrar múltiples niveles de permisos para un usuario concreto.
- ✓ Determinar con rapidez y fiabilidad el nivel de permisos del usuario en cualquier momento.
- ✓ Gestionar cambios en los requisitos de acceso de los usuarios.
- ✓ Restringir los permisos de acceso a los usuarios no autorizados.
- ✓ Mantener una base de datos actualizada donde se encuentren todos los usuarios y los permisos que poseen.

2.7.6. Ventajas del proceso de control de acceso

En contraposición a los retos que presenta la gestión de acceso existen una serie de ventajas o beneficios a las organizacionales según (Osiatis), entre los que se encuentran:

- ✓ Mayor garantía de confidencialidad de la información, gracias a un acceso controlado a los servicios.
- ✓ Mayor efectividad de los empleados, al minimizarse los conflictos y problemas derivados de la asignación de permisos.
- ✓ Menor probabilidad de errores en servicios críticos relacionados con la actividad de usuarios no cualificados.
- ✓ Capacidad de monitorizar el uso de los servicios y detectar casos de abuso de los mismos.
- ✓ Mayor rapidez y eficacia al revocar permisos en caso de ser necesario, algo que puede ser crítico para la seguridad en determinadas circunstancias.
- ✓ La gestión de acceso puede, además, ser un requisito indispensable para la adecuación a determinados estándares de calidad.

2.7.7. Elementos del proceso de control de acceso

A continuación, se van a definir los elementos conceptuales necesarios para comprender el proceso de control de accesos lógicos en una organización:

- Componente

Es toda aplicación, servicio o producto que proporciona una organización a sus empleados para que estos puedan ejecutar sus labores según su posición funcional. Existen diversos tipos de componentes, como las aplicaciones de negocio o sistemas, los servicios bancarios, dispositivos de red como servidores, bases de datos, entre otros.

- Perfil/Rol

Es el nivel de permiso o privilegio que puede ser otorgado dentro de un componente. Este define qué acciones puede y que acciones no puede ejecutar un usuario dentro de dicho componente. Un usuario podría tener el perfil "Consulta" el cual solo le permitiría realizar acciones de lectura sobre la información en el componente, mientras que un usuario con perfil "Ingresador" podría realizar acciones tanto de lectura como de escritura y actualización de la información.

- Unidad Organizacional

Es toda área, unidad, departamento o dirección de negocio que representa un nivel jerárquico dentro de una empresa u organización, y donde sus funcionarios realizan actividades y labores homogéneas. Ejemplos de unidades organizacionales podrían ser la "Unidad de Seguridad de Información" y la "Dirección de Tecnología de Información".

2.8. Estado del arte

2.8.1. Descripción del proceso de solicitudes de accesos de la plataforma Ultimus

CAF Banco de Desarrollo de América Latina, ha manejado el proceso de solicitud de los accesos en las aplicaciones de negocio y servicios bancarios de sus empleados a través de una solución de *Workflow* o Flujo de Trabajo creada por la empresa Ultimus Enterprise Solutions llamada “Perfiles de Acceso”.

Según (Ultimus Enterprise Solutions, 2016), la empresa busca automatizar, mejorar y racionalizar las operaciones de negocio del día a día de las organizaciones que requieran sus servicios. Este software en particular, llamado Perfiles de Acceso, es una herramienta de automatización simple para dirigir solicitudes de acceso y tareas a los usuarios responsables en el proceso de control de acceso para tomar acciones. Proporciona información y apoyo para cada etapa del ciclo del proceso y del negocio. Las solicitudes realizadas se transfieren de un usuario a otro cuando han culminado las actividades correspondientes.

Sin embargo, este flujo fue desarrollado para satisfacer las necesidades particulares que tenía CAF en su momento y no se contempló el crecimiento de las necesidades de la organización, imposibilitando la inclusión de mejoras y cambios en el proceso. Un ejemplo de este crecimiento, es el Perfilamiento Corporativo, el cual se está llevando a cabo en dicha organización, pero que con el actual sistema no es capaz de implementar.

El sistema de Perfiles de Acceso de Ultimus no le garantiza a la organización el cumplimiento de los tres principios básicos de la seguridad en su totalidad. La integridad de la información de que perfiles o que accesos tiene cada funcionario dentro de la empresa no es manejada por dicho sistema, ya que este no contempla lo que se conoce como la Matriz de Control de Acceso y no dispone de un módulo de reportes y gestión de estadísticas, pudiendo sólo canalizarse a través de extracciones de información directamente de la base de datos, sin lógica de procesamiento y sin la oportunidad de entrega requerida para este tipo de información.

La disponibilidad también se ve comprometida debido a que el sistema no posee de un administrador que facilite las actividades para permitir el crecimiento de la aplicación, y debido a esto, cuando se quiere hacer algún tipo de cambio menor en el sistema es necesario dar de baja al sistema irrumpiendo así la continuidad del negocio.

A continuación, se puede apreciar en la Ilustración 19 el formulario de solicitud de Perfiles de Acceso de Ultimus. Un aspecto importante de este formulario, es el hecho de que el sistema solo permite escoger perfiles genéricos (Consulta, Ingreso o Verificación), agregando un trabajo adicional tanto al solicitante como a los demás participantes del flujo al tener que especificar en el “Motivo de la Solicitud” exactamente lo que se quiere, ocasionando que muchas de las solicitudes sean rechazadas por no contar con explicaciones acordes.

PERFILES DE ACCESO, 0 : Solicitar Acceso - Windows Internet Explorer

Enviar Formulario Guardar Plantilla Ver Comentarios Imprimir Ayuda

PerfilesAcceso

CAF Corporación Andina de Fomento

Perfiles de Acceso

Solicitar Acceso

Información de Cliente

Apellido y Nombre	Unidad Administrativa	No. Carnet	Extensión
CASTRO LAZO, JOSÉ GABRIEL	DIRECCION CORPORATIVA DE CAPITAL HUMANO		0

Instancia Aprobatoria

BELLIDO VALERIO, JOSÉ

Motivo de la Solicitud

Solicitud de Usuario

☐ Creación de Usuario
 ☐ Actualización de Usuario
 ☐ Reemplazo Temporales
 ☐ Eliminación de Usuario

Fecha Desde:
 Fecha Hasta:
☐ Cambio de Contraseña
 ☐ Desbloqueo de Usuario

Tipo de Perfil Solicitado

☐ Creación de Perfil
 ☐ Actualización de Perfil
 ☐ Reemplazo Temporal de Perfil
 ☐ Eliminación de Perfil

Fecha Desde:
 Fecha Hasta:

Mecanismo de Autenticación

☐ Emisión de Token/Certificado
 ☐ Reemplazo de Token/Certificado
 ☐ Revocación de Token/Certificado

Sistemas Solicitados

	Consulta	Ingreso Modificación Operador	Verificación/ Aprobación	No Aplica
Sistema de Crédito Phoenix	☐	☐	☐	☒
Flujo de autorización de Desembolsos Workflow	☐	☐	☐	☒
Sistema de Inversiones Portia	☐	☐	☐	☒
Mercantil En Línea Empresa Venezuela	☐	☐	☐	☒
Swift - Sistema de Transferencias Electrónicas	☐	☐	☐	☒

ILUSTRACIÓN 19 FORMULARIO DE SOLICITUD DE PERFILES DE ACCESO DE ULTIMUS

Como se muestra en la Ilustración 20, el sistema permite ver el estatus actual de una solicitud junto con los tiempos que se tomó cada participante en el flujo. También es posible ver el estatus de forma gráfica como se muestra en la Ilustración 21, donde se aprecia un caso donde la solicitud fue atendida en su totalidad.

Step	Client	Begin	End	Status
Solicitar Acceso	CAF.COM/MPARD...	8/24/2011 10:59:18 AM	8/24/2011 10:59:1...	Completed
Aprobar Solicitud	REQUENA, BERNA...	8/24/2011 10:59:19 AM	8/30/2011 5:09:58...	Completed
Gestionar Solicitud	NAVARRETE, ELIO	8/30/2011 5:09:58 PM	8/30/2011 7:31:53...	Completed
Notificar Aprobaci...	RAXUS2_FLOBOT	8/30/2011 5:09:59 PM	8/30/2011 5:10:11...	Completed
Autorizar Solicitud	PEÑA, REINALDO	8/30/2011 7:31:53 PM	9/21/2011 3:21:54...	Completed
Notificar Autoriza...	RAXUS2_FLOBOT	9/21/2011 3:21:54 PM	9/21/2011 3:22:04...	Completed

ILUSTRACIÓN 20 ESTATUS DEL INCIDENTE

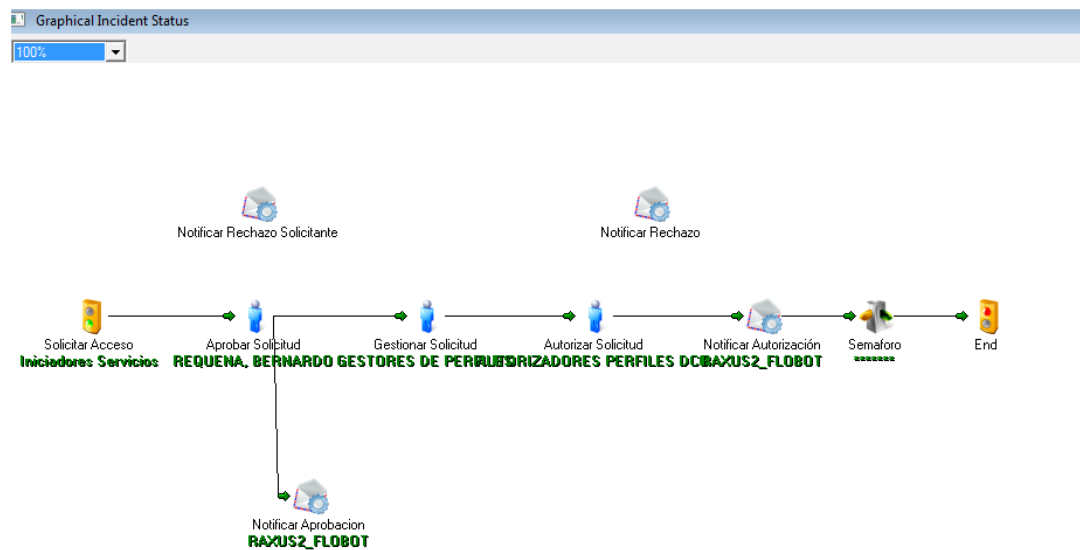


ILUSTRACIÓN 21 GRÁFICO DEL ESTATUS DEL INCIDENTE

En conclusión, el sistema tiene una gran cantidad de aspectos que resaltar para mejorar, y como plantea el requerimiento del control de acceso “Mantenibilidad”, un sistema que es demasiado complicado para entender o difícil de mantener es uno que va a caer ya sea rápidamente en desorden o será sustituido por un sistema que sea más fácil de manejar.

2.8.2. Descripción del proceso de solicitudes de accesos de la plataforma Bizagi

Bizagi, la cual es una de las empresas líderes en la automatización de procesos y que además “fue nombrada por Gartner en el 2010 en su Cuadrante Mágico de Suites BPM” (Bizagi, 2016) realizó un documento de construcción donde describen el proceso de control de acceso de forma general mediante un diagrama BPMN que se encuentra en la Ilustración 22.

En este proceso propuesto por Bizagi existen cuatro actores que interactúan el flujo, estos son:

- Solicitante: pudiendo ser el mismo usuario que requiere del acceso, o un tercero como personal de Recursos Humanos o un Administrador de Seguridad.
- Jefe Solicitante: quien, de ser necesario, aprueba o rechaza la solicitud realizada por un usuario según corresponda el caso.
- Administrador de Accesos: Es el oficial de seguridad o de tecnología que se encarga de otorgar los permisos al solicitante.
- Equipo de Soporte: es la persona a la que el administrador de accesos puede pedir gestiones adicionales para realizar la activación de un permiso de ser necesario.

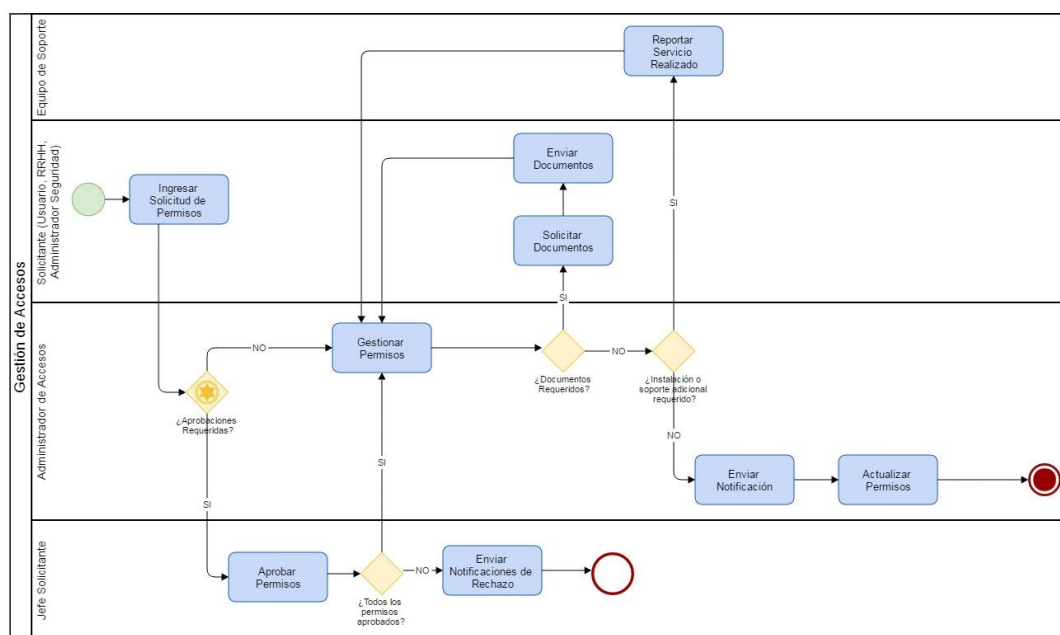


ILUSTRACIÓN 22 FLUJO DE SOLICITUD DE ACCESOS PROPUESTO POR BIZAGI

FUENTE: ADAPTACIÓN DE (BIZAGI, 2014)

2.9. Modelo propuesto

Tomando en cuenta tanto el proceso planteado por Ultimus, como el de Bizagi, se han encontrado varios puntos que pueden ser mejorados en la implementación de un nuevo proceso de control de

acceso que siga con la metodología y buenas prácticas tanto de la gestión de seguridad de información, como de la gestión de procesos de negocio. Dichas mejoras y buenas prácticas son explicadas a continuación:

1.3.7. Doble participación

Se incluye dentro del proceso a un nuevo participante, que también es un funcionario encargado de gestionar la seguridad de la información dentro de la organización. Dicho participante se conoce como "Verificador de Accesos", y lo que se busca con su inclusión es agregar un módulo de doble participación o doble verificación, donde si este se percata de un error en el otorgamiento, o rechazo indebido de uno o más accesos, tiene la posibilidad de regresar la solicitud al módulo de administración (regresar la solicitud al Administrador de Accesos) para hacer las correcciones correspondientes.

1.3.8. Posición Funcional

Representa las funciones que ejecuta un empleado dentro de una Unidad Organizacional. Por ejemplo, dentro de la "Unidad De Seguridad de Información" pueden trabajar varios funcionarios, donde cada uno tiene una labor específica, como lo son el encargado del control de acceso, el de monitoreo y el de incidentes. Tomando esto en cuenta, una posición funcional podría ser "Administrador de Accesos", el funcionario que tenga asignado dicha posición funcional tendrá permisos diferentes al "Administrador de incidentes" aunque ambos pertenezcan a la misma Unidad dentro de la organización.

Este concepto intenta cumplir con el requerimiento "Transparencia" del control de acceso, ya que un proceso transparente sería en el que el sistema de acceso deba tener una estructura basada en roles. Esto requiere menos trabajo e interacción por parte del usuario y dará lugar a la decisión de control de acceso más precisos y seguros ya que el acceso se basa en la necesidad predefinida y no la preferencia del usuario. (Hernandez, 2012)

1.3.9. Perfilamiento Corporativo

Debido al gran crecimiento que han tenido muchas organizaciones a nivel de recurso humano, ha crecido proporcionalmente la cantidad de componentes que se requieren para llevar a cabo todas las tareas necesarias de la organización, y consiguiente ha aumentado la cantidad de perfiles que se otorgan a los funcionarios que ejecutan dichas tareas.

Este crecimiento ha aumentado la complejidad de varios de los retos con los que deben lidiar las organizaciones, ya que la unidad responsable de brindar los accesos debe ser capaz de llevar un control íntegro y confiable de que permisos tiene cada funcionario, encargarse de remover los accesos a quienes no lo requieren y mantener siempre una homogeneidad en los permisos que tienen funcionarios con posiciones funcionales iguales o parecidas. De no poseer este control de forma eficiente, podría causar diversas brechas de seguridad, vulnerabilidades en los componentes e interrupciones en la continuidad del negocio.

El Perfilamiento Corporativo no es más que un marco de trabajo que permite definir y organizar que perfiles están asociados a una posición funcional dentro de una organización permitiéndole a los usuarios cumplir con sus funciones haciendo uso de una correcta segregación de funciones.

Una adecuada segregación de funciones reduce la probabilidad de que los errores, sean intencionales o involuntarios, no sean detectados. Asimismo, puede brindar asistencia en la protección de los activos de la organización. (KPMG, 2015)

Además de lo antes mencionado, el perfilamiento corporativo disminuye la cantidad de solicitudes generadas por persona, ya que teniendo bien definido las posiciones funcionales de la organización con sus respectivos accesos, solo sería necesario realizar una única solicitud que indique lo que eres y no varias solicitudes indicando lo que el usuario quiere o hace.

Por todo lo antes mencionado, se decidió que las solicitudes se basen en posiciones funcionales y no en accesos individuales por cada aplicación dentro de la organización.

Finalmente, al incluir estos puntos como mejoras a los procesos de control de acceso ya existente, se puede generar un nuevo proceso optimizado como se muestra en la Ilustración 23, donde el flujo inicia con el ingreso de una solicitud de activación o desactivación de una posición funcional con sus respectivos accesos a un empleado, la cual puede ser ingresada por el usuario que requiere el acceso o a través de un tercero, como recursos humanos cuando ingresa un nuevo funcionario, o los mismos administradores de seguridad. Una vez se ingresa la información general de la solicitud junto con la lista de permisos y acciones requeridas, se evalúa la necesidad de que una Instancia Aprobatoria apruebe la solicitud que contiene cada uno de los permisos requeridos. De ser este el caso, dicha Instancia Aprobatoria evalúa la solicitud y una vez aprobada, el Administrador de accesos procede a ejecutarlas. Este paso se repite tantos permisos haya requerido el usuario y una vez todas las acciones de la solicitud han sido ejecutadas, será el turno del Verificador de accesos de hacer la doble participación en el proceso, donde sí se percata de un error en la administración tiene la posibilidad de regresar la solicitud para hacer las correcciones correspondientes, de lo contrario se actualiza la lista de permisos activos del usuario y se le envía una notificación con el resumen de los mismos. Posteriormente el caso es cerrado.

En las Ilustraciones 23 y 24, se muestra el proceso de cancelación (en el caso de que ya no se quiera realizar la solicitud) y modificación (en caso de que el solicitante haya cometido algún error al enviar la solicitud) respectivamente.

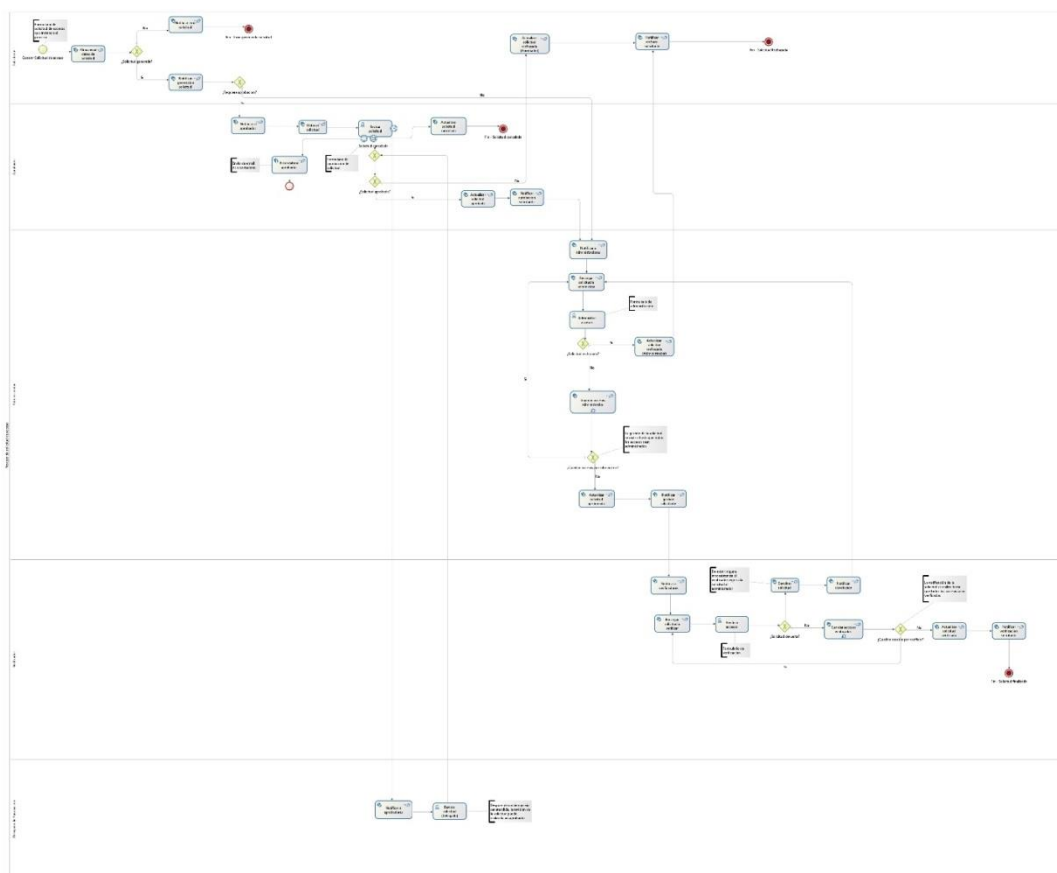


ILUSTRACIÓN 23 PROCESO DE CONTROL DE ACCESO PROPUESTO (FLUJO BÁSICO)

FUENTE: ELABORACIÓN PROPIA

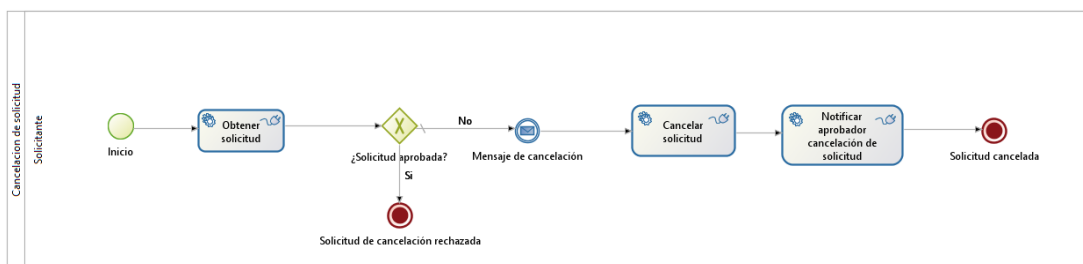


ILUSTRACIÓN 24 PROCESO DE CONTROL DE ACCESO PROPUESTO (CANCELACIÓN)

FUENTE: ELABORACIÓN PROPIA

CAPÍTULO 2

MARCO METODOLÓGICO

Una vez identificado el problema de investigación, definido los objetivos y argumentado teóricamente el mismo, es pertinente indicar cuáles serán los procedimientos utilizados para alcanzar dichos objetivos. De esta manera, se proporcionará al lector la información detallada sobre la metodología empleada para la realización del proyecto investigativo.

2.10. Metodología de desarrollo

La Gestión de Procesos de Negocio (BPM) es un marco de trabajo con un enfoque empresarial operativo basado en la coordinación de las actividades y decisiones que todas las partes involucradas deben realizar durante un proceso de negocio, con el objetivo de convertirse en una organización altamente eficiente, ágil, innovadora y adaptable.

Las etapas del ciclo de vida del BPM están condicionadas por varios autores o fabricantes de BPMS. Se puede apreciar en diversos materiales que el número y nomenclatura de las fases son diferentes en cada ciclo, es decir, estas son distribuidas de manera distinta, pero en general conllevan su enfoque al mismo contexto. Dicho esto, se decidió emplear la metodología basada en las mejores prácticas del ciclo de vida BPM que se aprecia en la Ilustración 25 y fue propuesto por (Smith & Fingar, 2003), la cual está compuesta por dos macro procesos: la creación del proceso de negocio (engloba las fases de descubrimiento, modelado, despliegue y ejecución) y la administración del proceso una vez este ejecutado (engloba las fases de monitoreo y optimización).

La primera fase del ciclo BPM llamada descubrimiento, también conocida como etapa de análisis, se refiere al momento en el que el proceso, ya sea nuevo o uno existente, es estudiando a profundidad para determinar los requerimientos y/o mejoras perfectamente. La siguiente fase es el modelado o diseño, y en esta etapa se definen los diferentes participantes del proceso, las reglas de negocio, los indicadores claves de rendimiento y todos los elementos que requiera el proceso, por lo que se requiere que intervengan los analistas del negocio. Luego toma lugar el despliegue, donde ya con una idea menos abstracta el proceso toma vida con la ayuda de alguna forma tecnológica que asista a la implementación para luego ser ejecutado. Por último, el proceso es monitoreado, y si existen aspectos a mejorar entra en fase de optimización.

Finalmente, el ciclo vuelve a su punto inicial, con el fin de realizar adaptaciones permanentes que van a la mano con la premisa de que los procesos, como las organizaciones, cambian constantemente. Al iterar los procesos se pueden generar nuevos conocimientos producto de la experiencia que sirven para incluirlos y garantizar el mejoramiento continuo.



ILUSTRACIÓN 25 CICLO DE VIDA BPM

FUENTE: ELABORACIÓN PROPIA

2.10.1. Descubrimiento

Con esta primera fase lo que se quiere obtener es la descripción de cada una de las actividades que componen el proceso, especificando todos los detalles de cada uno de los requisitos y centrándose, principalmente, en las funcionalidades clave. Estas actividades generalmente están estrechamente relacionadas con los participantes del proceso y con los sistemas que lo soportan, y lo que se busca es convertir el proceso en algo claro a través del conocimiento contenido en estas fuentes. En este punto se quiere detallar como es el comportamiento actual de forma objetiva, en vez de conciliar las opiniones subjetivas de los diferentes participantes del proceso.

2.10.2. Modelado

La segunda fase comprende el modelado, manipulación y rediseño de los procesos de negocio. Dicha fase toma en cuenta actividades, reglas, relaciones, participantes, sistemas e información para construir un modelo fácil de comprender por el dueño del proceso y que pueda adaptarse sin problemas a la hora de que surjan modificaciones internas del negocio o cambios del mercado.

Para la construcción de estos modelos dinámicos, las herramientas existentes no son suficiente, es aquí donde entra en juego la Notación de Modelado de Procesos de Negocio (BPMN), la cual logra el entendimiento entre las partes (el negocio y la tecnología), y adicionalmente, se necesitan herramientas que faciliten la captura de los elementos abstractos del negocio y que impacten al

proceso y la aplicación rápida y efectiva de los cambios en este, estas herramientas son las denominadas Suites BPM (BPMS).

2.10.3. Despliegue

Esta fase del ciclo es en la cual se traslada el proceso y sus actividades a la plataforma tecnológica sobre la cual va a correr, y se fijan las relaciones que dicho proceso va a tener con otros procesos y al llevar el proceso a sus participantes, se distribuye el trabajo de cada uno de estos y se asignan los recursos que van a ser utilizados durante la ejecución del proceso.

En esta fase se integran los componentes necesarios para implementar el proceso. Para implementar los procesos es necesaria una serie de configuraciones y reglas descritas a continuación:

- ✓ Importación y configuración de procesos y actividades.
- ✓ Definición de reglas de negocio.
- ✓ Integración con sistemas (EAI).

2.10.4. Ejecución

En esta fase se quiere gestionar las actividades realizadas por cada participante del proceso para asegurar la correcta ejecución del mismo. El sistema administrador de procesos es el que se encarga de esta fase y es responsable de que las diferentes plataformas o sistemas que soportan el proceso sean transparentes para el usuario. Este sistema administrador de procesos debe asegurar la comunicación entre los diferentes entes que intervienen en el proceso y el correcto funcionamiento de los mismos. Además, en este punto es cuando se recopila la información para el monitoreo de los procesos.

Es la fase donde se aprovecha el proceso desarrollado previamente mediante:

- ✓ Espacio de trabajo.
- ✓ Lista de tareas pendientes.
- ✓ Gestión de excepciones.
- ✓ Inicio de procesos desde formularios.
- ✓ Configuración y personalización del espacio de trabajo.

2.10.5. Monitoreo

El proceso de negocio debe ser medible para saber su grado de éxito y calidad con el que se ha desarrollado. De esta forma, se pueden analizar los resultados del proceso para que pueda ser redefinidos y optimizados.

Esta fase realiza seguimiento continuo a las actividades del proceso con el fin de asegurar que éste se realice adecuadamente. El monitoreo se realiza durante la ejecución del proceso debiendo identificar y administrar las excepciones o errores que se presenten, la necesidad y asignación de recursos, los cambios que se produzcan durante la marcha y en general, toda situación que represente un cambio

o mejora en el proceso. Este trabajo puede llevarse a cabo manualmente o apoyarse en una herramienta tecnológica.

2.10.6. Optimización

Si el proceso no ha cumplido las expectativas deseadas, ya sea porque no posee un conjunto coherente de tareas, o porque las necesidades ya no son las mismas, debe ser optimizado para que pueda mejorar su rendimiento y así también el de la organización. Esto garantiza el mejoramiento continuo del mismo, eliminando inconsistencias para asegurar que su ejecución corresponda con el diseño del mismo.

La optimización se lleva a cabo juntando información de la fase de modelado y los datos de desempeño de la fase de monitoreo, para que así, puedan ser comparados, logrando identificar los problemas que pueda presentar el proceso y se proponen acciones correctivas. Dichas acciones se aplican en la primera fase del ciclo, es decir, en la fase de descubrimiento.

CAPÍTULO 3

MARCO APLICATIVO

En este capítulo se presenta la implementación de la propuesta de solución del Trabajo Especial de Grado. Dicha propuesta se basa en la aplicación de la metodología BPM para el desarrollo del proceso de control de acceso o de solicitudes de acceso. Esta metodología está basada en las mejores prácticas en el proceso de desarrollo de un sistema de Gestión de Procesos de Negocio. De esta manera, se expone la síntesis del proyecto, las herramientas tecnológicas utilizadas y cada una de las fases asociadas al enfoque aplicado.

3.1. Sistema de solicitudes de acceso

El presente Trabajo Especial de Grado, se basó en la elaboración de una guía apoyada en la ISO 27001 que permitió implementar, a través de la Gestión de Proceso de Negocio, parte de un Sistema de Gestión de la Seguridad de la Información, tomando las tareas y reglas de negocio pertinentes y necesarias dentro del ámbito del control de acceso, para generar un proceso que permita la generación de solicitudes de acceso sobre las aplicaciones de una organización. Las fases de la metodología BPM que fueron llevadas a cabo son: descubrimiento, modelado, despliegue y ejecución. Las etapas de monitoreo y optimización no se encontraron en el alcance del presente trabajo, ya que estas se realizan cuando se lleva la implementación a producción dentro de una organización.

La plataforma BPM que se utilizó para esta implementación fue la versión community de Bonitasoft, la cual permitió un control total del proceso, sus casos, actividades, usuarios, notificaciones, entre otros. Adicional a esto, se contó con la implementación de unos servicios web que permitieron acceder a la información de una organización y llevar el control de las solicitudes de acceso que se generan dentro del sistema.

3.2. Herramientas tecnológicas

A continuación, se describen las herramientas seleccionadas para la implementación de la solución propuesta en el Capítulo 1.

3.2.1. Bonita BPM

Bonita BPM es una poderosa plataforma de aplicaciones basadas en BPM para crear aplicaciones empresariales personalizadas y basadas en procesos altamente atractivas para hacer las cosas, aprovechar al máximo el BPM y adaptarse a los cambios del negocio en tiempo real. (BonitaSoft, 2016)

Bonita BPM tiene dos partes: el entorno de desarrollo (Bonita BPM Studio), y el entorno de ejecución (Bonita BPM Platform).

Bonita BPM proporciona dos ediciones en la actualidad (BonitaSoft, 2016):

- ✓ **Community:** Es la edición de código abierto, la cual permite entre las funcionalidades más importantes: modelado, conectores, generación de aplicaciones empresariales basadas en procesos, entre otros.
- ✓ **Suscription:** sus principales características son:
 - Construcción de aplicaciones aún más rápido
 - Funciones avanzadas de diseño de interfaz de usuario
 - Colaboración en equipo
 - Integración y pruebas continuas
 - Conectividad avanzada a sistemas empresariales
 - Personalización de las necesidades de usuario final
 - Personalización completa de look & feel
 - Personalización de la interfaz de usuario final
 - Lista para dispositivos móviles
 - Construcción de aplicaciones que se adapten en tiempo real a los cambios del negocio
 - Actualizaciones en vivo sin interrupciones
 - Definir las tareas ad-hoc sobre la marcha
 - Escala para satisfacer las demandas de la empresa
 - Clustering
 - Multi-alquiler
 - Gestión de errores
 - Supervisión de las aplicaciones
 - Supervisión del tablero de instrumentos y visualización gráfica
 - Informes empresariales definidos por el usuario

La edición Community tiene licencia GNU GPL v2. Disponible para todas las plataformas de sistemas operativos. Esta desarrollada bajo el lenguaje Java.

3.2.1.1. Bonita BPM Studio

Es un entorno gráfico para crear procesos, aplicaciones, modelos de datos y vistas de usuarios (páginas y formularios). Contiene tres herramientas principales de diseño:

- ✓ La pizarra, que se muestra en la Ilustración 26, para dibujar un diagrama de flujo de proceso y definir el detalle de pasos, transiciones, puntos de decisión y otros elementos de proceso
- ✓ El menú de desarrollo, para ampliar las capacidades del estudio y crear sus modelos de datos
- ✓ El *UI Designer*, que se utiliza para crear páginas de aplicación y formularios de proceso

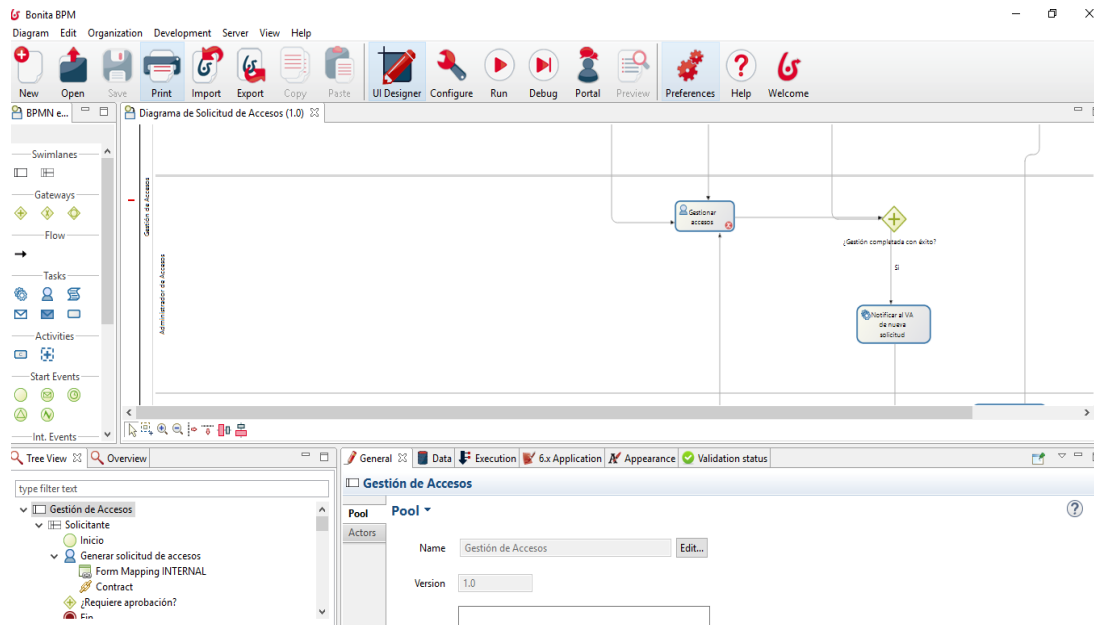


ILUSTRACIÓN 26 BONITA BPM STUDIO

3.2.1.2. Plataforma Bonita BPM

Bonita BPM Studio contiene la Plataforma Bonita BPM (Tomcat, *UI Designer*, el Portal Bonita BPM, el Motor Bonita BPM y una base de datos h2)

- ✓ Adecuada para probar una aplicación que está en desarrollo.
- ✓ Cuando se ejecuta un proceso, se despliega automáticamente en la plataforma de desarrollo.
- ✓ Los usuarios pueden utilizar Bonita BPM Portal (con su perfil de usuario), mostrado en la Ilustración 27, para ver y completar las tareas de proceso de todos los procesos.
- ✓ *Bonita BPM Engine* es el motor de ejecución de Bonita BPM.

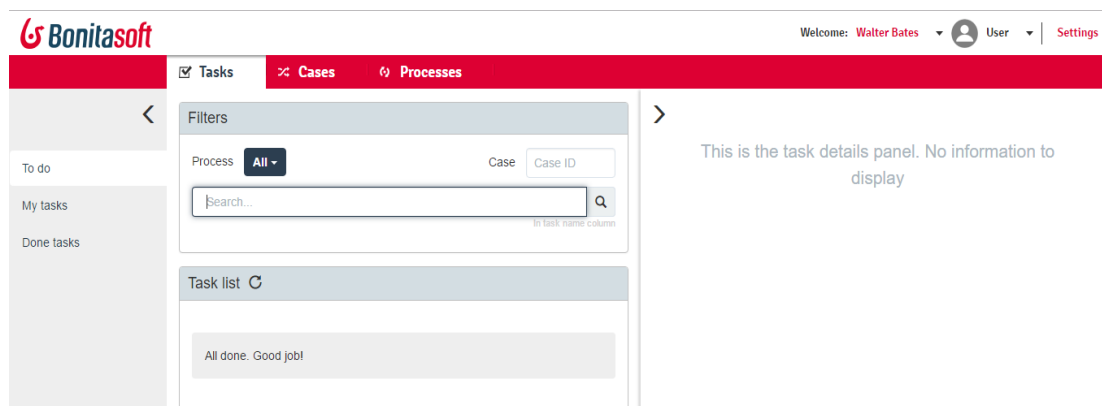


ILUSTRACIÓN 27 BONITA BPM PORTAL

3.2.1.3. REST API

Bonita BPM proporciona una API REST Web con la cual se puede integrar aplicaciones que utilicen otras tecnologías además de Java. Dicha API provee acceso a todos los objetos de Bonita BPM (como

procesos, tareas, usuarios, conectores, entre otros), para ejecutar operaciones sobre estos. En la Ilustración 28 se muestra como una aplicación cliente se conecta al motor de Bonita BPM a través de la API REST.

Entre las APIs que proporciona Bonita se encuentran: bdm API, bpm API, identity API y customuserinfo API.

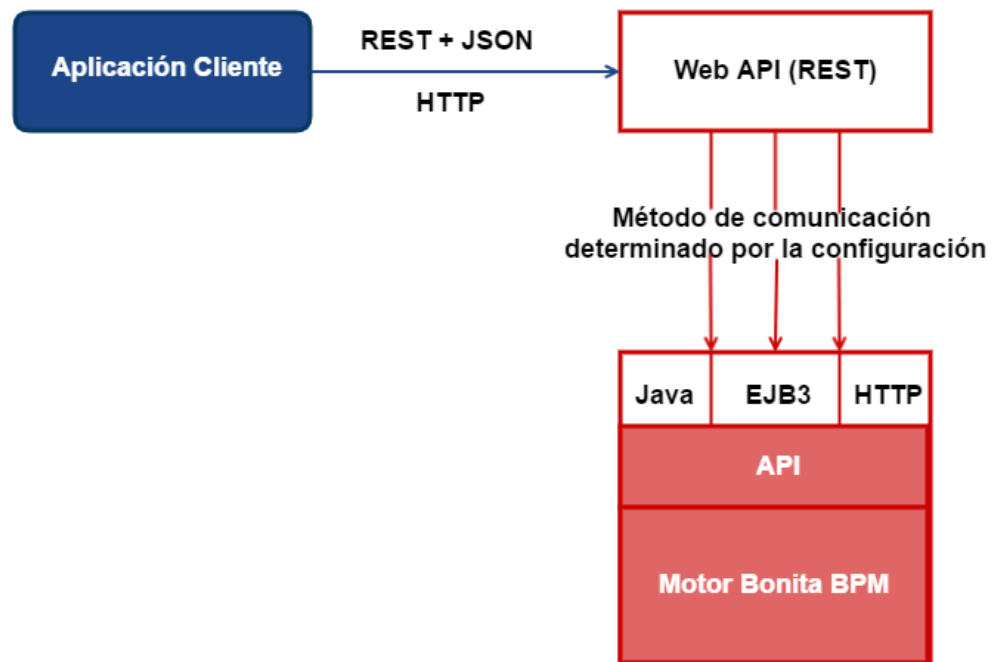


ILUSTRACIÓN 28 DIAGRAMA DE ARQUITECTURA DE UN CLIENTE REST INTEGRADO CON BONITA BPM (BONITASOFT, 2017)

3.2.2. Servicios Web

Un servicio web es un conjunto de protocolos y estándares abiertos utilizados para el intercambio de datos entre aplicaciones o sistemas. Los servicios web son utilizados por aplicaciones realizadas en distintos lenguajes de programación y que se ejecutan en diferentes plataformas para interoperar a través de Internet con el fin de ofrecer servicios entre ellas. Los proveedores ofrecen sus servicios como procedimientos remotos y los usuarios solicitan un servicio llamando a estos procedimientos a través de la web. (W3C)

Estos servicios proporcionan mecanismos de comunicación estándares entre diferentes aplicaciones, que interactúan entre sí para presentar información dinámica al usuario. Para proporcionar interoperabilidad y extensibilidad entre estas aplicaciones, y que al mismo tiempo sea posible su combinación para realizar operaciones complejas, es necesaria una arquitectura de referencia estándar.

La Ilustración 29 muestra cómo interactúa un conjunto de Servicios Web, donde un usuario (el cliente), a través de una aplicación, solicita información sobre un viaje que desea realizar haciendo una petición a una agencia de viajes que ofrece sus servicios a través de Internet. La agencia de viajes ofrecerá a su cliente (usuario) la información requerida. Para proporcionar al cliente la información que necesita, esta agencia de viajes solicita a su vez información a otros recursos (otros Servicios Web) en relación con el hotel y la compañía aérea. La agencia de viajes obtendrá información de estos recursos, lo que la convierte a su vez en cliente de esos otros Servicios Web que le van a proporcionar la información solicitada sobre el hotel y la línea aérea. Por último, el usuario realizará el pago del viaje a través de la agencia de viajes que servirá de intermediario entre el usuario y el servicio Web que gestionará el pago.

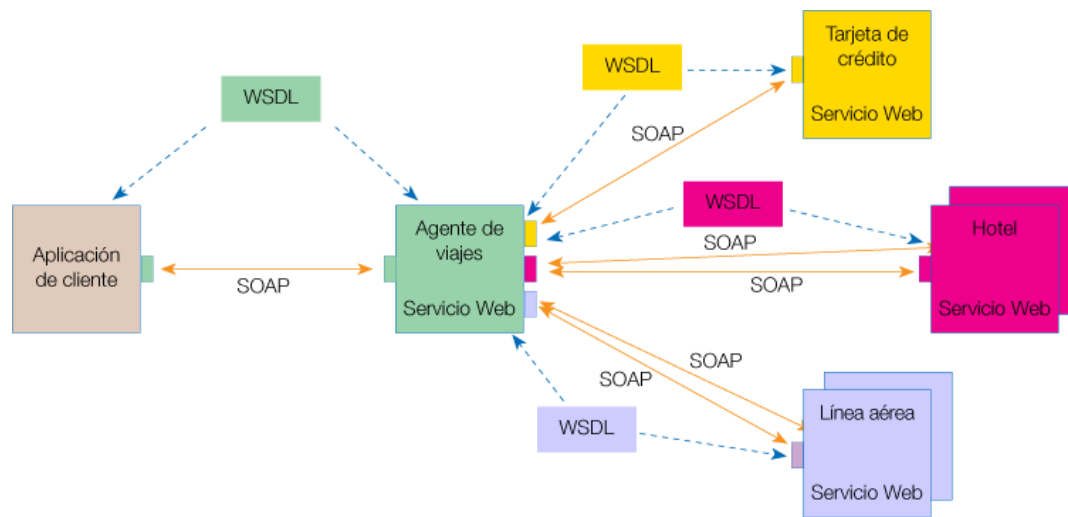


ILUSTRACIÓN 29 INTEROPERABILIDAD DE LOS SERVICIOS WEB (W3C)

3.2.3. MySQL

Según (Oracle, 2017), MySQL es el sistema manejador de bases de datos de código abierto más popular del mundo. Se ha convertido en una de las mejores opciones de base de datos relacionales para aplicaciones basadas en la Web. Gracias a su confiabilidad y facilidad de uso, se decidió optar por este manejador para almacenar toda la información referente al proceso de control de acceso. Es importante mencionar que MySQL no será conectada directamente con Bonita BPM, sino que como muestra la Ilustración 28, se accederá a la base de datos a través de servicios web y a su vez, serán estos los que se conectarán a Bonita.

3.2.3.1. Características

A continuación, se mencionan algunas de las características de MySQL según (Morales Carrizosa, 2017):

- Aprovecha la potencia de sistemas multiprocesador, gracias a su implementación multihilo.
- Soporta gran cantidad de tipos de datos para las columnas.
- Dispone de API's en gran cantidad de lenguajes (C, C++, Java, PHP, etc).

- Gran portabilidad entre sistemas.
- Soporta hasta 32 índices por tabla.
- Gestión de usuarios y contraseñas, manteniendo un muy buen nivel de seguridad en los datos.
- La condición de código abierto de MySQL hace que la utilización sea gratuita y se puede modificar con total libertad.
- Se puede descargar su código fuente. Esto ha favorecido muy positivamente en su desarrollo y continuas actualizaciones.
- Es una de las herramientas más utilizadas por los programadores orientados a Internet.
- Infinidad de librerías y otras herramientas que permiten su uso a través de gran cantidad de lenguajes de programación.
- MySQL, es el manejador de base de datos considerado como el más rápido de Internet.
- Gran rapidez y facilidad de uso.
- Infinidad de librerías y otras herramientas que permiten su uso a través de gran cantidad de lenguajes de programación.
- Fácil instalación y configuración.

3.3. Etapas del proyecto

3.3.1. Descubrimiento

En esta etapa, se tomaron los aspectos positivos de sistemas anteriores que intentan manejar el proceso de control de acceso, y a su vez, se evaluaron los aspectos negativos que permitieron encontrar mejoras para el flujo final. Los dos sistemas o diseños presentados en el Estado del Arte en el Capítulo II, fueron de mucha utilidad para estudiar y analizar a fondo la serie de tareas involucradas en las fases del control de acceso general de una organización, las cuales plantea (Hernandez, 2012), con el fin de crear un flujo de trabajo que representará al proceso de estudio y que pudiera ser modelado mediante el estándar BPMN y soportado bajo una herramienta tecnológica BPM.

La primera actividad del control de acceso para cualquier organización es la definición de los recursos que podrán ser accedidos dentro de la misma. Esta actividad está muy ligada a la gestión de activos y es algo que debe realizar la organización para tener claro que es lo que se está intentando proteger. Por esta razón, se asume como premisa que la organización tiene bien definido y documentado estos recursos que deberán ser protegidos y accedidos mediante roles y perfiles de acceso.

La siguiente actividad dentro del control de acceso es la especificación de los usuarios que podrán acceder a los recursos dados. Se busca identificar, a través de sus credenciales, quien tiene los permisos para los accesos dentro de la organización. Es necesario entender las necesidades del usuario y la confianza que tiene la organización sobre el mismo, por esto, se basa en la posición funcional de la persona dentro de la organización, evaluando las actividades que debe realizar diariamente y analizando que activos no son de su incumbencia. Es aquí donde comienza el proceso de control de acceso que se llevó a cabo en el presente trabajo, ya que la forma de identificar al usuario es a través de una solicitud que realiza el mismo para pedir o remover accesos. Estos accesos

no deberían ser escogidos al libre albedrío, si no que en vez de solicitar los accesos que el usuario desee, se debe seleccionar la posición funcional del usuario, la cual representa lo que realmente es y necesita. Luego, debe existir un ente aprobador en la organización que sea el encargado de decidir si esos accesos los puede tener el solicitante, en caso afirmativo aprobaría la solicitud realizada, y en caso contrario sería rechazado y los accesos no se le deberían asignar al mismo.

Por último, se tiene una actividad que busca especificar el nivel de utilización de un recurso dado y las acciones que puede ejecutar un usuario al que se le permita el acceso a dicho recurso. Esto debido a que no basta con la identificación y la autenticación de un usuario, sino que se necesita controlar el nivel de autorización que este poseerá para que ejecute solo las acciones que le sean correspondidas dentro del recurso en base a su posición funcional.

Luego del análisis de las diferentes fases del control de acceso básico propuesto por (Hernandez, 2012), se tomaron todas las actividades o tareas extraídas de cada una de las fases antes mencionadas y se organizaron secuencialmente, se definieron entradas y salidas y se desarrolló un proceso el cual simula de forma genérica el control de acceso de una organización.

Se pudo observar, que el proceso de control de acceso está conformado por al menos tres actividades de usuario y necesita de al menos tres usuarios para llevarlas a cabo. La primera actividad es la solicitud de los accesos por parte de un empleado o solicitante. La segunda actividad es la revisión de dicha solicitud, en la que se tiene un usuario que la aprueba o la rechaza. Finalmente, una actividad donde existe un usuario que da o quita dichos accesos. Sin embargo, con estas tres actividades no se garantiza que se le otorguen de forma adecuada los accesos a un empleado dentro de una organización, debido a que el encargado de otorgar dichos accesos podría cometer un error. Por lo antes mencionado, se decidió utilizar una de las buenas prácticas y recomendaciones planteadas en el área de la seguridad de la información, la cual es la doble participación, donde existe otro usuario que tiene la tarea de verificar que la solicitud fue gestionada adecuadamente.

Por lo tanto, se determinó que en el proceso resultante interactúan cuatro actores, los cuales son:

- Solicitante: es el usuario que generara la solicitud de acceso hacia los accesos de la organización.
- Aprobador: es el encargado de aprobar o rechazar las solicitudes de acceso realizadas por un solicitante. Este podría ser el jefe del usuario que realizo la solicitud, o bien, una Instancia Aprobatoria de la organización.
- Administrador: es el oficial de seguridad encargado de otorgar y/o revocar accesos en los diferentes componentes de la organización.
- Verificador: es el oficial de seguridad que vela porque los accesos otorgados y/o revocados por el Administrador se hayan realizado de manera correcta y efectiva.

Una vez identificadas las actividades y los participantes, se presenta a continuación el flujo de trabajo diseñado para cada uno de ellos mediante la tabla x:

TABLA 6 FLUJO DISEÑADO EN LA FASE DE DESCUBRIMIENTO

Actor	Actividad	Descripción	Regla de negocio
Solicitante	Generar solicitud de acceso	El usuario dispondrá de un formulario para generar una solicitud de accesos. Existen dos tipos de solicitudes, una de asignación de accesos y otra para remover los que ya tiene. Las solicitudes de acceso se realizan en base a una posición funcional y no en base a accesos individuales, es decir, se solicita en base a lo que se es, y no en base a lo que se quiere.	Si el tipo de solicitud es "Solicitud de Accesos" será necesario una aprobación. Por otro lado, si es una "Remoción de Accesos" no será necesaria dicha aprobación.
			Si el solicitante no posee ninguna posición funcional registrada en el sistema, se procederá a agregarle todos los accesos de la misma. En caso contrario, si el solicitante ya posee una posición funcional, esta será reemplazada.
			Si el solicitante no tiene accesos asignados en el sistema, no podrá realizar solicitudes de "Remoción de accesos".
Aprobador	Revisar solicitud	El aprobador es el encargado de revisar las solicitudes de acceso que se generen a través de un formulario. De ser correcta y pertinente, podrá ser aprobada. En caso contrario, será rechazada.	El aprobador asignado es el jefe directo del solicitante.
			En caso de rechazar la solicitud, será necesario colocar un motivo por el cual se realizó esta acción.
			Si el aprobador no ha revisado una solicitud por un periodo de 24 horas se le enviara un recordatorio vía email para que lleve a cabo la revisión.
			Si el aprobador no ha revisado una solicitud por un periodo de 48 horas, se procederá a realizar una delegación de la actividad, donde podrán realizar la misma, todos los usuarios que tengan el perfil "Aprobador" en el sistema.
Administrador	Administrar accesos	El administrador se encargará de otorgar y/o revocar los accesos necesarios según corresponda. El administrador tendrá la opción de gestionar uno o más accesos y guardar los cambios antes de finalizar la actividad en su totalidad. También, tiene la potestad de rechazar una solicitud, en el caso de darse cuenta de un error o inconveniente por parte del	Las solicitudes por gestionar podrán ser ejecutadas por todos los usuarios que tengan el perfil "Administrador" en el sistema.
			La solicitud no puede ser cerrada hasta que no se hayan gestionado cada uno de los accesos que contiene la misma.
			En caso de rechazar la solicitud, será necesario colocar un motivo por el cual se realizó esta acción.

		solicitante o del aprobador.	
Verificador	Verificar accesos	En esta actividad, el verificador deberá evaluar cada uno de los accesos dentro de una solicitud para avalar que todos hayan sido gestionados correctamente. En caso de que exista algún error o inconveniente, el verificador podrá regresar la solicitud al paso anterior. Sino, finalizara el proceso.	Las solicitudes por verificar podrán ser ejecutadas por todos los usuarios que tengan el perfil "Verificador" en el sistema.
			La solicitud no puede ser cerrada hasta que no se hayan verificado cada uno de los accesos que contiene la misma.
			En caso de devolución de la solicitud, será necesario colocar un motivo por el cual se realizó esta acción.
Solicitante	Cancelar solicitud	El usuario cancela una solicitud que haya generado previamente en caso de errores.	Si la solicitud está en estado "Pendiente" podrá ser cancelada. En caso contrario, no podrá ser cancelada.

FUENTE: ELABORACIÓN PROPIA

3.3.2. Modelado

Ya culminado la fase del descubrimiento del proceso de control de acceso, y después de haber analizado y detallado sus actividades, actores y reglas de negocio, se puede realizar la fase de modelado con la notación BPMN. En esta fase se utilizó la herramienta de gestión de procesos de negocio Bonita BPM.

Primero, fue pertinente la creación de la base de datos en el sistema manejador de bases de datos MySQL, la cual sirvió como repositorio centralizado para toda la información del control de acceso. Dicha base de datos, contiene ocho tablas relacionadas en las que se almacenan todos los datos necesarios para llevar a cabo el flujo y poder tener una traza de auditoria de las solicitudes en la conocida Matriz de Control de Acceso. En la Ilustración 30 se puede observar la estructura de la base de datos, y las tablas con sus atributos y tipos de datos respectivos.

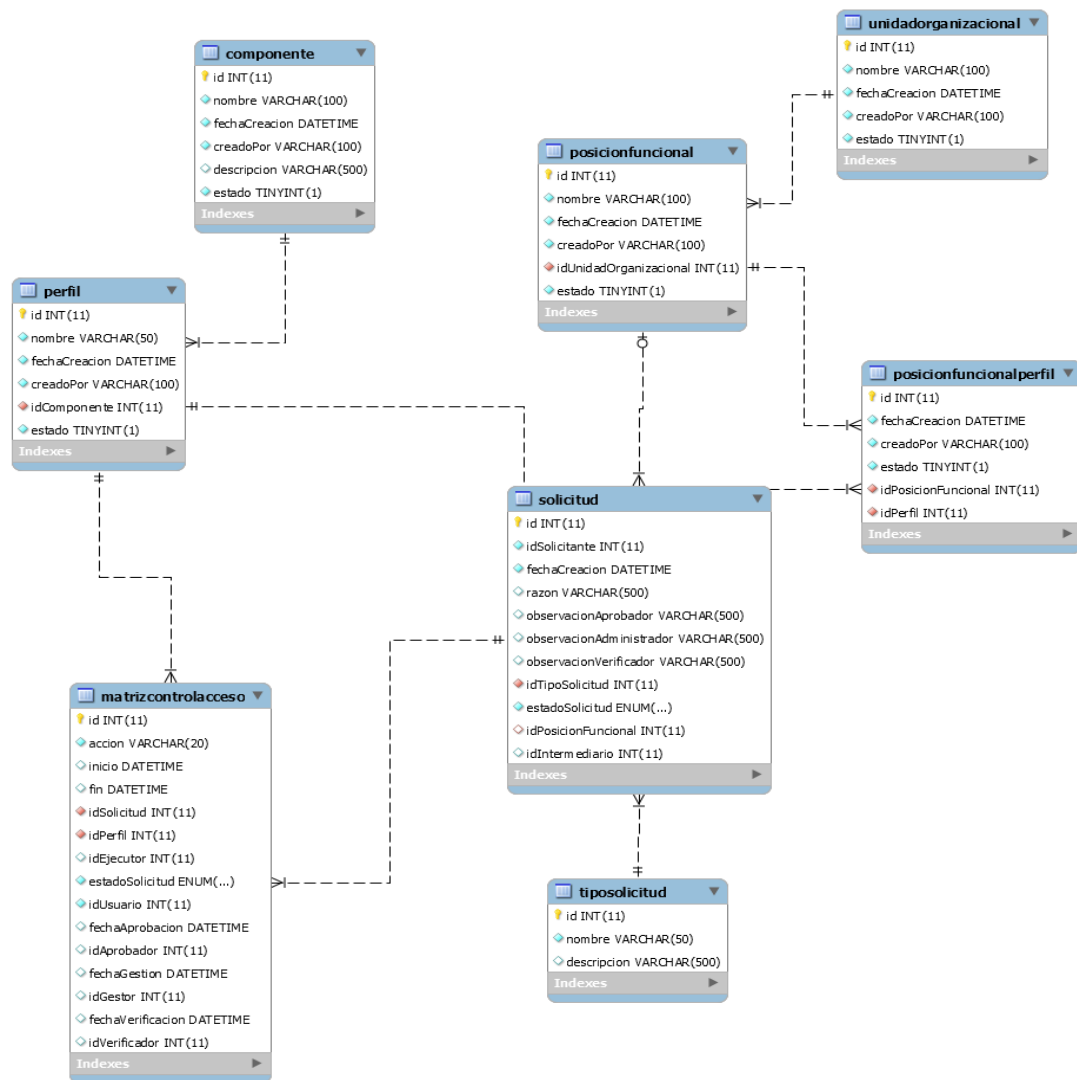


ILUSTRACIÓN 30 ESTRUCTURA DE LA BASE DE DATOS PARA EL CONTROL DE ACCESO

Seguidamente, se procedió a crear los servicios web que se utilizarían para conectarse con el proceso de control de acceso en Bonita BPM y que finalmente, serían los encargados de guardar la información en la base de datos. Estos servicios web se realizaron en el lenguaje Java con el IDE Netbeans. Se crearon ocho servicios web, uno para cada tabla dentro de la base de datos. En la Ilustración 31 se muestran los ocho servicios web desde el menú de Netbeans con todos sus endpoints.

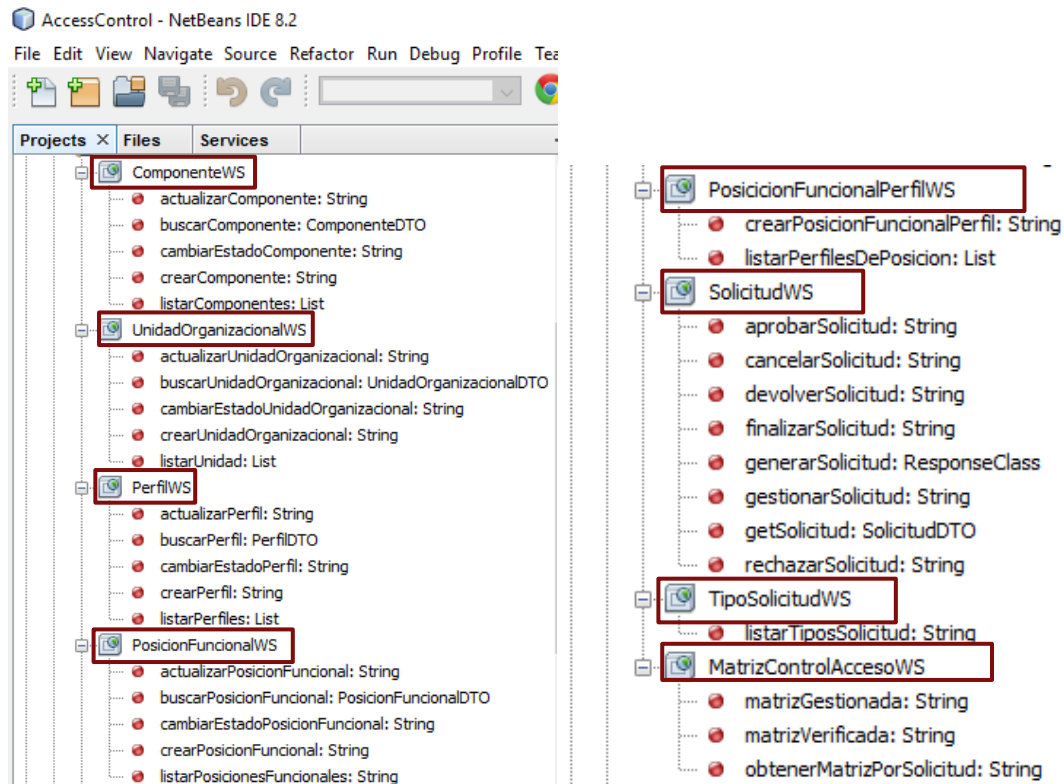


ILUSTRACIÓN 31 SERVICIOS WEB CON ENDPOINTS

Entrando en materia del modelado del proceso, lo primero que se realizó fue el diagrama de procesos de negocio en Bonita BPM Studio. En este diagrama es donde se modeló todo el proceso, incluyendo actores, tareas y las respectivas reglas de negocio. Los actores, fueron representados a través del elemento “Canal” de BPMN. De esta forma, se tienen los canales “Solicitante”, “Aprobador”, “Administrador” y “Verificador”. Nótese en la Ilustración 32, que hay un quinto canal llamado “Delegado de Aprobación”, este actor es el que se utilizara para intentar cumplir con los acuerdos de servicio a nivel de tiempo del aprobador si el mismo no ha realizado la revisión de una solicitud, permitiendo que otro usuario con perfil de Aprobador pueda llevar a cabo la revisión en el tiempo acordado.

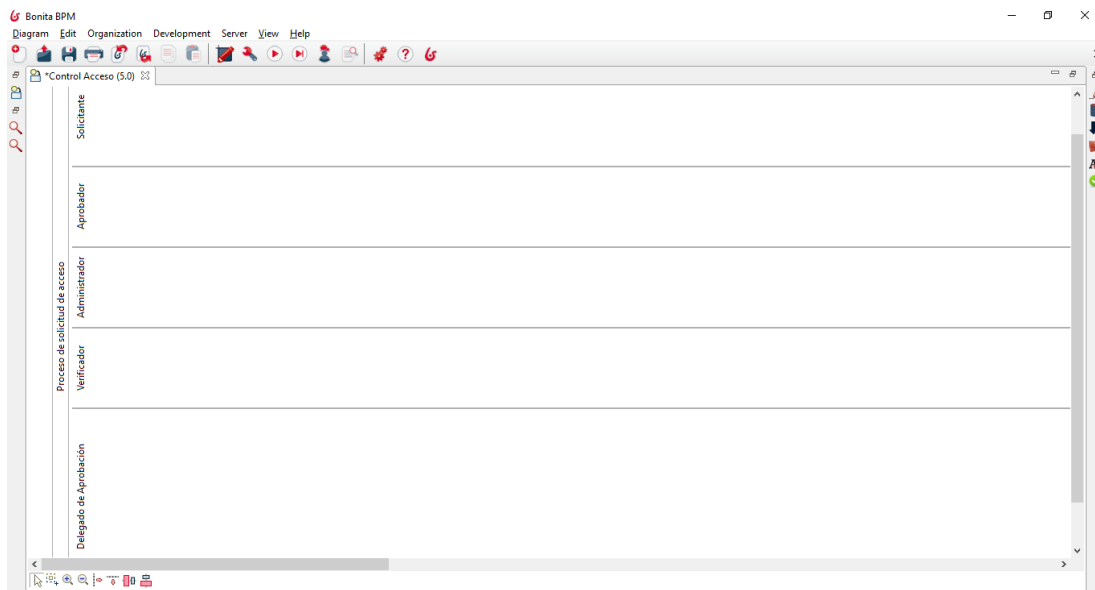


ILUSTRACIÓN 32 CANALES DEL PROCESO DE CONTROL DE ACCESO

El siguiente paso para poder agregar las actividades mencionadas en la etapa de descubrimiento y todas aquellas tareas, decisiones y reglas necesarias para completar el flujo fue crear los modelos de datos del negocio o BDM. Estos BDM contienen los datos que se utilizan a lo largo del proceso dentro de variables de negocio. A continuación, se explican cada uno de los cuatro BDM creados:

- **ListaPosicionFuncional:** sirve para obtener desde un servicio web la lista actualizada de las posiciones funcionales registradas en la organización.
- **ListaTipoSolicitud:** sirve para obtener desde un servicio web la lista actualizada de los posibles tipos de solicitud que pueden realizar los solicitantes.
- **McaObject:** este BDM contiene los atributos necesarios para guardar la matriz de control de acceso.
- **SolicitudAcceso:** es el BDM que contiene el resto de los atributos que serán utilizados en el proceso. Es importante destacar que este BDM contiene a su vez un atributo de tipo **mcaObject** de tipo múltiple, el cual es utilizado para guardar cada uno de los accesos dentro de una solicitud.

En la Ilustración 33 se muestra la lista de los cuatro Modelos de datos del negocio (BDM).

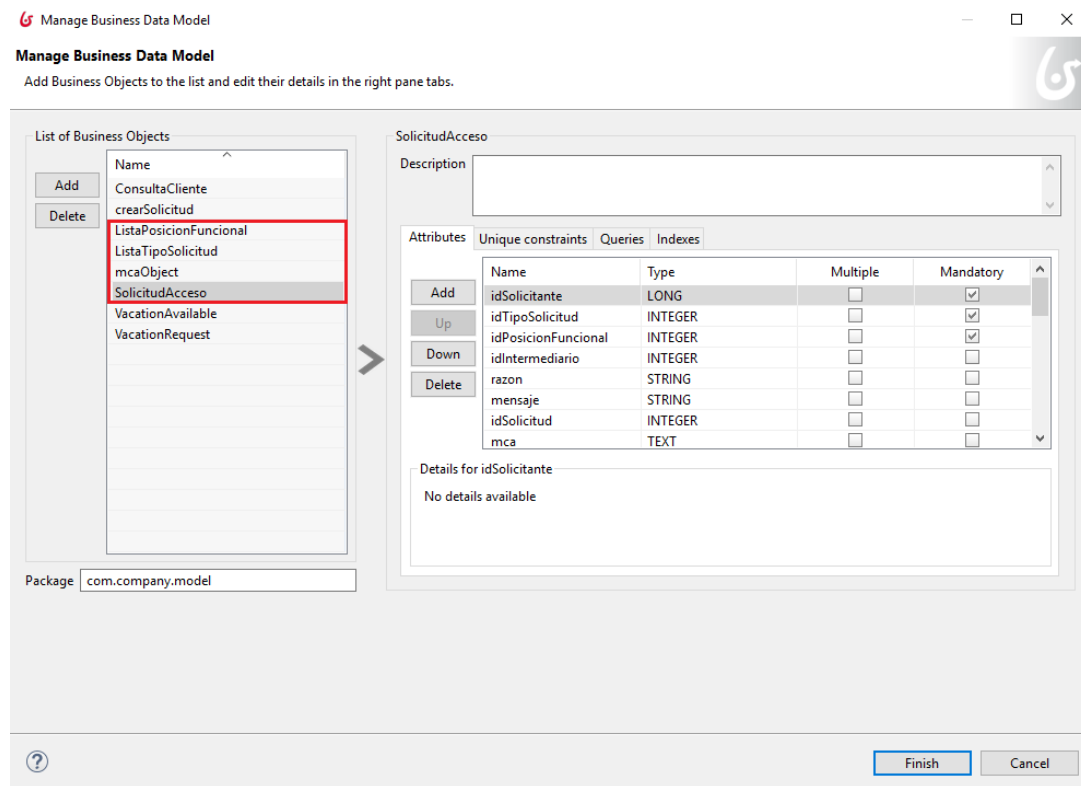


ILUSTRACIÓN 33 MODELOS DE DATOS DE NEGOCIO

Luego, fue necesario crear las instancias de los BDM en el proceso como variables de negocio. Se crearon las variables de negocio que se muestran en la Ilustración 34. Como se puede apreciar, no se ha instanciado el BDM mcaObject, ya que como se mencionó anteriormente, este está contenido como un atributo múltiple dentro de SolicitudAcceso.

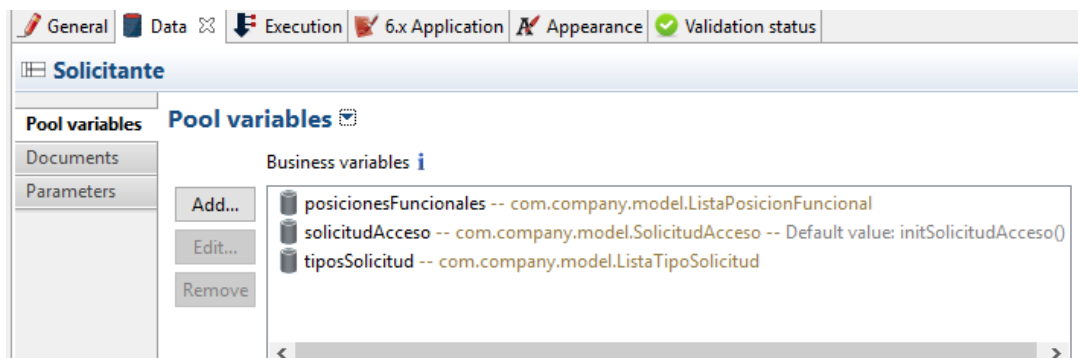


ILUSTRACIÓN 34 VARIABLES DE NEGOCIO

El siguiente paso fue establecer el contrato de instanciación del proceso, que no es más que definir que variables serán necesarias utilizar para iniciar el proceso, es decir, los datos necesarios para que el solicitante genere una solicitud. Dicho contrato se nombró solicitudAccesoEntrada y se utilizaron atributos de la variable solicitudAcceso que se detallan en la Ilustración 35.

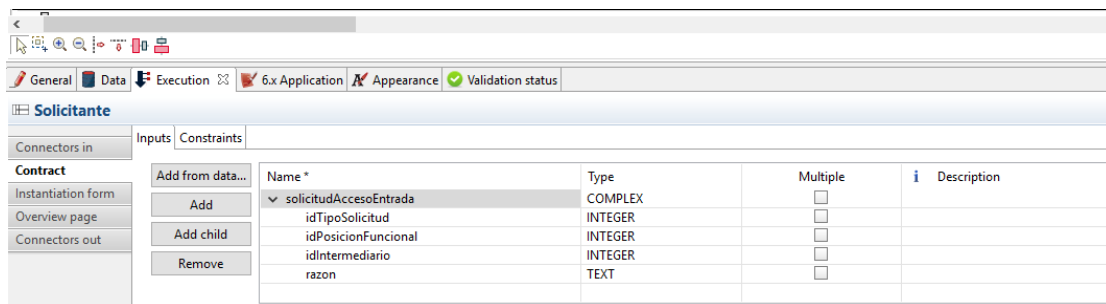


ILUSTRACIÓN 35 CONTRATO DE INSTANCIACIÓN DEL PROCESO

Con el contrato ya creado, se actualizo la variable de negocio solicitudAcceso para colocar el valor por defecto de las variables como se muestra en la Ilustración 36.

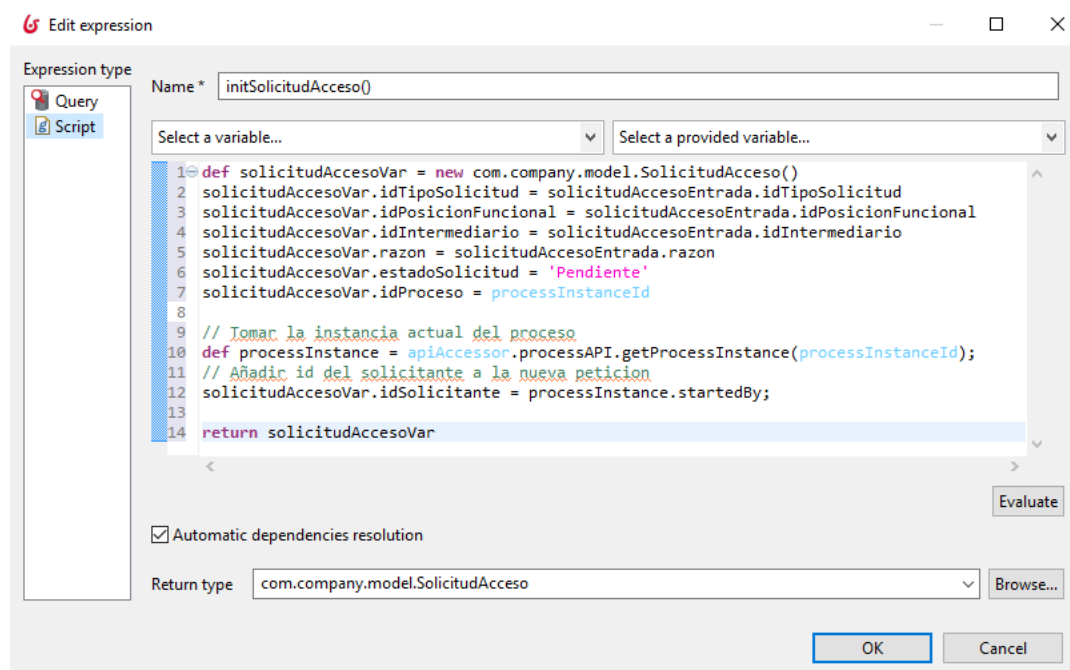


ILUSTRACIÓN 36 INICIALIZACIÓN DE LAS VARIABLES DEL CONTRATO DE INSTANCIACIÓN

Solicitante

Después de tener las variables de negocio y el contrato de instancia creados, se llevó a cabo un formulario para generar la solicitud de acceso por parte de un solicitante, donde dicho formulario instancia el proceso en general. Como se muestra en la Ilustración 37, el evento de inicio contiene el formulario de instancia, cuando este sea completado por un solicitante procederá a llamar a un servicio web que se encargara de almacenar los datos de la solicitud.

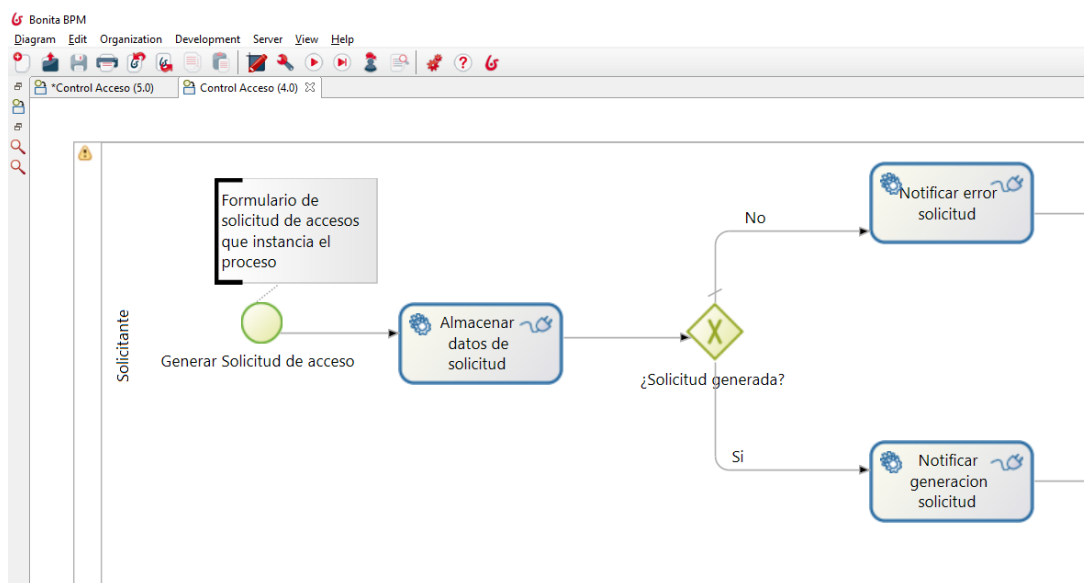


ILUSTRACIÓN 37 CREACIÓN DE ACTIVIDADES PARA EL FORMULARIO DE INICIO

En la Ilustración 38, se aprecia el formulario que se utilizó para generar la solicitud de acceso e instanciar el proceso en el UI Designer de Bonita. En el mismo se puede controlar el comportamiento y opciones del formulario a través de variables de tipo String, Json, External API o Expresiones de javascript. Al final todo es transformado en código del framework AngularJS.

Name	Value	Type
condicionIntermediario	if(!data.intermediario.intermediario){ \$data.formInput.s...	Javascript expression
formInput	{ "solicitudAccesoEntrada": { "idTipoSolicitud": null, "id...	JSON
formOutput	return { "solicitudAccesoEntrada": \$data.formInput.solic...	Javascript expression

ILUSTRACIÓN 38 FORMULARIO PARA GENERAR SOLICITUD DE ACCESO DESDE UI DESIGNER

La Ilustración 39 muestra el esqueleto de la petición que se realiza al servicio web para la generación de una nueva solicitud, donde se le pasa como parámetros los atributos colocados por el solicitante previamente en el formulario.

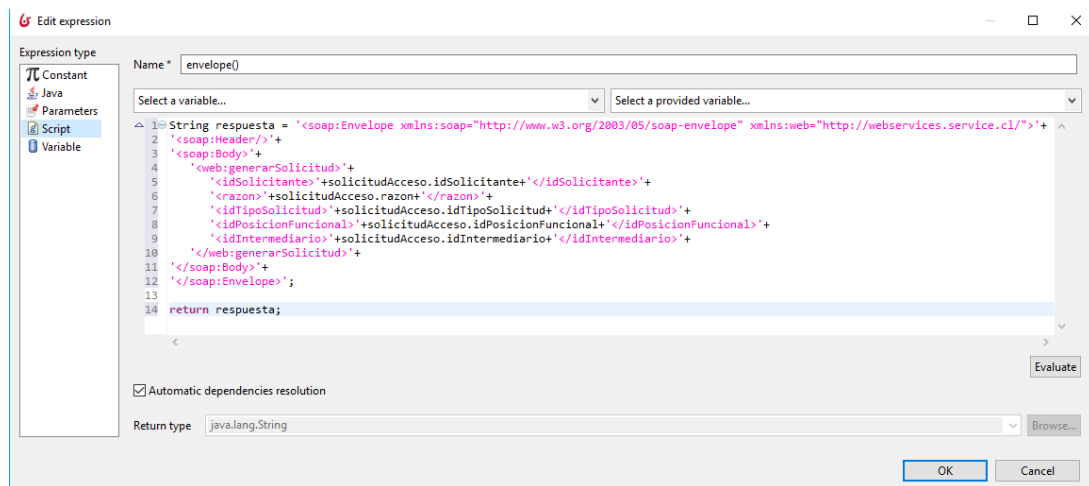


ILUSTRACIÓN 39 ENVELOPE PARA LA GENERACIÓN DE UNA NUEVA SOLICITUD DE ACCESOS

En la Ilustración 37, también se muestra como con un elemento BPMN de decisión es utilizado en el flujo para evaluar si la solicitud fue generada exitosamente o si hubo alguna falla. En caso de una falla, se le notificara al usuario sobre la misma y el proceso finalizara. Por otro lado, si se genera con éxito, se le enviara un correo al solicitante para informarle que la solicitud fue generada. A continuación, en la Ilustración 40 se muestra parte del script utilizado para generar el mensaje que va en el cuerpo del correo electrónico.

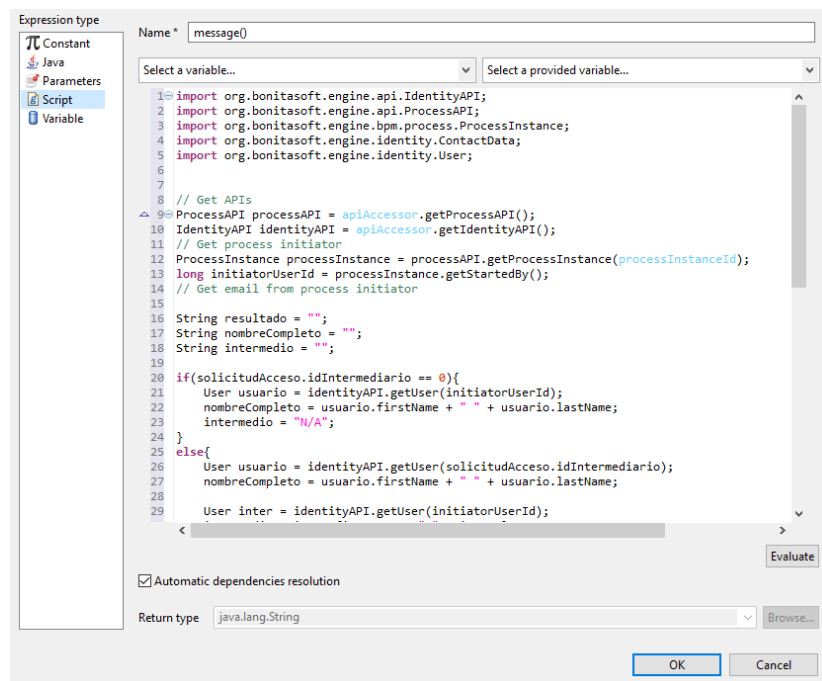


ILUSTRACIÓN 40 SCRIPT PARA GENERAR CUERPO DE CORREO ELECTRÓNICO A SOLICITANTE

Aprobador

Al finalizar la generación de la nueva solicitud, en el modelo se encuentra una decisión llamada ¿Requiere aprobación?, que dependiendo del tipo de solicitud necesitara o no una aprobación por parte de un Aprobador. Cuando se genere una solicitud donde se pidan accesos esta deberá pasar por una revisión y posterior aprobación, en caso contrario, si es una solicitud para remover accesos, no necesita una aprobación y pasaría directo a la actividad de administrar accesos. Para el caso de requerir aprobación, lo primero que se hizo fue una tarea que notificara a través de correo electrónico al aprobador sobre la nueva solicitud en su bandeja de pendientes. Y, a través de un conector que llama a un servicio web, se obtiene los datos de la solicitud actualizados, que serán utilizados para mostrar en el formulario de revisión por parte del aprobador. Los datos que se obtienen de la solicitud son los de la matriz de control de acceso y el script que se detalla en la Ilustración 41 es la forma que se utilizó para tomar la información que retorna el servicio web.

En la Ilustración 42, se muestran todas estas actividades que se realizan desde la decisión de si necesita aprobación hasta la tarea humana que contiene el formulario de revisión.

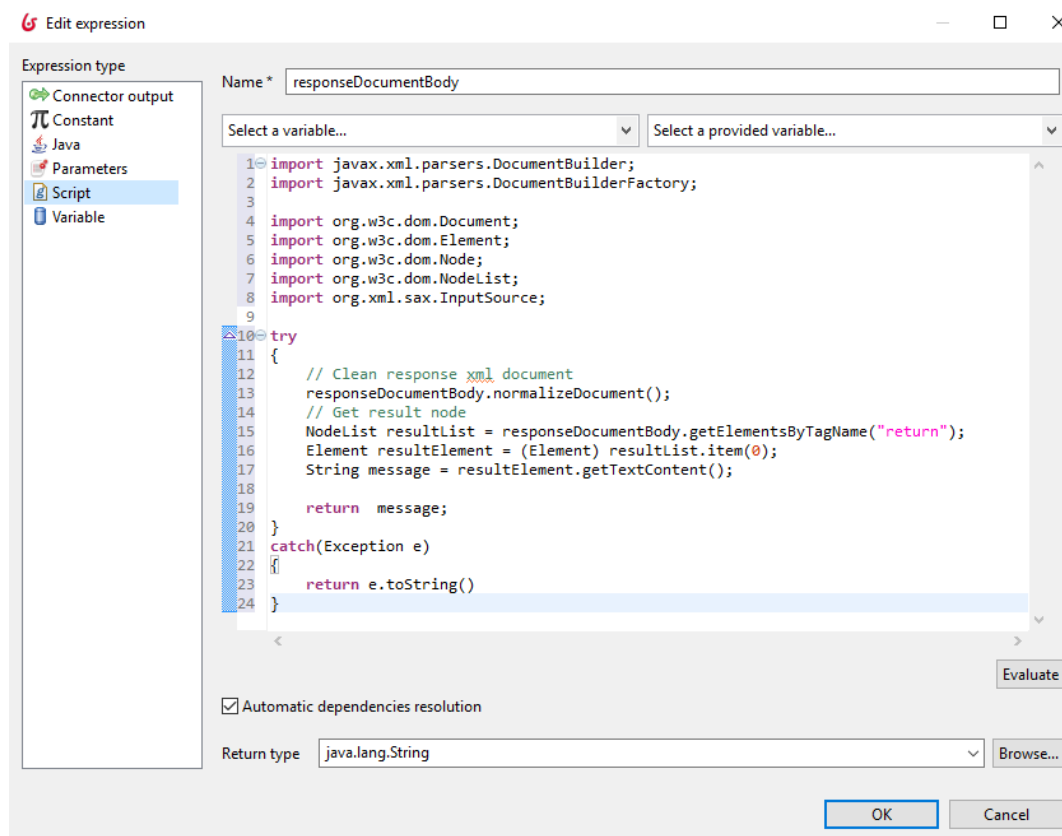


ILUSTRACIÓN 41 SCRIPT QUE RETORNA LOS DATOS DEL ENDPOINT *OBTENERMATRIZPOR SOLICITUD*

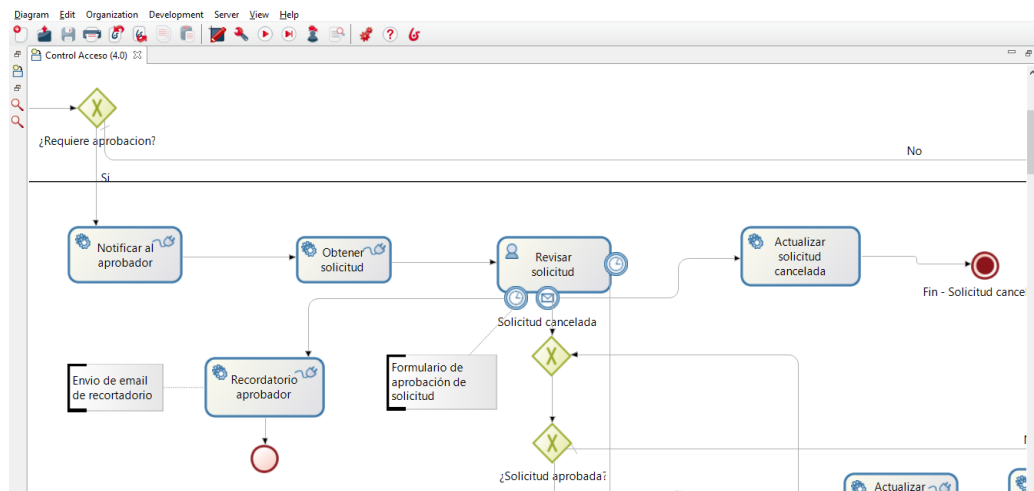


ILUSTRACIÓN 42 REVISIÓN DE FORMULARIO

En la tarea humana “Revisar solicitud” existen varias reglas de negocio que destacar. Una de ellas es un temporizador, que, al cumplirse el tiempo establecido, enviaría un correo electrónico al responsable de la tarea para que este recuerde ejecutarla. Se estableció un tiempo de cuatro horas como se aprecia en la Ilustración 43.

ILUSTRACIÓN 43 CONDICIÓN DE TEMPORIZADOR PARA ENVIAR RECORDATORIO AL APROBADOR

Otra de las reglas que se colocaron fue otro temporizador que, al cabo de cumplir el tiempo establecido, realiza una delegación de la tarea de revisión de solicitud. Como se muestra en la Ilustración 44, se envía un correo electrónico a todos los usuarios que tengan perfil “Aprobador”, es decir, todos los entes autorizados por la organización que puedan decidir que usuarios necesitan o no los accesos solicitados. Posteriormente, se crea una tarea de revisión de solicitud por parte de estos aprobadores, la cual puede ser tomada por cualquier de ellos para ejecutarla. Es importante mencionar que al aprobador inicial no se le quita la posibilidad de poder revisar la solicitud, sino que se da la oportunidad de que el aprobador inicial u otro de los aprobadores puedan realizar la revisión.

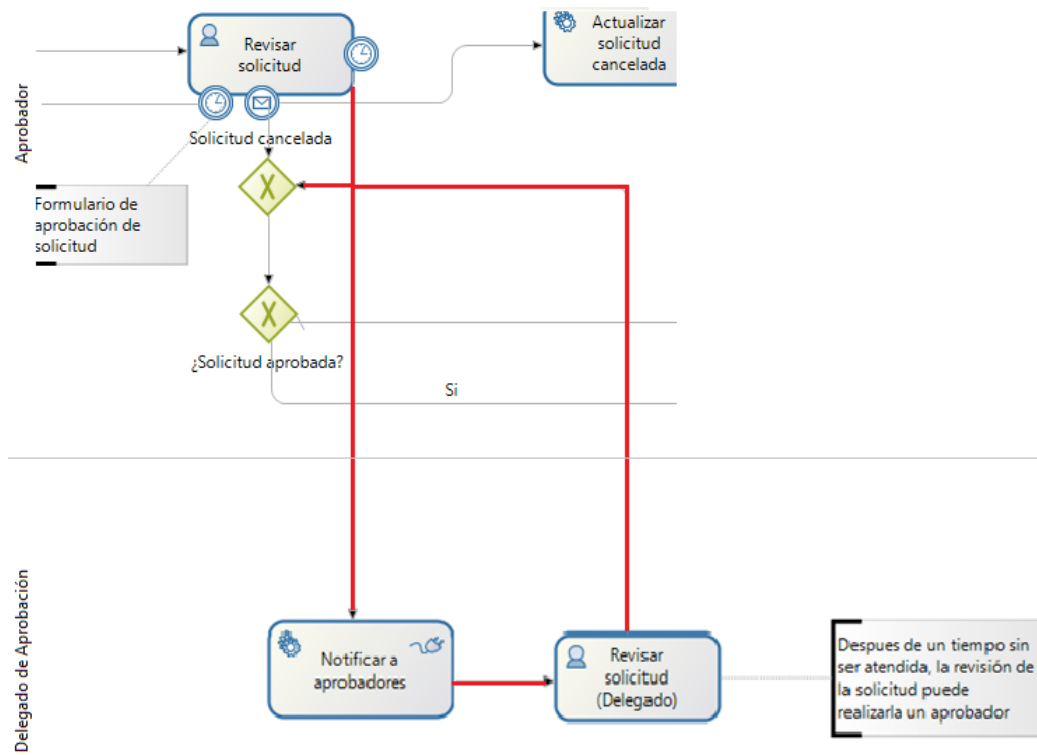


ILUSTRACIÓN 44 HABILITACIÓN DEL FLUJO DE DELEGADO DE APROBACIÓN

Por último, en la tarea “Revisar solicitud”, puede ocurrir que un usuario que haya generado una solicitud y la misma se encuentra en estado “Pendiente” sea cancelada por el mismo. Cuando esto ocurre, la tarea recibe un mensaje de la notación BPMN para culminar el proceso debido a que el solicitante lo cancelo. El proceso de cancelación será explicado a detalle más adelante.

El formulario de revisión de solicitud que se les mostrara a los aprobadores se muestra en la Ilustración 45. Se aprecia la vista previa que provee el UI Designer para los formularios y las páginas.

UI Designer - Google Chrome

localhost:18637/designer/#/en/preview/page/d487fe7f-a9f4-4972-9847-f54f1376a9c9

Preview - revisarSolicitud

Formulario de Aprobacion

Solicitante

Tipo solicitud

Posición Funcional

Razón

Perfil	Componente	Accion
Estado * ☐ Aprobado ☐ Rechazado		
Comentarios		

Enviar

ILUSTRACIÓN 45 FORMULARIO DE LA TAREA “REVISAR SOLICITUD” Y “REVISAR SOLICITUD (DELEGADO)”

Luego de que el aprobador envíe el formulario de aprobación puede ocurrir una de dos vertientes que son manejadas por un gateway o decisión. La solicitud podría ser aprobada o rechazada. Si la solicitud es rechazada se dispararía el flujo que se encuentra marcado en rojo en la Ilustración 46, de lo contrario, ocurriría el flujo que se marca con el verde

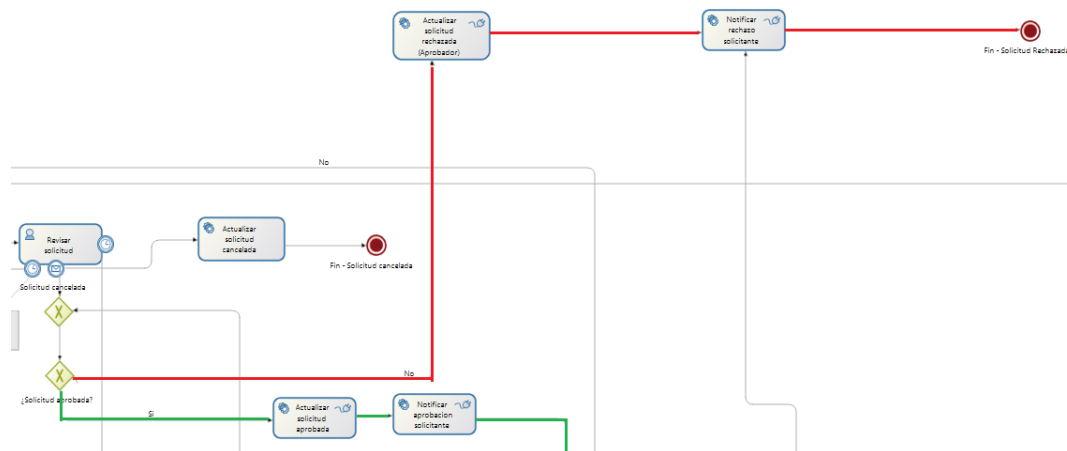


ILUSTRACIÓN 46 FLUJO DEL PROCESO SEGÚN LA REVISIÓN DEL APROBADOR

Para tomar la decisión de cual camino tomar, se utiliza una variable que es establecida por el aprobador en el formulario y se llama "aprobacion". En la Ilustración 47 se muestra como se utiliza una expresión que comprueba si la solicitud fue Aprobada o Rechazada como condición para la decisión.

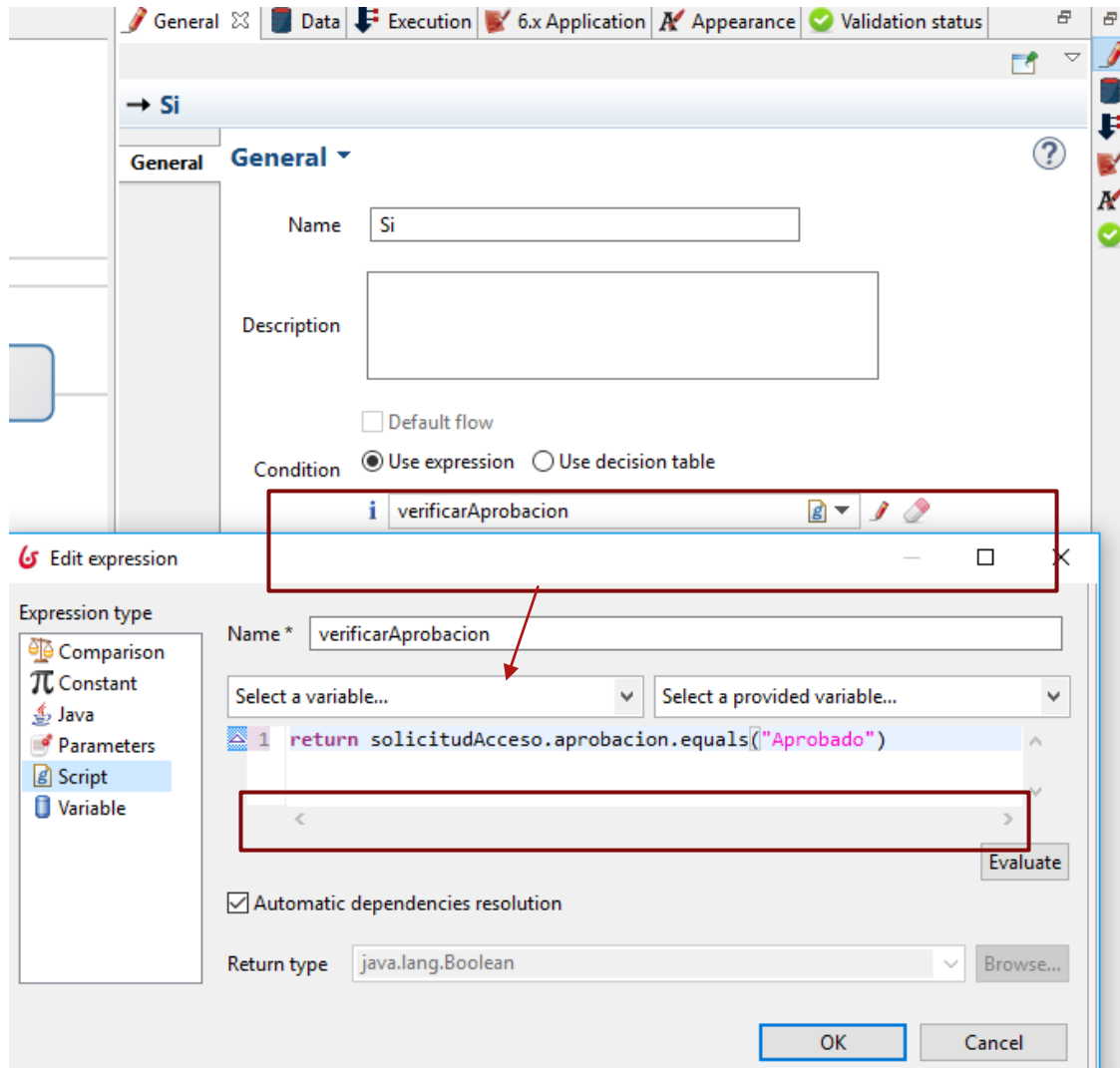


ILUSTRACIÓN 47 EXPRESIÓN DE CONDICIÓN DE ¿SOLICITUD APROBADA?

En caso de rechazo: Cuando un aprobador rechaza una solicitud, se tiene que realizar la actualización de la solicitud para colocar en estado rechazado. Esto se hace a través de un conector al servicio web al igual que el resto de las operaciones. El envelope que es utilizado para enviar los datos al servicio web rechazarSolicitud se encuentra en la Ilustración 48. Luego, se creó una tarea que utiliza un conector de envío de correo electrónico para notificar al solicitante del rechazo de la solicitud. El script que genera el cuerpo del correo electrónico se encuentra en la Ilustración 49. Finalmente, se coloca un evento de terminación que finaliza por completo todas las actividades el proceso.

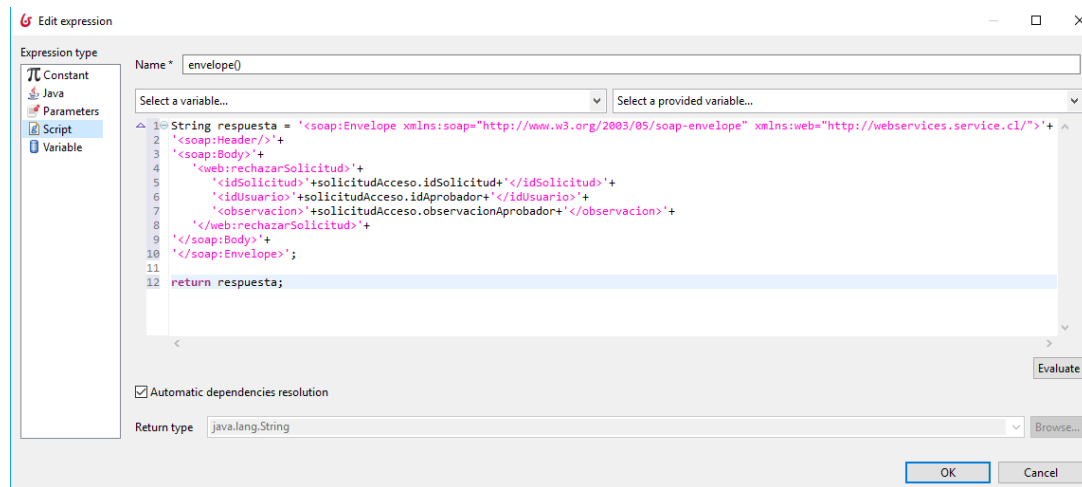


ILUSTRACIÓN 48 ENVELOPE PARA ACTUALIZAR LA SOLICITUD RECHAZADA

```

1  import org.bonitasoft.engine.api.IdentityAPI;
2  import org.bonitasoft.engine.api.ProcessAPI;
3  import org.bonitasoft.engine.bpm.process.ProcessInstance;
4  import org.bonitasoft.engine.identity.ContactData;
5  import org.bonitasoft.engine.identity.User;
6
7
8  // Get APIs
9  ProcessAPI processAPI = apiAccessor.getProcessAPI();
10 IdentityAPI identityAPI = apiAccessor.getIdentityAPI();
11 // Get process initiator
12 ProcessInstance processInstance = processAPI.getProcessInstance(processInstanceId);
13 long initiatorUserId = processInstance.getStartedBy();
14 // Get email from process initiator
15
16 String resultado = "";
17 String nombreCompleto = "";
18 String intermedio = "";
19
20 if(solicitudAcceso.idIntermediario == 0){
21     User usuario = identityAPI.getUser(initiatorUserId);
22     nombreCompleto = usuario.firstName + " " + usuario.lastName;
23     intermedio = "N/A";
24 }
25 else{
26     User usuario = identityAPI.getUser(solicitudAcceso.idIntermediario);
27
28     nombreCompleto = usuario.firstName + " " + usuario.lastName;
29     User inter = identityAPI.getUser(initiatorUserId);
30     intermedio = inter.firstName + " " + inter.lastName;
31 }
32
33 //Buscar Posicion Funcional
34
35 int posIndex = posicionesFuncionales.jsonData.indexOf(''+solicitudAcceso.idPosicionFuncional);
36 String idPos = solicitudAcceso.idPosicionFuncional.toString();
37 int longitud = idPos.length() + 12 + posIndex;
38 String posicion = posicionesFuncionales.jsonData.substring(longitud);
39 posIndex = posicion.indexOf('');
40 posicion = posicion.substring(0, posIndex);
41
42 //Buscar Tipo de solicitud
43 int tipoIndex = tiposSolicitud.jsonData.indexOf(''+solicitudAcceso.idTipoSolicitud);
44 String idTipo = solicitudAcceso.idTipoSolicitud.toString();
45 int longitud2 = idTipo.length() + 12 + tipoIndex;
46 String tipo = tiposSolicitud.jsonData.substring(longitud2);
47 tipoIndex = tipo.indexOf('');
48 tipo = tipo.substring(0, tipoIndex);
49
50 String observacion = solicitudAcceso.observacionAdministrador.equals(null) ? solicitudAcceso.observacionAprobador : solicitudAcceso.observacionAdministrador;
51
52 resultado = "<center><h3>La solicitud de acceso #" + solicitudAcceso.idSolicitud + " ha sido rechazada</h3></center>" +
53 "<br><br>" +
54 "<b>Usuario:</b>" + nombreCompleto + "<br>" +
55 "<b>Intermediario:</b>" + intermedio + "<br>" +
56 "<b>Tipo de Solicitud:</b>" + tipo + "<br>" +
57 "<b>Posición Funcional:</b>" + posicion + "<br>" +
58 "<b>Razón:</b>" + solicitudAcceso.razon + "<br><br>" +
59 "<b>Motivo del rechazo:</b>" + observacion
60 resultado += "<br><br><a href='http://localhost:18637/bonita/apps/sca/index/'>Ir a la bandeja de entrada</a>"
61 return resultado;
62

```

ILUSTRACIÓN 49 SCRIPT CUERPO DE CORREO DE RECHAZO DE SOLICITUD

En caso de aprobación: Cuando un aprobador aprueba una solicitud, se tiene que realizar la actualización de la solicitud para colocarla en estado aprobado. Esto se hace a través de un conector al servicio web al igual que el resto de las operaciones. El envelope que es utilizado para enviar los datos al servicio web aprobarSolicitud se encuentra en la Ilustración 50. Luego, se creó una tarea que utiliza un conector de envío de correo electrónico para notificar al solicitante de la aprobación de la solicitud. El script que genera el cuerpo del correo electrónico se encuentra en la Ilustración 51.

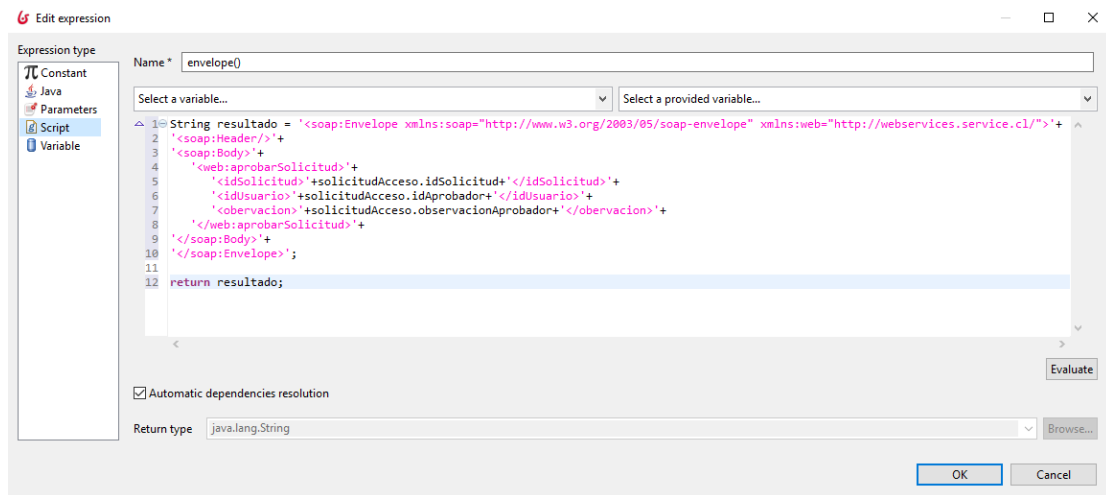


ILUSTRACIÓN 50 ENVELOPE PARA ACTUALIZAR LA SOLICITUD APROBADA

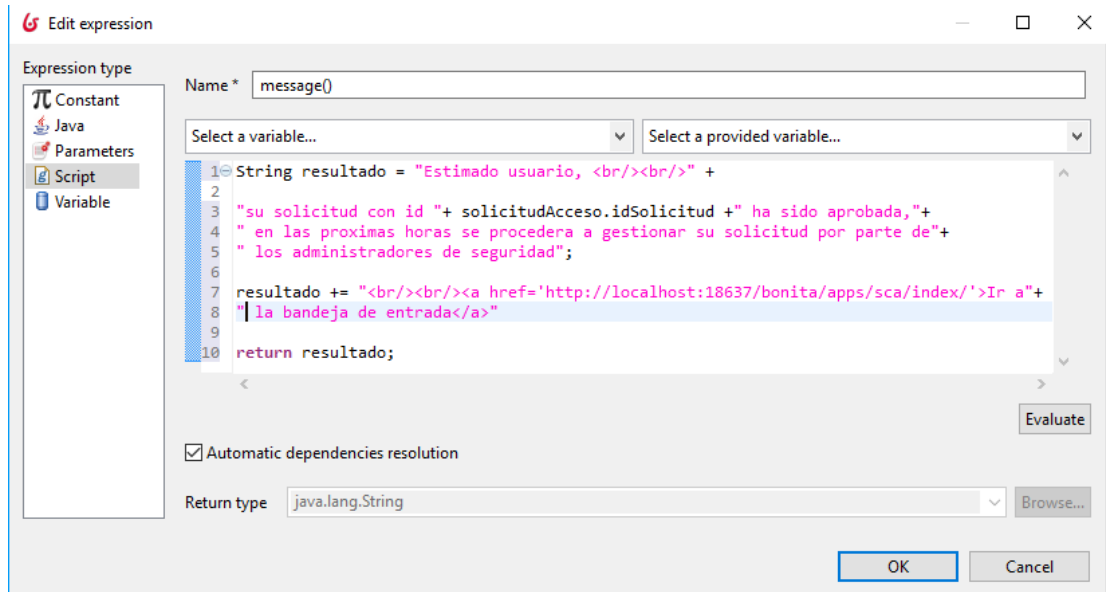


ILUSTRACIÓN 51 SCRIPT CUERPO DE CORREO DE APROBACIÓN DE SOLICITUD PARA EL SOLICITANTE

Administrador

Las siguientes actividades en el modelado que se muestra en la Ilustración 52 corresponden al Administrador, donde lo primero que se lleva a cabo es una tarea automática que notifica a los administradores vía correo electrónico que tienen una nueva solicitud pendiente por gestionar en su bandeja de entrada. Para buscar los correos de los administradores, el conector genera un script que se muestra en la Ilustración 53, donde se utiliza el identity API para buscar los id de los usuarios con Perfil de Administrador.

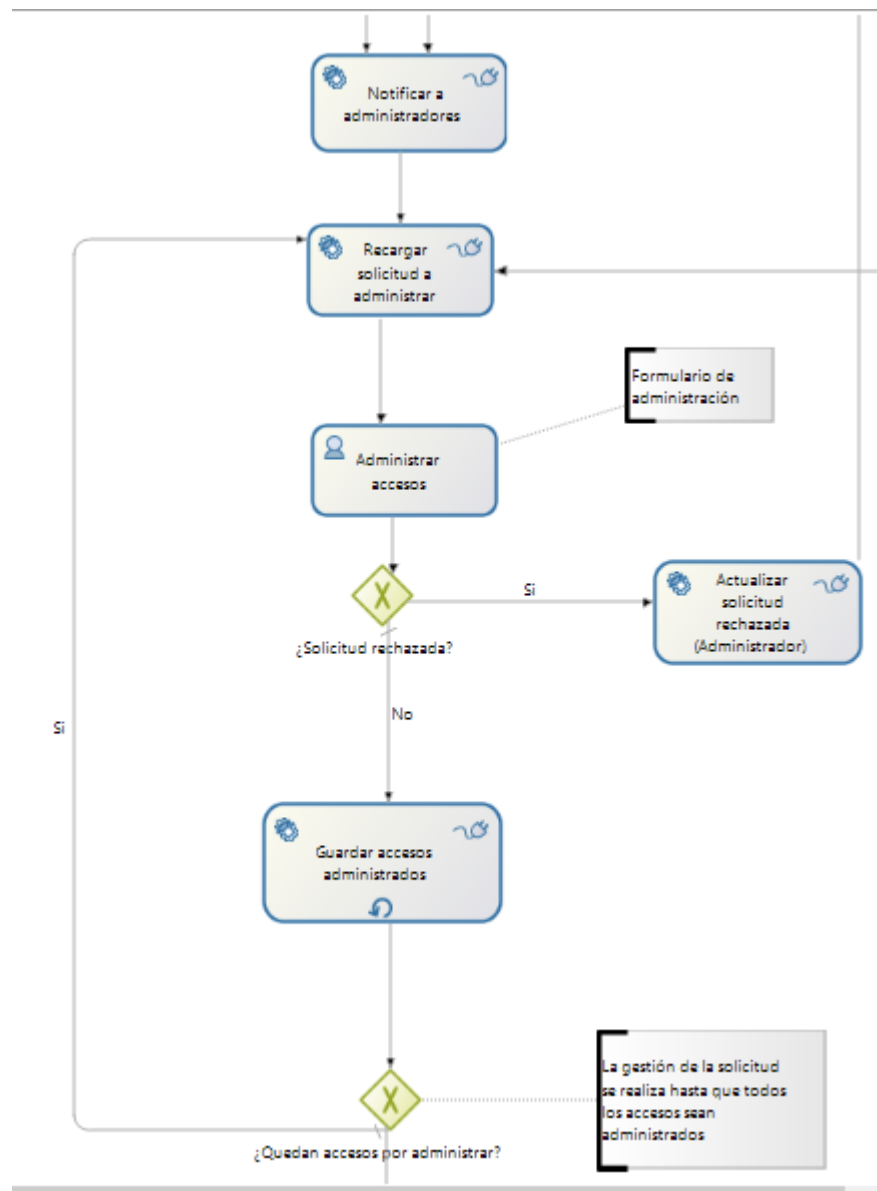


ILUSTRACIÓN 52 FLUJO DEL ADMINISTRADOR

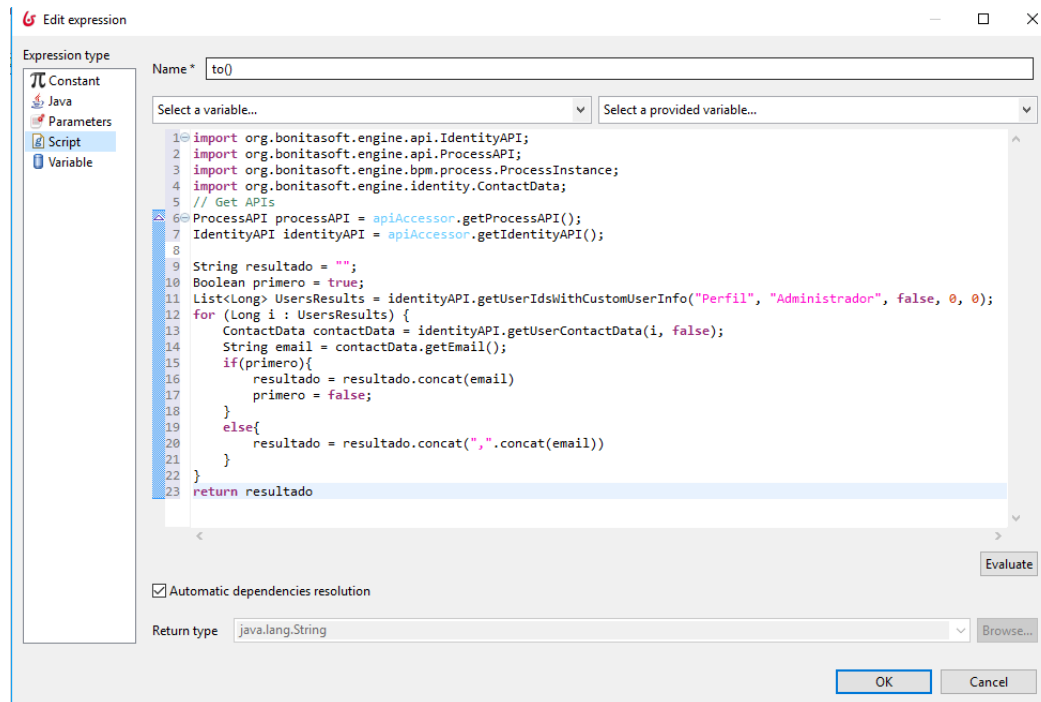


ILUSTRACIÓN 53 SCRIPT PARA BUSCAR CORREOS DE LOS ADMINISTRADORES

Nuevamente, se recarga la solicitud, para mostrar los datos actualizados al administrador utilizando de esta forma la misma lógica y estructura que el conector de la actividad “Obtener solicitud” en el carril del Aprobador. La siguiente actividad, llamada “Administrar accesos” es el formulario utilizado por el Administrador de seguridad para otorgar, revocar o rechazar los accesos de la solicitud uno por uno. En esta actividad se creó un contrato que contiene los datos necesarios para completar el formulario de administración. Las entradas del contrato se muestran en la Ilustración 54.

General Data Execution 6.x Application Appearance Validation status				
Administrar accesos				
Connectors in				
Task Inputs				
Contract				
Inputs Constraints				
Form				
Operations				
Connectors out				
Add from data...	Name *	Type	Multiple	Description
Add	▼ mca	COMPLEX	☒	
Add child	estado	TEXT	☐	
Remove	id	INTEGER	☐	
	accion	TEXT	☐	
	componente	TEXT	☐	
	perfil	TEXT	☐	
	resultado	TEXT	☐	
	observacionAdministrador	TEXT	☐	

ILUSTRACIÓN 54 CONTRATO DE LA ACTIVIDAD “ADMINISTRAR ACCESOS”

También se realizaron varias operaciones sobre la actividad, las cuales son ejecutadas luego de que el administrador culmine la tarea. Las variables “observacionAdministrador” y “resultadoAdministracion” de la variable de negocio “solicitudAcceso” son actualizadas utilizando el contrato. La variable

“idAdministrador” se actualiza con un script que toma el id de la persona que realizo la tarea. “Index” y “Top” son dos variables que se utilizan para llevar el control de cuantos accesos contiene una solicitud y cuantos ya fueron gestionados, siendo el primero de estos colocado en 0 y el segundo la cantidad total de accesos dentro de la solicitud. En la Ilustración 55 se muestran las operaciones mencionadas.

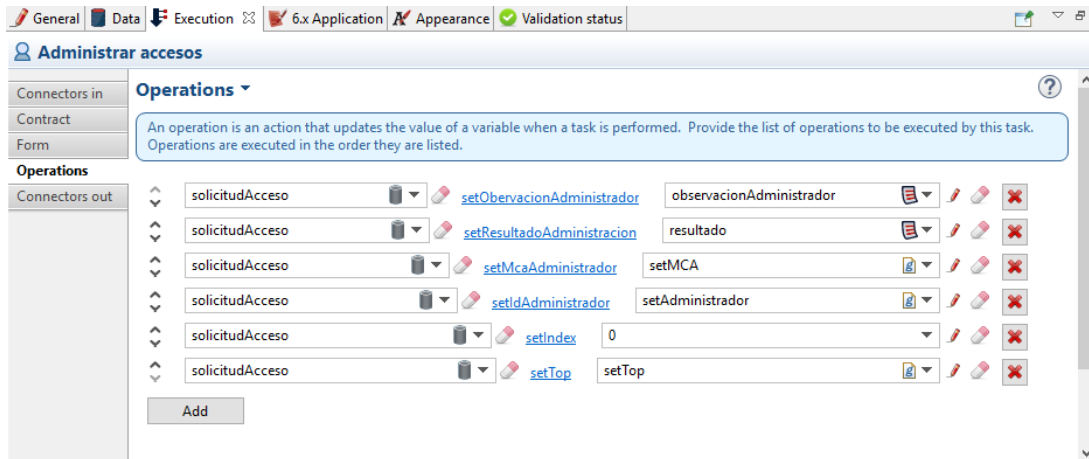


ILUSTRACIÓN 55 OPERACIONES EN LA ACTIVIDAD “ADMINISTRAR ACCESOS”

Por otro lado, la operación que actualiza la variable “McaAdministrador”, también es tomada de los datos introducidos por el administrador en el formulario y guardados en el contrato, pero al ser una variable múltiple se debe realizar un ciclo que la rellene como se muestra a continuación en la Ilustración 56.

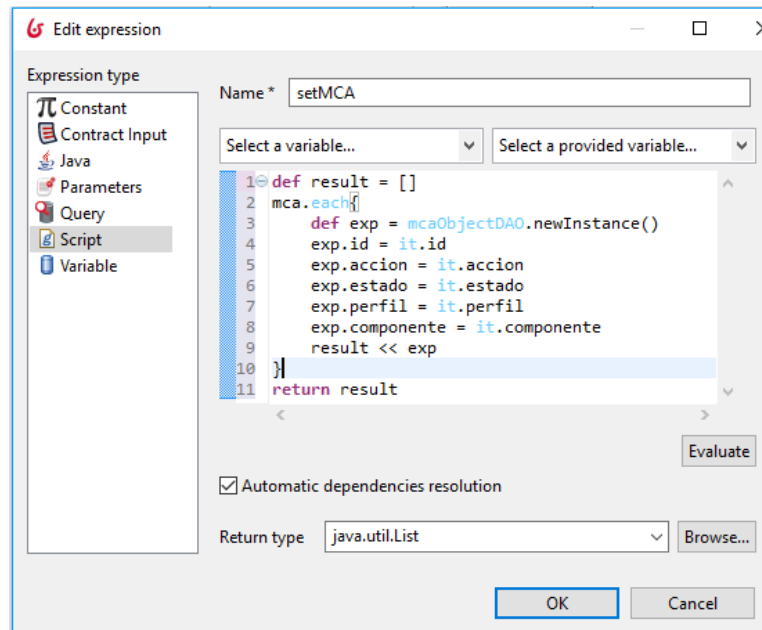


ILUSTRACIÓN 56 SCRIPT QUE ACTUALIZA LA MATRIZ DE CONTROL DE ACCESO DE UNA SOLICITUD

El formulario de administración desde la vista previa que proporciona el UI Designer es mostrada en la Ilustración 57. Es importante mencionar que la vista previa no muestra muchos de los elementos HTML que realmente se encuentran presentes, pero que están condicionados según el tipo de solicitud y opciones del propio usuario y por ello se ocultan.

Preview - gestionarSolicitud

Formulario de Administración

Solicitante

Tipo Solicitud

Posición Funcional

Razón

Perfil	Componente	Accion	Estado
Comentario *			

Guardar **Rechazar** **Finalizar**

ILUSTRACIÓN 57 FORMULARIO DE LA TAREA “ADMINISTRAR ACCESOS”

Dos ejemplos claros de elementos que no se muestran en la vista previa son “Motivo de la devolución” y el “Intermediario”. Ya que son dos elementos que no siempre están presentes en las solicitudes y por ello, tienen una condición que los oculta si la expresión detecta que no deben ser mostrados, como se muestra en la ilustración 58.

Formulario de Administración

Motivo de la devolución: `{{solicitudAcceso.observacionVerificador}}`

Solicitante
data:nombreSolicitante

Intermediario
data:nombreIntermediario

Tipo Solicitud
data:ts

Hidden
solicitudAcceso.observacionVerifica

Text
Use basic html tags and `{{ dataVariable }}` to access data
`<b>Motivo de la devolución:</b>{{solicitudAcceso.observacionVerificador}}`

ILUSTRACIÓN 58 ELEMENTOS OCULTOS EN EL UI DESIGNER

Al igual que el aprobador, el administrador tiene la opción de rechazar la solicitud de un solicitante. Esto debido a que un aprobador pudo haber cometido una equivocación, o se rechaza a petición del solicitante. El flujo para ambos rechazos es exactamente el mismo, primero se realiza la actualización de la solicitud a rechazado, luego se envía un correo electrónico indicándole al solicitante que su solicitud fue rechazada. Finalmente, se coloca el evento de terminación que finaliza con todas las actividades y el proceso en general.

Si la solicitud no es rechazada, se lleva a cabo la actividad “Guardar accesos administrados”, la cual utiliza un conector de servicio web para actualizar los accesos que haya gestionado el administrador. Como una solicitud tiene uno o más accesos dentro de la misma, esta actividad itera por cada uno de los accesos que haya gestionado el administrador, en la Ilustración 59 se muestra la expresión utilizada para la iteración.

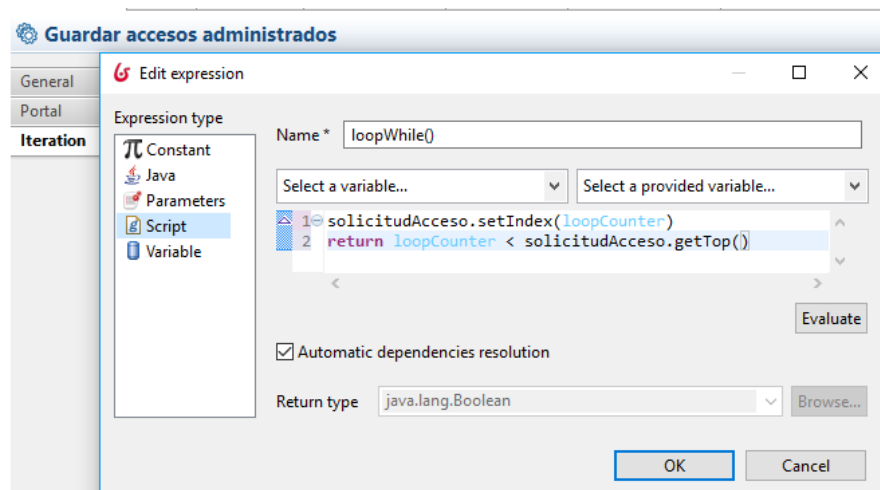


ILUSTRACIÓN 59 EXPRESIÓN DE ITERACIÓN DE LA ACTIVIDAD “GUARDAR ACCESOS ADMINISTRADOS”

El envelope mostrado en la Ilustración 60, es el que se envía para gestionar los accesos de la solicitud.

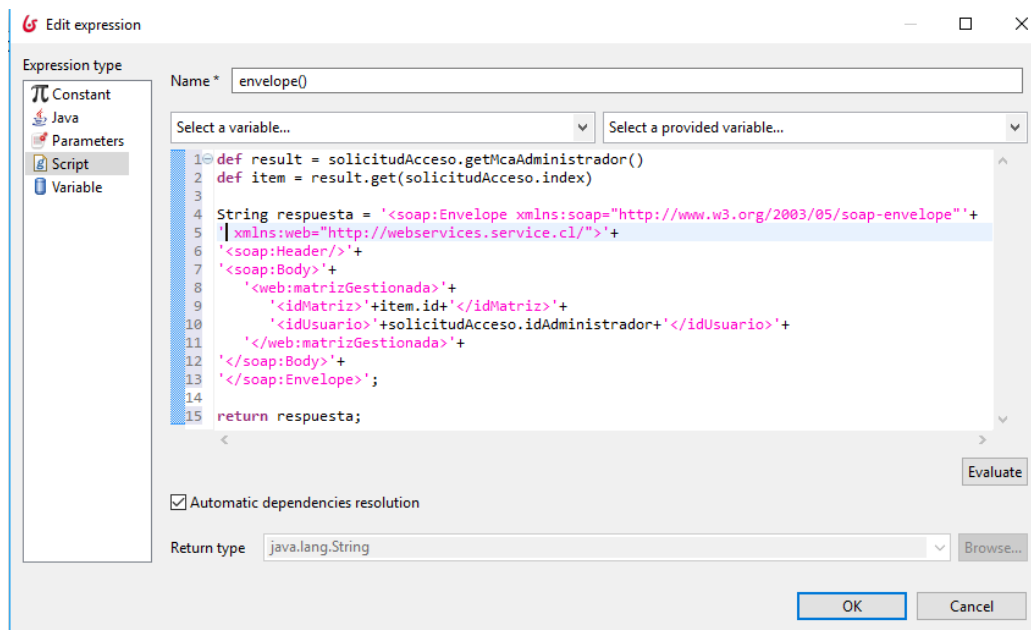


ILUSTRACIÓN 60 ENVELOPE PARA GESTIONAR LOS ACCESOS EN LA MATRIZ DE CONTROL DE ACCESO

En esta actividad también hay una operación que actualiza la variable “estadoSolicitud” al enviar el formulario. En la Ilustración 61 se aprecia como el estado que se coloca dependiendo de lo que haya realizado el Administrador, ya que si culmina con la gestión de todos los accesos de la solicitud esta pasa a estar “Gestionada”, pero si aún quedan accesos por gestionar pasaría al estado “En Gestión”.

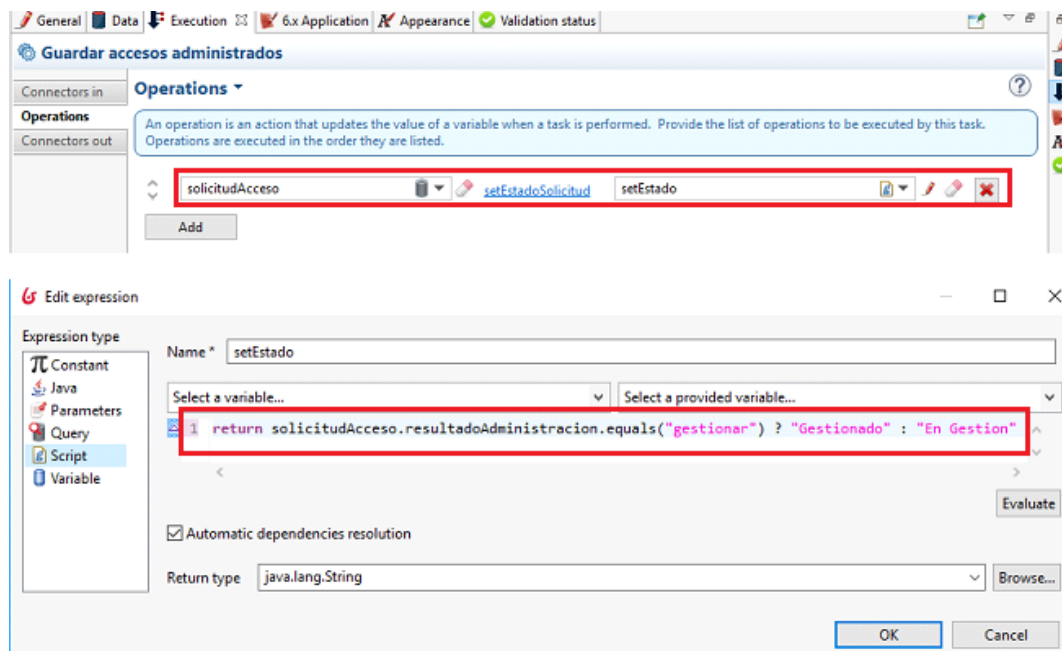


ILUSTRACIÓN 61 SCRIPT QUE ACTUALIZA EL ESTADO DE LA SOLICITUD EN EL CARRIL DEL ADMINISTRADOR

Luego, se colocó una decisión para comprobar si ya todos los accesos fueron gestionados o si aún faltan algunos por gestionar. Dicha decisión se nombró “¿Quedan accesos por administrar?” y la expresión de la condición para saber qué camino del flujo tomar se encuentra en la Ilustración 62. Si aún quedan accesos por gestionar, el flujo se regresará a la actividad “Recargar solicitud a administrar” y volverá a ejecutar todas las actividades desde ese punto hasta que finalmente todos los accesos sean gestionados.

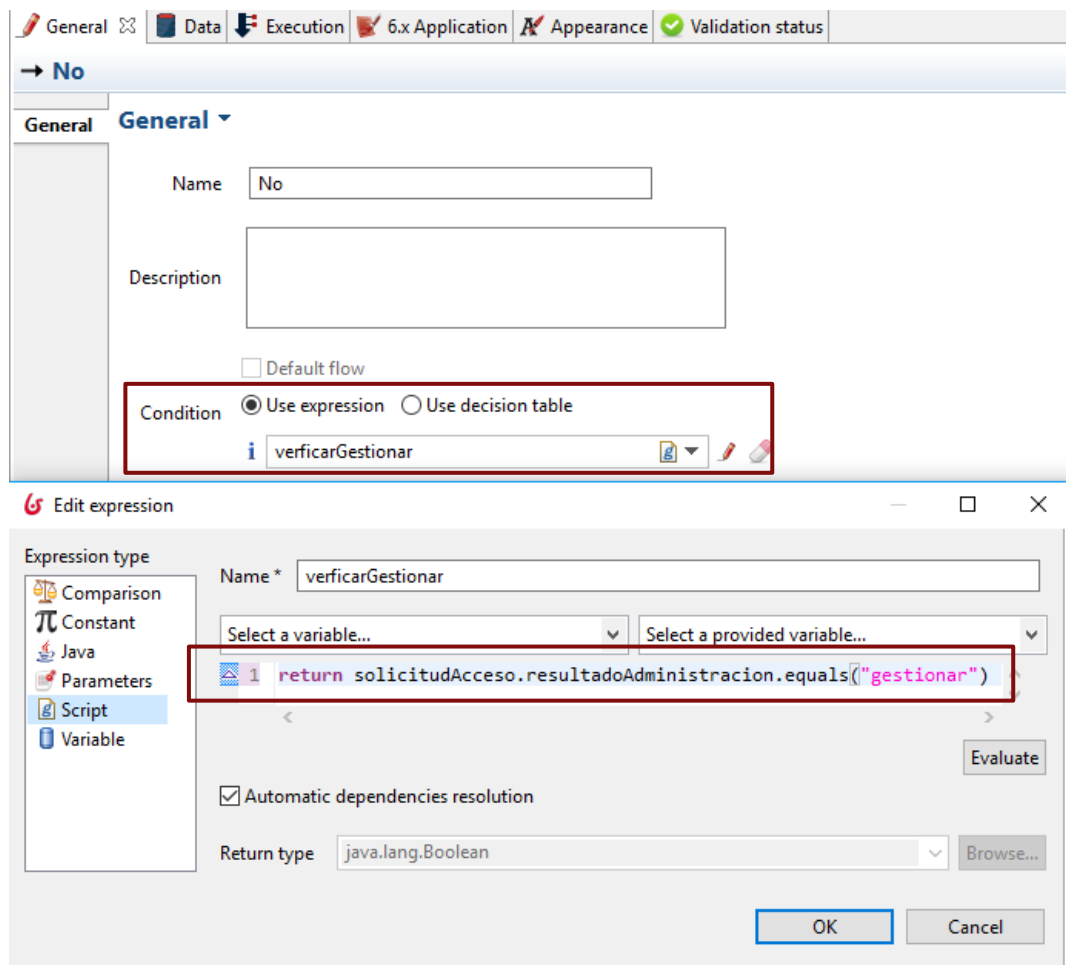


ILUSTRACIÓN 62 EXPRESIÓN DE CONDICIÓN DE ¿QUEDAN ACCESOS POR ADMINISTRAR?

Si ya no quedan accesos por gestionar y el administrador presiona el botón “Finalizar” en el formulario, el flujo que correspondería sería el que se muestra en la Ilustración 63, donde primero se llevaría a cabo la actividad “Actualizar solicitud gestionada”. En la Ilustración 64 se muestran los datos enviados al servicio web para realizar esta acción. Luego, se procede a notificar al solicitante que su solicitud ya fue gestionada a través de un conector de envío de correo electrónico.

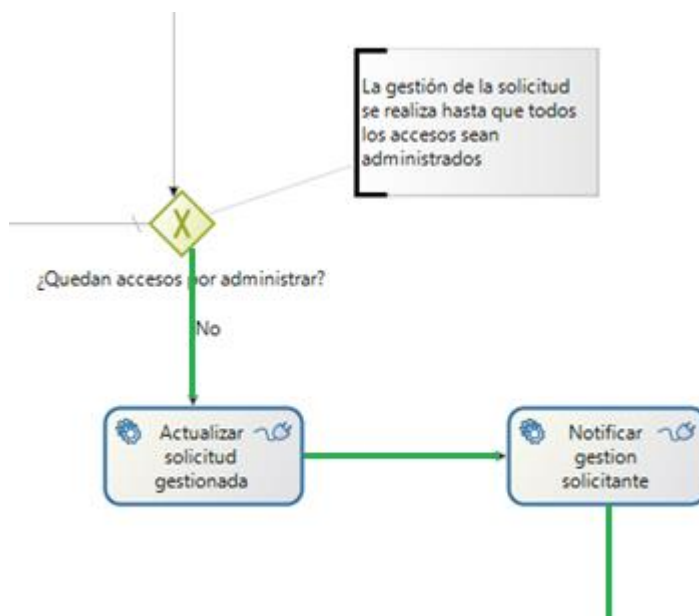


ILUSTRACIÓN 63 FLUJO AL FINALIZAR LA GESTIÓN POR PARTE DEL ADMINISTRADOR

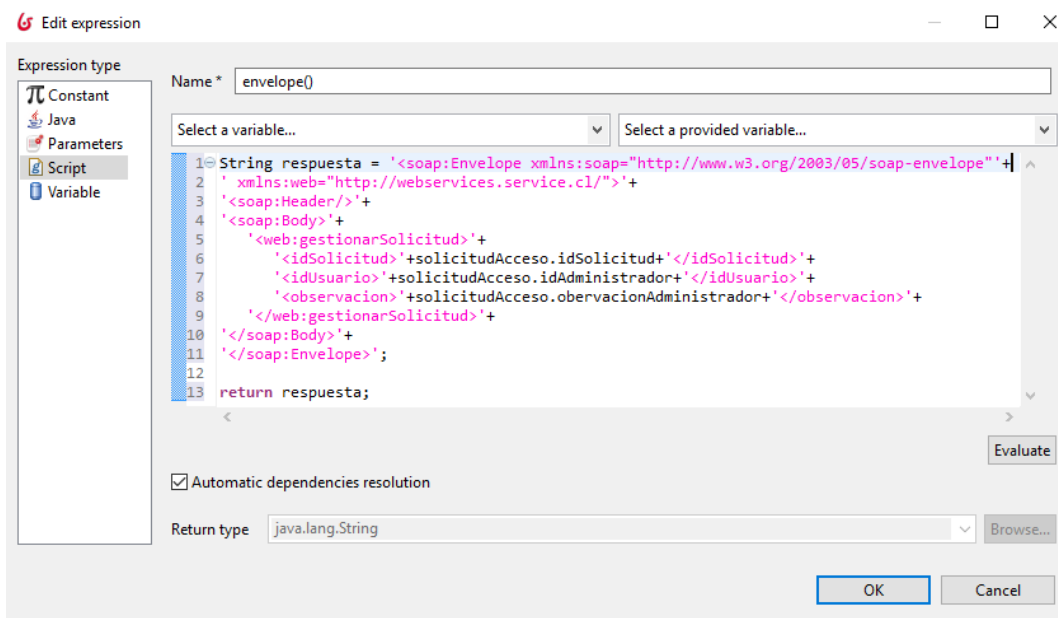


ILUSTRACIÓN 64 ENVELOPE PARA GESTIONAR LA SOLICITUD POR PARTE DEL ADMINISTRADOR

Verificador

Las siguientes actividades en el modelado que se muestra en la Ilustración 65 corresponden al Verificador, donde lo primero que se lleva a cabo es una tarea automática que notifica a los verificadores vía correo electrónico que tienen una nueva solicitud pendiente por verificar en su

bandeja de entrada. Para buscar los correos de los verificadores, el conector genera un script que se muestra en la Ilustración 66, donde se utiliza el identity API para buscar los id de los usuarios con Perfil de Verificador tal como se hizo para los Administradores.

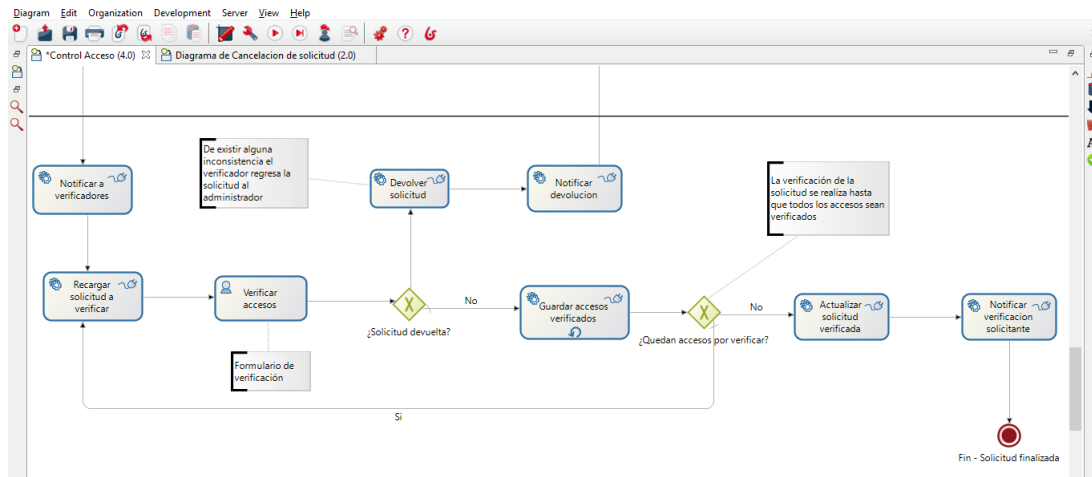


ILUSTRACIÓN 65 FLUJO DEL VERIFICADOR

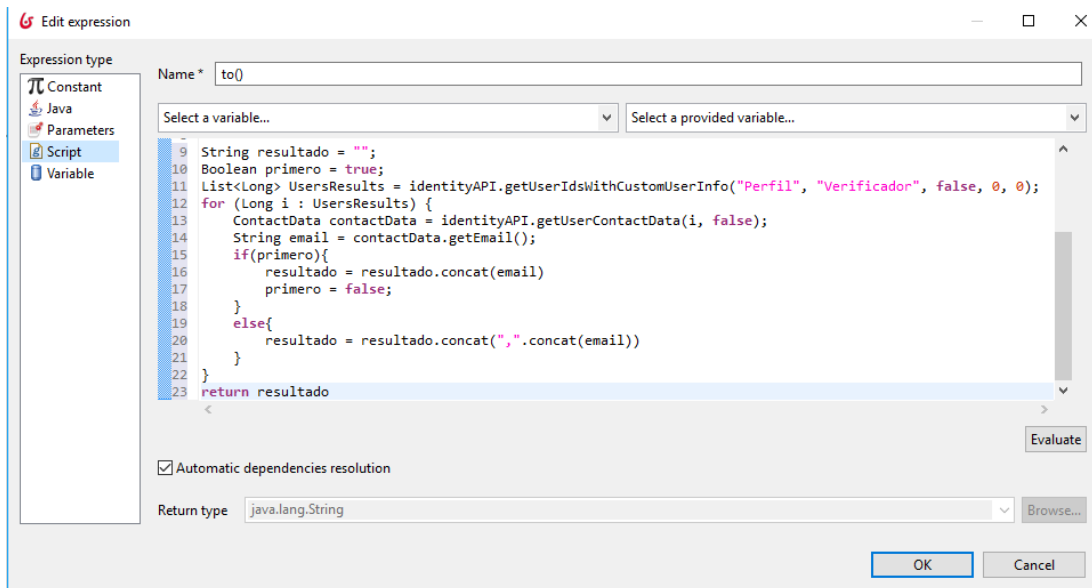


ILUSTRACIÓN 66 SCRIPT PARA BUSCAR CORREOS DE LOS VERIFICADORES

Una vez más, se recarga la solicitud, esta vez para la verificación y así mostrar los datos actualizados al verificador. La siguiente actividad, llamada “Verificar accesos” es el formulario utilizado por el Verificador, que también es un oficial de seguridad, para avalar que todos los accesos gestionados por el administrador, se hayan realizado de forma correcta y no existan errores operativos. En esta actividad se creó un contrato que contiene los datos necesarios para completar el formulario de verificación. Las entradas del contrato se muestran en la Ilustración 67.

Verificar accesos

Connectors in **Task Inputs**

Contract Inputs Constraints

Form Operations Connectors out

Add from data... Add Add child Remove

Name *	Type	Multiple	Description
observacionVerificador	TEXT	☐	
resultado	TEXT	☐	
▼ mca	COMPLEX	☒	
id	INTEGER	☐	
perfil	TEXT	☐	
componente	TEXT	☐	
accion	TEXT	☐	
estado	TEXT	☐	

ILUSTRACIÓN 67 CONTRATO DE LA ACTIVIDAD “VERIFICAR ACCESOS”

También se realizaron varias operaciones sobre la actividad, las cuales son ejecutadas luego de que el verificador culmine la tarea. Las variables “observacionVerificador” y “resultadoVerificacion” de la variable de negocio “solicitudAcceso” son actualizadas utilizando el contrato. La variable “idVerificador” se actualiza con un script que toma el id de la persona que realizo la tarea. “Index” y “Top” son dos variables que se utilizan para llevar el control de cuantos accesos contiene una solicitud y cuantos ya fueron verificados, siendo el primero de estos colocado en 0 y el segundo la cantidad total de accesos dentro de la solicitud. En la Ilustración 68 se muestran las operaciones mencionadas.

Verificar accesos

Connectors in **Operations**

Contract Form Operations Connectors out

An operation is an action that updates the value of a variable when a task is performed. Provide the list of operations to be executed by this task. Operations are executed in the order they are listed.

solicitudAcceso	setObservacionVerificador	observacionVerificador	
solicitudAcceso	setResultadoVerificacion	resultado	
solicitudAcceso	setMcaAdministrador	mca	
solicitudAcceso	setIdVerificador	setIdVerificador	
solicitudAcceso	setIndex	0	
solicitudAcceso	setTop	mcaSize	

Add

ILUSTRACIÓN 68 OPERACIONES DE LA ACTIVIDAD “VERIFICAR ACCESOS”

Por otro lado, la operación que actualiza la variable “McaAdministrador”, también es tomada de los datos introducidos por el verificador en el formulario y guardados en el contrato, pero al ser una variable múltiple se debe realizar un ciclo que la rellene como se muestra a continuación en la Ilustración 69.

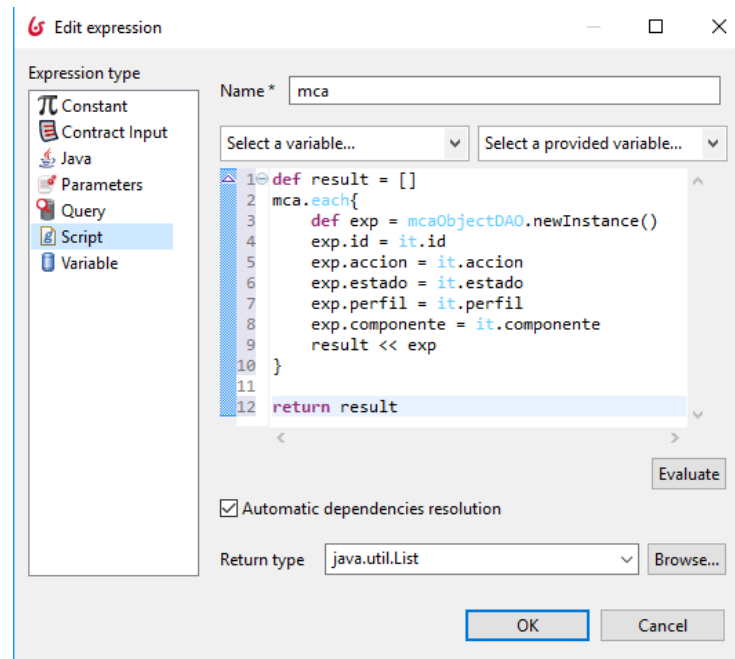


ILUSTRACIÓN 69 SCRIPT QUE ACTUALIZA LA MATRIZ DE CONTROL DE ACCESO DE UNA SOLICITUD VERIFICADA

El formulario de verificación desde la vista previa que proporciona el UI Designer es mostrada en la Ilustración 70. Nuevamente, hay elementos que no son proporcionados por la vista previa debido a que la lógica no lo permite.

localhost:18637/designer/#/en/preview/page/68de81a0-3e51-40f4-9aa0-b57497eaae8d

Preview - verificarSolicitud

Formulario de Verificación

Solicitante

Tipo Solicitud

Posición Funcional

Razón

☐ Datos del administrador

Perfil	Componente	Accion	Estado
Comentario *			

ILUSTRACIÓN 70 FORMULARIO DE LA TAREA “VERIFICAR ACCESOS”

A diferencia del aprobador y del administrador, el verificador no tiene la posibilidad de rechazar la solicitud, ya que, para esta parte del flujo, los accesos de un solicitante ya han sido otorgados o revocados. Sin embargo, nace una nueva opción para el verificador en el caso de que encuentre algo inusual en uno o más de los accesos de una solicitud que es devolver la solicitud al paso anterior. El flujo para la devolución se muestra en la Ilustración 71 marcada con verde, y la primera actividad que se ejecuta es la actualización de la solicitud devuelta a través de un conector de servicio web que se encuentra en la actividad “Devolver solicitud”. Luego se envía un correo electrónico indicándole al administrador que ejecuto la gestión que la solicitud fue devuelta por algún motivo como se muestra en la Ilustración 72.

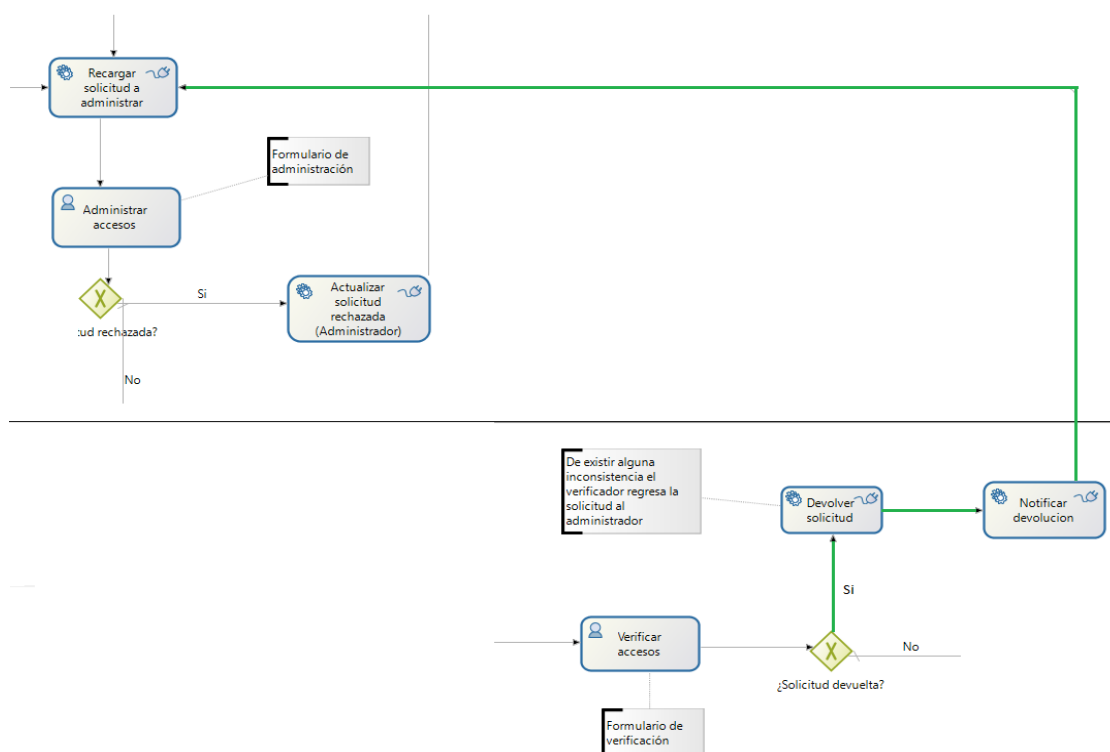


ILUSTRACIÓN 71 FLUJO DE DEVOLUCIÓN DE SOLICITUD

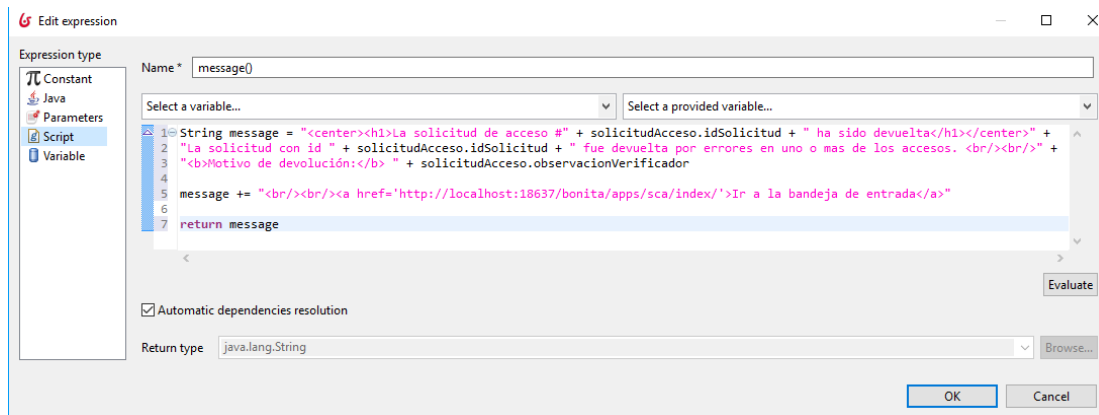


ILUSTRACIÓN 72 CUERPO DE CORREO DE DEVOLUCIÓN DE SOLICITUD

Si la solicitud no es devuelta, se lleva a cabo la actividad “Guardar accesos verificados”, la cual utiliza un conector de servicio web para actualizar los accesos que hayan sido verificados por el verificador. Como una solicitud tiene uno o más accesos dentro de la misma, esta actividad itera por cada uno de los accesos que haya avalado el verificador. En la Ilustración 73 se muestra la expresión utilizada para la iteración.

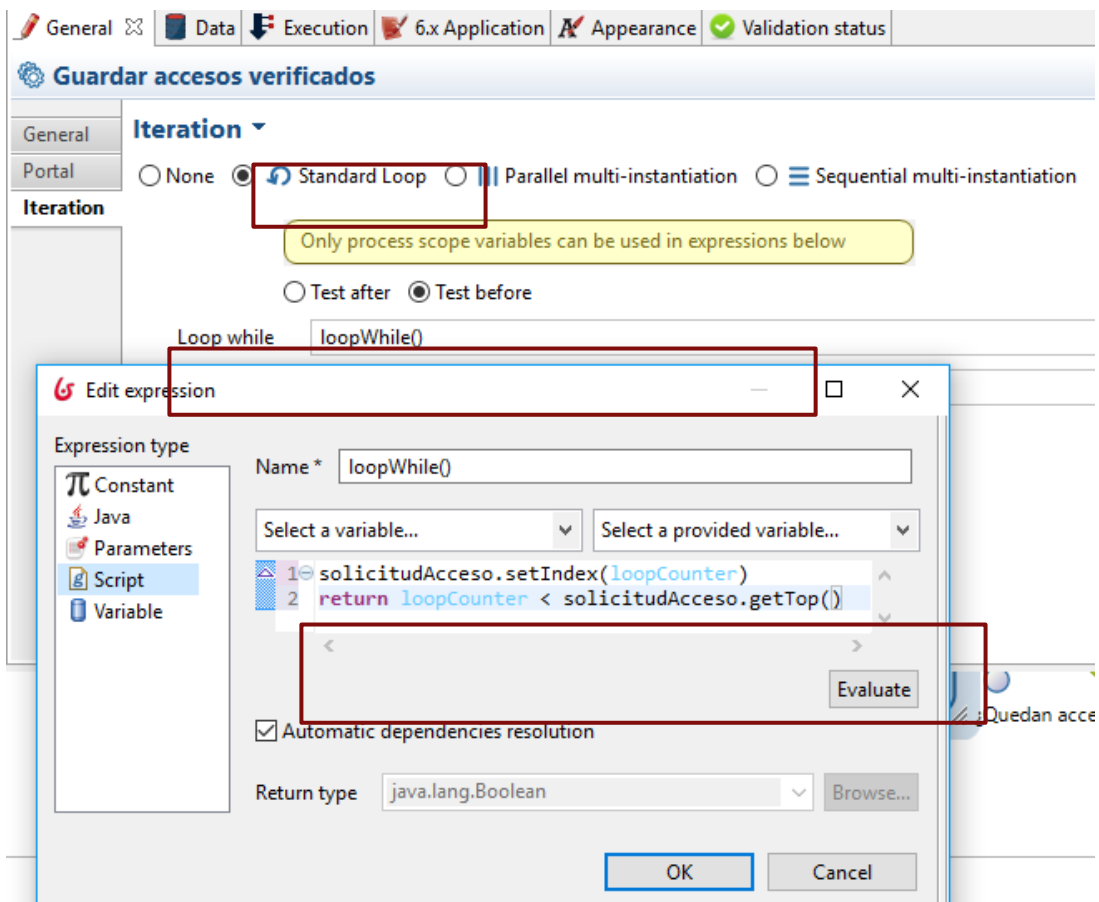


ILUSTRACIÓN 73 EXPRESIÓN DE ITERACIÓN DE LA ACTIVIDAD “GUARDAR ACCESOS VERIFICADOS”

El envelope mostrado en la Ilustración 74, es el que se envía para verificar los accesos de la solicitud.

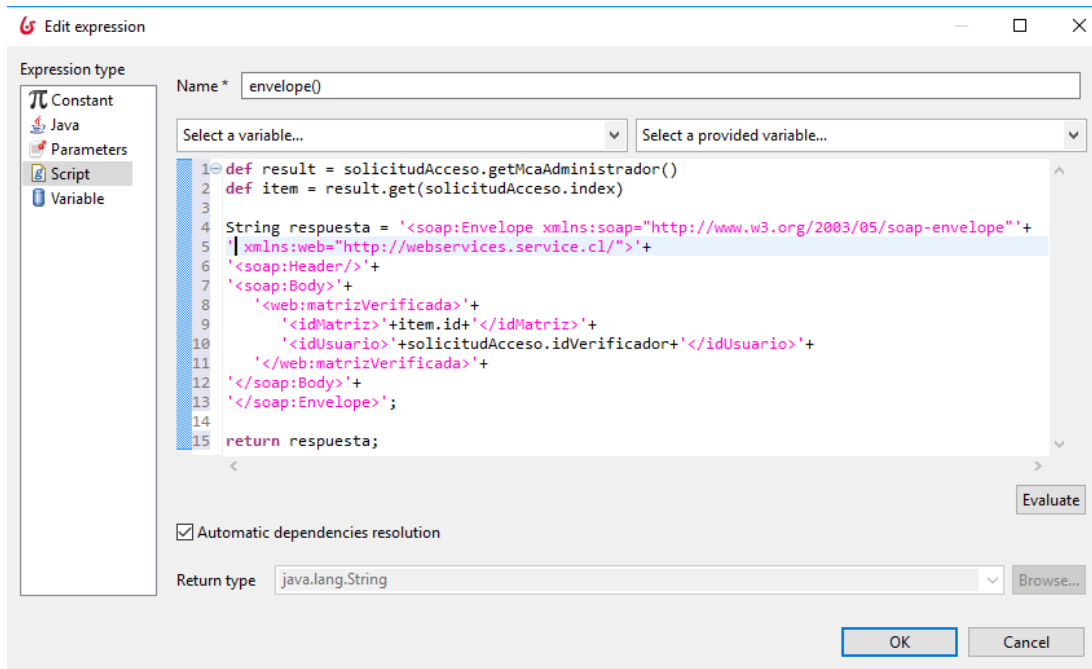


ILUSTRACIÓN 74 ENVELOPE PARA VERIFICAR LOS ACCESOS EN LA MATRIZ DE CONTROL DE ACCESO

En esta actividad también hay una operación que actualiza la variable “estadoSolicitud” al enviar el formulario. En la Ilustración 75 se aprecia como el estado que se coloca dependiendo de lo que haya realizado el Verificador, ya que si culmina con la verificación de todos los accesos de la solicitud esta pasa a estar “Finalizado”, pero si aún quedan accesos por gestionar pasaría al estado “En Verificación”.

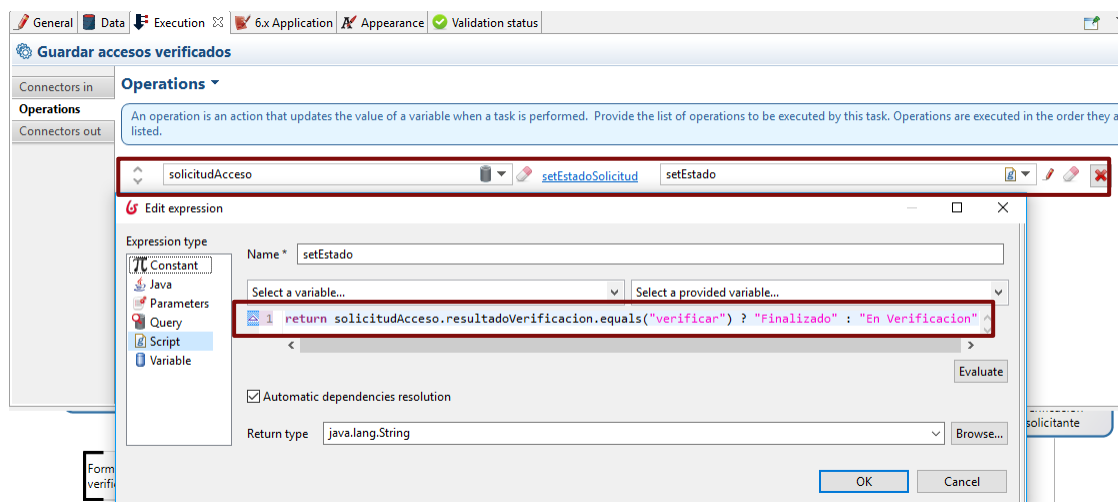


ILUSTRACIÓN 75 SCRIPT QUE ACTUALIZA EL ESTADO DE LA SOLICITUD EN EL CARRIL DEL VERIFICADOR

Luego, se colocó una decisión para comprobar si ya todos los accesos fueron verificados o si aún faltan algunos por verificar. Dicha decisión se nombró “¿Quedan accesos por verificar?” y la expresión de la condición para saber qué camino del flujo tomar se encuentra en la Ilustración 76. Si aún quedan accesos por verificar, el flujo se regresará a la actividad “Recargar solicitud a verificar” y volverá a ejecutar todas las actividades desde ese punto hasta que finalmente todos los accesos sean verificados.

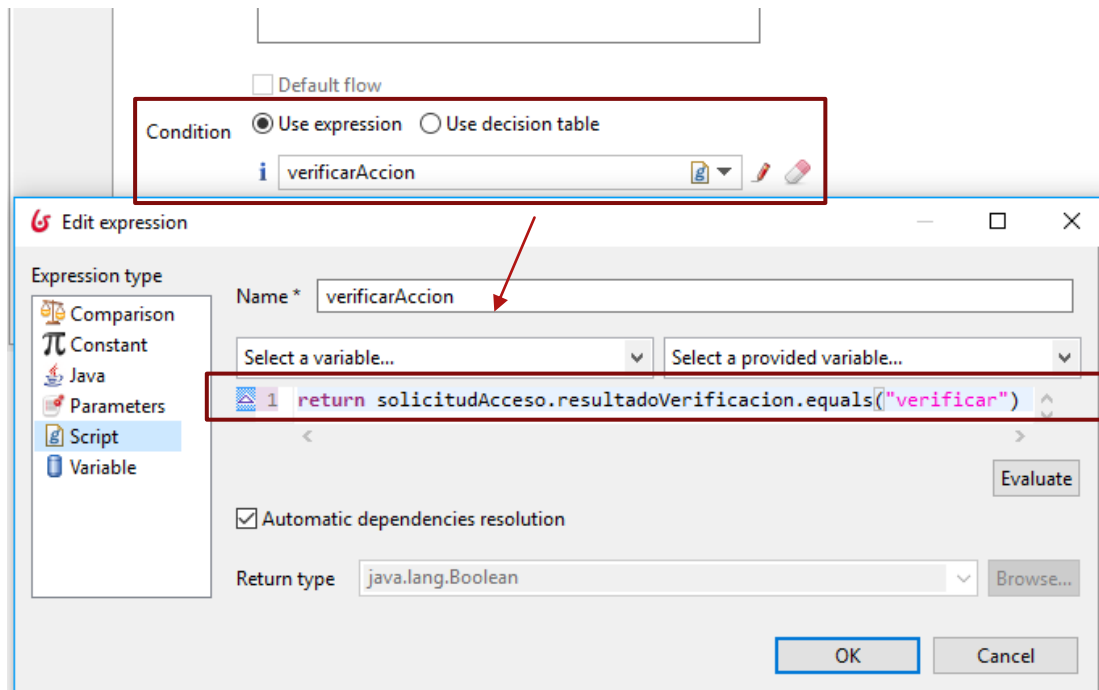


ILUSTRACIÓN 76 EXPRESIÓN DE CONDICIÓN DE ¿QUEDAN ACCESOS POR VERIFICAR?

Si ya no quedan accesos por verificar y el verificador presiona el botón “Finalizar” en el formulario, el flujo que correspondería sería el que se muestra en la Ilustración 77, donde primero se llevaría a cabo la actividad “Actualizar solicitud verificada”. En la Ilustración 78 se muestran los datos enviados al servicio web para realizar esta acción. Luego, se procede a notificar al solicitante que su solicitud ya finalizó a través de un conector de envío de correo electrónico. Por último, se colocó un evento de terminación llamado “Fin – Solicitud finalizada” el cual finaliza con el proceso y todas las actividades.

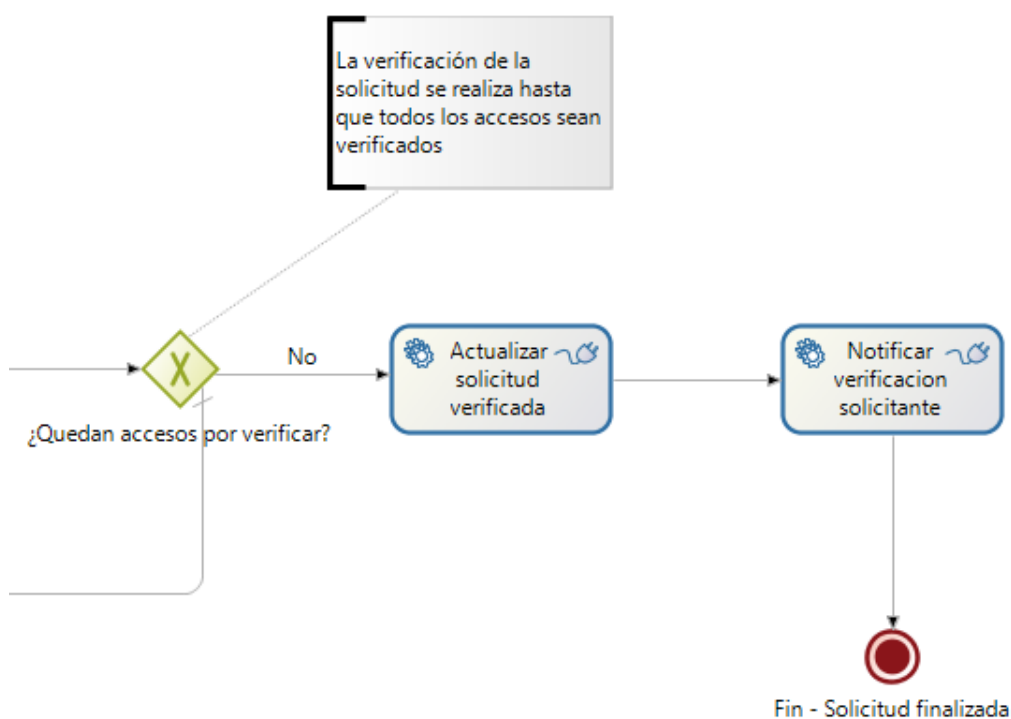


ILUSTRACIÓN 77 FLUJO AL FINALIZAR LA VERIFICACIÓN POR PARTE DEL VERIFICADOR

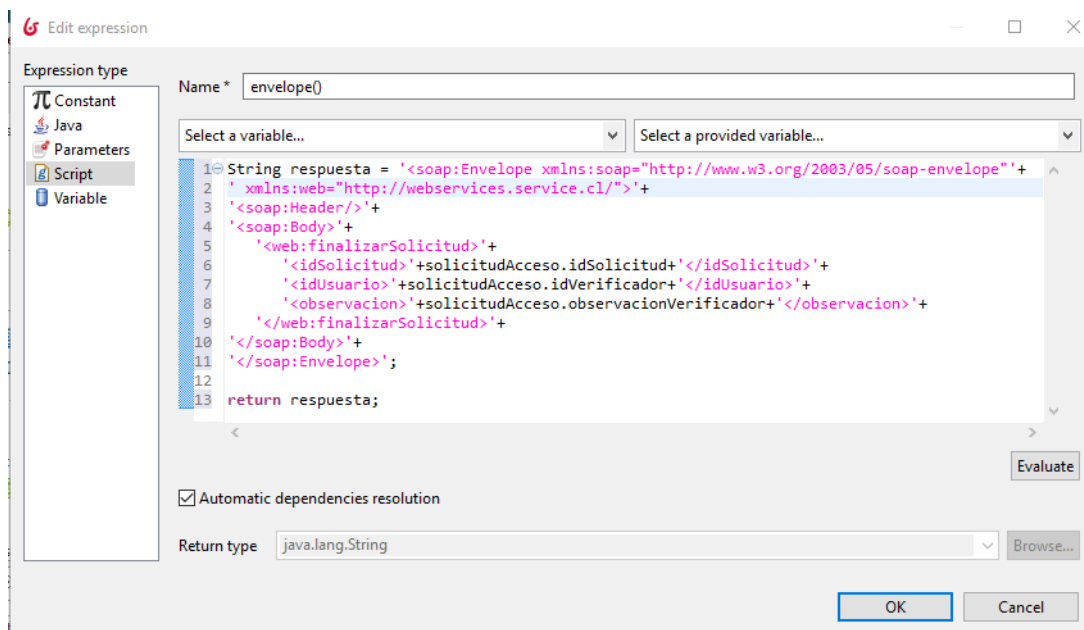


ILUSTRACIÓN 78 ENVELOPE PARA FINALIZAR UNA SOLICITUD

Proceso de cancelación de solicitud

Ya para finalizar con el modelado, se muestra el proceso que se realizó para que los solicitantes puedan cancelar una solicitud previamente realizada. En la Ilustración 79, se muestra el proceso completo, el cual se inicializa a través de un query personalizado en el que al pasarle el id de una solicitud en específico, te regresa toda la información referente a la misma. El query se muestra en la Ilustración 80.

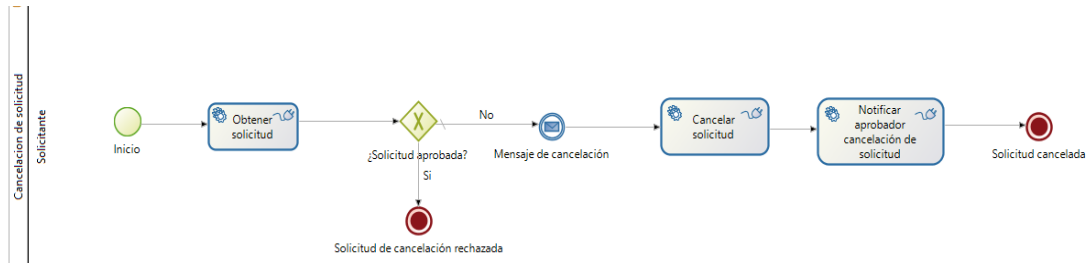


ILUSTRACIÓN 79 FLUJO DEL PROCESO DE CANCELACIÓN DE SOLICITUD

Edit query

Edit findOneByIdSolicitud on SolicitudAcceso

Edit the query using JPQL. Then adapt the list of parameters.
If needed, modify the result type.

JPQL Query *

```
SELECT s
FROM SolicitudAcceso s
WHERE s.idSolicitud = :idSolicitud
```

Parameters

Name *	Type
idSolicitud	java.lang.Integer

Result type ⚠

Single (com.company.model.SolicitudAcceso)

OK Cancel

ILUSTRACIÓN 80 QUERY PARA OBTENER LA INFORMACIÓN DE UNA SOLICITUD POR SU ID

En la Ilustración 82 se detalla cómo se utiliza el query “findOneByIdSolicitud” para inicializar la variable “SolicitudAcceso”, donde el valor que se le da al idSolicitud es la que se encuentra en el contrato de la Ilustración 81.

General Data Execution 6.x Application Appearance Validation status

Solicitante

Connectors in **Process instantiation inputs**

Contract Inputs Constraints

Instantiation form
Overview page
Connectors out

Add from data... Add Add child Remove

Name *	Type	Multiple	Description
idSolicitud	INTEGER	☐	ID de la solicitud

ILUSTRACIÓN 81 CONTRATO DE INSTANCIACIÓN DEL PROCESO DE CANCELACIÓN

Edit Business variable

Edit Business variable
Edit an existing Business variable

Name * solicitudAcceso

Description

Business Object * SolicitudAcceso [Create a new Business Object...](#)

☐ Is multiple

Default value SolicitudAcceso.findOneByIdSolicitud

Edit expression

Expression type Query Script

Select the Business Object and the corresponding query to execute. Set the value for each parameter required by the query.

Business Object	Queries
SolicitudAcceso	findOneByIdSolicitud

Query content

```
SELECT s
FROM SolicitudAcceso s
WHERE s.idSolicitud = :idSolicitud
```

Parameters

Name	Value
idSolicitud	idSolicitud

Return type com.company.model.SolicitudAcceso

ILUSTRACIÓN 82 INICIALIZACIÓN DEL CONTRATO

La actividad “Obtener solicitud” llama a un servicio web para traerse todos los datos que serán necesarios durante el proceso de cancelación de la solicitud. Estos datos se muestran en la Ilustración 83.

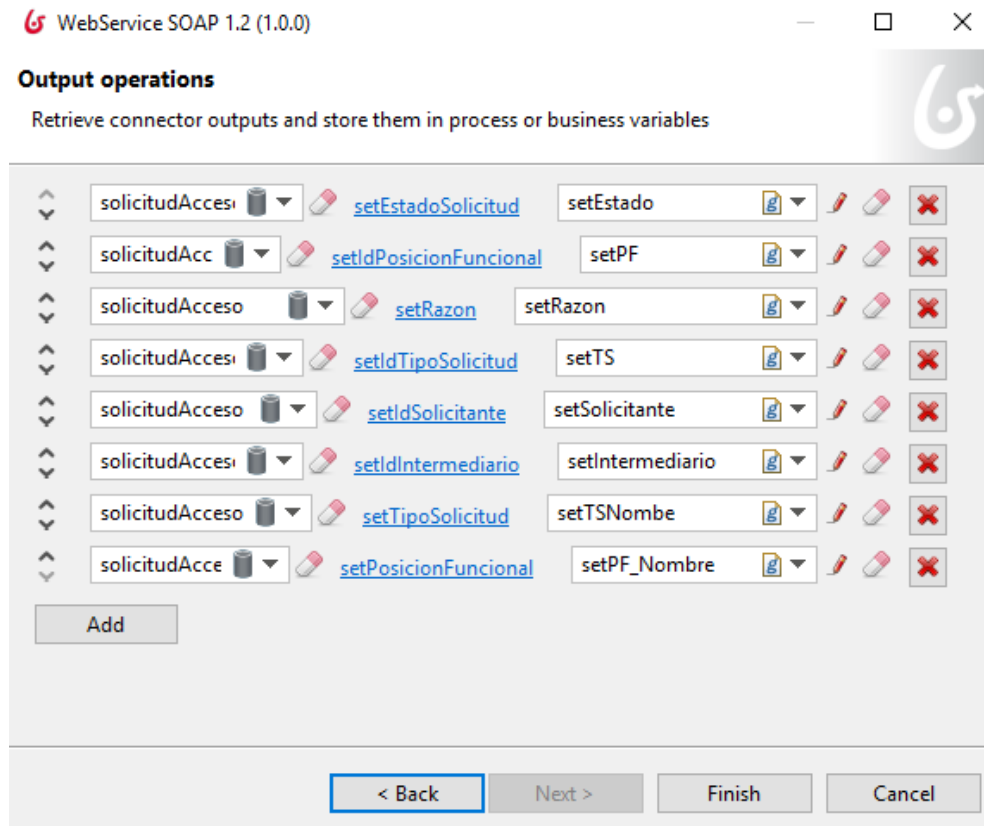


ILUSTRACIÓN 83 INFORMACIÓN OBTENIDA DEL SERVICIO WEB PARA REALIZAR LA CANCELACIÓN

Una vez se tengan las variables actualizadas para el proceso, se colocó un gateway llamado ¿Solicitud aprobada?, el cual es el encargado de evaluar a través de una expresión si la solicitud ya fue aprobada o si aún se encuentra en estado Pendiente. Dicha expresión para la condición se muestra en la Ilustración 84.

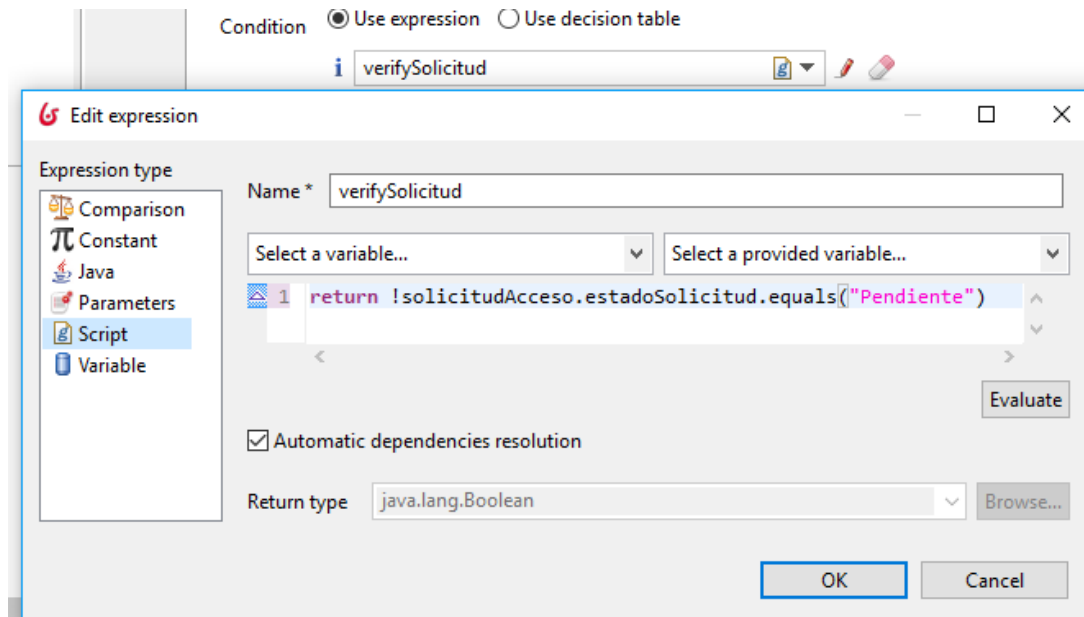


ILUSTRACIÓN 84 EXPRESIÓN DE LA CONDICIÓN DE ¿SOLICITUD APROBADA?

Si la solicitud ya no se encuentra en estado “Pendiente” el proceso terminará y no se podrá realizar la cancelación. En caso contrario, se ejecutará el flujo que se muestra en la Ilustración 85.

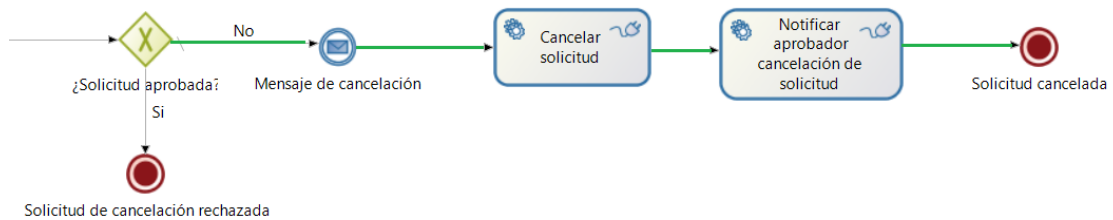


ILUSTRACIÓN 85 FLUJO DE CANCELACIÓN SI LA SOLICITUD TIENE ESTADO “PENDIENTE”

El primer elemento que se encuentra en el modelo luego de la decisión es el evento “Arrojar mensaje” al cual se le agrega un mensaje que será enviado al “Proceso de solicitud de acceso” como se muestra en la Ilustración 86 y la Ilustración 87. El mensaje que se le pasa es una cadena de caracteres que dice “Solicitud cancelada”.

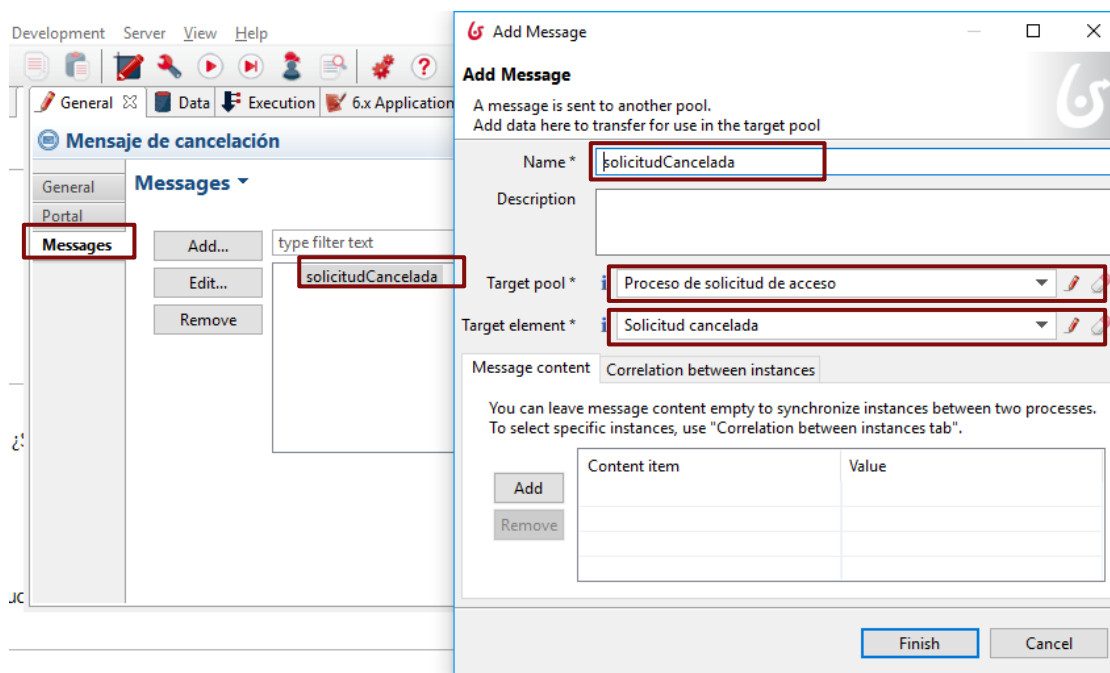


ILUSTRACIÓN 86 MENSAJE A ENVIAR AL OTRO POOL

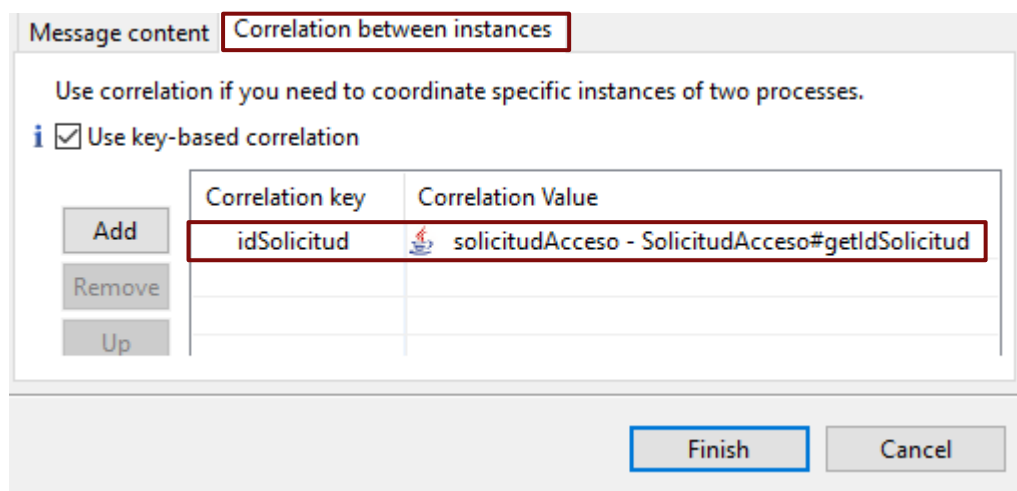


ILUSTRACIÓN 87 CORRELACIÓN ENTRE LAS DOS INSTANCIAS

Luego, dicho mensaje es recibido en el “Proceso de solicitud de acceso”, pero para ello, se deben colocar las configuraciones que se encuentran en la Ilustración 88 y de esta forma ambos procesos se relacionan.

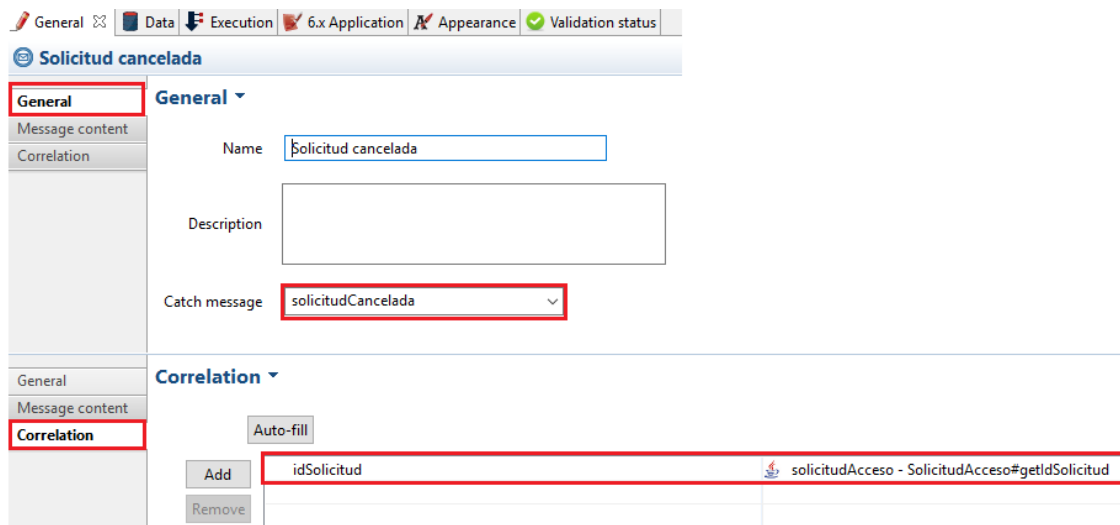


ILUSTRACIÓN 88 CAPTURA DE MENSAJE Y CORRELACIÓN EN EL “PROCESO DE SOLICITUD DE ACCESO”

Por último, se realiza una tarea de servicio que se conecta a un servicio web para cancelar la solicitud y registrarlo en la base de datos, donde el formato del envío del servicio web se aprecia en la Ilustración 89. Luego se le notifica al aprobador que tenía asignado la tarea que se ha cancelado la solicitud y ya no necesitaría ser revisada. El cuerpo del mensaje que se le muestra al aprobador se muestra en la Ilustración 90.

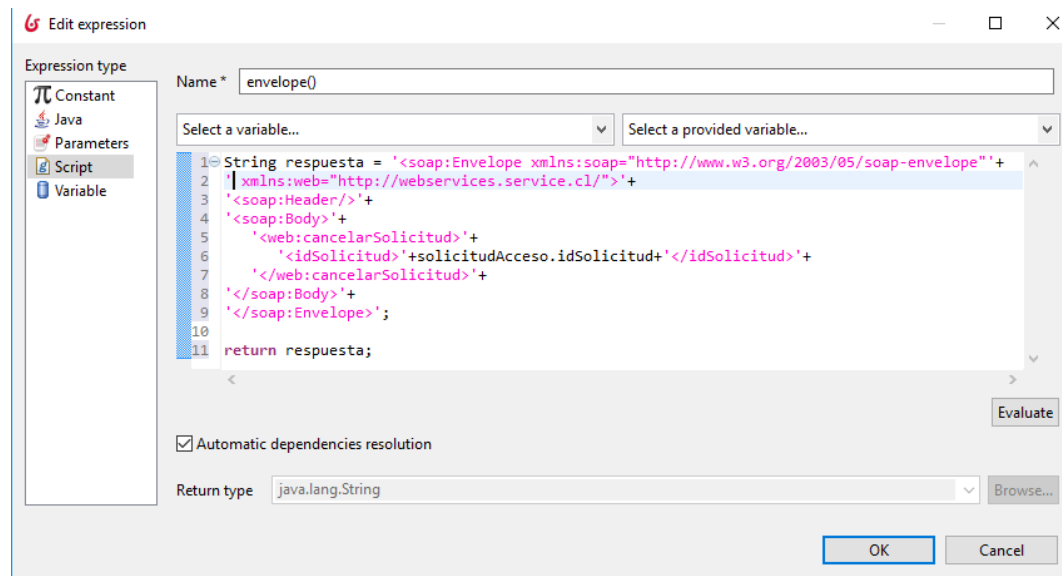


ILUSTRACIÓN 89 ENVELOPE PARA CANCELAR UNA SOLICITUD

```

1 import org.bonitasoft.engine.api.IdentityAPI;
2 import org.bonitasoft.engine.api.ProcessAPI;
3 import org.bonitasoft.engine.bpm.process.ProcessInstance;
4 import org.bonitasoft.engine.identity.ContactData;
5 import org.bonitasoft.engine.identity.User;
6
7 // Get APIs
8 ProcessAPI processAPI = apiAccessor.getProcessAPI();
9 IdentityAPI identityAPI = apiAccessor.getIdentityAPI();
10 // Get process initiator
11 ProcessInstance processInstance = processAPI.getProcessInstance(processInstanceId);
12 long initiatorUserId = processInstance.getStartedBy();
13 // Get email from process initiator
14
15 String resultado = "";
16 String nombreCompleto = "";
17 String intermedio = "";
18
19 if(solicitudAcceso.idIntermediario == 0){
20     User usuario = identityAPI.getUser(initiatorUserId);
21     nombreCompleto = usuario.firstName + " " + usuario.lastName;
22     intermedio = "N/A";
23 }
24
25 }
26 else{
27     User usuario = identityAPI.getUser(solicitudAcceso.idIntermediario);
28     nombreCompleto = usuario.firstName + " " + usuario.lastName;
29
30     User inter = identityAPI.getUser(initiatorUserId);
31     intermedio = inter.firstName + " " + inter.lastName;
32 }
33 String posicion = solicitudAcceso.posicionFuncional;
34 String tipo = solicitudAcceso.tipoSolicitud;
35
36 resultado = "<center><h1>Solicitud de acceso #</h1> " +
37     solicitudAcceso.idSolicitud +
38     "<br>ha sido cancelada</h1></center>" +
39     "Información de la solicitud.<br><br>" +
40     "<b>Usuario:</b> " + nombreCompleto + "<br>" +
41     "<b>Intermediario:</b> " + intermedio + "<br>" +
42     "<b>Tipo de Solicitud:</b> " + tipo + "<br>" +
43     "<b>Posición Funcional:</b> " + posicion + "<br>" +
44     "<b>Razón:</b> " + solicitudAcceso.razon + "<br>"
45
46 return resultado;
47

```

ILUSTRACIÓN 90 SCRIPT QUE GENERA CUERPO DE CORREO DE CANCELACIÓN AL APROBADOR

3.3.3. Despliegue

Una vez culminada la etapa de modelado, la etapa de despliegue corresponde a la configuración de la plataforma tecnológica sobre la cual se va a ejecutar el proceso modelado en la etapa anterior, en este caso Bonita BPM.

Se pueden identificar 3 grandes actividades en esta fase: Exportar la plantilla de la página de inicio “ControlAccesoHome” en el UI designer, agregar la página dentro del Portal de Bonita y crear la aplicación dentro del Portal de Bonita.

Exportar la plantilla de la página de inicio:

El primer paso es exportar la página generada en el UI designer para posteriormente generar la aplicación, para esto se debe ingresar al UI designer y seleccionar la página a exportar. Una vez dentro del editor de la página, se debe presionar el botón para exportar que se señala en la Ilustración 91. Luego, se descargará un archivo .zip y ya se habrá exportado la página.

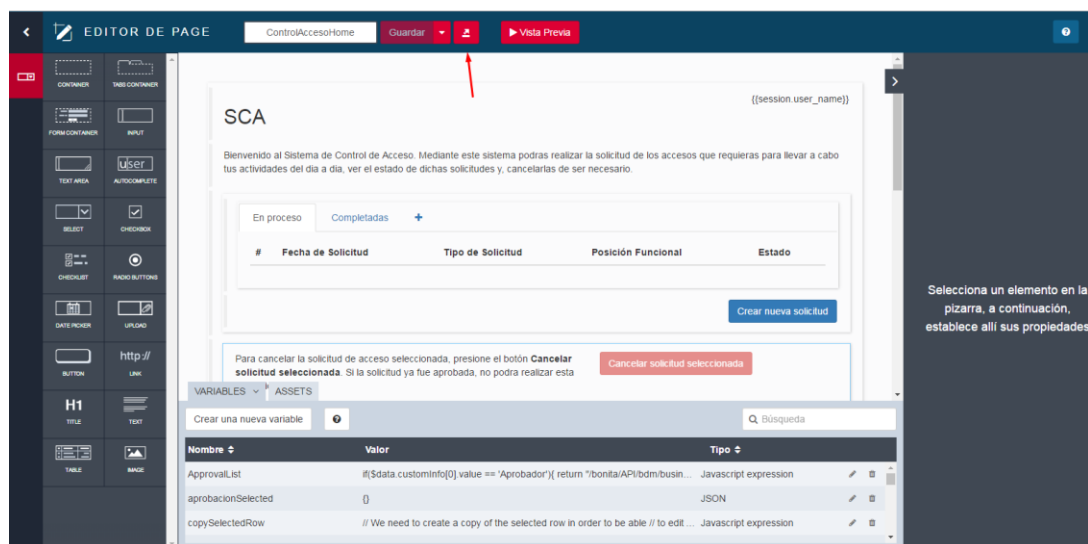


ILUSTRACIÓN 91 EXPORTAR PÁGINA “CONTROLACCESOHOME”

Agregar la página dentro del Portal de Bonita:

Una vez exportado y descargado la plantilla de la página de inicio de la aplicación, se procede a agregar la página dentro del Portal de Bonita. La Ilustración 92 muestra que dentro del portal con un rol administrador y posicionado en la opción del menú “Recursos”, se debe añadir la página buscando el archivo .zip antes generado y presionando el botón “siguiente”.

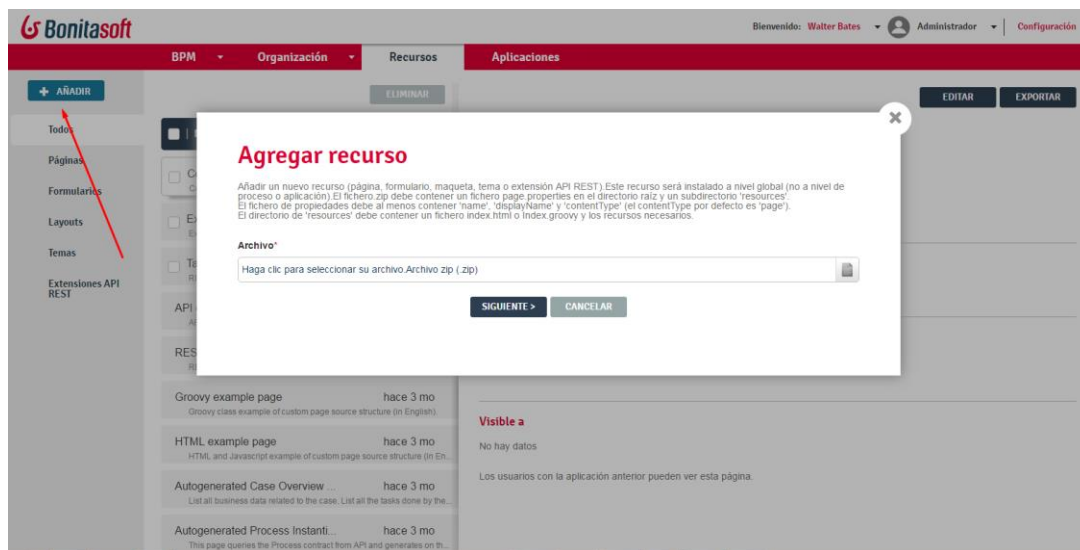


ILUSTRACIÓN 92 AGREGAR PÁGINA COMO UN RECURSO EN EL PORTAL

Creación de la aplicación dentro del Portal Bonita:

El paso final para el despliegue de la aplicación dentro del Portal de Bonita es la creación de la aplicación, para esto se debe ingresar al Portal con un usuario con permisos de administrador y navegar hasta la sección “Aplicaciones”. La Ilustración 93 muestra el formulario a llenar para realizar la creación de la aplicación. Los datos mostrados en la Ilustración 93 significan:

- Título dinámico: Título que se mostrará en la pestaña del navegador al ingresar a la aplicación.
- URL: Dirección lógica de la aplicación por la cual se podrá acceder mediante un navegador web.
- Versión: Versión de la aplicación.
- Perfil: Rol de los usuarios que pueden acceder a la información.
- Descripción: Explicación breve de la aplicación

Crear una Aplicación

Título dinámico *

Proceso de Control de Acceso

URL *

./apps/ sca

Version *

1.0

Perfil *

User

Descripción

Aplicación para solicitar los accesos lógicos necesarios para el buen desenvolvimiento de las tareas diarias.

CREAR CANCELAR

ILUSTRACIÓN 93 FORMULARIO DE CREACIÓN DE UNA APLICACIÓN EN EL PORTAL

Una vez generada la aplicación, se agrega la página generada en la segunda actividad, para ello se debe editar la aplicación y rellenar el formulario como se muestra en la Ilustración 94, en donde se puede observar que se seleccionó la página “ControlAccesoHome” que se generó en la segunda actividad y la sub ruta dentro de la aplicación mediante la cual se podrá acceder a ella.

Añade página

Página *

custompage_ControlAccesoHome - ControlAccesoHome page

URL *

./apps/sca/ index

ANADIR CANCELAR

ILUSTRACIÓN 94 FORMULARIO PARA AÑADIR UNA PÁGINA A UNA APLICACIÓN

Al agregar la página se tendrán dos páginas en la aplicación, una autogenerada por el portal y la que se acaba de cargar. Se debe colocar la nueva como la página home y eliminar la autogenerada de la aplicación como se muestra en la Ilustración 95.

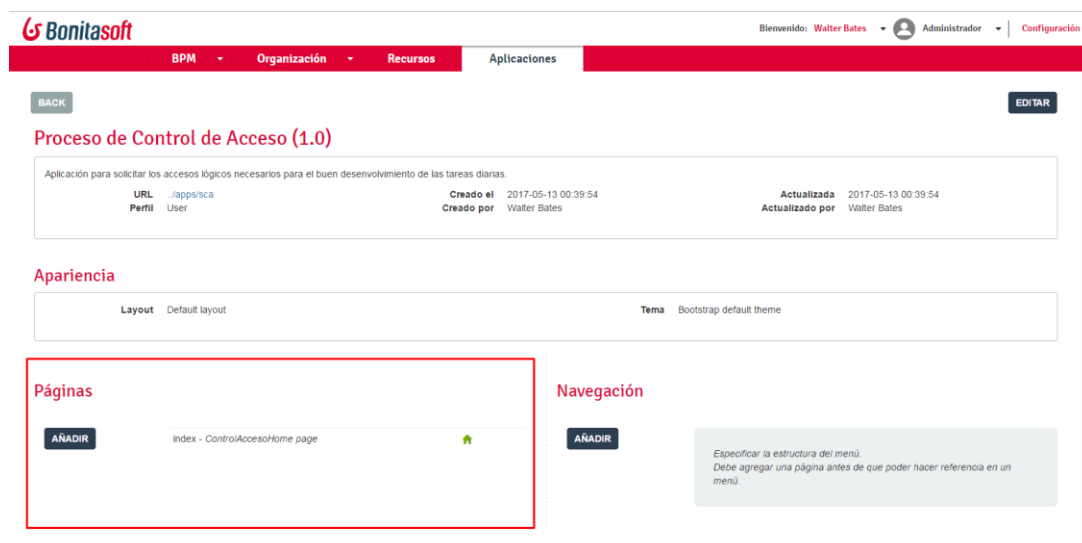


ILUSTRACIÓN 95 “CONTROLACCESOHOME” COMO PÁGINA DE INICIO DE LA APLICACIÓN

Una vez se finalizan estas tres actividades, se podrá acceder a la aplicación a través de la ruta `http://HOST/sca/index` (siendo HOST la dirección donde se levantó la instancia del Motor Bonita).

3.3.4. Ejecución

Una vez terminada la fase de despliegue, se generará una dirección web mediante la cual se podrá acceder a la aplicación y realizar todas las tareas concernientes al proceso de control de accesos. La Ilustración 96 muestra la vista principal de la aplicación, en donde los usuarios podrán realizar una solicitud, revisar el estado de sus solicitudes y para los usuarios con roles “Aprobador”, “Administrador” o “Verificador”, también se le permitirá revisar las tareas pendientes según su rol.



ILUSTRACIÓN 96 PÁGINA DE INICIO (SOLICITANTE)

El usuario que muestra la Ilustración 96 no tiene solicitudes en proceso ni completadas, además por no ser “Aprobador”, “Administrador” o “Verificador” no se le muestran las actividades pendientes para cada de esos roles.

Generación de una solicitud

Para generar una nueva solicitud dentro del sistema, la aplicación dispone de un botón que se aprecia en la Ilustración 96 con el nombre de “Crear nueva solicitud”. Dicho botón despliega el formulario de solicitud o formulario de instanciación del proceso como se muestra en la Ilustración 97.



Proceso de Control de Acceso

Formulario de Solicitud

☐ ¿Es un intermediario?

Tipo de solicitud *

Solicitud de Accesos

Posición Funcional *

Ejecutivo principal DTI

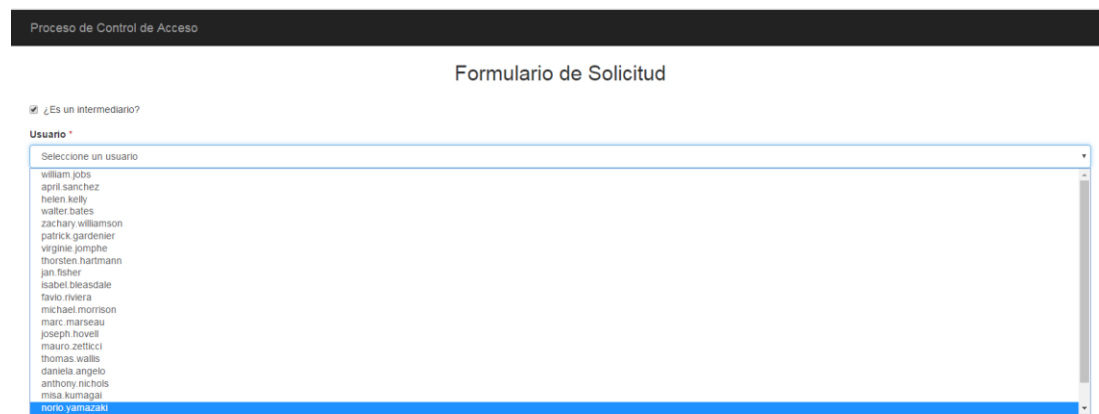
Razon

Solicitud de accesos

Enviar

ILUSTRACIÓN 97 FORMULARIO DE SOLICITUD

La casilla de selección llamada ¿Es un intermediario? Hace referencia a si la solicitud a generar es para el propio usuario o si se está solicitante por otra persona. De marcarse la casilla, la página desplegará una lista de posibles usuarios como se muestra en la Ilustración 98, para seleccionar el nombre del usuario al que se le quiere asociar la solicitud.



Proceso de Control de Acceso

Formulario de Solicitud

☒ ¿Es un intermediario?

Usuario *

Seleccione un usuario

- william jobs
- april sanchez
- helen kelly
- walter bates
- zachary williamson
- patrick gardenier
- virginie jomphe
- thorsten hartmann
- jan fisher
- isabel bleasdale
- favio riviera
- michael morrison
- marc marseau
- joseph howell
- mauro zettici
- thomas wallis
- daniela angelo
- anthony nichols
- misra kumagai
- norio yamazaki**

ILUSTRACIÓN 98 LISTA DE USUARIOS DESPLEGADA EN EL FORMULARIO DE SOLICITUD

Una vez generada la solicitud se le enviará un correo al solicitante informándole que la solicitud se generó exitosamente como se puede observar en la ilustración 99. Adicionalmente, se le enviará un correo electrónico con el formato de la Ilustración 100 al supervisor del solicitante indicándole que tiene una nueva solicitud pendiente por aprobar. Dicha tarea o solicitud, podrá ser observada en la página de la aplicación en la sección “Por Aprobar”.

Solicitud de acceso #240

La solicitud de acceso ha sido generada exitosamente.

Usuario: Giovanna Almeida

Intermediario: N/A

Tipo de Solicitud: Solicitud de Accesos

Posición Funcional: Ejecutivo principal DTI

Razón: Soy ejecutivo de la direccion de tecnologia de informacion y requiero de estos accesos

ILUSTRACIÓN 99 CORREO ELECTRÓNICO ENVIADO AL SOLICITANTE

Solicitud de acceso #240

Tiene una nueva solicitud por aprobar en su bandeja de entrada.

Usuario: Giovanna Almeida

Intermediario: N/A

Tipo de Solicitud: Solicitud de Accesos

Posición Funcional: Ejecutivo principal DTI

Razón: Soy ejecutivo de la direccion de tecnologia de informacion y requiero de estos accesos

[Ir a la bandeja de entrada](#)

ILUSTRACIÓN 100 CORREO ELECTRÓNICO ENVIADO AL SUPERVISOR DEL SOLICITANTE

Cancelación de una solicitud

Para cancelar una solicitud se debe ingresar a la aplicación y seleccionar alguna de las solicitudes que se encuentren en estado “Pendiente”. Al hacer esto, se desplegará una sección en la página que contiene un botón para disparar el proceso de cancelación de la solicitud como se muestra en la Ilustración 101.

Proceso de Control de Acceso

giovanna.almeida Logout

SCA

Bienvenido al Sistema de Control de Acceso. Mediante este sistema podras realizar la solicitud de los accesos que requieras para llevar a cabo tus actividades del dia a dia, ver el estado de dichas solicitudes y, cancelarlas de ser necesario.

En proceso Completadas

#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
102	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Pendiente

Crear nueva solicitud

Para cancelar la solicitud de acceso seleccionada, presione el botón **Cancelar solicitud seleccionada**. Si la solicitud ya fue aprobada, no podrá realizar esta operación.

Cancelar solicitud seleccionada

ILUSTRACIÓN 101 LISTADO DE SOLICITUDES PENDIENTES

Al presionar el botón “Cancelar solicitud seleccionada” se cancelará la solicitud, y la misma podrá ser vista en la pestaña “Completadas” de la aplicación, como se muestra en la Ilustración 102.



#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
102	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Cancelado

ILUSTRACIÓN 102 LISTADO DE SOLICITUDES COMPLETADAS

Aprobación, Administración y Verificación de una solicitud

En los dos primeros flujos, se describió el proceso de creación de una solicitud y la cancelación de la misma. Por otra parte, para que una solicitud sea finalizada satisfactoriamente se debe pasar por al menos 2 actividades, la “Administración” y la “Verificación”, y en caso de que sea necesario, dependiendo del tipo de solicitud, se necesitara una previa “Aprobación”. En este proceso también se pueden rechazar las solicitudes si se encuentra alguna falta dentro de la solicitud (solo el aprobador o el administrador pueden rechazar una solicitud).

Dentro de este proceso hay dos flujos posibles, si la solicitud es del tipo “Solicitud de Accesos” requiere aprobación, en caso contrario, si la solicitud es del tipo “Remoción de Accesos” no requiere aprobación.

Solicitud de accesos:

Si la solicitud es del tipo “Solicitud de Accesos”, una vez generada la solicitud se le notifica al supervisor directo del solicitante que tiene una solicitud pendiente por revisar. Si el supervisor ingresa a la aplicación observará una lista de solicitudes pendientes por aprobar como muestra la Ilustración 103, y adicional a esto, podrá ejecutar esta tarea desde la aplicación, seleccionando cualquiera de las solicitudes pendientes y presionando el botón “Revisar solicitud seleccionada” el cual es señalado en la Ilustración 103.

Proceso de Control de Acceso

SCA daniela.angelo Logout

Bienvenido al Sistema de Control de Acceso. Mediante este sistema podras realizar la solicitud de los accesos que requieras para llevar a cabo tus actividades del dia a dia, ver el estado de dichas solicitudes y, cancelartas de ser necesario.

En proceso Completadas

#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado	
Crear nueva solicitud					
Por Aprobar					
#	Solicitante	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
103	Giovanna Almeida	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Pendiente
101	Anthony Nichols	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Pendiente
99	Anthony Nichols	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Pendiente
98	Anthony Nichols	12/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Pendiente

Revisar solicitud seleccionada

ILUSTRACIÓN 103 LISTADO DE SOLICITUDES POR APROBAR

Al presionar este botón, se despliega el formulario donde el aprobador puede revisar los detalles de la solicitud, teniendo la opción de aprobar o de rechazar dicha solicitud. La Ilustración 104 muestra este formulario y señala la sección donde se selecciona si se aprueba o rechaza la solicitud.

Formulario de Aprobacion

Solicitante
Giovanna Almeida

Tipo solicitud
Solicitud de Accesos

Posición Funcional
Ejecutivo principal DTI

Razón
Accesos necesarios

Perfil	Componente	Accion
asdasd	Peoplenet	Agregar
Administrador Funcional	SCA	Agregar
Operador SAP	SAP	Agregar

Estado *

☒ Aprobado
☐ Rechazado

Comentarios
Todo bien

Enviar

ILUSTRACIÓN 104 FORMULARIO DE APROBACIÓN

Si la solicitud es aprobada, se le enviara un correo electrónico como el que se muestra en la Ilustración 105 a todos los administradores indicándoles que tienen una nueva solicitud pendiente por gestionar. Dicha tarea o solicitud, podrá ser observada en la página de la aplicación en la sección “Por Gestionar” como se muestra en la Ilustración 106, también podemos observar que, al seleccionar un elemento de la lista de solicitudes por gestionar, aparecerá un botón llamado “Gestionar solicitud seleccionada” que servirá para ejecutar la tarea.

Solicitud de acceso #240

Tiene una nueva solicitud por gestionar en su bandeja de entrada.

Usuario: Giovanna Almeida

Intermediario: N/A

Tipo de Solicitud: Solicitud de Accesos

Posición Funcional: Ejecutivo principal DTI

Razón: Soy ejecutivo de la direccion de tecnologia de informacion y requiero de estos accesos

Datos de la Aprobación

Aprobado por: Daniela Angelo

Observación Aprobador: perfecto

[Ir a la bandeja de entrada](#)

ILUSTRACIÓN 105 CORREO ELECTRÓNICO ENVIADO A LOS ADMINISTRADORES

The screenshot shows the SCA interface. At the top, there's a header "Proceso de Control de Acceso" and a user profile "thomas.wallis" with a "Logout" button. Below the header, there's a navigation bar with "En proceso" and "Completadas". The main content area is titled "Por Gestionar" and contains a table with the following data:

#	Solicitante	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
103	Giovanna Almeida	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Aprobado

Below the table, there is a button labeled "Gestionar solicitud seleccionada" with a red arrow pointing to it. To the right of the table, there is a button labeled "Crear nueva solicitud".

ILUSTRACIÓN 106 LISTADO DE SOLICITUDES POR GESTIONAR

La Ilustración 107 muestra el formulario en donde el administrador puede revisar toda la información de una solicitud, y donde puede “Guardar” los accesos gestionados, “Rechazar” en caso de algún error o inconveniente y “Finalizar” que solo se habilitara cuando todos los accesos de la solicitud ya hayan sido gestionados. Para gestionar cada uno de los accesos, se debe seleccionar cada perfil dentro de la tabla, luego se desplegará un botón llamado “Gestionar” como se muestra en la Ilustración 107.

Formulario de Administración

Solicitante
Giovanna Almeida

Tipo Solicitud
Solicitud de Accesos

Posición Funcional
Ejecutivo principal DTI

Razón
Accesos necesarios

☐ Datos del aprobador

Perfil	Componente	Acción	Estado
asdad	Peoplenet	Agregar	Aprobado
Administrador Funcional	SCA	Agregar	Aprobado
Operador SAP	SAP	Agregar	Aprobado


[Gestionar](#)

Comentario *

[Guardar](#) [Rechazar](#) [Finalizar](#)

ILUSTRACIÓN 107 FORMULARIO DE ADMINISTRACIÓN

El botón “Guardar” le permite al administrador guardar en la base de datos el estado de los accesos que ya fueron gestionados, pudiendo salirse del formulario y continuar con la gestión luego. En este caso, la solicitud pasa a estar “En Gestión”, como se aprecia en la Ilustración 108.

Proceso de Control de Acceso				
SCA				thomas.valle Logout
Bienvenido al Sistema de Control de Acceso. Mediante este sistema podras realizar la solicitud de los accesos que requieras para llevar a cabo tus actividades del día a día, ver el estado de dichas solicitudes y; cancelarlas de ser necesario.				
En proceso Completadas				
#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
				Crear nueva solicitud
Por Gestionar				
#	Solicitante	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional
103	Giovanna Almeida	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI
				En Gestion

ILUSTRACIÓN 108 LISTADO DE SOLICITUDES POR GESTIONAR (PREVIO GUARDADO)

Luego, si se vuelve a seleccionar y presionar el botón “Gestionar solicitud seleccionada”, se podrá ingresar nuevamente al formulario de administración y los perfiles que fueron gestionados previamente aparecerán con el estado “Gestionado”, como se muestra en la Ilustración 109.

Formulario de Administración

Solicitante
Giovanna Almeida

Tipo Solicitud
Solicitud de Accesos

Posición Funcional
Ejecutivo principal DTI

Razón
Accesos necesarios

☐ Datos del aprobador

Perfil	Componente	Acción	Estado
asdasd	Peoplenet	Agregar	Gestionado
Administrador Funcional	SCA	Agregar	Gestionado
Operador SAP	SAP	Agregar	Aprobado

Comentario *

ILUSTRACIÓN 109 FORMULARIO DE ADMINISTRACIÓN (PREVIO GUARDADO)

Una vez gestionados todos los accesos de la solicitud, se activará la opción “Finalizar” para terminar la administración y permitir que la solicitud vaya al paso de verificación. Como en la aprobación y en la administración, una vez finalizada la tarea se les notificara a todos los Verificadores que tienen una solicitud pendiente por verificar en la aplicación. Por ende, al ingresar cualquiera de estos usuarios a la aplicación, se les mostrara una lista de solicitudes o tareas pendientes en la sección “Por Verificar”. Seleccionando la solicitud y presionando en este caso el botón “Verificar solicitud seleccionada”, como se muestra en la Ilustración 110, podrán desplegar el formulario de verificación.

Proceso de Control de Acceso

misa.kumagai

SCA

Bienvenido al Sistema de Control de Acceso. Mediante este sistema podras realizar la solicitud de los accesos que requieras para llevar a cabo tus actividades del día a día, ver el estado de dichas solicitudes y, cancelarias de ser necesario.

#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
Crear nueva solicitud				

Por Verificar

#	Solicitante	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
103	Giovanna Almeida	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Gestionado

ILUSTRACIÓN 110 LISTADO DE SOLICITUDES POR VERIFICAR

En el formulario de verificación de la Ilustración 111, el verificador podrá ver el detalle de la solicitud. A diferencia del administrador, el verificador no tiene una opción para rechazar una solicitud, pero en vez de ello, tiene la posibilidad de devolver una solicitud al administrador en caso de errores o inconvenientes. Dicha devolución se puede realizar a través del botón “Devolver”.

Formulario de Verificación

Solicitante
Giovanna Almeida

Tipo Solicitud
Solicitud de Accesos

Posición Funcional
Ejecutivo principal DTI

Razón
Accesos necesarios

☐ Datos del aprobador

☐ Datos del administrador

Perfil	Componente	Acción	Estado
asdad	Peoplenet	Agregar	Gestionado
Operador SAP	SAP	Agregar	Gestionado
Administrador Funcional	SCA	Agregar	Gestionado

Comentario *

ILUSTRACIÓN 111 FORMULARIO DE VERIFICACIÓN

Si el verificador devuelve una solicitud, se le notificará al administrador que ejecuto la tarea a través de un correo electrónico como se muestra en la Ilustración 112, junto con un motivo de la devolución. La solicitud volverá a estar en la lista “Por Gestionar” del administrador con estado “Devuelto” como se muestra en la Ilustración 113.

La solicitud de acceso #240 ha sido devuelta

La solicitud con id 240 fue devuelta por errores en uno o mas de los accesos.

Motivo de devolución: esta mal

[Ir a la bandeja de entrada](#)

ILUSTRACIÓN 112 CORREO ELECTRÓNICO DE DEVOLUCIÓN

Proceso de Control de Acceso

thomas.wallis Logout

SCA

Bienvenido al Sistema de Control de Acceso. Mediante este sistema podras realizar la solicitud de los accesos que requieras para llevar a cabo tus actividades del día a día, ver el estado de dichas solicitudes y, cancelarlas de ser necesario.

En proceso [Completadas](#)

#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
Crear nueva solicitud				

Por Gestionar

#	Solicitante	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
103	Giovanna Almeida	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Devuelto

ILUSTRACIÓN 113 LISTADO DE SOLICITUDES POR GESTIONAR (PREVIA DEVOLUCIÓN)

Al ingresar de nuevo al formulario de administración, podrá observar que al tope del formulario se encuentra un mensaje con el motivo de la devolución en color rojo y en la tabla con los accesos uno o más de ellos se encontraran en estado “Devuelto” como se muestra en la Ilustración 114.

Formulario de Administración

Motivo de la devolución: Hay perfil asignado de forma incorrecta, por favor revisar

Solicitante
Giovanna Almeida

Tipo Solicitud
Solicitud de Accesos

Posición Funcional
Ejecutivo principal DTI

Razón
Accesos necesarios

☐ Datos del aprobador

Perfil	Componente	Acción	Estado
Administrador Funcional	SCA	Agregar	Devuelto
asdasd	Peoplenet	Agregar	Devuelto
Operador SAP	SAP	Agregar	Devuelto

Comentario *

ILUSTRACIÓN 114 FORMULARIO DE ADMINISTRACIÓN DE UNA SOLICITUD DEVUELTA

Una vez finalizada nuevamente la administración y habiendo ingresado al formulario de verificación, el verificador podrá volver a realizar su corroboración, y de estar todo en orden podrá seleccionar cada acceso y verificarlo uno a uno para finalmente finalizar la verificación. También se tiene la opción de guardar su trabajo para posteriormente continuar con la verificación como en la administración. La Ilustración 115 muestra el formulario de verificación y el botón de “Verificar” que se muestra al seleccionar cada acceso.

Formulario de Verificación

Solicitante
Giovanna Almeida

Tipo Solicitud
Solicitud de Accesos

Posición Funcional
Ejecutivo principal DTI

Razón
Accesos necesarios

☐ Datos del aprobador

☐ Datos del administrador

Perfil	Componente	Acción	Estado
asdasd	Peoplenet	Agregar	Gestionado
Administrador Funcional	SCA	Agregar	Gestionado
Operador SAP	SAP	Agregar	Gestionado

Comentario *

ILUSTRACIÓN 115 FORMULARIO DE VERIFICACIÓN DE LA SOLICITUD DEVUELTA

Una vez verificados los accesos de la solicitud y presionado el botón “Finalizar”, la solicitud finalizará con éxito. Posterior a esto, si el solicitante ingresa a la aplicación verá que su solicitud se encuentra en la pestaña de “Completadas” con el estado “Finalizado” como se muestra en la Ilustración 116.

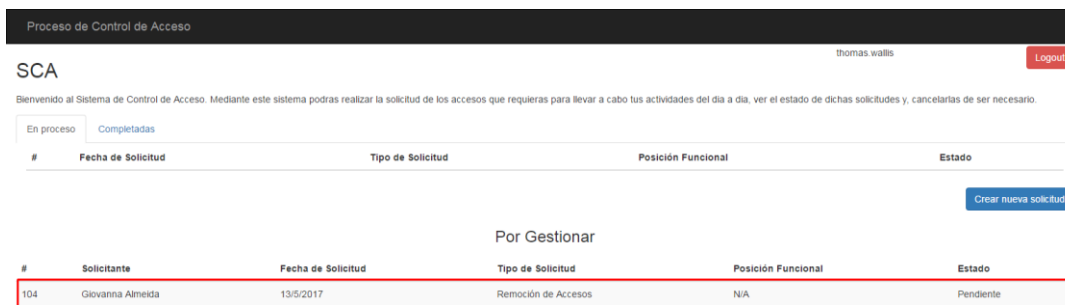


#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
103	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Finalizado
102	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Cancelado

ILUSTRACIÓN 116 SOLICITUDES COMPLETADAS (INCLUIDA LA SOLICITUD FINALIZADA)

Remoción de accesos:

Por otro lado, si al generar una solicitud se escoge la opción de remoción de accesos, el flujo será bastante parecido, con la excepción de que estas solicitudes no necesitan aprobación, por lo que automáticamente, pasaran a la gestión por parte de un Administrador como se muestra en la Ilustración 117, donde se observa una solicitud “Por Gestionar” con estado “Pendiente” y no “Aprobado”. De ahí en adelante los pasos coinciden con los descritos para la asignación de accesos.



#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
104	13/5/2017	Remoción de Accesos	N/A	Pendiente

ILUSTRACIÓN 117 LISTADO DE SOLICITUDES POR GESTIONAR (SOLICITUD DE REMOCIÓN)

Para finalizar, si en el paso de aprobación o de administración el usuario selecciona la opción de “Rechazar”, automáticamente la solicitud finalizará y aparecerá con el estado “Cancelado” dentro de la pestaña de solicitudes Completadas, esto se muestra en la Ilustración 118. También se le notificara al solicitante sobre el estado de su solicitud y el motivo de su rechazo a través de un correo electrónico como el que se muestra en la Ilustración 119.

Proceso de Control de Acceso				
SCA				giovanna almeida Logout
Bienvenido al Sistema de Control de Acceso. Mediante este sistema podras realizar la solicitud de los accesos que requieras para llevar a cabo tus actividades del dia a dia, ver el estado de dichas solicitudes y, cancelarlas de ser necesario.				
En proceso Completadas				
#	Fecha de Solicitud	Tipo de Solicitud	Posición Funcional	Estado
104	13/5/2017	Remoción de Accesos	N/A	Rechazado
103	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Finalizado
102	13/5/2017	Solicitud de Accesos	Ejecutivo principal DTI	Cancelado
Crear nueva solicitud				

ILUSTRACIÓN 118 LISTADO DE SOLICITUDES COMPLETADAS CON LOS 3 POSIBLES ESTADOS

La solicitud de acceso #241 ha sido rechazada

Usuario: Giovanna Almeida

Intermediario: N/A

Tipo de Solicitud: Solicitud de Accesos

Posición Funcional: PF2

Razón: solicitud

Motivo del rechazo: No corresponde con tus funciones en la organizacion

[Ir a la bandeja de entrada](#)

ILUSTRACIÓN 119 CORREO ELECTRÓNICO DE RECHAZO DE SOLICITUD

CONCLUSIONES

Una vez finalizado del presente Trabajo Especial de Grado, cuyo objetivo principal es el Desarrollo de una guía de implementación para un Sistema de Gestión de la Seguridad de la Información mediante el uso de la ISO 27001 y la Gestión de Procesos de Negocio, se puede afirmar que es totalmente factible y útil el acoplamiento de estos marcos de trabajo para el manejo eficiente de los procesos referentes a la seguridad de la información dentro de las organizaciones.

La investigación se consolidó con la realización de los pasos planteados en la guía para el descubrimiento, modelado, despliegue y ejecución de un sistema que les permite a las organizaciones gestionar el proceso de control de acceso a sus aplicaciones, el cual forma parte de los catorce requerimientos para cumplir con la norma ISO 27001. Con este sistema, apoyado en la herramienta de gestión de procesos de negocio Bonita, se puede afirmar que se logró modelar y ejecutar un proceso que cumple con la norma ISO 27001.

La incorporación de las primeras cuatro fases del ciclo de vida de la metodología BPM (descubrimiento, modelado, despliegue y ejecución) lograron concretarse exitosamente para el proceso de control de acceso. Cabe acotar, que estas fases del ciclo de vida BPM se adaptan a la recomendación de la ISO para la implementación de un SGSI, la cual define el PDCA. Ambas definen etapas cíclicas, que una vez completadas deben repetirse para optimizar el proceso, enfocándose siempre en la mejora continua.

Adicionalmente, se puede concluir que la herramienta Bonita contiene un conjunto de módulos y herramientas que facilitaron la solución propuesta. Pudiendo llevarse a cabo el modelado de forma satisfactoria con la utilización de los elementos del lenguaje BPMN, así como la documentación y descripción de cada una de las actividades modeladas.

Es importante destacar que el proceso de control de acceso modelado en Bonita se realizó con la aplicación de servicios SOAP que, finalmente, son los que permiten la comunicación con la base de datos y, además, da pie para la posible interacción con otros sistemas que lo complementen, por ejemplo, un administrador de unidades organizacionales, permisos, posiciones funcionales, componentes, entre otros; o para la interacción con otros sistemas.

Este trabajo de investigación da cabida a próximos estudios que busquen consolidar la posibilidad de tener una herramienta desde la cual se pueda centralizar e implementar cada uno de los dominios planteados por la ISO 27001. Un sistema que sirva como orquestador y administrador documental para el cubrimiento de todos los procesos que presenta la seguridad de la información.

3.4. Recomendaciones

A continuación, se presentan algunas recomendaciones para motivar y promover la continuación del presente trabajo de investigación:

- Reforzar la importancia y el alcance que tiene la seguridad de la información en las organizaciones, tomando en cuenta que cada día la información está aún más expuesta a amenazas que puedan ocasionar daños considerables.
- Entender que la seguridad de la información no solo afecta al área de tecnología, sino a toda la organización incluyendo al negocio.
- Investigar a fondo los otros trece dominios planteados por ISO que se deben tomar en cuenta para la implementación de un sistema de gestión de la seguridad de la información y dar prioridad a estos, según las necesidades de las organizaciones que quieren aportar dicha implementación.

BIBLIOGRAFÍA

- Alonso López, Y. I., Espinosa Toledo, A., Gijón Canseco, A., Juárez Sosa, K., López Avendaño, E. A., & Ramírez Villanueva, L. Á. (5 de Octubre de 2015). *Seguridad Informática*. Recuperado el Julio de 2016, de <http://equipocobao104.blogspot.com/2015/10/seguridad-informatica.html>
- Araujo Sandoval, F., Mejia Pardo, I., Castrejon, K., & Salirrosas Cerna, J. (26 de Diciembre de 2014). *Módulo 3 del Curso Gerencia de Operaciones*. Obtenido de https://www.youtube.com/watch?v=Ub_mNcU_4rM
- Baldecchi Q., R. (4 de Septiembre de 2014). *Implementación efectiva de un SGSI ISO 27001*. Obtenido de <https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%20%20CIGRAS%20ISO%2027001%20-%20rbq.pdf>
- Bizagi. (2014). *Gestión de Permisos*. Recuperado el 5 de Julio de 2016, de <http://www.bizagi.com/processcentral/Documents/e249a73d-55f2-474d-9051-81c3678d0122/docs/Gestion%20de%20Permisos%20-%20Const.pdf>
- Bizagi. (2016). *Bizagi Oficial Plataforma de negocios digitales y BMPS*. Recuperado el 17 de Julio de 2016, de <http://www.bizagi.com/>
- BonitaSoft. (2016). *Documentación BonitaSoft*. Obtenido de <http://documentation.bonitasoft.com/?page=bonita-bpm-overview>
- BonitaSoft. (2016). *Documentación BonitaSoft*. Obtenido de <http://www.bonitasoft.com/products#versions>
- Bonitasoft. (Mayo de 2017). *REST API overview*. Obtenido de <http://documentation.bonitasoft.com/?page=rest-api-overview>
- BS Grupo. (18 de Diciembre de 2014). *Gestión de la Seguridad de la Información*. Obtenido de <https://www.youtube.com/watch?v=FpQetPH4tB4>
- BS Grupo. (27 de Enero de 2014). *Webinar Planeando e Implementando ISO 27001*. Obtenido de <https://www.youtube.com/watch?v=JgG9Xj2V2as&t=1664s>
- Captio. (s.f.). *La gestión basada en procesos. Cómo mejorar el desempeño de tu empresa*. Obtenido de <http://landing.captio.net/gestion-por-procesos-como-mejorar-el-desempeno-de-tu-empresa-guia-gratuita-en-pdf>
- CENELEC. (Mayo de 2017). *Defence and security*. Obtenido de <https://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Pages/default.aspx>
- Clemson School of Computing. (s.f.). *Trusted Computer System Evaluation Criteria (TCSEC)*. Obtenido de <https://www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf>

- Club BPM. (3 de Noviembre de 2009). *BPM Business Process Management – Gestión de Procesos de Negocio*. Obtenido de <http://www.club-bpm.com/ApuntesBPM/ApuntesBPM01.pdf>
- ECC International. (2015). *ISMS (ISO 27001)*. Recuperado el Julio de 2016, de <http://www.eccinternational.com/consulting/it-process-excellence/iso-27001-information-security-management-system>
- Girón Arévalo, A. C., & Quishpe Villafuerte, P. A. (2008). *Estudio Comparativo de Tecnologías BPM - Gestión de Procesos de Negocio, Caso Practico Escuela Superior Politécnica de Chimborazo*. Obtenido de <http://dspace.esPOCH.edu.ec/bitstream/123456789/473/1/18T00361%20UDCTFIYE.pdf>
- GlobalLogic. (12 de Abril de 2012). *BPM... ¿Qué nos trajo hasta aquí?* Obtenido de https://www.globallogic.com/latam/gl_news/bpm-que-nos-trajo-hasta-aqui/
- Hansche, S., Berti, J., & Hare, C. (2004). *Official (ISC)2 Guide to the CISSP Exam*. US: Auerbach Publications.
- Hernandez, S. (2012). *Official (ISC)2 Guide to the CISSP CBK: Third Edition*. US: Auerbach Publications.
- ISO. (2005). *ISO 27002:2005*.
- ISO. (2005). *ISO 9000, Sistemas de gestión de la calidad*. Obtenido de http://www.umc.edu.ve/pdf/calidad/normasISO/Norma_ISO_9000_2005.pdf
- ISO. (Mayo de 2017). *About ISO*. Obtenido de <https://www.iso.org/about-us.html>
- ISO. (Mayo de 2017). *International Organization for Standardization*. Obtenido de <https://www.iso.org/home.html>
- ISO. (21 de Marzo de 2017). *ISO Survey of certifications to management system standards*. Obtenido de <http://isotc.iso.org/livelink/livelink?func=ll&objId=18808885&objAction=download&viewType=1>
- ISO. (21 de Marzo de 2017). *ISO Survey of certifications to management system standards - Full results*. Obtenido de ISO/IEC 27001 - data per country and sector 2006 to 2015 : <http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1>
- ISO. (Mayo de 2017). *ISO/IEC 27001 - Information security management*. Recuperado el 17 de Julio de 2016, de <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>
- ISO2700.es. (s.f.). *ISO 27000*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

- ISOTools Excellence. (7 de Mayo de 2015). *¿Por qué implantar un SGSI basado en la norma ISO 27001?* Obtenido de <http://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/>
- ISOTools Excellence. (14 de Junio de 2016). *La norma ISO 27002 complemento para la ISO 27001.* Obtenido de <http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/>
- ITU-T. (2017). *El UIT-T en breve.* Obtenido de <http://www.itu.int/es/ITU-T/about/Pages/default.aspx>
- ITU-T. (2017). *Sobre la UIT.* Obtenido de <http://www.itu.int/es/about/Pages/default.aspx>
- KPMG. (2015). *Segregación de Funciones.* Recuperado el 5 de Julio de 2016, de <https://www.kpmg.com/PE/es/IssuesAndInsights/ArticlesPublications/Documents/Factsheets/Segregaci%C3%B3n-de-Funciones.pdf>
- Ministerio de Fomento. (Mayo de 2015). *La gestión por procesos.* Obtenido de <http://www.fomento.es/NR/rdonlyres/9541ACDE-55BF-4F01-B8FA-03269D1ED94D/19421/CaptuloIVPrincipiosdelagestindelaCalidad.pdf>
- Morales Carrizosa, F. X. (Mayo de 2017). *Características de MYSQL.* Obtenido de <https://packo.wikispaces.com/Caracteristicas+de+MYSQL>
- OMG. (Enero de 2011). *Documents Associated With Business Process Model And Notation™ (BPMN™) Version 2.0.* Obtenido de <http://www.omg.org/spec/BPMN/2.0/>
- OMG. (2016). *Object Management Group - Business Process Model and Notation.* Obtenido de <http://www.bpmn.org/>
- Oracle. (Mayo de 2017). *La base de datos de código abierto más popular del mundo.* Obtenido de <https://www.oracle.com/latam/mysql/index.html>
- Osiatis. (s.f.). *Curso ITIL Foundation.* Recuperado el 5 de Julio de 2016, de http://itilv3.osiatis.es/operacion_servicios_TI/gestion_acceso_servicios_ti/introduccion_objetivos.php
- Palmer, N. (26 de Marzo de 2014). *What is BPM?* Obtenido de <http://bpm.com/what-is-bpm>
- Pérez Fernández de Velasco, J. A. (2004). *Gestión por Procesos, Cómo utilizar ISO 9001:2000 para mejorar la gestión de la organización.* Madrid: ESIC.
- S. Rodríguez, A., Bazan, P., & Diaz, F. (2015). *Características funcionales avanzadas de los BPMS: Análisis comparativo de herramientas.* Obtenido de http://www.linti.unlp.edu.ar/uploads/docs/caracteristicas_funcionales_avanzadas_de_los_bpms__analisis_comparativo_de_herramientas_.pdf

- Smith, H., & Fingar, P. (2003). *Business Process Management BPM: The Thrid Wave*. Tampa: EUA: Meghan-Kiffer Press.
- STATUM. (2014). *BPMS, UN NUEVO CONCEPTO PARA GESTIONAR PROCESOS DE NEGOCIO*. Obtenido de <http://www.statum.biz/statum/type1/8/productos-bpms-informacion>
- Ultimus Enterprise Solutions. (2016). Recuperado el 16 de Julio de 2016, de <http://www.ultimus.com/es>
- Universidad Autónoma de Mexico. (s.f.). *Fundamentos de Seguridad Informática*. Obtenido de Estandares Information Technology Security Evaluation Criteria. ITSEC.: <http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ITSEC.php>
- Universidad Nacional Autónoma de Mexico. (s.f.). *Fundamentos de Seguridad Informática*. Obtenido de Estandares Trusted Computer Security Evaluation Criteria. TCSEC.: <http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/TCSEC.php>
- W3C. (s.f.). *Guía Breve de Servicios Web*. Recuperado el 2016, de <http://www.w3c.es/Divulgacion/GuiasBreves/ServiciosWeb>
- White, S., & Miers, D. (2009). *BPMN Guía de Referencia y Modelado*. Obtenido de <http://users.dcc.uchile.cl/~nbaloian/DSS-DCC/Software/ModeladoBPMN.pdf>