Universidad Técnica Particular de Loja
La Universidad Católica de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

TEMA:

Implementación del proceso de Release Management dentro del gobierno de TI en el Banco Nacional de Fomento

Tesis previa a la obtención del Título de Ingeniero en Informática

Autores:

Lenni Tatiana Carrión Sánchez

Julio Martín Viteri Córdova

Directores:

Ing. Armando Cabrera S.

Ing. Patricio Abad E.

Loja – Ecuador

2011

CERTIFICACION

Ing. Armando Cabrera S.

DIRECTOR DE TESIS

Ing. Patricio Abad E.

CODIRECTOR DE TESIS

CERTIFICA:

Que el presente trabajo de tesis realizado por Lenni Tatiana Carrión Sánchez y Julio Martín Viteri Córdova cuyo tema es Implementación del proceso de Release Management dentro del gobierno de TI en el Banco Nacional de Fomento, ha sido dirigido, orientado y evaluado en todas sus fases, habiendo constatado que cumple con los requisitos de fondo y forma exigidos por la Escuela de Ciencias de la Computación, en consecuencia autorizo su presentación, sustentación y defensa.

Ing. Armando Cabrera S.

DIRECTOR

Ing. Patricio Abad E.

CODIRECTOR

Loja, mayo de 2011

CESION DE DERECHOS

Nosotros, Lenni Tatiana Carrión Sánchez y Julio Martín Viteri Córdova, declaramos ser autores del presente trabajo y eximimos expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaramos conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero, académico o institucional (operativo) de la Universidad.

……..……

Lenni Tatiana Carrión Sánchez

……..……

Julio Martín Viteri Córdova

AUTORIA

Los conceptos, ideas opiniones desarrolladas en el presente trabajo son de exclusiva responsabilidad de los autores.

……..……

Lenni Tatiana Carrión Sánchez

……..……

Julio Martín Viteri Córdova

AGRADECIMIENTO

Mi agradecimiento a Dios por haber trazado este camino de lucha y oportunidades para demostrarme cuanto más puedo llegar a ser en beneficio de los seres que amo y la sociedad a la que sirvo a través de mi trabajo diario.

A mi familia que nunca reclamó mis ausencias, necesarias para cumplir esta meta, y al contrario, con paciencia y amor celebraron mis logros y apoyaron mis dificultades.

A mis amigos que siempre estuvieron al tanto de la evolución de esta decisión de profesionalización.

A mi gran amigo Julito, que en los momentos de desesperanza, me animó a seguir adelante y no permitió que este objetivo quede inconcluso.

Lenni.

A mi Dios todopoderoso, quien con su guía, bendición y protección, me ha permitido compartir a lo largo de esta etapa de mi vida, con personas quienes con su carisma, comprensión, amistad, entrega y amor, me han brindado el apoyo y empuje necesario desde su rol de padre, esposa e hijos. A mi amiga y compañera de Tesis, Lenni, quien con su apoyo incondicional, ejemplo y fortaleza, permitió construir y cristalizar nuestro sueño. Al ser que me dio la vida, mi Madre, a quien deseo expresar un agradecimiento muy especial y profundo por todo lo que ella hizo y configuró en mi persona, quisiera que esté junto a mí en estos momentos y compartir estos sentimientos de alegría y orgullo; ya no es posible, pero mi corazón y mi mente te recordaran por siempre madre querida.

Julio.

DEDICATORIA

Dedicado a:

Los cuentos sin contar de mi Mauro Nicolás

Los secretos sin confesar de mi Sebastián

Los pies calientitos de mi esposo que me abrigaron tantas noches desveladas

La memoria de mí adorado padre

La perseverancia heredada de mi madre

Lenni

A Mariani, esposa querida, este es el producto de tu sacrifico como esposa y madre, aquellos momentos en los cuales tuve que dejarte sola, fueron difíciles pero necesarios para construir este sueño de superación que hoy lo comparto contigo; te invito a que tomes la posta y empecemos juntos a vislumbrar tus metas y realizaciones profesionales. A mis hijos, Mateo y Mártin, que se encuentran formándose en las aulas, que el ejemplo de su padre sea uno de los factores que motiven a la consecución de sus metas y logros. A ti Julio, mi padre, dedicarte la feliz culminación de mi carrera profesional, prometerte retransmitir y multiplicar estas experiencias hacia tus nietos queridos.

Julio

ESQUEMA DE CONTENIDOS

CONTENIDO

CAPITULO I

1.1 VISION GENERAL

El Banco Nacional de Fomento, con 82 años de existencia dentro del sector financiero del Ecuador, con 144 oficinas distribuidas en las 24 provincias existentes, con más de un millón de clientes en su sistema crediticio especialmente el de microcrédito, 120.000 cuenta corrientistas y 800.000 cuenta ahorristas, dentro de su estrategia de desarrollo organizacional; apuntala su servicio a la comunidad de pequeños y medianos productores de los sectores menos favorecidos, en una infraestructura tecnológica que le permite, hoy por hoy, manejar niveles adecuados de servicio nunca antes ofrecidos debido al estancamiento tecnológico de varias décadas.

Actualmente, el rol protagónico adquirido por ser ejecutor de las políticas de gobierno en el aspecto económico – productivo, lo enfrentan al reto de responder con inmediatez, eficacia y eficiencia, a las diferentes estrategias de apoyo a los sectores básicos del desarrollo productivo de nuestro país.

Es en este marco de referencia, que la Gerencia Nacional de Sistemas enfrenta el reto de entregar servicios que soporten la amplia y cambiante gama de necesidades del Banco, para lo cual se enmarca en un enfoque sistemático del servicio, centrado en los procesos y procedimientos y a la vez, requiere establecer estrategias para la gestión operativa de su creciente infraestructura. Con este antecedente, decide adoptar como modelo de gobierno de TI la metodología ITIL que cubre básicamente las áreas de Soporte del Servicio y Prestación del Servicio

El soporte del servicio, al preocuparse de todos los aspectos que garantizan la continuidad, disponibilidad y calidad del servicio prestado al usuario, involucra las siguientes gestiones canalizadas a través de Help Desk:

- Gestión de Incidentes
- Gestión de Problemas
- Gestión de Cambios
- Gestión de Versiones
- Gestión de Configuraciones

La provisión del servicio que se ocupa de los servicios ofrecidos en si debe gestionar los siguientes procesos:

- Gestión del Nivel de Servicio
- Gestión de Disponibilidad
- Gestión de Capacidad
- Gestión Financiera
- Gestión de Continuidad

A la par y con el respaldo del convenio BNF-PNUD firmado con las Naciones Unidas para la automatización y renovación tecnológica, se empezó en junio de 2008 el proceso de selección de un sistema bancario integrado; una vez transcurrido el proceso de convocatoria, análisis y selección del mismo, se determina que COBIS es la solución de Core Bancario Integral que sería implementada en el Banco Nacional de Fomento.

El Proyecto de Implementación del Core Bancario, obligó a toda la institución y particularmente a la Gerencia Nacional de Sistemas a madurar sus procesos, consolidarlos y administrarlos de manera adecuada, considerando el crecimiento exponencial en infraestructura necesaria para soportar la solución escogida.

Se inicia un permanente ciclo de mejora continua para la gestión de cada uno de los procesos involucrados, tanto en el soporte como en la entrega del servicio. Considerando la compleja arquitectura de la solución bancaria integrada, como uno de los puntos de apoyo visible, se define la optimización de la Gestión de Versiones (Release Management) para garantizar disponibilidad y continuidad del servicio para la atención de todos nuestros clientes en cada una de las localidades a nivel nacional.

La arquitectura del Core Bancario Integral, con programas residentes en cada máquina usuaria de los módulos que conforman este Core y con las reglas del negocio definidas a nivel de base de datos en el servidor central, maneja un estricto control de Versionamiento en sus diferentes ambientes (Desarrollo, Calidad y Producción) por lo que, la distribución del aplicativo a nivel nacional, se convierte en un proceso de misión crítica para el área de Producción de la Gerencia Nacional de Sistemas.

En función de darle continuidad a los servicios que el Banco actualmente ofrece a sus clientes, y apoyando los tiempos definidos en el cronograma de implementación del Core Bancario Integral, existen dos grupos paralelos de trabajo que de forma coordinada llevan adelante cada una de las actividades planificadas. En este contexto, cada uno de los subprocesos que conforman el proceso de Release, deben ser ejecutados sin impactar ni degradar la disponibilidad establecida para los sistemas actuales; por ello, la distribución del software de aplicación para el Core Bancario Integral debe ser realizada fuera de horarios normales de atención al público, sin interrumpir las labores del personal a cargo de los actuales servicios y cubriendo exitosamente el total de los aproximadamente 3.030 equipos destino de las diferentes distribuciones; lo que aumenta notablemente la criticidad del Proceso de Release.

Por las razones descritas, el motivo de desarrollo del presente trabajo de Tesis, establecerá el marco de referencia adecuado para implementar el Proceso de Release Management en el gobierno de TI de la Gerencia Nacional de Sistemas, implementando los controles adecuados obtenidos a través de la aplicación de la metodología de análisis de riesgos que la Gerencia Nacional de Riesgos recomienda para todos los procesos del Banco Nacional de Fomento.

1.2 ESTRUCTURA ORGANIZACIONAL DEL BANCO NACIONAL DE FOMENTO

Resultado de la consultoría contratada con la empresa auditora Price Waterhouse Coopers, el Banco Nacional de Fomento aprobó en sesión de directorio de la institución, la estructura descrita en la Figura 1.1, enmarcada dentro de la normativa establecida por el Ministerio de Relaciones Laborales, vigente para todas las instituciones del sector público.

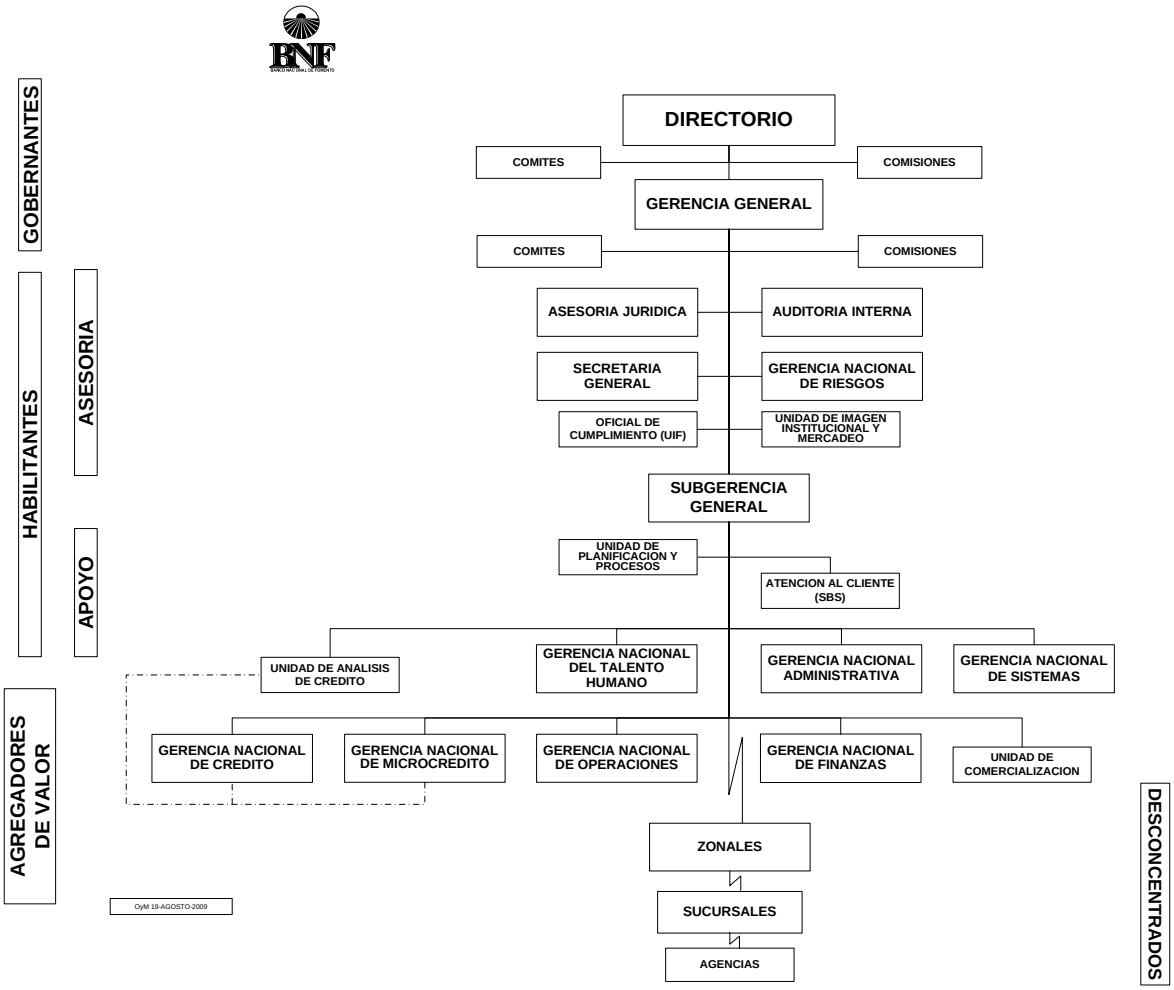


Figura 1.1 Estructura Orgánico Funcional del Banco Nacional de Fomento
Tomado de: Estatuto Orgánico por Procesos del Banco Nacional de Fomento (2010)

La Gerencia Nacional de Sistemas del BNF, a la presente fecha, es la única gerencia que maneja su estructura orgánica funcional considerando los procesos a su cargo, para lo cual se ha basado en ITIL como marco de referencia para la gestión de los servicios que oferta a toda la institución, esto en respuesta a la necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del BNF, y que satisfagan los requisitos y las expectativas de sus clientes.

La estructura orgánica por procesos de la Gerencia Nacional de Sistemas, se encuentra definida según lo describe la Figura 1.2

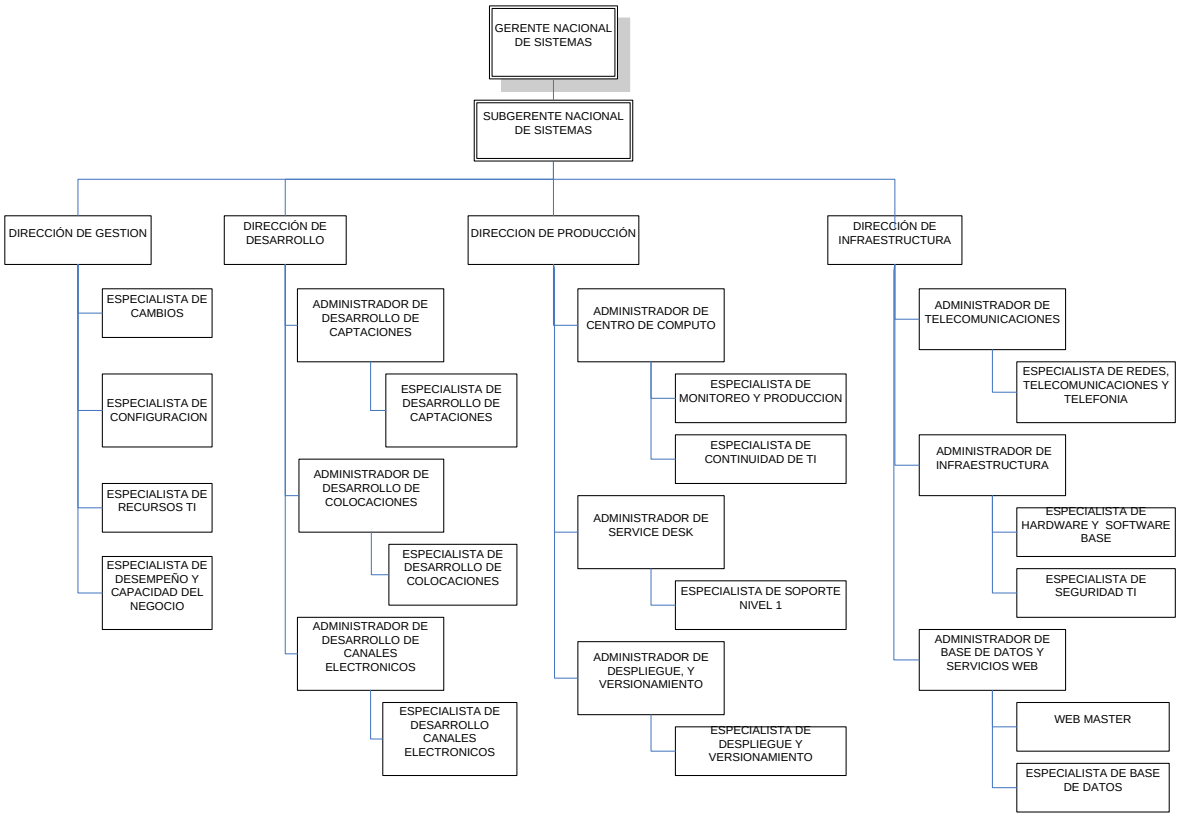


Figura 1.2 Estructura Orgánica por Procesos de la Gerencia Nacional de Sistemas
Tomado de: Estatuto Orgánico por Procesos del Banco Nacional de Fomento (2010)

1.3 SITUACION ACTUAL DEL PROCESO DE RELEASE MANAGEMENT

El proceso de Release de la Gerencia Nacional de Sistemas, es un proceso puntualmente definido, control de fuentes, ejecutado por una sola persona y un backup, por lo tanto su rol dentro del proceso de Control de Cambios, en forma macro corresponde a:

- Entregar fuentes, a los desarrolladores previo el análisis del documento de solicitud de fuentes para solventar un requerimiento que implique desarrollo y validando los niveles de autorización vigentes para cada desarrollador.
- Recibir fuentes, previo el análisis del documento de entrega de fuentes para registrar la versión y grabar el historial de versionamiento del programa entregado o nuevo cuando el requerimiento obliga a que un cambio entre en producción.
- Registrar en la herramienta de control de fuentes (DSL), el historial de desprotección y protección de cada programa perteneciente al Banco Nacional de Fomento.
- No existe el proceso de obtención de nuevos ejecutables en ambiente de pre-producción, siendo este un control indispensable que evita los cambios no autorizados que introducen vulnerabilidades en la seguridad.

Estas actividades se ven suficientes, debido al carácter de las aplicaciones, las cuales pese a ser centralizadas, corresponden a una arquitectura cliente-servidor, pero con un cliente liviano residente en el equipo de escritorio de cada usuario final del sistema, que no incluye ningún tipo de ejecutable ni maneja librerías o componentes.

No existe ningún control establecido producto de un análisis de riesgo, por lo tanto no se monitorea ni se minimiza el riesgo operativo de este proceso, desde el punto de vista de seguridad de la información.

En octubre de 2009, fecha en la que, se da término al proceso de selección del nuevo Core Bancario Integral, se firma el contrato entre BNF y la empresa COBIS Corp., la misma que dentro de un proyecto multidisciplinario integrado por Técnicos Funcionales, Ingenieros de Procesos, Analistas de Desarrollo de la Gerencia Nacional de Sistemas del Banco por una parte; y Técnicos Especialistas de COBIS Corp. por otra, cada uno con Gerentes de Proyecto a la cabeza, dieron inicio a la implementación del Core Bancario Integral de la institución. Esta solución bancaria integral (27 módulos), significa una reingeniería operativa de los procedimientos, manuales y automatizados del Banco, así como la centralización de datos, aplicaciones y procesos a través de una solución bancaria de modelo cliente-servidor.

El equipo de escritorio de cada usuario del Core Bancario, tiene en su disco local, residentes los componentes, librerías, ejecutables y recursos de cada módulo para operar contra el servidor central, validando en línea la versión utilizada.

Por otra parte, los cambios al Core Bancario, incluyen actualizaciones a nivel de Back-End (servidor central) y Front-End (equipo cliente del usuario final), por lo tanto, el proceso de despliegue de software se vuelve crítico para la continuidad del negocio, por el alto impacto en caso de cambio o error (aproximadamente 3.030 equipos clientes a nivel nacional).

En caso de errores en la distribución de software y/o el aplicativo, la continuidad del negocio, se ve altamente impactada con una paralización total, la única solución, al identificarse el error a nivel de Front End, exige distribuciones de software inmediatas y altamente eficaces y eficientes, o planes de Roll-Back (regreso a la situación original) debidamente documentados y probados, de tal manera que el tiempo de retorno a la normalidad del sistema, sea el mínimo posible.

Para cubrir estas necesidades es importante que el proceso de Release, dentro del gobierno de TI de la Gerencia Nacional de Sistemas, tenga una interacción con todas las áreas de tal forma que garanticen y apoyen esta necesidad de eficacia y eficiencia; es por ello que se determina la existencia de otros subprocesos dentro del proceso de release que son algo más que proteger fuentes.

Definir políticas, diseñar y configurar el proceso de despliegue, planificar el despliegue, compilar el nuevo ejecutable en ambiente de pre-producción, establecer una logística adecuada para la distribución y ejecutar en sí la distribución; implica realizar un levantamiento adecuado de cada subproceso, aprobarlo, difundirlo y ejercer sobre cada uno de ellos periódicamente un plan de mejora continua. Dentro de este contexto, control de fuentes se vuelve un subproceso más de Release y sobre él se introducen nuevos y mejores controles.

Producto de la inclusión de estos nuevos subprocesos, aparecen los niveles de autorización y responsabilidad de los cargos directivos dueños de este proceso de Release, así lo definirán las políticas propuestas.

La generación de nuevos subprocesos, obliga a que existan nuevas actividades, las mismas que deberán ser llevadas a cabo por personal técnico con un perfil adecuado de experiencia y conocimiento, es

inminente la inclusión de un administrador para el proceso, y el apoyo de automatización del mismo a través de una herramienta adecuada y completa, considerando una plataforma tecnológica solvente, y que se definan sobre ella, adecuados planes de continuidad y de recuperación ante desastres.

De lo anteriormente expuesto se desprende que el proceso actual de Release, debe evolucionar, de simplemente controlar fuentes a implementar y controlar la calidad del software instalado en el entorno de producción del Banco Nacional de Fomento, para ello deberá implementar los controles adecuados y a través de indicadores de gestión medir la efectividad y el mejoramiento de todo el proceso.

CAPITULO II

2.1 RELEASE MANAGEMENT

Las áreas de la Gerencia Nacional de Sistemas continúan luchando con la incorporación de aplicaciones, infraestructura y cambios operacionales en los ambientes de producción de TI. De la misma manera buscan mantener/aumentar el cambio-administración de los niveles de servicio formalizando y adoptando los procesos que permiten aumentar la aceptación del cambio en el ambiente de producción.

Tan pronto como la Administración de Control de Cambios aprueba un cambio, recae sobre el proceso de Administración de Release ejecutar el cambio en el ambiente apropiado.

La administración de Release realiza control de las versiones del software, hardware y de otros componentes de infraestructura del ambiente de desarrollo al ambiente de producción.

Administra a su vez la Librería de Software Definitivo (Definitive Software Library- **DSL**), en la cual se almacena la copia maestra de los elementos de configuración (Configuration Items **CI´s**). La Librería Definitiva de Hardware (Definitive Hardware Storage **DHS**) es un área de almacenamiento físico con todas las partes autorizadas de Hardware. Los detalles de estos componentes, sus estructuras y contenidos respectivos se deben registrar en la Configuration Management Database - **CMDB**.

Todos los productos que están en las DSL y DHS necesitan ser verificados como libres de daños y virus antes de ser almacenados.

El foco de la Administración de Release es la protección del ambiente de producción y de sus servicios con el uso de procedimientos formales y chequeos.

La Administración de Release trabaja en conjunto con los procesos de la Administración de Cambios y la Administración de Configuración, para asegurarse de que la CMDB compartida, se actualiza de acuerdo a los cambios implementados a través de los nuevos release, y que el contenido de estos release está almacenado en la DSL. Las especificaciones del hardware, las instrucciones de ensamblaje y las configuraciones de red también se almacenan en la CMDB.

Los componentes principales que se deben controlar son:

- Aplicaciones desarrolladas por la institución
- Desarrollos externos de software
- Software utilitario (para uso general)
- Software de sistema proporcionado por proveedores.
- Instrucciones y documentación, incluyendo manuales de usuario

Todos los entregables necesitan ser administrados eficientemente, desde el desarrollo o compra, hasta la personalización y configuración, así como su operación y afinamiento en el ambiente de producción.

Descritas las relaciones entre las áreas operacionales y los componentes de la administración de release, es necesario expresar las expectativas de servicio y las responsabilidades de soporte entre las partes involucradas a través de un Acuerdo de Operación de Servicio (OLA).

Es importante que las condiciones de calidad afecten a todos los elementos implicados en el servicio de release llegando a establecer Acuerdos de Niveles de Servicio (SLA) en los que se especifique el servicio de TI, los objetivos de nivel de servicio y las responsabilidades del proveedor de servicios de TI y del cliente.

Algunas definiciones son necesarias, para poder comprender la Administración de Release:

- **Release:** este término hace referencia a toda la descripción de Cambios autorizados para los servicios TI. Un release es definido por un conjunto de Control de Cambio (Request for Change **RFC's)** que implementa. El lanzamiento típicamente consistirá en la corrección de un número de problemas y de actualizaciones. El release consiste en nuevos cambios o software modificado, requerido para cualquier hardware nuevo o modificado, necesario para implantar el cambio aprobado. Los Release se dividen:
    - Release de software mayor y actualizaciones de hardware, normalmente conteniendo grandes áreas de nueva funcionalidad, algunas de las cuales pueden hacer modificaciones que intervienen sobre los problemas redundantes.
    - Release de software menor y actualizaciones de hardware, normalmente contiene las actualizaciones y modificaciones pequeñas, algunos de los cuales se pudieron haber colocado ya, como un cambio de emergencia.
    - Software de emergencia y modificaciones de hardware, conteniendo normalmente las correcciones a un pequeño número de Problemas Conocidos.
- **Tipos de Release:**
    - Release Full, la ventaja principal de los release full es que todos los componentes del release están desarrollados, probados, distribuidos e implantados juntos.
    - Release Delta: Un delta, o un release parcial, es uno que incluye solamente los CI's dentro de la unidad del release que han cambiado o son nuevos, con respecto al Release Full o Delta anterior.

      Puede haber ocasiones en que el Release Full no sea justificable; en esos casos lo más apropiado es un Release Delta. Se recomienda, que para este tipo de release se analice caso por caso.
    - Release empaquetado: Para proporcionar estabilidad por períodos más largos al ambiente en producción, reduciendo la frecuencia de los release. Se recomienda cuando sea apropiado y donde la gran cantidad de cambios se pueda manejar con confianza sin problemas. Los release individuales, unidades completas, release delta o ambos, se agrupan juntos bajo la forma de "Release empaquetado".
- **Librería Definitiva de Software (DSL)**: Este término es usado para describir un componente seguro en el cual, las versiones autorizadas definitivas de todo el software de los CI's se almacenan y se protegen. Esta es un área de almacenamiento, que puede en realidad consistir de una o más librerías de software o áreas de almacenamiento, que deben estar aparte del desarrollo, prueba o áreas de producción. Contiene las copias maestras de todo el software controlado en una organización.
- **Almacenamiento Definitivo de Hardware (DHS)**: En esta área se almacena de forma segura las partes definitivas del hardware. Éstos son las partes de los componentes y los conjuntos de repuestos que se mantienen en el mismo nivel que los sistemas en el ambiente de producción. Los detalles de estos componentes, sus estructuras y contenido respectivos se deben registrar en la CMDB.
- **Base de datos de Administración de la Configuración (CMDB)**: En las infraestructuras grandes y complejas de hoy en día, para administrar las configuraciones se requiere el uso de instrumentos de apoyo, tales como una base de datos para la administración de la configuración (CMDB). Las bibliotecas físicas y electrónicas, también son necesarias junto con la CMDB, para contar con copias

definitivas del software y de la documentación. La CMDB debe estar basada en la tecnología de base de datos que proporcione posibilidades de consultas flexibles y de gran alcance.

La CMDB debe mantener las relaciones entre todos los componentes de un sistema, incluyendo: Incidencias, Problemas, Errores Conocidos, Cambios y Release. Debe contener también información sobre: datos corporativos, empleados, proveedores, localizaciones y unidades de negocio. La CMDB es actualizada y referida, a través del proceso de Administración de Release en forma concurrente con las actualizaciones a la DSL. Debe contener la siguiente información como soporte al proceso de Administración de Release:

- Definiciones de los release previstos, incluyendo el hardware y el software de los CI's, junto con una referencia a los requerimientos originales de cambio.
- Registro de los CI's impactados por release planeados y pasados, cubriendo el HW & SW.
- Información sobre los objetivos de los componentes del release (por ejemplo: la localización física del hardware y los servidores receptores de los cambios de software).

- **Planes de roll-back**: Un plan de roll-back debe contener un documento con las acciones a tomar para restaurar el servicio una vez que el roll-out de un release haya fallado, ya sea parcial o totalmente. La generación de los planes de roll-back para cada cambio es responsabilidad de la Administración del Cambio, pero la Administración de Release, tiene que asegurarse que los planes del roll-back debidamente probados y certificados, funcionen para cada release liberado.
- **OLA (Acuerdo de Nivel Operacional)**: Se trata de un acuerdo entre un proveedor de servicios de TI y otra parte de la misma organización.
  - Un Acuerdo de Nivel Operacional (Operational Level Agreement, OLA) brinda apoyo en la prestación de servicios al cliente por parte de proveedor de servicios de TI.
  - El OLA define los bienes y servicios que se proveen y las responsabilidades de ambas partes.
  - Por ejemplo, podría haber un Acuerdo de Nivel Operacional entre el proveedor de servicios de TI y un departamento de compras para la obtención de equipos en determinado momento, o entre el Service Desk y algún grupo de apoyo para proveer soluciones a Incidentes en ocasiones acordadas previamente.
- **SLA** (**Acuerdo de Nivel de Servicio)**: Es un acuerdo entre un proveedor de servicios de TI y un cliente.
  - El Acuerdo de Nivel de Servicio (Service Level Agreement, SLA) define los términos y parámetros sobre los que se adquiere el compromiso en el servicio.
  - Debe indicar el modo de cálculo (métrica e intervalos) del índice de cumplimiento, cuál es el objetivo pactado; indicando el valor o márgenes de referencia, cuáles las posibles compensaciones por incumplimiento y por último las exclusiones o limitaciones en dichos cálculos.
  - Un SLA mínimamente debe contemplar los siguientes aspectos:
    - Definición: Descripción de las características del servicio.
    - Provisión: Tiempo transcurrido desde la firma del pedido o contrato hasta la entrega o puesta en marcha del servicio.
    - Disponibilidad: Se trata del aspecto fundamental en el Acuerdo de Nivel de Servicio y es necesario que contemple la plataforma tecnológica (sistemas), las comunicaciones y el soporte técnico.
    - Atención al cliente: Describe el método a seguir por el cliente frente a incidencias o consultas sobre el servicio. Es vital un soporte técnico cualificado y eficiente para asegurar el nivel de servicio adecuado y con atención 24*7.
    - Tiempo de respuesta: Compromiso de tiempo mínimo en cuanto a resolución de incidencias.

- Mantenimiento: Condiciones sobre el mantenimiento, la reparación de equipos y las posibles intervenciones que afecten al servicio de forma programada.
- Penalizaciones: Garantías y compensaciones relativas al incumplimiento del nivel de servicio comprometido.

Tomado de: http://wiki.es.it-processmaps.com/index.php/Glosario_ITIL

hhtp://www.acens.com

Documento de Gestión de Tecnología de Ia Información y Seguridades. Procesos de Administración de TI de la Gerencia Nacional de Sistemas del BNF-2009.

2.2 NORMAS Y METODOLOGIAS APLICABLES PARA EL PROCESO DE RELEASE

2.2.1 ITIL

IT Infrastructure Library o ITIL® con 20 años de edad, en su tercera versión actualmente es el marco más ampliamente adoptado para la Gestión de Servicios en el mundo.

A principios de los 80's, la tecnología informática evolucionó pasando de una infraestructura centralizada a sistemas informáticos distribuidos y con recursos geográficamente dispersos. Si bien la capacidad de distribuir la tecnología ofrece más flexibilidad a las organizaciones, el efecto secundario es coordinar en forma eficaz y eficiente la entrega de tecnología de apoyo. La orientación ITIL ha sido un mecanismo exitoso para lograr la coherencia de unidad, eficiencia y excelencia en la gestión de servicios de TI para el negocio.

Dado que ITIL (Figura 2.1) es un enfoque de gestión de servicios de TI, la noción de servicio debe ser discutida. Un servicio es algo que proporciona valor a los clientes. Servicios que los clientes pueden utilizar directamente o consumen para generar otros servicios son conocidos como "empresas" de servicios.

Una infraestructura de servicio realiza su trabajo en segundo plano, de tal manera que el negocio no interactúa directamente con él, pero son los servicios de tecnología necesarios como parte de la cadena de valor global de la Institución.

Figura 2.1 Enfoque ITIL
Tomado de:
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Tradicionalmente se ha centrado en la "infraestructura" la gestión de los servicios de los silos de la tecnología. La Gestión de Servicios TI en ITIL sugiere un enfoque más holístico a la gestión de los servicios de extremo a extremo. Administrar el servicio de negocio de una manera completa junto con sus componentes, asegura que estamos considerando todos los aspectos de un servicio (y no sólo la tecnología de los silos individuales) para asegurar que estamos cumpliendo la funcionalidad requerida y los niveles de servicio al cliente del negocio.

Aunque las tecnologías de hoy nos permiten proporcionar sólidas capacidades y ofrecer una flexibilidad significativa, esto es muy complejo. El alcance global disponible para las empresas a través de la Internet ofrece enormes oportunidades de negocio, mientras que puede presentar problemas adicionales con respecto a la confidencialidad, la integridad y la disponibilidad tanto de nuestros servicios como de nuestros datos. Además, TI debe trabajar tan eficientemente como le sea posible para cumplir o superar las expectativas de calidad del servicio que tiene el negocio, por lo tanto en un proceso de mejora continua, deberá garantizar con eficiencia y efectividad la capacidad no solo de entregar servicio sino de mejorarlo.

2.2.2 ISO 27002

La norma ISO 27002 es un estándar internacional de buenas prácticas sobre la gestión de Seguridad de la Información, cuyo objetivo es crear una cultura organizacional sobre el manejo e implementación de la seguridad a través de controles (políticas, procesos, procedimientos) para minimizar el impacto de las diferentes amenazas a las que está expuesta la información.

Esta norma describe los objetivos de control (Figura 2.2) y controles recomendables, además de proporcionar las pautas para la implementación basada en sugerencias que deben ser consideradas por una organización para poder construir un sistema comprensivo de gestión de Seguridad de la Información (Sistema de Gestión de Seguridad de la Información, SGSI) reconocido internacionalmente.

Figura 2.2 Objetivos de control de la norma ISO 27002
Tomado de: iSEC INFORMATION SECURITY INC. (2010) Curso de Análisis de Riesgo en Seguridad de la Información

El SGSI ayuda a establecer políticas y procedimientos en relación a los objetivos del negocio con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la Institución ha decidido asumir.

Con un SGSI (Figura 2.3), la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una metodología sistemática, definida, documentada y conocida por todos que se revisa y mejora constantemente.

Figura 2.3 SGSI

Tomado de: iSEC INFORMATION SECURITY INC. (2010) Curso de Análisis de Riesgo en Seguridad de la Información

Con el apoyo de la Gerencia Nacional de Riesgos, la Unidad de Seguridad de la Información ha adoptado este estándar como referencia para desarrollar e implementar un SGSI para el Banco Nacional de Fomento considerando los objetivos de control dentro de cada dominio de seguridad como una entidad conceptual definida por parámetros de seguridad físicos y lógicos (los parámetros definen el espacio de control). Los dominios de seguridad sirven como la base para la evaluación del riesgo.

La norma aplicada, sugiere una evaluación metódica del riesgo, dejando el tipo y el nivel de evaluación abierto a la interpretación que la institución escoge llevar a cabo. El resultado deseado es una manera de cuantificar el riesgo para poder seleccionar los controles apropiados y pertinentes requeridos para mitigar el riesgo.

La norma requiere de un acercamiento sistemático para la evaluación de riesgo, incluyendo el desarrollo de un plan de tratamiento de riesgo para:

- Relacionar el riesgo a la confidencialidad, integridad y disponibilidad.
- Establecer objetivos para reducir el riesgo a un nivel aceptable.
- Determinar el criterio para aceptar el riesgo; y
- Evaluar las opciones de tratamiento de los riesgos.

La norma define a la información como un activo que tiene valor en una organización; y como todos los activos, es imperativo mantener su valor para el éxito de una organización.

2.3 RECURSOS NECESARIOS PARA IMPLEMENTAR EL PROCESO DE RELEASE

Dentro de los marcos de referencia descritos anteriormente y considerando que en todo sistema de información se requieren insumos gravitantes como Procesos, Recurso Humano, Infraestructura Tecnológica, etc. con el propósito de garantizar el cumplimiento de objetivos de estabilidad, eficiencia, eficacia y de continuidad del negocio, a continuación se describen cada uno de estos elementos.

2.3.1 PROCESOS

El proceso de Release Management, requiere de un análisis profundo para identificar sus subprocesos, sus responsables, sus entradas y salidas, por ello en el Capítulo III se los describe detalladamente para dejar claro sus objetivos, roles y responsabilidades de sus actores, criterios de entrada y entradas que los habilitan, pasos o actividades del procedimiento, diagrama SIPOC, diagrama de flujo, criterios de salida y salidas, métricas del subproceso entre otros.

2.3.2 RECURSO HUMANO

Se propone que la Gerencia Nacional de Sistemas establezca dentro de la estructura organizacional, la estructura de puestos que se requieren (basados en la normativa y formato emitido por el Ministerio de Relaciones Laborales), sus atribuciones, responsabilidades, así como el perfil técnico necesario para cubrir cada uno de los subprocesos del proceso de Release.

Los puestos propuestos son: Administrador de Despliegue y Versionamiento, y Especialista de Despliegue y Versionamiento. En los Anexos 2.1 y 2.2 se describen las fichas técnicas de cada uno, conformadas de las siguientes secciones:

1. Datos de identificación
2. Misión del puesto
3. Actividades del puesto
4. Interfaz del puesto
5. Conocimientos requeridos
6. Instrucción formal requerida
7. Experiencia laboral requerida
8. Destrezas técnicas requeridas
9. Destrezas / habilidades conductuales
10. Requerimientos de selección y capacitación
11. Valoración del puesto

2.3.3 INFRAESTRUCTURA TECNOLOGICA

2.3.3.1 ARQUITECTURA DE LA SOLUCION

La herramienta que permita automatizar el proceso de distribución de software, de preferencia deberá tener una arquitectura cliente servidor (Figura 2.4) en la que se identifique:

1. Un servidor central con un sistema de almacenamiento de datos en una plataforma de base de datos relacional, no propietaria de la solución y que funcione en dos capas, lo cual

garantice presentar al servidor espacios de almacenamiento externos. La referencia de las características mínimas requeridas constan en el Anexo 2.3.

2. Un servidor de escalamiento ubicado en cada localidad que permita optimizar el uso del medio de transmisión de datos, de tal manera que la red WAN no se vea congestionada. La referencia de las características mínimas requeridas constan en el Anexo 2.4.
3. Una consola de administración vía browser que permita la conexión al servidor central de la herramienta a través de una dirección IP y un puerto. La referencia de las características mínimas requeridas constan en el Anexo 2.5.
4. Equipos de escritorio con características mínimas de software y hardware. La referencia de las características mínimas requeridas constan en el Anexo 2.6.
5. Agentes de la herramienta, residentes en cada equipo de escritorio que reporten la información necesaria al servidor central de la herramienta.

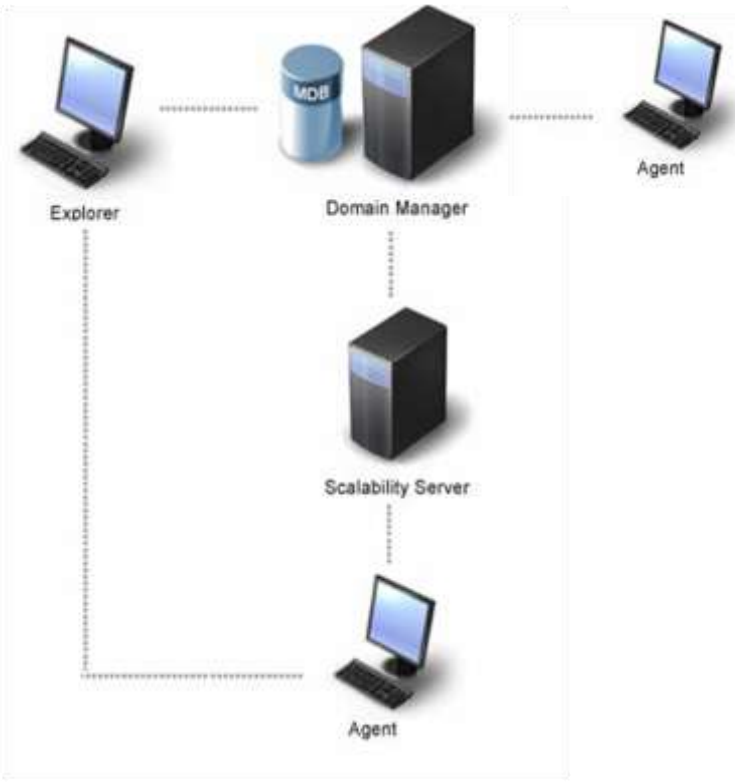


Figura 2.4 Arquitectura de la solución
Tomado de: Proyecto de implementación de ITCM en Banco Nacional de Fomento.

2.3.3.2 ESPECIFICACIONES DE FUNCIONALIDAD

Los requerimientos de funcionalidad para Administración de Equipos de Escritorio son:

- Uso de una única Base de Datos.
- Diseño dimensionado para soportar la infraestructura actual y proyectada.
- Generación de datos Inteligentes basados en el hardware y software de los equipos de escritorio bajo la responsabilidad del especialista de configuración.

- Distribución de parches de seguridad a todos los equipos de escritorio del entorno IT, que reduzca el esfuerzo y participación del personal del área de Reléase en gestión de producción.

- Las configuraciones de los productos de la herramienta a implementarse debe realizarse de tal manera que optimicen el ancho de banda y la carga de trabajo.

- Integración con otras suites o herramientas existentes

2.3.3.3 ESQUEMA DE RESPALDOS

Al convertirse release management en un proceso crítico para el negocio, se debe asegurar que todos sus componentes (DSL, CMDB, Infraestructura del servicio, etc.), se incluyan dentro del esquema general de respaldo adoptado por la Gerencia Nacional de Sistemas. Esto implica que la política general de respaldos contemple:

1. Especificación de los medios de almacenamiento disponibles, mecanismos de mantenimiento de los mismos y manejo de planes de caducidad.
2. La asignación de niveles de responsabilidad por la custodia e integridad de los respaldos.
3. La adecuada planificación en tiempos de ejecución que garantice que la frecuencia y los periodos de retención solicitados por el dueño de la información se cumplan.
4. Proceso aprobados para la eliminación de respaldos que concuerden con el periodo de retención solicitado por el dueño de la información.
5. Procedimientos de restauración de datos que ejecutados periódicamente y certificados por el dueño de la información, garanticen la integridad de la información almacenada en los medios de respaldo.
6. Procedimientos de recuperación de datos que garanticen la confidencialidad y disponibilidad de la información.
7. Procedimientos de custodia en el data center y fuera del data center (out site) que eliminen la posibilidad de pérdida total de la información respaldada.
8. Procedimientos de auditoría al proceso de respaldo adoptado que permitan mantener una línea de supervisión y cumplimiento evidenciada tanto interna como externamente.

2.4 VENTAJAS DE IMPLEMENTAR EL PROCESO DE RELEASE

GESTION DE RELEASE MANAGEMENT			
Con procesos definidos		**Sin procesos definidos**	
1	Reconocimiento e interacción de las áreas de TI que apoyan el proceso	**1**	Uso de información sin previa validación
2	Gestoría y control por cada subproceso identificado	**2**	Mal uso de información confidencial
3	Fácil identificación y actualización de proveedores, entradas, procesos, salidas y clientes de cada subproceso	**3**	Inexistencia o desconocimiento de políticas
4	Análisis e identificación de los riesgos asociados a cada subproceso	**4**	Olvidos
5	Definición de políticas y estándares aplicables al proceso	**5**	Inclusión errónea de datos críticos

6	Selección del Recurso Humano con el perfil adecuado	**6**	Falta o llenado incompleto de documentos con especificaciones técnicas
7	Garantiza la estandarización de versiones tanto a nivel de Front-End como de Back-End	**7**	Interpretación errónea de información
8	Garantiza el mínimo impacto en la continuidad del servicio entregado	**8**	Imposibilidad de garantizar continuidad en el servicio
9	Se logra identificar puntos de fallo para establecer adecuados planes de contingencia que garanticen tiempos aceptables de retorno a la normalidad	**9**	Procesos de análisis de riesgo incompletos o errados
10	Se pueden establecer métricas que indiquen el estado del servicio entregado para adoptar planes de mejora continua	**10**	Recurso Humano sin el perfil técnico adecuado
11	Definición de niveles de autorización y responsabilidad	**11**	Envío extemporáneo de información o documentos
12	Facilita la automatización del proceso al adoptar estándares en los cuales se basan la mayoría de herramientas en el mercado		

CAPITULO III

3.1 DEFINICION DEL MAPA DE PROCESOS DE TI

El mapa de procesos, es un inventario gráfico de los procesos de una organización. Para elaborar el mapa de procesos se ha determinado una metodología sencilla que parte de los objetivos principales definidos por la Gerencia Nacional de Sistemas y fundamentado en las mejores prácticas.

El Modelo de Gestión de la Gerencia Nacional de Sistemas del Banco Nacional de Fomento, debe estar diseñado y desarrollado para cumplir con los siguientes objetivos principales:

- Asegurar la alineación de la tecnología con los objetivos y estrategias del Banco Nacional de Fomento, con la entrega continua y oportuna de los Servicios TI requeridos por la Institución.
- Organizar las necesidades de alineación de objetivos y entrega de servicios en función de procesos de negocio para su asignación a unidades organizativas existentes o requeridas.
- Definir los roles y responsabilidades de los integrantes de las unidades organizativas en función de los procesos a ser ejecutados.
- Asegurar el valor agregado de la tecnología como componente estratégico del BNF en la definición y logro de los objetivos institucionales.
- Definir la relación fundamental entre los procesos, la tecnología y el recurso humano.

En la Figura 3.1, se ilustra el Mapa de Procesos de la Gerencia Nacional de Sistemas, lo cual permite identificar el proceso de Release dentro de este contexto.

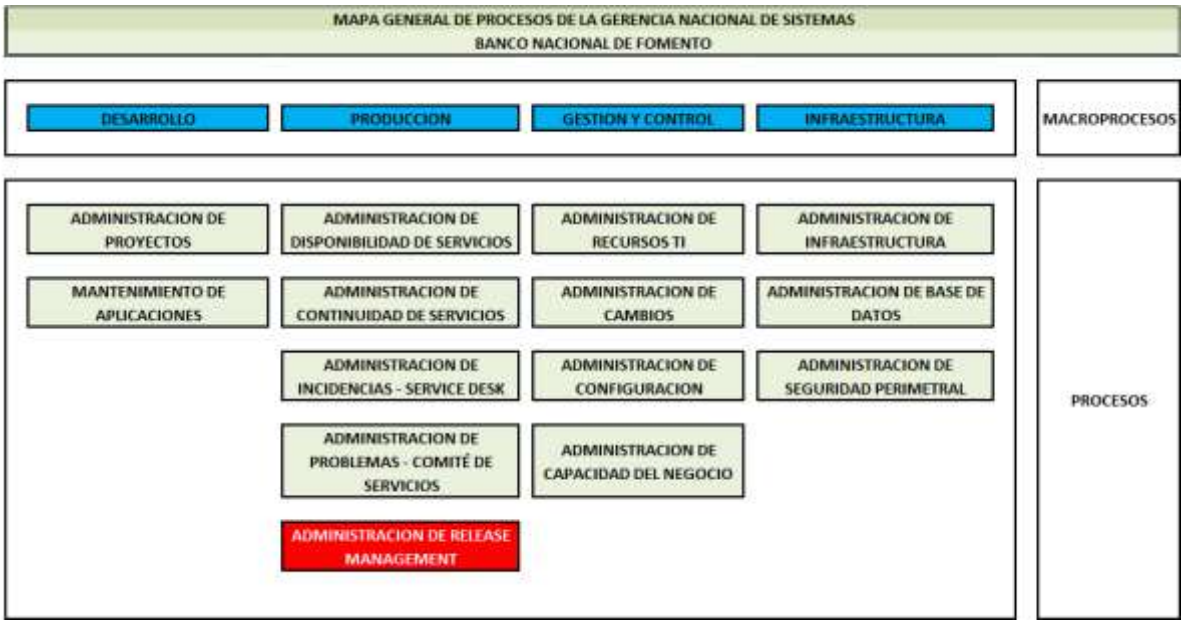


Figura 3.1 – Mapa de Procesos de la Gerencia Nacional de Sistemas

3.2 PROCESO DE RELEASE

3.2.1 ITIL EN EL GOBIERNO DE TI

La Gerencia Nacional de Sistemas dentro de su enfoque de gobierno de TI, define su estrategia gerencial en cinco ejes fundamentales, tal como lo resume la Figura 3.2:

Figura 3.2 Ejes de la estrategia gerencial de la Gerencia Nacional de Sistemas del Banco Nacional de Fomento

1. Alineamiento Estratégico, garantizando el vínculo entre los planes del Banco Nacional de Fomento y la infraestructura tecnológica que los viabiliza.
2. Entrega de Valor, asegurando que la Gerencia Nacional de Sistemas, genere los beneficios comprometidos en la estrategia, optimizando costos y brindando un valor intrínseco.
3. Administración de Riesgos, materializando las políticas definidas por la Gerencia Nacional de Riesgos.
4. Administración de Recursos, ejecutando inversiones óptimas y administrando adecuadamente los recursos críticos: aplicaciones, información, infraestructura y personas.
5. Medición del desempeño, monitoreando el estado de los proyectos, el desempeño de los procesos, y la entrega del servicio.

La calidad en la entrega y definición del servicio tecnológico enfocado en los usuarios y clientes que se favorecen de él, la definición adecuada de los procesos que soportan el servicio, y su correcta administración, son las razones predominantes que hacen que la Gerencia Nacional de Sistemas, adopte ITIL. El camino que se siguió para implementar ITIL a través de su enfoque sistemático para servicios de tecnología con calidad, abarcó tres aspectos determinantes:

a. Implementar las funciones ITIL juntas para que la adopción sea racional.
b. Integrar y automatizar las mejores prácticas empleando soluciones basadas en software.
c. Y finalmente, sacar partido permanentemente a una base de datos de gestión de configuración (CMBD) para incrementar la distribución y la precisión de la información en la Gerencia Nacional de Sistemas.

3.2.2 INTERACCION DEL PROCESO DE RELEASE CON LAS AREAS DE TI

ITIL, nace como un código de buenas prácticas dirigidas a alcanzar una buena gestión del servicio mediante un enfoque sistemático del servicio TI centrado en los procesos y procedimientos, y el establecimiento de estrategias para la gestión operativa de la infraestructura TI.

Considerando lo complejo de enmarcar la entrega del servicio dentro de lo que dicta la metodología, pues si bien es cierto ITIL dice que, pero no dice cómo, en el sector público financiero al que pertenece el Banco Nacional de Fomento, resulta complicado, aunque no imposible, estructurar los procesos del Soporte y la Entrega del Servicio en una estructura organizacional piramidal; sin embargo, la Gerencia Nacional de Sistemas lo ha logrado, delegando equitativamente las gestiones a las cuatro áreas que la nueva estructura ha aprobado que existan, delineando claramente la responsabilidad del Director en los procesos encomendados. Pese a ello, se tiene la claridad del proceso como para gestionarlo en forma lineal, atravesando las direcciones en todas sus etapas (análisis, desarrollo, certificación, implementación y seguimiento post-producción).

Si bien la estructura actual, no es apropiada para la administración óptima de todas las gestiones, pues existen direcciones con un nivel alto de responsabilidad, tanto en la ejecución como en el control de los procesos delegados, se debió equilibrar esta necesidad, contra la obligatoriedad de no engrosar la estructura organizacional (crear direcciones por cada gestión), este es el principal reto que se enfrenta en la implementación de ITIL en el sector público, dependiendo de la actividad a la que este orientada la institución pública, es evidente que en el sector financiero, todas las gestiones aplican y deben ser tomadas en cuenta.

A continuación, en la Tabla 3.1, de acuerdo a las áreas que ITIL cubre, que son dos: El Soporte al Servicio, y, la Provisión del Servicio; se detallan los procesos que se deben gestionar en cada área y la dirección que los lidera dentro de la estructura organizacional de la Gerencia Nacional de Sistemas.

Areas de ITIL	Procesos	Direcciones de la Gerencia Nacional de Sistemas
Provisión del Servicio: Se ocupa de los servicios ofrecidos en sí mismos. En particular de los niveles de servicio, su disponibilidad, su continuidad, su viabilidad financiera, la capacidad necesaria de la infraestructura TI y los niveles de seguridad requeridos	Gestión de Niveles de Servicios	Dirección de Producción
	Gestión de la Disponibilidad	Dirección de Producción
	Gestión de la Continuidad	Dirección de Producción
	Gestión Financiera	Dirección de Gestión y Control
	Gestión de la Capacidad	Dirección de Gestión y Control
	Gestión de la Seguridad	Dirección de Infraestructura
Soporte al Servicio: Se preocupa de todos los aspectos que garanticen la continuidad, disponibilidad y calidad del servicio prestado al usuario.	Gestión de Incidentes	Dirección de Producción
	Gestión de Problemas	Dirección de Producción
	Gestión de Configuraciones	Dirección de Gestión y Control
	Gestión de Cambios	Dirección de Gestión y Control
	Gestión de Versiones	Dirección de Producción

Tabla 3.1 Detalle de las gestiones de Provisión y Entrega de servicio en ITIL para las direcciones de la Gerencia Nacional de Sistemas del Banco Nacional de Fomento

La Administración de Release (Gestión de Versiones), se encuentra directamente ligada con la Administración de Cambios (Gestión de Cambios), asegurando (Figura 3.3) que, toda la información que tiene que ver con las versiones en producción, se encuentra correctamente versionada, resguardada y disponible dentro de los parámetros de autorización establecidos al interior de la Gerencia Nacional de Sistemas.

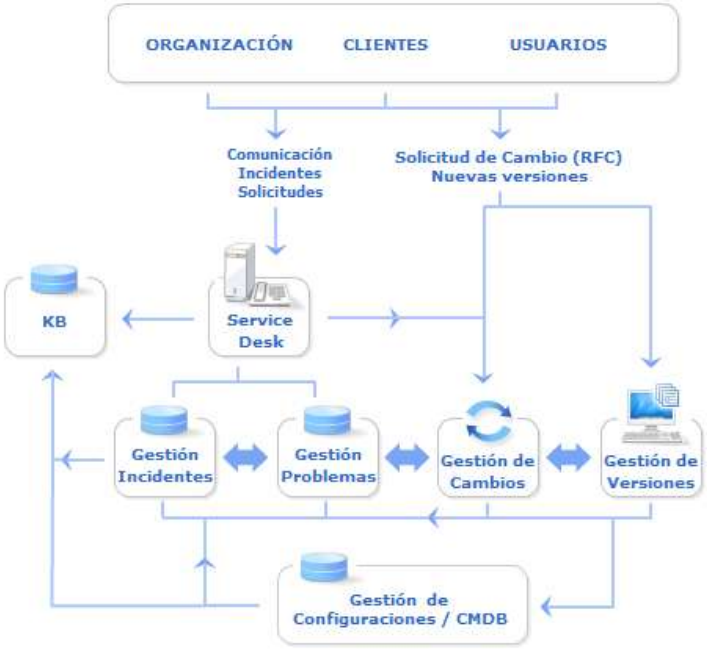


Figura 3.3 Interacción de las gestiones de Servicio en ITIL
Tomado de:
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/soporte_al_servicio.php

3.3 DESCRIPCION DE SUBPROCESOS DE RELEASE

Es importante tener definido un proceso de administración de Release dado que el cambio en un proyecto de software es inevitable. La evolución de alguna herramienta implica que se creen nuevas versiones de ésta, y surge la necesidad de tener definido con claridad, cuál es el proceso que se debe seguir para administrar las versiones que se producen.

También se especifica este proceso para conocer cuáles son los pasos que se deben seguir para poner en producción una nueva versión de una herramienta, sin que se desestabilice el ambiente que se encuentra en producción.

Es fundamental entonces, coordinar todas las actividades involucradas en el proceso de Administración de Release, para hacer disponible una nueva versión, sin que haya ningún inconveniente en la integración con el ambiente en producción. En la figura 3.4 se ilustra la Interacción de los subprocesos de Release en un proceso de Control de Cambios.

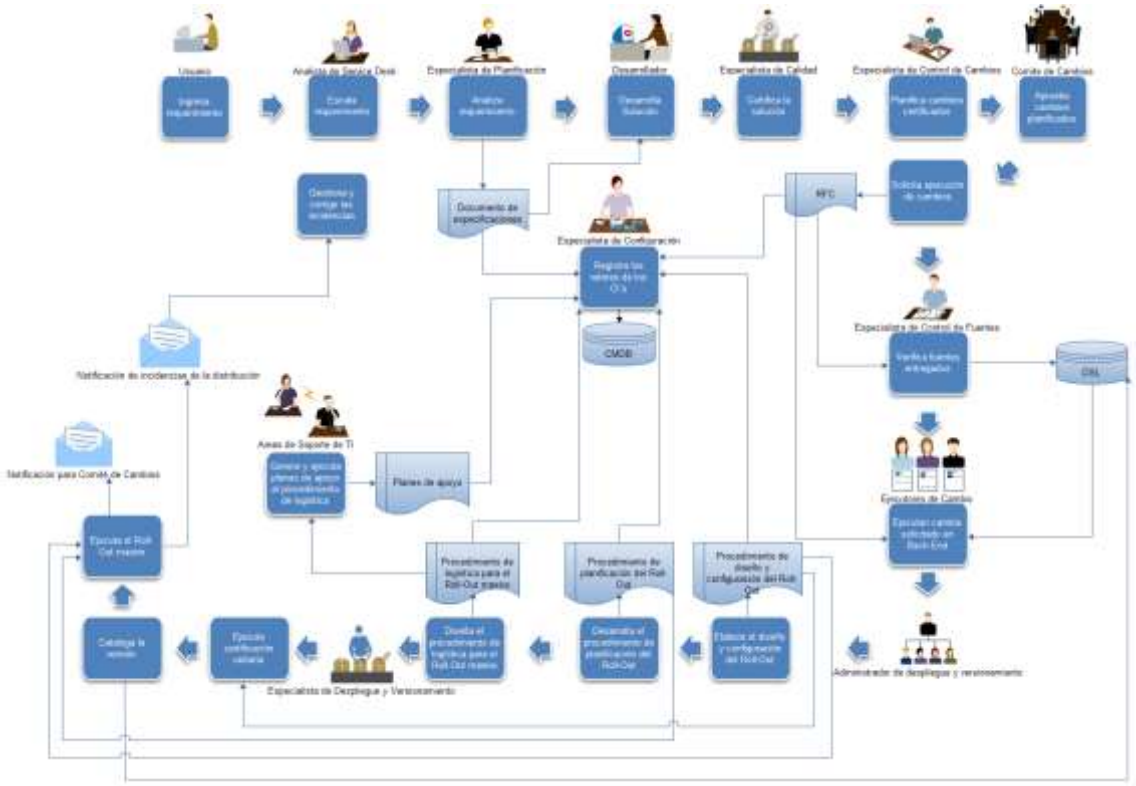


Figura 3.4 Interacción de los subprocesos de Release en un proceso de Control de Cambios

La Gerencia Nacional de Sistemas a través de la Dirección de Producción ha establecido los siguientes subprocesos que integran el Proceso de Administración de Release:

1. Subproceso de Definición de Políticas de Release.
2. Subproceso de Control de Fuentes.
3. Subproceso de Diseño y Configuración del Roll-Out
4. Subproceso de Planificación del Roll-Out
5. Subproceso de Certificación unitaria previa el Roll-Out masivo.
6. Subproceso de Logística para el Roll-Out masivo.
7. Subproceso de Ejecución del Roll-Out masivo.

Cada uno de los cuales se especificará a nivel de detalle en las plantillas definidas, a lo cual se suma el diagrama de flujo del proceso, en el que se identifican los actores del mismo.

3.3.1 SUBPROCESO DE DEFINICION DE POLITICAS DE RELEASE

Definición de Procesos

Proceso:	AR – DPR: Administración de Release – **Definición de Políticas de Release.**	**Cod.Doc**	AR-DPR	
Responsable:	Director de Producción	**Versión:**	1.3	
Mantenimiento:	Director de Producción Administrador de Despliegue y Versionamiento	**Estado:**	Borrador	
			Publicado	X

Descripción:	Establecer políticas que aseguren el control e implantación de las diferentes versiones de software desde los ambientes de desarrollo y calidad a Producción.

Alcance:	Definir las políticas de Release, contempla los siguientes procedimientos: • Las políticas iniciales, mantenimiento e inclusión de nuevas políticas están a cargo de la Dirección de Producción • La aprobación, de las políticas están a cargo de la Gerencia Nacional de Sistemas • La inclusión y difusión de las políticas en el Manual del Sistema de gestión de Seguridad de la Información (MSGSI) está a cargo del Oficial de Seguridad de la Información • El conocimiento de la actualización del MSGSI con las nuevas políticas, está a cargo del Secretario General • La inclusión o actualización de las políticas en la CMDB de la Gerencia Nacional de Sistemas, están a cargo del Especialista de Configuración

Guías de Personalización:	No aplica

Documentos de Referencia:	• Manual del Sistema de Gestión de Seguridad de la Información • Políticas y reglamentos del Banco Nacional de Fomento • Políticas generales de la Gerencia Nacional de Sistemas • Normativa para Gestión de Riesgo Operativo • Normas de Control Interno de entidades del sector público • Fundamentos de ITIL • Fundamentos COBIT • Dominios y Controles ISO 27002

Abreviaciones y	En este documento se usan las siguientes abreviaciones y acrónimos:

Acrónimos:	• AR: Administración de Release • DPR : Definición de Políticas de Release • CMDB: Configuration Management Database • Roll-Out: Despliegue • Roll-back: Vuelta atrás de un despliegue • MSGSI: Manual del Sistema de Seguridad de la Información

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	12/06/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.2	14/06/2010	Lenni Carrión Julio Viteri	Todo	M	Primera revisión
1.3	16/07/2010	Lenni Carrión Julio Viteri	Todo	A	Diagramas SIPOC *(Anexo 3.1)*

A. Diagrama de Flujo del Proceso

- *Anexo 3.2*

B. Resumen del Proceso

Criterios de Entrada:	**Criterios de Salida:**
• Entender las necesidades de definir políticas, adoptar estándares y describir normas, directrices y procedimientos que apoyen el proceso de Release	• Normar de manera eficaz y eficiente el proceso de Release en todos sus ámbitos
Entradas:	**Salidas:**
• Manual del Sistema de Gestión de Seguridad de la Información • Políticas y reglamentos del Banco Nacional de Fomento • Políticas generales de la Gerencia Nacional de Sistemas • Normativa para Gestión de Riesgo Operativo • Normas de Control Interno de entidades del sector público • Fundamentos de ITIL • Fundamentos COBIT	• Políticas Generales de Release • Estándar de versionamiento • Norma para el control de fuentes • Procedimiento de Planificación del Roll-Out • Procedimiento de Diseño del Roll-Out y Roll-Back • Procedimiento de Logística para el Roll-Out masivo • Procedimiento de notificación del Roll-Out

• Dominios y Controles ISO 27002	

Roles:

- Diseño: Director de Producción
- Elaboración: Administrador de Despliegue y Versionamiento
- Aprobación: Gerente Nacional de Sistemas
- Inclusión y difusión en el MSGSI del BNF: Oficial de Seguridad de la Información
- Notificación de inclusión en MSGSI: Secretario General
- Actualización en la CMDB: Especialista de Configuración

Activos/Referencias:

- Computador Personal
- Política General de Release
- Software de Procesador de Documentos
- Estándar de Versionamiento
- Norma para control de fuentes
- Procedimiento de Planificación del Roll-Out
- CMDB
- Procedimiento de Diseño del Roll-Out y Roll-Back
- Procedimiento de Logística para el Roll-Out masivo
- Procedimiento de notificación del Roll-Out
- RRHH

Tareas:

1. Determinar las políticas generales de Release
2. Determinar el estándar de Versionamiento a adoptar para el control de versiones
3. Determinar la norma para el control de fuentes
4. Determinar el procedimiento de planificación de roll-out de las versiones
5. Determinar el procedimiento de diseño del roll-out y roll-back de las versiones
6. Determinar el procedimiento de logística para el Roll-Out masivo
7. Determinar el procedimiento de notificación del Roll-Out
8. Incluir, modificar o eliminar las políticas de Release dentro de un proceso de mejora continua

Métricas:

- Número de políticas, estándares, normas, procedimientos aprobados y difundidas satisfactoriamente

C. Definición Detallada del Proceso

Definición de Políticas de Release

Objetivo del Procedimiento:	Establecer políticas y planes que aseguren el control e implantación de las versiones de Software en ambientes de Producción
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Diseño: Director de Producción • Elaboración: Administrador de Despliegue y Versionamiento • Aprobación: Gerente Nacional de Sistemas • Inclusión y difusión en el MSGSI del BNF: Oficial de Seguridad de la Información • Notificación de inclusión en el MSGSI: Secretario General • Actualización en la CMDB: Especialista de Configuración
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: Entender las necesidades de elaboración de políticas que apoyen el proceso de Release: Control de Fuentes, Despliegue, Certificación, Versionamiento, Logística y Notificaciones
Entradas:	Las entradas para este procedimiento se listan a continuación: a. Manual del Sistema de Gestión de Seguridad de la Información b. Políticas y reglamentos del Banco Nacional de Fomento c. Políticas generales de la Gerencia Nacional de Sistemas d. Normativa para Gestión de Riesgo Operativo e. Normas de Control Interno de entidades del sector público f. Fundamentos de ITIL g. Fundamentos COBIT h. Dominios y Controles ISO 27002
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Diseña y Define la política** Plantear en formato borrador el *Documento de Políticas Generales de Release*, el mismo que se convierte en el marco de referencia para el Control de Fuentes, Despliegue a nivel de Back-End y Front-End, Certificaciones y Manejo de Versiones en ambientes de Producción y Calidad **2. Elabora la Política** El Administrador de Despliegue y Versionamiento, coloca en el formato establecido (plantilla política general de release.doc) el diseño elaborado por el director de producción y lo pone en modo de revisión 3. **Revisa la política** El Gerente nacional de Sistemas, revisa y emite correcciones para el documento **4. Ejecuta correcciones** El Administrador de Despliegue y Versionamiento, es el responsable de acoger las correcciones en el formato establecido y someterlo a un proceso de revisión hasta obtener la aprobación del documento por parte del Gerente Nacional de Sistemas

	5. Aprueba la Política El Gerente Nacional de Sistemas aprueba la política **6. Solicita la inclusión de la política en el MSGSI** El Gerente Nacional de Sistemas, remite la política aprobada al Oficial de Seguridad de la Información para que sea incluida en el MSGSI **7. Incluye la Política en el MSGSI** El Oficial de Seguridad de la Información, realiza la inclusión de la política en el Manual del Sistema de Gestión de Seguridad de la Información 8. **Difunde las políticas a las áreas operativas** El Oficial de Seguridad de la Información, se encarga de difusión a nivel de las áreas operativas del Banco el MSGSI actualizado conteniendo la política aprobada **9. Almacena en la CMDB la política** Una vez que la política está aprobada y formalizada, el especialista de configuración la registra en la CMDB **10. Conoce la actualización del MSGSI** El Secretario General del Banco, conoce a través del Oficial de Seguridad de la Información, de la inclusión de la política en el MSGSI **Consideraciones especiales** Este proceso se ejecuta para cada uno de los documentos definidos como salidas de este proceso Es política de la Gerencia Nacional de Sistemas, mantener un proceso de mejora continua para las políticas, estándares, normas y procedimientos generados, de tal manera que se mantengan alineados a las estrategias definidas y que apoyen el cumplimiento de los objetivos que constan en el plan estratégico de la Institución
Salidas:	Las salidas para este procedimiento se listan a continuación: a. Políticas Generales de Release b. Estándar de Versionamiento c. Norma para el control de fuentes d. Procedimiento de Planificación del Roll-Out e. Procedimiento de Diseño del Roll-Out y Roll-Back. f. Procedimiento de Logística para el Roll-Out masivo g. Procedimiento de notificación del Roll-Out
Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: a. Se tiene políticas que dan un marco de referencia apropiado para la ejecución del proceso de Administración de Release b. Se han establecido los procedimientos adecuados de control de fuentes, diseño, planificación, certificación, ejecución y vuelta atrás de los despliegues de versiones tanto a nivel de Back-End como de Front-End c. Se han establecido procedimientos para el adecuado uso de recurso humano involucrado en el proceso de Administración de Release, garantizando continuidad y mejora del proceso d. Se ha establecido el proceso de actualización de estas políticas, planificaciones y procedimientos cuando las circunstancias de mejora continua lo ameriten
Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: 1. Número de políticas, estándares, normas, procedimientos aprobados y difundidas satisfactoriamente vs. Número de políticas, estándares, normas, procedimientos planteados

3.3.2 SUBPROCESO DE CONTROL DE FUENTES

Definición de Procesos

Proceso:	AR – CFS – EFP : Administración de Release – **Control de Fuentes – Entrega de Fuentes para Producción**	**Cod.Doc**	AR-CFS	
Responsable:	Especialista de Control de Fuentes	**Versión:**	1.0	
Mantenimiento:	Especialista de Control de Fuentes	**Estado:**	Borrador	
			Publicado	X

Descripción:	Describe el manejo a nivel de autorización y registro de los fuentes que se reciben en Producción previo a la aplicación de un cambio

Alcance:	La entrega de fuentes para producción contempla los siguientes procedimientos: • Recibir la notificación del cambio a aplicar • Verificar que la solicitud de fuentes coincida con la entrega realizada • Notificar la verificación exitosa o no de la entrega de fuentes en producción • Proteger los fuentes entregados en la DSL

Guías de Personalización:	No aplica

Documentos de Referencia:	• Políticas de Release • Procedimiento de llenado de solicitud de fuentes • Formulario de Solicitud de fuentes • Estándar de Versionamiento

Abreviaciones y Acrónimos:	En este documento se usan las siguientes abreviaciones y acrónimos: • AR: Administración de Release • DSL: Definitive Software Library- Librería de Software Definitivo • RFC: Request for Change – Requerimiento de Cambio • CMDB: Configuration Management Database

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	20/07/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.2	14/06/2010	Lenni Carrión Julio Viteri	Todo	M	Primera revision
1.3	16/07/2010	Lenni Carrión Julio Viteri	Todo	A	Diagramas SIPOC *(Anexo 3.3)*

A. Diagrama de Flujo del Proceso

- *Anexo 3.4*

B. Resumen del Proceso

Criterios de Entrada:	**Criterios de Salida:**
• Entrega de Fuentes para Desarrollo • RFC para aplicar cambio.	• Fuente debidamente registrados su historial y versión y almacenados en la DSL.
Entradas:	**Salidas:**
• RFC aprobado por Comité de Control de cambios para puesta en producción • Documento de entrega de fuentes para Producción	• Fuentes protegidos. • DSL actualizada. • Solicitud de fuentes verificada

Roles:

- Entrega de Fuentes: Especialista de Control de Cambios
- Verificación: Especialista de Control de Fuentes
- Notificación de revisión exitosa o no: Especialista de Control de Fuentes
- Notificación de aplicación de cambio: Especialista de Control de Cambios

Activos/Referencias:

- Estándar de Versionamiento
- DSL
- Recurso Humano

- Roles y perfiles
- Documento de Entrega de Fuentes
- Notificaciones

Tareas:

1. Notificar cambio
2. Verificar fuentes entregados
3. Proteger fuentes en la DSL
4. Notificar revision

Métricas:

- Número de fuentes entregados versus número de fuentes solicitados

C. Definición Detallada del Proceso

Control de Fuentes – Entrega de Fuentes para Desarrollo

Objetivo del Procedimiento:	Garantizar los fuentes que permitan obtener el ejecutable que en etapa de certificación cumplió con los objetivos del cambio propuesto tanto a nivel de Back-End como de Front-End
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Entrega de Fuentes: Especialista de Control de Cambios • Verificación : Especialista de Control de Fuentes • Notificación de revisión exitosa o no: Especialista de Control de Fuentes • Notificación de aplicación de cambio: Especialista de Control de Cambios
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: a. Existió previamente un proceso de solicitud de fuentes por parte del desarrollador, que garantiza que se manejó la última versión en producción b. Los fuentes entregados en producción se encuentran en el directorio de desprotección definido por el Especialista de Control de Fuentes c. Ningún usuario podrá acceder al directorio de verificación de tal manera que la verificación pueda ser completada exitosamente y no exista duda del resultado
Entradas:	Las entradas para este procedimiento se listan a continuación: a. RFC aprobado por Comité de Control de cambios para puesta en producción b. Documento de entrega de fuentes para Producción
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Notificar aplicación de cambio** El Especialista de Control de Cambios, notifica el cambio a aplicar al Especialista de Control de Fuentes, de tal manera que el primer paso de verificación de fuentes permita identificar si los nuevos fuentes entregados fueron modificados en base a la última versión de fuentes

	disponible 2. **Verificar fuentes entregados** El documento de entrega de fuentes, debe coincidir con el contenido del directorio y a la vez con el documento de solicitud de fuentes para desarrollo, si estas condiciones no se cumplen, el cambio se considera devuelto por error en la entrega de fuentes para Producción. **3. Proteger directorio de entrega de Fuentes** El especialista de control de fuentes, retira los permisos de acceso (lectura, escritura) en el directorio asignado al desarrollador para colocar los fuentes en revisión 4. **Proteger Fuentes en la DSL** El Especialista de Control de Fuentes procede a guardar en la DSL cada uno de los fuentes entregados considerando en el historial del fuente la versión, el RFC asociado al cambio y el desarrollador responsable **5. Notificar entrega de fuentes satisfactoria** El especialista de control de fuentes notifica a los ejecutores de cambio, la recepción satisfactoria para que se continúe con la aplicación del cambio 6. **Devolver cambio por inconsistencia de entrega de fuentes** El especialista de control de fuentes ante cualquier novedad de la entrega de fuentes (fuentes entregados sin haberse solicitado, fuentes entregados por otro desarrollador) debe notificar al especialista de control de cambios para que a su vez proceda a notificar el cambio como devuelto
Salidas:	Las salidas para este procedimiento se listan a continuación: • Procedimiento de Solicitud/Entrega de Fuentes • Formulario de Entrega de Fuentes a Producción • RFC • Estándar de Versionamiento • DSL
Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: a. Se ha verificado que los fuentes entregados en producción son los recibidos por el desarrollador en un inicio b. Se ha verificado que el desarrollador que originalmente solicito los fuentes es quien entrega al especialista de control de fuentes c. De existir novedades se declara el cambio devuelto
Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: 1. Número de fuentes entregados versus número de fuentes solicitados 2. Número de cambios devueltos por error en la entrega de fuentes a producción 3. Número de fuentes sin entregar que rebasan el tiempo límite sin reportar novedades

3.3.3 SUBPROCESO DE DISEÑO Y CONFIGURACION DEL ROLL-OUT

Definición de Procesos

Proceso:	AR – DDC: Administración de Release – **Diseño y Configuración del Roll-Out.**	**Cod.Doc**	AR-DCR	
Responsable:	Administrador de Despliegue y Versionamiento	**Versión:**	1.3	
Mantenimiento:	Administrador de Despliegue y Versionamiento	**Estado:**	Borrador	
			Publicado	X

Descripción:	Definir el procedimiento de aplicación del cambio a nivel de Back-End y Front-End, validando el estándar de ejecución entregado para el RFC

Alcance:	El Diseño y Configuración del Roll-Out , contempla los siguientes procedimientos: • Determinar si existe una entrega de fuentes de producción exitosa • Determinar si existen cambios a nivel de Back-End y Front-End • Revisar y validar que el estándar de ejecución contenga todos los pasos a seguir • Obtener un paquete de distribución correcto y valido • Elaborar el Procedimiento de Diseño y Configuración del Roll-Out

Guías de Personalización:	No aplica

Documentos de Referencia:	• Formulario de Solicitud de Fuentes • RFC • Base de Datos de Control de Fuentes • Directorio de Entrega de Fuentes a Producción

Abreviaciones y Acrónimos:	En este documento se usan las siguientes abreviaciones y acrónimos: • AR: Administración de Release • DDC: Diseño, Desarrollo y Configuración • DSL: Definitive Software Library- Librería de Software Definitivo • RFC: Request for Change – Requerimiento de Cambio • Roll-out: Despliegue

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	13/06/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.2	14/06/2010	Lenni Carrión Julio Viteri	Todo	A	Revisión 1
1.3	22/07/2010	Lenni Carrión Julio Viteri	Todo	M	Diagrama SIPOC *(Anexo 3.5)*

A. Diagrama de Flujo del Proceso

- *Anexo 3.6*

B. Resumen del Proceso

Criterios de Entrada: a) Puesta en Producción de Control de Cambio certificado	**Criterios de Salida:** • Cambio aplicado exitosamente y previa certificación de entrega de fuentes y validación de pasos de estándar de ejecución
Entradas:	**Salidas:**
• RFC aprobado por Comité de Control de cambios para puesta en producción • Estándar de ejecución asociado al RFC de cambio • Directorio de Entrega de fuentes a Producción	• Notificación de aplicación de cambio Back-End exitoso • Notificación de aplicación de cambio Front-End exitoso • Nuevo paquete de distribución para Front-End almacenado y codificado • Procedimiento de diseño y configuración del Roll-Out

Roles:

- Notificación de cambio y entrega de RFC: Especialista de Control de Cambios
- Verificación de fuentes: Especialista de Control de Fuentes
- Aplicar control de cambios en Back-End: Ejecutor de Cambios
- Generar paquetes de distribución Front-End: Especialista de Despliegue y Versionamiento
- Codificar paquete de distribución y almacenar: Administrador de despliegue y Versionamiento
- Elaborar Procedimiento de Diseño y configuración del Roll-Out: Administrador de Despliegue y Versionamiento

Activos/Referencias:

- PC's
- Políticas de Release
- RFC y Estándar de Ejecución del cambio a aplicar

- Estándar de Versionamiento
- File Server de fuentes entregados en producción
- DSL
- Recurso Humano
- Roles y perfiles
- Paquete de distribución generado
- Procedimiento de Diseño y configuración del Roll-Out:
- Planes de Prueba

Tareas:

1. Confirmar entrega de fuentes en producción
2. Revisar estándar de Ejecución en Back-End y Front-End
3. Solicitar fuentes para aplicación de cambio
4. Entregar fuentes para aplicación de cambio
5. Aplicar cambios en Back-End
6. Generar paquete/s de distribución de Front-End
7. Codificar y Almacenar en la DSL el/los paquetes de distribución
8. Elaborar el procedimiento de Diseño y Configuración del Roll-Out

Métricas:

- Número de cambios devueltos por error en la entrega de fuentes a Producción
- Número de cambios devueltos por error en el estándar de ejecución
- Número de cambios devueltos por error en el paquete de distribución para Front End
- Número de cambios aplicados exitosamente

C. Definición Detallada del Proceso

Diseño y Configuración del Roll-Out

Objetivo del Procedimiento:	Aplicar de manera exitosa y certificada el estándar de ejecución a nivel de Back-End y Front-End definido para el cambio a aplicar en Producción
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Entrega de RFC: Especialista de Control de Cambios • Revisión de Fuentes: Especialista de Control de Fuentes • Generar nuevos paquetes: Especialista de Despliegue y Versionamiento • Almacenar y codificar en la DSL el Paquete de Distribución: Administrador de Despliegue y Versionamiento • Elaborar el Procedimiento de Diseño y Configuración del Roll-Out: Administrador de Despliegue y Versionamiento
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: a. El estándar de ejecución del RFC del cambio a aplicar ha sido certificado en calidad (ambiente símil a producción) b. La entrega de fuentes a Producción, debe coincidir con el directorio de entrega de fuentes y la solicitud de fuentes para desarrollo c. El cambio puede tener dos partes a ejecutar, a nivel de Back-End y Front-End

Entradas:	Las entradas para este procedimiento se listan a continuación: a. RFC aprobado por Comité de Control de cambios para puesta en producción b. Estándar de ejecución asociado al RFC de cambio c. Directorio de Entrega de fuentes a Producción
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Notificar aplicación de cambio** El Especialista de Control de Cambio, notifica el cambio a aplicar al Especialista de Control de Fuentes, para que proceda a aplicar el proceso de entrega de fuentes a producción 2. **Entrega de fuentes para Producción** El documento de entrega de fuentes, debe coincidir con el contenido del directorio y a la vez con el documento de solicitud de fuentes para desarrollo, si estas condiciones no se cumplen, el cambio se considera devuelto por error en la entrega de fuentes para Producción **3. Solicitar Fuentes para aplicación de cambio en Back-End** EL ejecutor de cambio verifica el estándar de ejecución para Back-End y solicita fuentes al Especialista de Control de Fuentes para aplicar el cambio y notifica **4. Solicitar Fuentes para aplicación de cambio en Front-End** El Especialista de Despliegue y Versionamiento verifica el estándar de ejecución para Front-End y solicita fuentes al Especialista de Control de Fuentes para generar el paquete de distribución **5. Generar paquete/s de distribución** Es el proceso de aplicación de los pasos especificados en el estándar de Front-End para la generación del paquete de distribución sin errores y que cumple a satisfacción el objetivo del cambio especificado en el RFC **6. Codificar y Almacenar en la DSL el paquete de distribución** Las copias maestras de los medios de instalación y las instrucciones de instalación, deben ser almacenadas en la DSL. Responsabilidad del Especialista de Despliegue y Versionamiento
Salidas:	Las salidas para este procedimiento se listan a continuación: • Notificación de aplicación de cambio Back-End exitoso • Notificación de aplicación de cambio Front-End exitoso • Paquete de Despliegue codificado y almacenado para Front-End • Procedimiento de Diseño y Configuración del Roll-Out
Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: a. Se ha elaborado el paquete de despliegue que permite cumplir con los objetivos de la distribución aprobada en el RFC del control de cambios aprobado b. Se ha codificado y almacenado correctamente en la DSL los nuevos paquetes de distribución, sus planes de prueba asociados y el procedimiento de distribución

Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: 1. Número de cambios devueltos por error en la entrega de fuentes a Producción 2. Número de cambios devueltos por error en el estándar de ejecución 3. Número de cambios devueltos por error en el paquete de distribución para Front End 4. Número de cambios aplicados exitosamente

3.3.4 SUBPROCESO DE PLANIFICACION DEL ROLL-OUT

Definición de Procesos

Proceso:	AR – PRO: Administración de Release – **Planificación del Roll-Out**	**Cod.Doc**	AR-PRO	
Responsable:	Administrador de Despliegue y Versionamiento	**Versión:**	1.3	
Mantenimiento:	Administrador de Despliegue y Versionamiento	**Estado:**	Borrador	
			Publicado	X

Descripción:	La planificación del Roll-Out de una nueva versión, determina la estrategia a adoptar para el despliegue masivo de la versión certificada en ambiente de Producción, garantizando el mínimo de impacto en el servicio comprometido

Alcance:	La Planificación de la nueva versión a ser distribuida, contempla los siguientes procedimientos: • Diseñar el Procedimiento de Planificación de Implantación de la nueva versión • Adecuar el Plan de Implantación de la versión al cronograma de tiempos de los Ingenieros de Procesos a cargo de la versión • Obtener la aprobación del Plan de Implantación de la nueva versión. • Registrar el Procedimiento

Guías de Personalización:	No aplica

Documentos de Referencia:	• Políticas de Release • Procedimiento de Planificación del Roll-Out • Procedimiento de Distribución • Procedimiento de Planificación del Roll-Back

Abreviaciones y Acrónimos:	En este documento se usan las siguientes abreviaciones y acrónimos: • AR: Administración de Release • PLA: Planificación • DSL: Definitive Software Library- Librería de Software Definitivo. • RFC: Request for Change – Requerimiento de Cambio • CMDB: Configuration Management Database • Roll-Out: Despliegue • Roll-Back: Vuelta atrás

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	13/06/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.3	20/07/2010	Lenni Carrión Julio Viteri	P	M	Diagrama SIPOC *(Anexo 3.7)*

A. Diagrama de Flujo del Proceso

- *Anexo 3.8*

B. Resumen del Proceso

Criterios de Entrada:	**Criterios de Salida:**
• Despliegue masivo de una nueva versión de software	• Planificación adecuada para la distribución de una nueva versión
Entradas:	**Salidas:**
• RFC aprobado por Comité de Control de cambios para puesta en producción • Planes de prueba de la versión • Procedimiento de Distribución certificado • CI's de pre-producción certificados	• Plan de Implantación aprobado • DSL actualizada • CMDB actualizada

Roles:

- Diseño y corrección del procedimiento de planificación: Administrador de Despliegue y Versionamiento
- Revisión del Procedimiento del plan de implantación: Director de Producción
- Especificar y validar cumplimiento del cronograma: Ingeniero de Procesos
- Aprobar Plan de Implantación: Gerente Nacional de Sistemas
- Registrar el Plan de Implantación aprobado: Especialista de Configuración

Activos/Referencias:

- PC's
- Políticas de Release
- Procedimiento de planificación del Roll-Out
- Procedimiento de distribución certificado
- Procesador de documentos
- DSL
- CMDB
- Recurso Humano con perfil idóneo
- Roles y perfiles definidos
- Paquete de distribución generado

Tareas:

1. Diseñar y corregir el Plan de Implantación de la versión
2. Revisar el Plan de Implantación de la versión
3. Especificar y validar el cumplimiento del cronograma en el Plan de Implantación
4. Aprobar el Plan de Implantación de la versión

Métricas:

- Número de revisiones del diseño del procedimiento de Planificación del Roll-Out
- Número de revisiones del diseño del procedimiento para el cumplimiento del cronograma del proyecto
- Número de diseños elaborados versus número de diseños aprobados

C. Definición Detallada del Proceso

Planificación

Objetivo del Procedimiento:	Obtener un Procedimiento de Planificación de Implantación de una nueva versión aprobado, que coordine el uso adecuado de tiempos y ambientes de producción, sin impacto en los servicios y que cumpla con los tiempos establecidos en los cronogramas de cada proyecto, alcanzando un porcentaje alto de éxito, y en caso de un Roll-Back, tiempos mínimos de recuperación de los servicios afectados
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Diseño y corrección del plan de implantación: Administrador de Despliegue y Versionamiento • Revisión del Plan de implantación: Director de Producción • Especificar y validar cumplimiento de cronograma de tiempos: Ingeniero de Procesos. • Aprobar Procedimiento de Planificación: Gerente Nacional de Sistemas • Registrar el Plan de Implantación aprobado: Especialista de Configuración
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: • Despliegue masivo de una nueva versión de software

Entradas:	Las entradas para este procedimiento se listan a continuación: • RFC aprobado por Comité de Control de cambios para puesta en producción • Planes de prueba de la versión • Procedimiento de Distribución certificado • CI's de pre-producción certificados
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Diseñar y corregir el Procedimiento de planificación de Roll-Out** El Administrador de Despliegue y Versionamiento define un Proceso de Implantación inicial que considera los detalles exactos necesarios para la distribución como son: Alcance, Horarios, Equipos destino de la distribución, Comunicaciones antes, durante y después de la distribución, Manejo de Incidencias post-distribución, Tiempos de Recuperación en caso de Roll-Back de la distribución, Niveles de comunicación del Plan, Estadísticas, SLA´s, Disponibilidad de los Servicios involucrados, capacitación De la misma manera considerara el cumplimiento de los tiempos especificados en los cronogramas de los Ingenieros de Procesos a cargo del proyecto a fin de definir: Recursos involucrados, Horarios de Trabajo, Horas Extras, apoyo de Operadores y Analistas de Service Desk 2. **Revisar el Procedimiento de Implantación de la versión.** El Director de Producción, realizará la revisión del Procedimiento de Implantación propuesto por el Administrador de despliegue y Versionamiento a fin de controlar que el entorno de producción no se vea afectado por la distribución de la versión. Su revisión deberá ser amplia y a todo nivel a fin de garantizar que el Plan cumple con el objetivo del despliegue y las expectativas de plazos 3. **Especificar y validar el cumplimiento de tiempos en el Plan de Implantación** El Ingeniero de Proceso deberá especificar y validar el cumplimiento de tiempos necesarios por parte del Plan de Implantación diseñado por el Administrador de Despliegue y Versionamiento, aunque esta consideración involucre el uso de mayor número de recursos o el pago de horas extras debidamente autorizadas por la Gerencia Nacional de Sistemas **4. Aprobar el Procedimiento de Implantación de la versión** El Gerente Nacional de Sistemas mediante su aprobación permite obtener el Plan de Implantación Aprobado, mismo que deberá ser registrado en la CMDB por el Especialista de Configuración
Salidas:	Las salidas para este procedimiento se listan a continuación: • Procedimiento de Planificación del Roll-Out aprobado • CMDB actualizada
Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: a. Se ha obtenido un Procedimiento de Implantación de la versión aprobado para la distribución de la versión
Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: 1. Número de revisiones del diseño del procedimiento de Planificación del Roll-Out 2. Número de revisiones del diseño del procedimiento para el cumplimiento del cronograma del proyecto 3. Número de diseños elaborados versus número de diseños aprobados

3.3.5 SUBPROCESO DE CERTIFICACION UNITARIA PREVIA AL ROLL-OUT MASIVO

Definición de Procesos

Proceso:	AR – CUPROM: Administración de Release – **Certificación Unitaria Previa al Roll-Out Masivo.**	**Cod.Doc**	AR-CUPROM	
Responsable:	Administrador de Despliegue y Versionamiento	**Versión:**	1.0	
Mantenimiento:	Especialista de Despliegue y Versionamiento	**Estado:**	Borrador	
			Publicado	X

Descripción:	La prueba de la versión a ser distribuida es realizada por el personal independiente al proceso (Ingeniero de Procesos) junto con el Especialista de Despliegue y Versionamiento para verificar cualquier procedimiento de soporte modificado. El procedimiento de Roll-Back también es probado. Esto incluye la prueba de los procedimientos de instalación y la funcionalidad del sistema final

Alcance:	La prueba de la versión a ser distribuida, contempla los siguientes procedimientos: • Habilita el ambiente de pre-producción • Ejecutar una distribución unitaria • Afinar los valores de los CI's del ambiente de pre-producción si es necesario • Certificar el procedimiento de distribución de la versión

Guías de Personalización:	No aplica

Documentos de Referencia:	• Políticas de Release • Procedimiento de planificación del Roll-out • Procedimiento de distribución • Procedimiento de planificación del Roll-back

Abreviaciones y Acrónimos:	En este documento se usan las siguientes abreviaciones y acrónimos: • AR: Administración de Release • CUPRON: Certificación Unitaria Previa al Roll-Out Masivo • DSL: Definitive Software Library- Librería de Software Definitivo. • RFC: Request for Change – Requerimiento de Cambio

	• CMDB: Configuration Management Database • Roll-Out: Despliegue • Roll-Back: Vuelta atrás

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	13/06/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.3	20/07/2010	Lenni Carrión Julio Viteri	P	M	SIPOC (*Anexo 3.9*)

A. Diagrama de Flujo del Proceso

- *Anexo 3.10*

B. Resumen del Proceso

Criterios de Entrada:	**Criterios de Salida:**
• Despliegue masivo de una nueva versión de software	• Procedimiento de distribución certificado en ambiente de pre-producción, almacenado en la DSL y valores de CI's del ambiente registrados en la CMDB
Entradas:	**Salidas:**
• RFC aprobado por Comité de Control de cambios para puesta en producción • Planes de prueba de la versión • Procedimiento de distribución	• Procedimiento de distribución certificado • DSL actualizada • CMDB actualizada

Roles:

- Habilitar ambiente de pre-producción, elaborar procedimientos de despliegue, certificación y registro en la DSL de Procedimiento de distribución: Administrador de Despliegue y Versionamiento
- Realizar despliegue unitario y aplicar correcciones: Especialista de Despliegue y Versionamiento
- Revisar funcionalidades del despliegue y especificar correcciones a los CI's de pre-producción: Ingeniero de Procesos.
- Registrar CI's certificados para la distribución en la CMDB: Especialista de Configuración

Activos/Referencias:

- PC's
- Políticas de Release
- Procedimiento de planificación del Roll-Out
- Procedimiento de distribución
- Procedimiento de planificación del Roll-Back
- Procesador de documentos
- DSL
- CMDB
- Recurso Humano
- Roles y perfiles
- Paquete de distribución generado
- Planes de Prueba

Tareas:

1. Habilitar ambiente de pre-producción
2. Realizar despliegue unitario
3. Certificar procedimiento de distribución
4. Rectificar o ratificar los valores de los CI's para el ambiente de pre-producción

Métricas:

- Porcentaje de fallas en la distribución de la versión
- Lanzamientos construidos e implementados dentro del cronograma horario, y dentro de los recursos presupuestados
- Grabación exacta y oportuna de las actividades de distribución en la CMDB

C. Definición Detallada del Proceso

Certificación Unitaria Previa al Roll-Out Masivo

Objetivo del Procedimiento:	Ejecutar la certificación unitaria del paquete de distribución a fin de obtener un procedimiento de distribución certificado con los valores de los CI's del ambiente de pre-producción validados, de tal manera que se garantice una distribución de software exitosa.
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Habilitar ambiente de pre-producción, elaborar procedimientos de despliegue, certificación y registro en la DSL de Procedimiento de distribución: Administrador de Despliegue y Versionamiento • Realizar despliegue unitario y aplicar correcciones: Especialista de Despliegue y Versionamiento • Revisar funcionalidades del despliegue y especificar correcciones a los CI's de pre-producción: Ingeniero de Procesos. • Registrar CI's certificados para la distribución en la CMDB: Especialista de Configuración
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: a. Despliegue masivo de una nueva versión de software

Entradas:	Las entradas para este procedimiento se listan a continuación: • RFC aprobado por Comité de Control de cambios para puesta en producción • Planes de prueba de la versión • Procedimiento de distribución
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Habilitar ambiente de pre-producción** El Administrador de Despliegue y Versionamiento prepara el ambiente de pre-producción para el despliegue unitario, para lo cual consulta en la DSL los valores de los CI's del último entorno de pre-producción certificado. Una vez recreado el ambiente se notifica al Especialista de despliegue y Versionamiento para que proceda a ejecutar los despliegues unitarios necesarios 2. **Realizar despliegue unitario.** Tomando como base el Procedimiento de despliegue detallado en el subproceso de Diseño, Desarrollo y Configuración, se ejecuta el despliegue en el ambiente de pre-producción preparado por el Administrador de Despliegue y Versionamiento. El despliegue unitario se ejecuta hasta obtener la certificación por parte del Ingeniero de Procesos de que el Procedimiento de despliegue es correcto y adecuado para la distribución **3. Certificar procedimiento de distribución.** El Ingeniero de Proceso deberá certificar después de cada despliegue unitario que los cambios esperados con la versión funcionan adecuadamente, de no ser así, deberá identificar los valores correctos de los CI's del ambiente de pre-producción y notificarlos al Administrador de Despliegue y Versionamiento a fin de que los registre en el ambiente de pre-producción y autorice un nuevo despliegue
Salidas:	Las salidas para este procedimiento se listan a continuación: • Procedimiento de Distribución certificado • CI's de pre-producción certificados
Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: a. Se ha comprobado los valores de los CI's de pre-producción que garantizan una distribución exitosa de la versión b. Se ha certificado el Procedimiento de Distribución especificado en el subproceso de Diseño, Desarrollo y Configuración de la versión a distribuir
Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: 1. Porcentaje de fallas en la instalación del release 2. Lanzamientos construidos e implementados dentro del cronograma horario, y dentro de los recursos presupuestados 3. Grabación exacta y oportuna de todas las actividades de distribución e implementación en la CMDB

3.3.6 SUBPROCESO DE LOGISTICA PARA EL ROLL-OUT MASIVO

Definición de Procesos

Proceso:	AR – LROM: Administración de Release – **Logística para el Roll-Out Masivo.**	**Cod.Doc**	AR-LROM	
Responsable:	Administrador de Despliegue y Versionamiento	**Versión:**	1.3	
Mantenimiento:	Administrador de Despliegue y Versionamiento	**Estado:**	Borrador	
			Publicado	X

Descripción:	Los usuarios y el personal de soporte (Service Desk) necesitan saber que se planea y como puede afectarlos. Esto se logra dar a conocer con sesiones de entrenamiento, períodos de funcionamiento en paralelo y la participación en la etapa de aceptación de Release. Los problemas y los cambios que necesitan ser realizados durante Roll-Out, se deben comunicar a todas las partes para mantenerlos informados y para fijar sus expectativas

Alcance:	La logística para el Roll-Out Masivo para la versión a ser distribuida, contempla los siguientes procedimientos: • Diseñar el Procedimiento de Logística para el Roll-Out masivo • Adecuar el Procedimiento de Logística para el Roll-Out masivo en función de las correcciones emitidas por la Dirección de Producción • Obtener la aprobación del Procedimiento de Logística para el Roll-Out masivo • Registrar el Procedimiento • Obtener planes de apoyo de las áreas de TI que soportan el proceso de Roll-Out

Guías de Personalización:	No aplica

Documentos de Referencia:	• Políticas de Release • Procedimiento de planificación del Roll-Out • Procedimiento de distribución • Procedimiento de planificación del Roll-Back

Abreviaciones y Acrónimos:	En este documento se usan las siguientes abreviaciones y acrónimos: • AR: Administración de Release • CPE: Planificación • DSL: Definitive Software Library- Librería de Software Definitivo • RFC: Request for Change – Requerimiento de Cambio • CMDB: Configuration Management Database • Roll-Out: Despliegue

	• Roll-Back: Vuelta atrás

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	14/06/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.3	21/07/2010	Lenni Carrión Julio Viteri	P	M	SIPOC (*Anexo 3.11*)

A. Diagrama de Flujo del Proceso

- *Anexo 3.12*

B. Resumen del Proceso

Criterios de Entrada:	**Criterios de Salida:**
• Despliegue masivo de una nueva versión de software	• Planificación adecuada para la distribución de una versión
Entradas:	**Salidas:**
• RFC aprobado por Comité de Control de cambios para puesta en producción • Planes de prueba de la versión • Procedimiento de Distribución certificado • CI's de pre-producción certificados • Plan de Implantación aprobado	• Plan de Comunicación Preparación y Entrenamiento aprobado • Plan de Manejo de Incidencias • DSL actualizada • CMDB actualizada

Roles:

- Diseño y corrección del Procedimiento de Logística para el Roll-Out Masivo: Administrador de Despliegue y Versionamiento
- Revisión, especificar correcciones y aprobar el Procedimiento de Logística para el Roll-Out Masivo: Director de Producción
- Especificar tipificación de errores y cambios esperados en la nueva versión: Ingeniero de Procesos
- Definir Plan de Manejo de Incidencias para la versión: Administrador de Service Desk
- Definir los planes de apoyo: Directores de TI
- Registrar el Procedimiento de Logística para el Roll-Out Masivo aprobado: Especialista de Configuración

Activos/Referencias:

- PC's
- Políticas de Release
- Tipificación de Incidencias
- Procedimiento de planificación del Roll-Out
- Procedimiento de distribución certificado
- Procedimiento de planificación del Roll-Back
- Procesador de documentos
- DSL
- CMDB
- Recurso Humano
- Roles y perfiles
- Paquete de distribución generado

Tareas:

1. Especificar tipificación de errores y cambios esperados de la nueva versión.
2. Diseñar y corregir el Procedimiento de Logística para el Roll-Out Masivo
3. Revisar y aprobar el Procedimiento de Logística para el Roll-Out Masivo
4. Diseñar el Plan de Manejo de Incidencias
5. Generar planes de apoyo al Roll-Out
6. Registrar el Procedimiento de Logística para el Roll-Out Masivo

Métricas:

- Número de revisiones del diseño del procedimiento de Planificación del Roll-Out
- Número de revisiones del diseño del procedimiento para el cumplimiento del cronograma del proyecto
- Número de diseños elaborados versus número de diseños aprobados

C. Definición Detallada del Proceso

Logística para el Roll-Out Masivo

Objetivo del Procedimiento:	Garantizar el mayor porcentaje de éxito de la distribución masiva, teniendo el adecuado funcionamiento de los activos de información involucrados en el proceso de Roll-Out. Obtener de sus responsables los planes preventivos y/o correctivos a ejecutar en caso de contingencias Comunicar eficaz y eficientemente a los usuarios sobre el despliegue de una nueva versión de software, de tal manera que se coordine las acciones necesarias con Service Desk y los Ingenieros de Proceso a cargo para minimizar el impacto de la liberación de una nueva versión y el manejo adecuado de incidencias asociadas a la misma
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Diseño y corrección del Procedimiento de Logística para el Roll-Out Masivo: Administrador de Despliegue y Versionamiento

	• Revisión, especificar correcciones y aprobar el Procedimiento de Logística para el Roll-Out Masivo: Director de Producción • Especificar tipificación de errores y cambios esperados en la nueva versión: Ingeniero de Procesos. • Definir Plan de Manejo de Incidencias para la versión: Administrador de Service Desk • Registrar el Procedimiento de Logística para el Roll-Out Masivo aprobado: Especialista de Configuración
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: • Despliegue masivo de una nueva versión de software
Entradas:	Las entradas para este procedimiento se listan a continuación: • RFC aprobado por Comité de Control de cambios para puesta en producción • Procedimiento de Distribución certificado • CI's de pre-producción certificados • Plan de Implantación aprobado
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Especificar tipificación de errores y cambios esperados de la nueva versión** El Ingeniero de Procesos entregara al Administrador de Despliegue y Versionamiento la *Tipificación de Incidencias* para la versión así como los cambios esperados por el Usuario con la liberación de la nueva versión de tal forma que estos integren el Procedimiento de Logística para el Roll-Out Masivo **2. Diseñar y corregir el Procedimiento de Logística para el Roll-Out Masivo** El administrador de Despliegue y Versionamiento define el Procedimiento de Logística para el Roll-Out Masivo en función del Plan de Implantación aprobado y las correcciones resultado de las revisiones a las que se somete el plan por parte de la Dirección de Producción 3. **Revisar y aprobar el Procedimiento de Logística para el Roll-Out Masivo.** El Director de Producción, realizará la revisión y aprobación del *Procedimiento de Logística para el Roll-Out Masivo* propuesto por el Administrador de Despliegue y Versionamiento a fin de controlar que el manejo de la comunicación con los actores involucrados en la distribución sea el adecuado. Su revisión deberá ser amplia y a todo nivel a fin de garantizar que el Plan cumple con el objetivo de comunicación y difusión esperado 4. **Definir Plan de Manejo de Incidencias** El administrador de Service Desk, generará un *Plan de Manejo de Incidencias* que será divulgado y de conocimiento de todos los analistas de Service Desk, para su ejecución y total cumplimiento en apoyo a la necesidad de capacitación de los usuarios finales de la nueva versión **5. Registrar el Procedimiento de Logística para el Roll-Out Masivo** El Especialista de Configuración deberá registrar en la CMDB el *Procedimiento de Logística para el Roll-Out Masivo.*
Salidas:	Las salidas para este procedimiento se listan a continuación: • Procedimiento de Logística para el Roll-Out Masivo aprobado. • Tipificación de Incidencias • Plan de Manejo de Incidencias • DSL actualizada • CMDB actualizada

Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: • Se ha obtenido un Procedimiento de Logística para el Roll-Out Masivo de la versión aprobado para su difusión y aplicación, durante y posterior a la distribución de la versión.
Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: • Número de revisiones del diseño del procedimiento de Planificación del Roll-Out • Número de revisiones del diseño del procedimiento para el cumplimiento del cronograma del proyecto • Número de diseños elaborados versus número de diseños aprobados

3.3.7 SUBPROCESO DE EJECUCION DE ROLL-OUT MASIVO

Definición de Procesos

Proceso:	AR – ERM: Administración de Release – **Distribución e Instalación.**	**Cod.Doc**	AR-ERM	
Responsable:	Administrador de Despliegue y Versionamiento	**Versión:**	1.0	
Mantenimiento:	Administrador de Despliegue y Versionamiento	**Estado:**	Borrador	
			Publicado	X

Descripción:	Especifica la ejecución misma de los pasos detallados en el Procedimiento de Diseño y Configuración del Roll-Out La distribución del software debe ser diseñada para mantener la integridad del software durante el manejo, empaquetado y entrega del mismo. La CMDB necesita ser actualizada después de la instalación definitiva de software, para asegurar que refleja la última situación.

Alcance:	La Distribución e Instalación de la versión, contempla los siguientes procedimientos: • Ejecutar el Procedimiento de Planificación de Diseño y Configuración del Roll-Out • Definir incidencias de despliegue y notificaciones a Service Desk • Notificar estado de la distribución y generar estadísticas • Notificar ejecución de control de cambios a los involucrados

Guías de Personalización:	No aplica

Documentos de Referencia:	• Políticas de Release • Procedimiento de planificación del Roll-Out • Procedimiento de diseño y configuración del Roll-Out

Abreviaciones y Acrónimos:	En este documento se usan las siguientes abreviaciones y acrónimos: • AR: Administración de Release • ERM: Ejecución del Roll-Out masivo • DSL: Definitive Software Library- Librería de Software Definitivo • RFC: Request for Change – Requerimiento de Cambio • CMDB: Configuration Management Database • Roll-out: Despliegue • Stakeholders: Usuarios finales interesados

Listado de Cambios

Versión	Fecha	Autor	Número (F)igura, (T)abla, o (P)árrafo	Acción (M)odificar (E)liminar (A)ñadir	Descripción
1.0	14/06/2010	Lenni Carrión Julio Viteri	Todo	A	Emisión Inicial
1.3	23/07/2010	Lenni Carrión Julio Viteri	Todo	A	Diagrama SIPOC (*Anexo 3.13*)

A. Diagrama de Flujo del Proceso

- *Anexo 3.14*

B. Resumen del Proceso

Criterios de Entrada:	Criterios de Salida:
• Despliegue masivo de una nueva versión de software	• Ejecución de la distribución de una nueva versión con un manejo adecuado de las incidencias, generando estadísticas que reflejen el porcentaje de éxito de la planificación para comunicación a todos los involucrados y responsables de la

	liberación de una versión
Entradas:	**Salidas:**
• RFC aprobado por Comité de Control de cambios para puesta en producción • Procedimiento de diseño y configuración del Roll-Out masivo aprobado • CI's de pre-producción certificados • Procedimiento de planificación del Roll-Out masivo aprobado	• Estadísticas de la distribución • Manejo de Incidencias de la distribución • RFC ejecutado • DSL actualizada • CMDB actualizada

Roles:

- Planificación, de la distribución, definición de incidentes, generación de estadísticas y notificación de estado de la distribución: Administrador de Despliegue y Versionamiento
- Ejecución de la distribución, y aplicación de correcciones específicas: Especialista de despliegue y Versionamiento.
- Ejecutar plan de manejo de incidencias y detallar correcciones aplicadas: Analista de Service Desk.
- Notificación de ejecución de cambio a los interesados: Especialista de Control de Cambios

Activos/Referencias:

- PC's
- Políticas de Release
- RFC aprobado por Comité de Control de cambios para puesta en producción
- Procedimiento de diseño y planificación del Roll-Out aprobado
- CI's de pre-producción certificados
- Procedimiento de Planificación del Roll-Out masivo aprobado
- DSL
- CMDB
- Recurso Humano
- Roles y perfiles
- Paquete de distribución generado

Tareas:

1. Planificar la distribución
2. Ejecutar el plan de distribución
3. Corregir incidentes de la distribución
4. Notificar el estado de la distribución

Métricas:

- Porcentaje de fallas en la instalación del release.
- Porcentaje distribución oportuna de la versión a todas las localidades
- La cantidad de problemas en el ambiente de producción que se pueden atribuir a nuevos release, qué necesitan ser medidos en los primeros meses de vida de un nuevo release, clasificados por causa de la raíz, (ejemplo: "versión incorrecta de archivo" o "archivos perdidos")
- El número de objetos nuevos, modificados y eliminados, introducidos por el nuevo release (ejemplo: cuantos módulos y programas hay)
- El número de release completados en los tiempos previstos; esto requiere la publicación por parte de la Administración de Release de los objetivos predefinidos (SLA's) para la distribución de software y otras tareas relacionadas

C. Definición Detallada del Proceso

Distribución e Implementación

Objetivo del Procedimiento:	Ejecutar el proceso de distribución e instalación del release probado, de la manera más eficiente, de acuerdo a la planificación diseñada y aprobada
Roles y Responsabilidades:	Los roles y responsabilidades asociados a este procedimiento se listan a continuación: • Planificación, de la distribución, definición de incidentes, generación de estadísticas y notificación de estado de la distribución: Administrador de Despliegue y Versionamiento • Ejecución de la distribución, y aplicación de correcciones específicas: Especialista de despliegue y Versionamiento • Ejecutar plan de manejo de incidencias y detallar correcciones aplicadas: Analista de Service Desk • Notificación de ejecución de cambio a los interesados: Especialista de Control de Cambios
Criterios de Entrada:	Los criterios de entrada asociados a este procedimiento se listan a continuación: • Despliegue masivo de una nueva versión de software
Entradas:	Las entradas para este procedimiento se listan a continuación: • RFC aprobado por Comité de Control de cambios para puesta en producción • Procedimiento de diseño y planificación del Roll-Out aprobado • CI's de pre-producción certificados • Procedimiento de Planificación del Roll-Out masivo aprobado
Pasos o Actividades del Procedimiento:	Los pasos necesarios para este procedimiento se listan a continuación: **1. Ejecutar el plan de distribución** El especialista de Despliegue y Versionamiento ejecuta lo especificado en el Procedimiento de Planificación del Roll-Out masivo aprobado **2. Corregir incidentes de la distribución** El Administrador de Despliegue y Versionamiento define los incidentes del despliegue y notifica a Service Desk a fin de que ejecute el *Plan de Manejo de Incidencias* **3. Notificar el estado de la distribución** El Administrador de Despliegue y Versionamiento, genera las *Estadísticas de distribución* que son entregadas a nivel gerencial y notifica el estado de la distribución dentro de los plazos acordados. De esta manera el Especialista de Control de Cambios, comunica a los stakeholders la aplicación exitosa del cambio e inicia el monitoreo post- implementación
Salidas:	Las salidas para este procedimiento se listan a continuación: • Estadísticas de la distribución

	• Manejo de Incidencias de la distribución • RFC ejecutado • DSL actualizada. • CMDB actualizada.
Criterios de Salida:	Los criterios de salida para este procedimiento se listan a continuación: a. Se ha ejecutado el Proceso de Distribución certificado en Producción.
Métricas del Proceso:	Las métricas que deben recopilarse en este procedimiento incluyen: 1. Porcentaje de fallas en la instalación del release 2. Porcentaje distribución oportuna de la versión a todas las localidades 3. La cantidad de problemas en el ambiente de producción que se pueden atribuir a nuevos release, qué necesitan ser medidos en los primeros meses de vida de un nuevo release, clasificados por causa de la raíz, (ejemplo: "versión incorrecta de archivo" o "archivos perdidos") 4. El número de objetos nuevos, modificados y eliminados, introducidos por el nuevo release (ejemplo: cuantos módulos y programas hay) 5. El número de release completados en los tiempos previstos; esto requiere la publicación por parte de la Administración de Release de los objetivos predefinidos (SLA's) para la distribución de software y otras tareas relacionadas

3.4 DEFINICION DEL MAPA DE PROCESOS DE RELEASE

En la Figura 3.5 se describe el mapa de procesos de Release en el que se identifican los siete principales subprocesos que lo conforman.

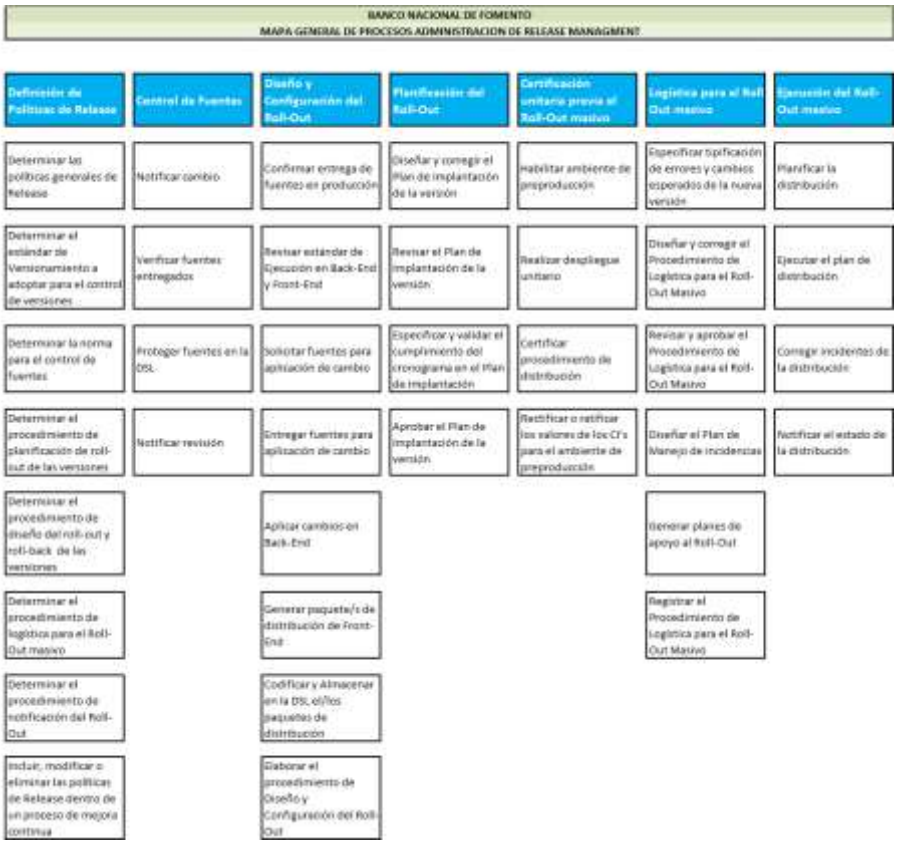


Figura 3.5 – Mapa de Subprocesos del Proceso de Release

CAPÍTULO IV

4.1 ANALISIS DE RIESGOS

El realizar un Análisis de Riesgos formal del proceso de Release del área de Producción de la Gerencia Nacional de Sistemas del Banco Nacional de Fomento, tiene por objetivo obtener mediciones y cálculos que nos lleven a seleccionar las medidas de protección que aporten el máximo retorno de la inversión en seguridad, equilibrando el coste total: los costes de los incidentes de seguridad sufridos, y los de los controles aplicados para prevenirlos; a través de la definición y aplicación de una metodología que se adapte al tamaño, estructura, y complejidad de las operaciones del Banco.

El objetivo principal al que apuntan todas las metodologías de gestión de la seguridad, claramente aceptadas y respaldadas internacionalmente, es garantizar los principios de Integridad, Confidencialidad y Disponibilidad de la Información, considerada hoy por hoy como el principal activo de una institución.

Para hacerlo es necesario revisar completamente el proceso y plantear todos los posibles incidentes de seguridad imaginables; lo que nos hace conscientes del peligro real.

El punto de partida deberá ser, necesariamente, el análisis de los subprocesos de Release, desde un punto de vista práctico, esto permitirá mejorar la efectividad y calidad del proceso, el resultado obtenido apuntará hacia los elementos cuya continuidad de servicio debería garantizarse, por encima de cualquier circunstancia (accidentes, fallos o ataques voluntarios e involuntarios).

Al ser la seguridad una cadena que se rompe por el eslabón más débil se obliga el plantear un análisis de riesgos muy riguroso, que no omita ningún elemento que forme parte del proceso o esté relacionado con él.

Existen varias metodologías para el análisis y gestión de Riesgos, como OCTAVE o CRAMM; la Gerencia Nacional de Riesgos a través de su Unidad de Seguridad de la Información, por el carácter de Institución Pública que tiene el Banco Nacional de Fomento, ha tomado como referencia la Metodología de Análisis y Gestión de Riesgos MAGERIT .

4.1.1 MAGERIT

El modelo planteado por MAGERIT sigue los siguientes procesos:

- *Identificación y valoración de activos*; definición de sus requerimientos de protección. Deben considerarse los activos materiales e inmateriales, la información, las personas, el entorno, y las actividades de la organización.

  Al valorarlos, tener en cuenta no solo el valor financiero de estos activos, sino también el coste en el que se incurre por la pérdida de su disponibilidad, integridad o confidencialidad.

- *Análisis de amenazas*. Deberán considerarse las vulnerabilidades conocidas de las aplicaciones y equipos instalados en los sistemas, las estadísticas sobre accidentes naturales en la zona e interrupciones de suministros -eléctrico o de ventilación-, y las amenazas intencionales -locales o remotas-.

- *Análisis de vulnerabilidades*. Procuramos detectar los puntos débiles del sistema, y aquellas circunstancias que pueden desencadenar un incidente de seguridad. Así, habrá que valorar el grado de exposición del sistema ante cada amenaza identificada sobre un activo.

- *Análisis de impacto*. Valoramos las consecuencias de que se produzca un incidente de seguridad en el sistema. Hay que considerar las consecuencias cuantitativas -que valoramos estimando el coste de paliar los daños producidos, o de reposición de los activos- y también considerar las consecuencias cualitativas -que valoraremos estimando el tiempo durante el cual no disponemos de los activos afectados, ya sean éstos documentos, datos, o programas no recuperables, información confidencial, know-how, prestigio, o credibilidad-.

- *Evaluación de riesgos*. Ni las amenazas, ni las vulnerabilidades, ni el impacto, por si solos, son realmente importantes; lo preocupante es el riesgo.

  Parece ampliamente reconocido que la manera más efectiva de definir el riesgo es la simple ecuación:

  Riesgo = Vulnerabilidad (Probabilidad) * Impacto.

  Lo que significa que si alguno de los componentes es cero, entonces el riesgo también es cero -aunque, siendo sinceros, no es posible asegurar que alguno de los componentes sea cero-. Pero otra manera de interpretar la ecuación es viendo que podemos reducir el riesgo si conseguimos reducir cualquiera de los dos componentes. Habitualmente lo que primero intenta reducirse es la vulnerabilidad, puesto que es lo que típicamente está más controlado (por ejemplo, podemos aplicar los parches necesarios sobre nuestras aplicaciones y sistemas; o podemos contratar varios proveedores de suministro eléctrico, para poder disponer de otro en caso de que uno falle). Existen, por tanto, soluciones sencillas y no muy caras que pueden ayudarnos a reducir parcialmente la vulnerabilidad de un sistema, o probabilidad de que sufra un ataque o incidente de seguridad, o el impacto que dicho incidente causaría en la organización (instalar un SAI = Sistema de Alimentación Ininterrumpida, que permita seguir trabajando durante un fallo de suministro eléctrico), reduciendo en cualquier caso el riesgo.

- *Interpretación de riesgos*. La política de seguridad de la organización debe establecer lo que se denomina un valor umbral de riesgo, que no es más que una estimación del nivel de riesgo mínimo que la empresa decide asumir. Y, una vez estimadas las valoraciones de todos los riesgos detectados sobre los activos de la organización, deben compararse estos valores con el valor umbral, de forma que los riesgos menores que el valor umbral se consideran aceptables (y, por tanto, no es necesario aplicar medidas de protección sobre ellos -aunque puede ser recomendable-). Por el contrario, si el riesgo calculado es mayor que el valor umbral, es necesario que se busquen medidas de protección para reducir la vulnerabilidad, la probabilidad o el impacto de la amenaza concreta sobre el activo. Para reducir la vulnerabilidad o la probabilidad hay que buscar medidas preventivas; para reducir el impacto, medidas curativas.

  Existe todavía otra posibilidad que es la de transferir el riesgo a una tercera parte -como proveedores de servicios, compañías de seguros, etc-.

- *Identificación y selección de salvaguardas*. En un análisis razonable, esta selección resulta ser un Análisis de Costes y Beneficios, en el que comparamos: el coste de prevenir un problema (coste de la salvaguarda) con el valor del riesgo calculado anteriormente - sin olvidar que para calcular el coste la salvaguarda hay que añadir al coste de implantación, y el coste del mantenimiento-.

  Y siempre teniendo en mente que el objetivo de implantar la salvaguarda es reducir el riesgo por debajo del valor umbral que se considera aceptable; de forma que si se estima que una salvaguarda no es suficientemente efectiva, habría que repetir el proceso desde el segundo proceso.

4.2 METODOLOGIA PARA EL ANALISIS Y GESTIÓN DE RIESGOS

La naturaleza, diversidad y complejidad de las actividades financieras propias del Banco Nacional de Fomento, y su condición de entidad bancaria regulada por la Superintendencia de Bancos y Seguros está obligada a adoptar lo citado en la normativa para la Administración y Gestión del Riesgo Operativo que en su artículo 4 dice "Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras."

Con este antecedente la Gerencia Nacional de Riesgos, establece la aplicación de una metodología que permite identificar causas, eventos, pérdidas que se pudieran producir dentro de un determinado proceso con frecuencias y severidades de alto impacto.

El proceso de modernización tecnológica por el cual está atravesando el Banco Nacional de Fomento evidencia que una falta de control en el mayor uso de la tecnología puede transformar los riesgos de errores de procesamiento, en riesgos de fallas del sistema (forma de materialización del riesgo).

En este contexto, la metodología para el análisis y gestión de riesgos adoptada para la presente tesis y que es parte integrante del Manual del Sistema de Seguridad de la Información (MSGSI) que la Gerencia Nacional de Riesgos ha estructurado, en síntesis, consta de los siguientes procesos (Figura 4.1):

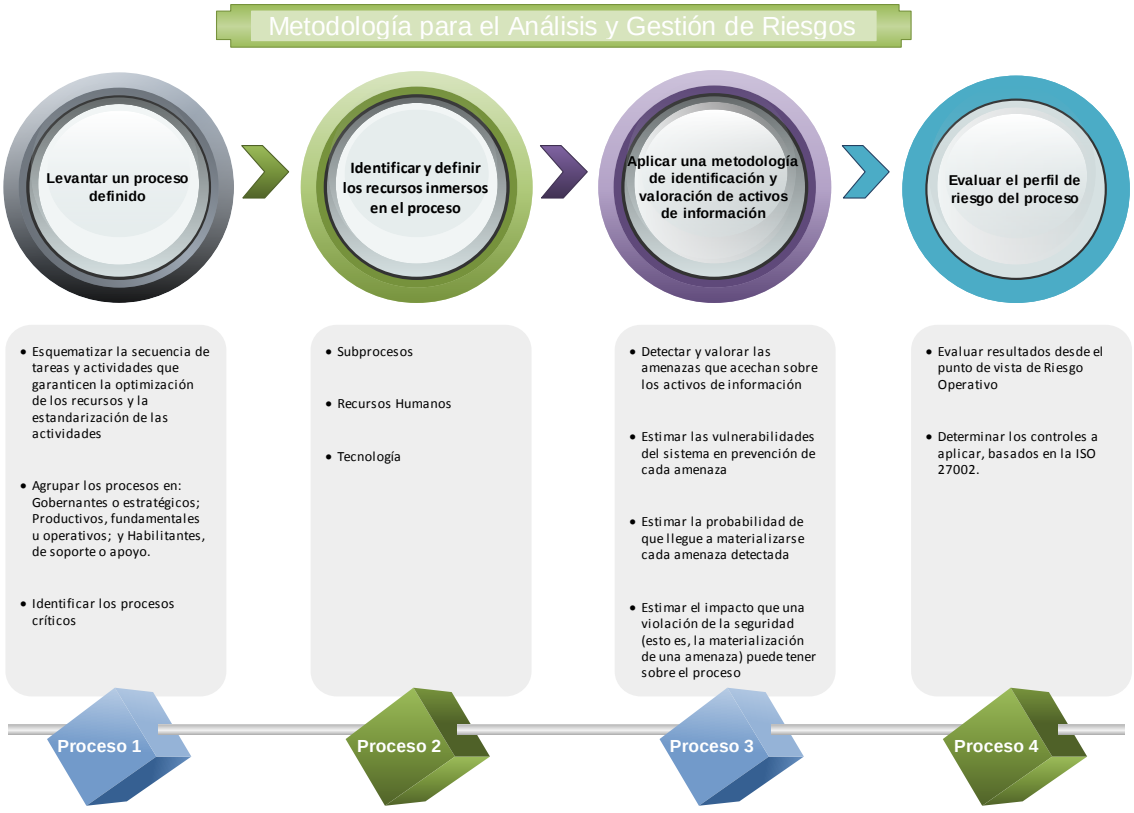


Figura 4.1 – Síntesis de la Metodología para el Análisis y Gestión de Riesgos

El insumo principal para que esta Metodología pueda aplicarse eficazmente, es contar con un proceso identificado y levantado por el área especialista, por ello esta actividad dentro del Banco Nacional de Fomento la realiza el Departamento de Organización y Métodos.

4.2.1 METODOLOGIA PARA LA IDENTIFICACION Y VALORACION DE ACTIVOS DE INFORMACION

Los criterios de identificación y valoración de los activos de información se realizarán como se indica en la Tabla 4.1, donde: Descripción, es la actividad, dentro del proceso respectivo, que se va a realizar para cumplir con los objetivos y alcance del presente documento; y, Responsables, serán las personas encargadas de ejecutar las actividades.

N.	Descripción	Responsables
1	Identificar dentro del flujo de información, sistemas o elementos informáticos que intervienen en el proceso bajo su responsabilidad: - Documentación impresa propia y de terceros - Información sistematizada de servicios, aplicaciones y/o equipos de procesamiento individuales y/o centralizados - Reportes y listados - Medios magnéticos móviles, y/o - Cualquier otro soporte físico que contenga información.	Unidad de Seguridad de la Información / Dirección de Producción
2	Realizar la tasación de activos de información, tomando en consideración como parámetros de valoración los principios de Seguridad de la Información los cuales pretenden: Que la información sea conocida solo por los funcionarios autorizados - **Confidencialidad**- Que la información refleje la realidad - **Integridad** - Que la información se pueda acceder oportunamente para desarrollar actividades con base en ella -**Disponibilidad –** A cada activo se le otorgará una ponderación de: Alto = 3 Medio = 2 Bajo = 1 Con esto se establece un promedio de valoración otorgada a cada activo con el objeto de obtener un ranking y continuar con el análisis de los activos de mayor ponderación.	Unidad de Seguridad de la Información / Dirección de Producción
3	Con los resultados obtenidos, analizar cada activo identificando sus amenazas y la probabilidad de ocurrencia de las mismas. Los tipos de amenazas que los activos están expuestos serán catalogados dentro de estos 5 grupos:	Unidad de Seguridad de la Información / Dirección de Producción

	- Desastres naturales - Pérdidas de Servicios - Humanos - Tecnológicos - Amenazas deliberadas Los niveles de probabilidad que una amenaza se materialice se clasificaran de acuerdo a las siguientes ponderaciones: Alta = 3 Media = 2 Baja = 1	
4	Identificar las vulnerabilidades - debilidades - , que permitirán que una amenaza se materialice. Una vez identificadas asignar la probabilidad de ocurrencia y el impacto si se materializa, tomando en cuenta la siguiente ponderación: Alta = 3 Media = 2 Baja = 1	Unidad de Seguridad de la Información / Dirección de Producción
5	Para la calificación del Riesgo de Vulnerabilidad, Amenaza y Activo, se utilizará las siguientes fórmulas: **Calificación Riesgo de Vulnerabilidad** = Promedio (Probabilidad + Impacto) **Calificación Riesgo Amenaza** = ((Promedio Calificación Riesgo de Vulnerabilidad) + Probabilidad Amenaza)) / 2 **Riesgo del Activo** = ((Promedio Calificación Riesgo Amenaza) + Tasación Activos)) / 2	Unidad de Seguridad de la Información
6	Con el resultado obtenido de Riesgo del Activo, identificar el tipo de Riesgo de acuerdo a los siguientes valores: Alto > 2,2 Medio > 1,6 Bajo < 1,7	Unidad de Seguridad de la Información

Tabla 4.1: Metodología a utilizar para la identificación y clasificación de activos de información
Tomado de: Manual del Sistema de Gestión de Seguridad de la Información (MSGSI)
Gerencia Nacional de Riesgos del Banco Nacional de Fomento

Basado en el impacto y disponibilidad de los servicios entregados a los usuarios internos y clientes, la Gerencia Nacional de Riesgos tiene el compromiso de socializar y monitorear la aplicación de esta metodología en todos los procesos críticos de la Institución, instaurando y fortaleciendo una cultura de riesgo que permita llevar a todos los funcionarios de la entidad a que cuenten con una visión amplia del negocio, identifiquen y realicen la gestión por procesos, apliquen Técnicas de gestión de riesgos, sean preventivos.

CAPITULO V

5.1 GESTION DE RIESGOS DEL PROCESO DE RELEASE

5.1.1 EVALUACION DE LOS RIESGOS CON EL MAPA DE PROCESOS DE TI

Basado en el estudio realizado por el departamento de riesgo Operativo de la Gerencia Nacional de Riesgos del Banco Nacional de Fomento, para cada proceso, se establece la matriz de valor de riesgo en función del riesgo operativo por proceso Tabla 5.1, la misma que basada en la normativa emitida por la Superintendencia de Bancos y Seguros considera los siguientes factores de riesgo operativo asignándoles sus respectivos pesos:

Factor de Riesgo	Porcentaje (%)
Pérdida de Experticia del Personal	20
Comportamiento del Cliente Interno / Proveedores	30
Potencial de errores en las operaciones	10
Potencial a pérdida o fraude	30
Errores por cambios y/o software	10

Tabla 5.1: Pesos de los factores de riesgo operativo

Cabe destacar que el mecanismo de obtención de esta matriz es de aplicación para toda la Institución, razón por la cual, para la Gerencia Nacional de Sistemas no se realizó ninguna diferenciación.

Descripción del Procedimiento de Cálculo:

1. Considerando los macro procesos de la Gerencia Nacional de Sistemas, para cada uno de los procesos que los integran, se establece, tanto la probabilidad de ocurrencia como el impacto de llegar a consumarse el factor de riesgo; considerando las condiciones actuales de desempeño de dicha Gerencia.
2. La ponderación de relación de probabilidad e impacto asignado es similar a la considerada en la metodología de identificación y valoración de activos de información Alto (3), Medio (2) y Bajo (1).
3. El valor de riesgo de cada proceso, se obtiene del promedio de multiplicar la probabilidad por el impacto de cada uno de los factores de riesgo definidos.
4. Se obtiene la media de los valores de riesgo de todos los procesos (umbral).
5. Si el valor de riesgo de cada proceso supera el valor de la media, se prioriza la gestión de los riesgos inherentes a ese proceso.

En la Figura 5.1 se puede observar claramente que la valoración permite identificar los procesos de alta, media y baja criticidad, permitiendo a la Gerencia Nacional de Sistemas tomar decisiones sobre qué proceso se debería iniciar con mayor prioridad el análisis, de esta manera tomar las acciones inmediatas a fin de mitigar los riesgos potenciales.

		FACTORES DE RIESGO										
		PERDIDA DE EXPERTICIA DEL PERSONAL 20%		CAMBIOS EN COMPORTAMIENTO DEL CLIENTE INTERNO 30%		POTENCIAL DE ERRORES EN OPERACIONES 10%		POTENCIAL A FRAUDE O PERDIDA 30%		ERRORES POR CAMBIOS Y/O SOFTWARE 10%		
MACROPROCESOS	PROCESOS	PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO	VALOR DE RIESGO
DESARROLLO	ADMINISTRACION DE PROYECTOS	1	3	3	3	2	2	1	1	1	3	4,00
	MANTENIMIENTO DE APLICACIONES	1	3	3	3	1	2	3	3	3	3	6,80
PRODUCCION	ADMINISTRACION DE DISPONIBILIDAD DE SERVICIOS	1	3	2	3	1	3	1	3	3	3	4,80
	ADMINISTRACION DE CONTINUIDAD DE SERVICIOS	2	3	3	3	1	3	1	3	1	3	4,80
	ADMINISTRACION DE INCIDENCIAS - SERVICE DESK	2	3	3	3	2	3	1	3	2	3	6,00
	ADMINISTRACION DE PROBLEMAS - COMITÉ DE SERVICIOS	2	3	1	2	1	3	1	3	2	3	4,00
	ADMINISTRACION DE RELEASE MANAGEMENT	2	3	3	3	2	3	3	3	3	3	7,80
GESTION Y CONTROL	ADMINISTRACION DE RECURSOS TI	2	1	3	3	2	1	3	3	1	2	4,80
	ADMINSITRACION DE CAMBIOS	2	2	3	3	2	3	1	3	3	3	6,20
	ADMINISTRACION DE CONFIGURACION	3	3	2	3	2	3	3	3	3	3	7,80
	ADMINISTRACION DE CAPACIDAD DEL NEGOCIO	3	3	3	3	2	3	1	3	1	2	5,80
INFRAESTRUCTURA	ADMINISTRACION DE INFRAESTRUCTURA	3	3	3	3	3	3	1	3	3	3	7,80
	ADMINISTRACION DE BASE DE DATOS	1	3	1	3	2	3	1	3	2	3	4,20
	ADMINISTRACION DE SEGURIDAD PERIMETRAL	2	3	2	3	2	3	2	3	3	3	6,80
										Promedio		5,8
										Media		5,9
										Mediana		5,9

Figura 5.1 – Mapa de Valor de Riesgo de la Gerencia Nacional de Sistemas
Tomado de: Metodología Departamento de Riesgo Operativo de la Gerencia Nacional de Riesgos del Banco Nacional de Fomento

5.2 EVALUACION DE RIESGOS CON EL MAPA DE PROCESOS DE RELEASE

Aplicando la metodología para el análisis y gestión de riesgos propuesta, y una vez priorizados los riesgos, la técnica se basa en el análisis de identificación de los Activos de Información que interactúan en este proceso, entendiéndose como activos a cualquier elemento que represente un valor para la organización. Esto incluye activos intangibles como la reputación de la empresa e información digital incluyendo datos u otra información que resulte valiosa para la organización, por ejemplo, transacciones bancarias, cálculos de intereses y especificaciones de desarrollo de productos; y, activos tangibles como la infraestructura física como centros de datos, servidores y propiedad.

- Identificación de los activos de información

  Para identificar los activos de información, también es necesario identificar o confirmar el responsable del activo o el grupo responsable de un activo; en este sentido, se debe respetar las competencias de cada actor del proceso y subproceso en función de la estructura organizacional de la Gerencia Nacional de Sistemas. Esta información resulta útil durante el proceso de asignación de prioridades para confirmar la información y comunicar los riesgos directamente a sus responsables.

- Valoración de activos de información

  Los activos identificados cualitativamente deben ser valorados para de esta manera establecer un proceso de medición cuantitativa según resulte adecuado para el área de la Gerencia Nacional de Sistemas y el Banco Nacional de Fomento. La valoración realizada deberá estar en función de los principios de Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad (CID).

- Identificación de amenazas a los activos de información

  El objetivo de este punto es identificar los potenciales eventos que pudiesen causar un incidente no deseado o un intento de hacer daño, en otras palabras, las cosas malas que les puede pasar a los activos de información ocasionando daños, afectación, degradación o destrucción. No solo se debe considerar lo malo que les está pasando sino lo que podría pasarles. De acuerdo a la metodología, las amenazas deben ser identificadas dentro de los siguientes tipos: Desastres naturales, Pérdidas de servicios públicos, Humanos, Tecnológicos, Amenazas deliberadas; además de considerar su probabilidad.

- Identificación de Vulnerabilidades

  Teniendo como premisa fundamental que una vulnerabilidad en sí mismo no causa daño, que son puntos débiles o que demuestran ausencia de controles que se pueden aprovechar para atacar un activo, se deben identificar las vulnerabilidades por cada activo de información, evaluando la probabilidad y el impacto de llegar a materializarse.

- Calificación del Riesgo

  La calificación del riesgo de cada activo es el resultado final esperado que permitirá definir el perfil de riesgo del activo dentro del subproceso analizado.

En el Anexo 5.1, se ilustra un modelo de plantilla propuesta aplicable a cada uno de los subprocesos del proceso de Release y que permite identificar y valorar los activos de información que requieren una gestión del riesgo, en función del valor de riesgo obtenido.

5.3 IMPACTO DE LA IMPLEMENTACION DEL PROCESO DE RELEASE DESDE EL PUNTO DE VISTA DE RIESGO OPERATIVO

En la actualidad, los sistemas de información se encuentran dispersos en toda la organización. El Banco Nacional de Fomento posee una arquitectura de redes, soportadas por sistemas operativos actualizados, usuarios internos y externos, computadoras personales, computación móvil, Internet, etc.

Debido al rápido avance de las tecnologías de la información y a la implementación de nuevo Core Bancario, es que existen nuevas oportunidades para la creación, acceso, comunicación y análisis de datos, es decir, nuevas oportunidades para llevar adelante las tareas cotidianas. Pero esta capacidad para procesar y transferir grandes caudales de datos en forma rápida implica, mayores y nuevos riesgos.

Estos riesgos o amenazas pueden ser atribuibles a factores humanos, como por ejemplo, robo, fraude, falta de confidencialidad, empleados infieles, empleados no capacitados, hackers; a factores tecnológicos, como interrupción del servicio, perdida de datos por falla de software o hardware, daños materiales; o bien a factores ambientales tales como inundaciones, terremotos, rayos, calor, etc.

A través de la evaluación de riesgos, se puede definir e implementar todas las acciones que impliquen una previsión de los hechos o riesgos predecibles y que minimicen los hechos impredecibles. En este sentido, al final de presente capítulo se detalla las consideraciones mínimas a tener en cuenta para la implementación de un plan de contingencia tecnológico que permita garantizar la disponibilidad del servicio de release.

Conceptualizando que es Riesgo Operativo, según el Comité de Basilea, es: “el riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, personas o sistemas internos o bien a causa de

acontecimientos externos"; por tanto, el Riesgo Operativo no representa un riesgo nuevo, sino un "riesgo antiguo" con un enfoque renovado.

El Comité de Supervisión Bancaria de Basilea ha definido principios para la conformación de un adecuado ambiente para la administración del riesgo operativo, estos principios han sido adoptados por los supervisores de distintos países, que han recomendado su aplicación en las instituciones del sistema financiero.

La administración del riesgo operativo implica: identificar, medir, controlar y monitorear los riesgos operativos que el Banco enfrenta. Para cada uno de estos procesos se observará:

5.3.1 IDENTIFICACION:

- Tipificar la exposición al Riesgo Operativo (RO), mediante la identificación de los eventos de RO agrupándolos por factores de riesgo.
- Mantener mapas de eventos de riesgo operativo actualizados.
- Mantener el portafolio de procesos actualizado, clasificándolos de acuerdo a la normativa en: gobernantes, productivos y habilitantes.
- Contar con planes de continuidad y contingencia aprobados y probados periódicamente.
- Contar con un Plan de Riesgo Operativo, que será ejecutado por todas las áreas del banco y monitoreado por el Departamento de Riesgo Operativo.

5.3.2 MEDICION:

- Conformar bases de datos de eventos de RO para: registrar, clasificar, analizar y proponer planes de mitigación cuando amerite.
- Analizar y proponer para decisión del Comité de Administración Integral de Riesgos -CAIR- y el Directorio del BNF, si los riesgos deben ser asumidos, compartidos o transferidos, a fin de minimizar sus consecuencias y efectos.

5.3.3 CONTROL:

- Contar con procesos, procedimientos y controles, formalmente aprobados, implementados y validados periódicamente.
- Diseñar / modificar controles.
- Revisar términos de pólizas de seguros para cambiar las coberturas, según corresponda.
- Integrar los conceptos de riesgo operativo en los procesos de control interno, contando con el apoyo de auditoría interna.
- Contar con un Código de ética formalmente aprobado, actualizado y de aplicación obligatoria.

5.3.4 MONITOREO:

- Diseñar, implementar y emitir periódicamente un esquema organizado de reportes, con información adecuada y suficiente para gestionar el RO en forma permanente.
- Establecer indicadores de gestión que permitan evaluar la eficiencia y la eficacia de las políticas, proceso y acciones de control implementadas.

- Remitir los reportes y recomendaciones al CAIR y Directorio para la toma de medidas que viabilicen una constante mejora en la gestión del RO.

5.4 IDENTIFICACION DEL RIESGO OPERATIVO

5.4.1 FACTOR DE RIESGO OPERATIVO

Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos Figura 5.2.

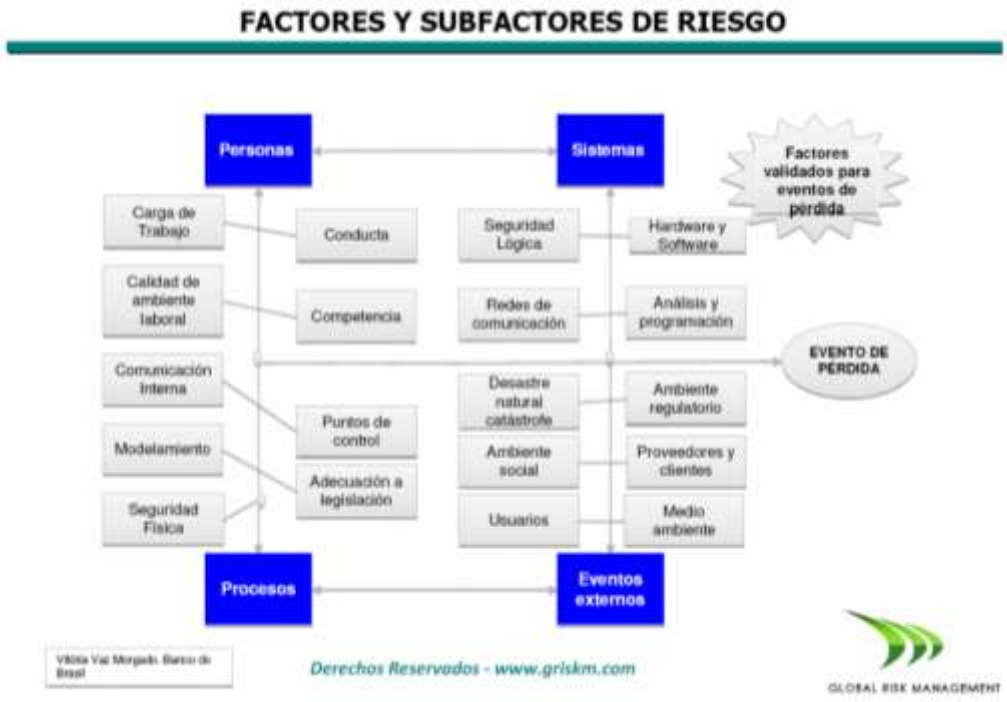


Figura 5.2: Factores de Riesgo Operativo
Tomado de Global Risk Management

5.4.1.1 PROCESOS

Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo; las instituciones deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

- Procesos gobernantes o estratégicos.

- Procesos productivos, fundamentales u operativos.
- Procesos habilitantes, de soporte o apoyo.

5.4.1.2 PERSONAS

Administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

- Procesos de incorporación
- Procesos de permanencia
- Procesos de desvinculación

5.4.1.3 TECNOLOGIA DE INFORMACION

Contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

5.4.1.4 EVENTOS EXTERNOS

En la administración del riesgo se debe considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

5.4.1.5 EVENTOS DE RIESGO

Es el hecho que puede derivar en pérdidas financieras para la institución.

5.4.3 TIPOS DE EVENTOS

1. Fraude interno;
2. Fraude externo;
3. Prácticas laborales y seguridad del ambiente de trabajo;
4. Prácticas relacionadas con los clientes, los productos y el negocio;
5. Daños a los activos físicos;
6. Interrupción del negocio por fallas en la tecnología de información; y,
7. Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

5.4.4 OPCIONES DE TRATAMIENTO DEL RIESGO

Aceptación de riesgo: una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Transferir el riesgo: cambiar la responsabilidad o carga por las pérdidas a una tercera parte mediante legislación, contrato, seguros u otros medios. Transferir riesgos también se puede referir a cambiar un riesgo físico, o parte el mismo a otro sitio.

Reducir el riesgo: una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas.

Evitar un riesgo: una decisión informada de no verse involucrado en una situación de riesgo, mediante la aplicación de técnicas apropiadas y principios de administración para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas.

En la Tabla 5.2 se ilustra las opciones de tratamiento del riesgo

FRECUENCIA						
Muy Frecuente	TRANSFERIR			EVITAR	
Frecuente					
Ocasional	ACEPTAR			REDUCIR	
Rara Vez					
	No Significativo	Bajo	Significativo	Importante	Alto
	IMPACTO				

Tabla 5.2: Opciones de tratamiento del riesgo

5.5 MATRIZ DE RIESGO

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una

adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende el logro de los objetivos de una organización.

La matriz debe ser una herramienta flexible que documente los procesos y evalúe de manera integral el riesgo de una institución, a partir de los cuales se realiza un diagnóstico objetivo de la situación global de riesgo de una entidad. Exige la participación activa de las unidades de negocios, operativas y funcionales en la definición de la estrategia institucional de riesgo de la organización. Una efectiva matriz de riesgo permite hacer comparaciones objetivas entre proyectos, áreas, productos, procesos o actividades. Todo ello constituye un soporte conceptual y funcional de un efectivo Sistema Integral de Gestión de Riesgo.

Las entidades financieras, al tomar posiciones en activos financieros, no buscan eliminar estos riesgos, sino gestionarlos y controlarlos, para lo cual necesitan, en primer lugar, identificarlos y medirlos. Sin embargo, antes es preciso establecer el perfil de riesgo que se quiere adoptar, lo que es decisión propia y exclusiva de cada entidad, en función de su estrategia de largo plazo.

El Departamento de Riesgo Operativo de la Gerencia Nacional de Riesgos, adopta oficialmente una Metodología con el objeto de generar Matrices de Riesgo por cada uno de los procesos considerados críticos y de esta manera determinar una medición cuantitativa sobre los mismos que permita definir alertas tempranas para mitigar los riesgos inherentes. A continuación se transcribe el material bibliográfico que fue adoptado por el Departamento anteriormente referido como la Metodología que se está utilizando para la generación de la Matriz de Riesgo. Es necesario mencionar que este material fue proporcionado durante la participación al Diplomado de Gestión y Administración Integral de Riesgos. SCALAR CONSULTING. OCTUBRE 2007.

5.5.1 METODOLOGIA PARA LA GENERACION DE LA MATRIZ DE RIESGO

5.5.1.1 EVALUACION Y GESTION DE RIESGOS

Cualquier actividad que el ser humano realice está expuesta a riesgos de diversa índole los cuales influyen de distinta forma en los resultados esperados.

La capacidad de identificar estas probables eventualidades, su origen y posible impacto constituye ciertamente una tarea difícil pero necesaria para el logro de los objetivos. En nuestro caso, el desempeño depende de la gestión de los riesgos inherentes a las actividades que desarrollamos, tales como riesgos de crédito, mercado, liquidez, operativo, entre otros; algunos de ellos de compleja identificación y de difícil medición.

En los últimos años las tendencias internacionales han registrado un importante cambio de visión en cuando a la gestión de riesgos: de un enfoque de gestión tradicional hacia una gestión basada en la identificación, monitoreo, control, medición y divulgación de los riesgos. El siguiente cuadro muestra la diferencia entre el modelo tradicional y el nuevo enfoque de evaluación de la gestión de riesgos, según las últimas tendencias (Tabla 5.3):

Esquema anterior	Enfoque nuevo
La evaluación de riesgo es histórica y se desempeña eventualmente.	La evaluación de riesgo es continua y recurrente.
La evaluación de riesgo detecta y reacciona.	La evaluación de riesgo anticipa y previene.

La evaluación de riesgos se enfoca en las transacciones financieras y los controles internos.	La evaluación de riesgos se enfoca en la identificación, medición y control de riesgos, velando que la organización logre sus objetivos con un menor impacto de riesgo posible.
Cada función es independiente. Pocas funciones tratan de la evaluación de riesgo.	La evaluación de riesgo está integrada en todas las operaciones y líneas de negocios.
No hay una política de evaluación de riesgo.	La política de evaluación de riesgo es formal y claramente entendida.

Tabla 5.3: Enfoque de evaluación de la gestión de riesgos

En este sentido gestionar eficazmente los riesgos para garantizar resultados concordantes con los objetivos estratégicos de la organización, quizás sea uno de los mayores retos de los administradores y gestores bancarios. Desde este punto de vista, la gestión integral de los riesgos se vuelve parte fundamental de la estrategia y factor clave de éxito en la creación de valor económico agregado para los accionistas, empleados, depositantes, inversionistas, entre otros. En este sentido, es imprescindible contar con herramientas que permitan:

1. Definir criterios a partir de los cuales se admitirán riesgos; dichos criterios dependerán de sus estrategias, plan de negocios y resultados esperados.

2. Definir a través de un mapa de riesgo, áreas de exposición a los riesgos inherentes a sus actividades, en consecuencia establecer el riesgo máximo aceptable así como el área no aceptable.

3. Monitoreo y medición de todas las categorías de riesgo que pueden impactar el valor de la entidad en forma global, por unidad de negocios, por productos y por procesos.

4. Definir el nivel de pérdida esperada aceptable y la metodología de medición.

5. Diseñar mecanismos de cobertura a los riesgos financieros, operativos estratégicos con una visión integral y comprensiva del negocio.

6. Relacionar el área de máxima exposición al riesgo con el capital que se desea arriesgar en forma global y por unidad estratégica de negocio.

7. Definir y estimar medidas de desempeño ajustada por riesgos.

Con relación a los numerales 1, 2 y 3, relacionados con la identificación y evaluación de riesgos, la “matriz de riesgos” constituye una herramienta útil en el proceso de evaluación continua de las estrategias y manejo de riesgos.

5.5.1.2 ELEMENTOS CONSIDERADOS EN EL DISEÑO DE LA MATRIZ DE RIESGOS

A partir de los objetivos estratégicos y plan de negocios, la administración de riesgos debe desarrollar un proceso para la “identificación” de las actividades principales y los riesgos a los cuales están expuestas; entendiéndose como riesgo la eventualidad de que una determinada entidad no pueda cumplir con uno o más de los objetivos (Figura 5.3).

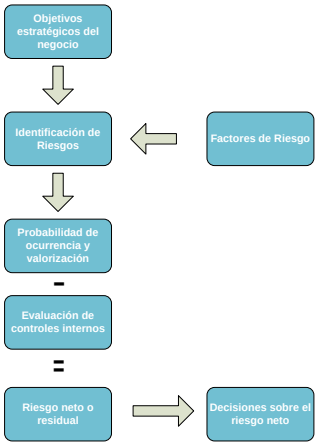


Figura 5.3 Fases de la elaboración de una matriz de riesgo

Consecuentemente, una vez establecidas todas las actividades, se deben identificar las fuentes o factores que intervienen en su manifestación y severidad, es decir los llamados "factores de riesgo o riesgos inherentes". El riesgo inherente es intrínseco a toda actividad, surge de la exposición y la incertidumbre de probables eventos o cambios en las condiciones del negocio o de la economía que puedan impactar una actividad. Los factores o riesgos inherentes pueden no tener el mismo impacto sobre el riesgo agregado, siendo algunos más relevantes que otros, por lo que surge la necesidad de ponderar y priorizar los riesgos primarios. Los riesgos inherentes al negocio pueden ser clasificados en riesgos crediticios, de mercado y liquidez, operacionales, legales y normativos estratégicos.

El siguiente paso consiste en determinar la "probabilidad" de que el riesgo ocurra y un cálculo de los efectos potenciales sobre el capital o las utilidades de la entidad. La valorización del riesgo implica un análisis conjunto de la probabilidad de ocurrencia y el efecto en los resultados; puede efectuarse en términos cualitativos o cuantitativos, dependiendo de la importancia o disponibilidad de información; en términos de costo y complejidad la evaluación cualitativa es la más sencilla y económica.

La valorización cualitativa no involucra la cuantificación de parámetros, utiliza escalas descriptivas para evaluar la probabilidad de ocurrencia de cada evento.

En general este tipo de evaluación se utiliza cuando el riesgo percibido no justifica el tiempo y esfuerzo que requiera un análisis más profundo o cuando no existe información suficiente para la cuantificación de los parámetros. En el caso de riesgos que podrían afectar significativamente los resultados, la valorización cualitativa se utiliza como una evaluación inicial para identificar situaciones que ameriten un estudio más profundo.

La evaluación cuantitativa utiliza valores numéricos o datos estadísticos, en vez de escalas cualitativas, para estimar la probabilidad de ocurrencia de cada evento, procedimiento que definitivamente podría brindar una base más sólida para la toma de decisiones, esto dependiendo de la calidad de información que se utilice.

Ambas estimaciones, cualitativa y cuantitativa, pueden complementarse en el proceso del trabajo de estimar la probabilidad de riesgo. Al respecto, debe notarse que si bien la valoración de riesgo contenida en una matriz de riesgo es mayormente de tipo cualitativo, también se utiliza un soporte cuantitativo basado en una estimación de eventos ocurridos en el pasado, con lo cual se obtiene una mejor aproximación a la probabilidad de ocurrencia del evento.

La valorización (Tabla 5.4) consiste en asignar a los riesgos calificaciones dentro de un rango, que podría ser por ejemplo de 1 a 5 (insignificante = 1, baja = 2, media = 3, moderada = 4 o alta = 5), dependiendo de la combinación entre impacto y probabilidad.

1	Insignificante
2	Baja

3	Media
4	Moderada
5	Alta

Tabla 5.4: Calificación RI

En la Figura 5.4 se puede observar un ejemplo de esquema de valorización de riesgo en función de la probabilidad e impacto de tipo numérico con escala:

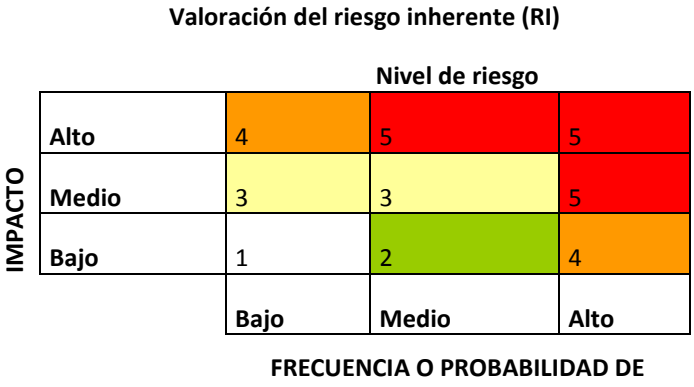


Figura 5.4 Ejemplo de esquema de valorización de riesgo

Una vez que los riesgos han sido valorizados se procede a evaluar la "calidad de la gestión", a fin de determinar cuán eficaces son los controles establecidos por la organización para mitigar los riesgos identificados. En la medida que los controles sean más eficientes y la gestión de riesgos pro-activa, el indicador de riesgo inherente neto tiende a disminuir. Por ejemplo una escala de valoración de efectividad de los controles podría ajustarse a un rango similar al siguiente (Tabla 5.5):

	Efectividad de los controles
1	Ninguno
2	Bajo
3	Medio
4	Alto
5	Destacado

Tabla 5.5: Escala de valoración de efectividad de los controles

Finalmente, se calcula el "riesgo neto o residual", que resulta de la relación entre el grado de manifestación de los riesgos inherentes y la gestión de mitigación de riesgos establecida por la administración. A partir del análisis y determinación del riesgo residual los administradores pueden

tomar decisiones como la de continuar o abandonar la actividad dependiendo del nivel de riesgos; fortalecer controles o implantar nuevos controles; o finalmente, podrían tomar posiciones de cobertura, contratando por ejemplo pólizas de seguro. Esta decisión está delimitada a un análisis de costo-beneficio y riesgo.

En la Tabla 5.6, se muestra la plantilla que se utiliza para calcular el riesgo neto o residual.

BANCO NACIONAL DE FOMENTO Matriz de Riesgos y Gestión GERENCIA NACIONAL DE RIESGOS Matriz de Riesgos y Calidad de Gestión PROCESO DE RELEASE					
PROCESO DE RELEASE	Nivel de riesgo	Calidad de gestión			Riesgo residual
		Tipo de medidas de control	Efectividad	Promedio	
FRAUDE INTERNO					
Manipulación fraudulenta, forjamiento de identidad o identificación					
Alteración fraudulenta de información					
Falsificación de firmas					
Falta de Verificación de datos (Intencional)					
Uso de información Confidencial					
Robo de claves de usuarios					
Uso no autorizado de claves					
Uso indebido de sistemas informáticos					
PERSONAS					
Desconocimiento de normativa aplicable					
Desconocimiento de políticas internas					
Extemporalidad en la ejecución de ordenes					
No validación de información					
Cálculos erróneos					
Confusión de valores, identidades, documentos o monedas					
Interpretación errónea de instrucciones					
Uso equivocado o inapropiado de información					
Olvidos					
Elaboración errónea de documentos					
Falta de Verificación de datos					
Mal uso de tecnología					
Interpretación errónea de información					
Falta de atención					
Introducir en los reportes información errónea que induzca a tomar decisiones equivocadas					
Generación errónea de información					
Ejecución de ordenes sin respaldo					
Interpretación errónea de instrucciones por idioma					
Ejecución de operaciones no autorizadas					
Revelación de información de clientes					
Introducción de datos inadecuados					
Mal uso de claves					
Documentar incorrectamente las operaciones					
Mala ejecución de ordenes					
No seguir el proceso adecuado para el diseño e implementación de cambios en los sistemas					
TECNOLOGIA					
Daño de equipos por razones no intencionales					
Daños al servidor					
Caída del sistema informático (por software)					
Caída del sistema informático (por hardware)					
Caída del sistema informático (por otros problemas internos de la institución)					
Caída del sistema informático (por problema externo a la institución)					
Imposibilidad de reconexión informática por falta de respaldo					
Imposibilidad de reconexión informática por falta de equipo secundario					
Bloqueo de servicio telefónico (causa externa)					
Bloqueo de servicio telefónico (causa interna)					
Interrupción de Internet-Correo electrónico					
Interrupción de servicio eléctrico (causa externa)					
Interrupción de servicio eléctrico (causa interna)					
PROCEDIMIENTOS, NEGOCIOS Y PRODUCTOS					
Falla procesos de capacitación de RRHH					
Falla procesos de evaluación de RRHH					
Equipo alta tecnología					
Perfil de riesgo					

Tabla 5.6 Plantilla de Matriz de Riesgo para el Proceso de Release

La plantilla referida, muestra en forma consolidada, los riesgos inherentes a una actividad o línea de negocio, el nivel o grado de riesgo ordenado de mayor a menor nivel de riesgo (priorización); las medidas de control ejecutadas con su categorización promedio y finalmente, se expone el valor del riesgo residual para cada riesgo y un promedio total que muestra el perfil global de riesgo de la línea de negocio.

Como se puede determinar, la matriz de riesgo tiene un enfoque principalmente cualitativo, para lo cual es preciso que quienes la construyan tengan experiencia, conocimiento profundo del negocio y su entorno y un buen juicio de valor, pero además es requisito indispensable la participación activa de todas las áreas de la entidad.

5.5.2 MATRIZ DE RIESGO Y EL NUEVO ENFOQUE DE SUPERVISION

En las últimas dos décadas los documentos publicados por el Comité de Basilea han tenido un gran impacto en el mundo de la supervisión bancaria, tanto en la regulación como en la práctica supervisora. Los principios establecidos en el Pilar 2 del documento consultivo del Comité de Basilea II, representan la base para reenfocar la supervisión, asignándole una doble finalidad: por un lado, asegurar que las entidades tienen el capital adecuado a sus riesgos y, por otro, alentar el desarrollo y uso de técnicas de gestión y control de riesgos.

En este contexto, Organismos Supervisores en diferentes países están en proceso de implementación de metodologías de supervisión basadas en la gestión de riesgos. Entre las experiencias desarrolladas podemos citar a la Office of the Superintendent of Financial Institutions (OSFI) de Canadá y al Banco de España.

En ambos casos la matriz de riesgos constituye una herramienta clave en el proceso de supervisión basada en riesgos, debido a que la misma les permite efectuar una evaluación cualitativa y cuantitativa de los riesgos inherentes de cada unidad de negocios o actividad significativa y la determinación del perfil de riesgo de la institución.

Los beneficios de esta metodología de supervisión, entre otros, son los siguientes:

- Identificación de instituciones que requieren mayor atención y áreas críticas de riesgo.
- Uso eficiente de recursos aplicados a la supervisión, basado en perfiles de riesgos de las entidades.
- Permite la intervención inmediata y la acción oportuna.
- Evaluación metódica de los riesgos.
- Promueve una sólida gestión de riesgos en las instituciones financieras.
- Monitoreo continuo.

De esta manera la matriz de riesgo permite establecer de un modo uniforme y consistente el perfil de riesgo de cada una de las entidades y permite profundizar en el proceso de establecimiento de planes de supervisión a fin de que se ajusten a las características específicas de cada entidad.

Tomado de:

Material Bibliográfico durante la participación al Diplomado de Gestión y Administración Integral de Riesgos. SCALAR CONSULTING. OCTUBRE 2007

5.6 PLAN DE CONTINGENCIA TECNOLOGICO

Es necesario identificar las principales escenarios de riesgo tomando en cuenta el impacto y la probabilidad de que sucedan; el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar aquellos eventos de riesgo.

Considerando los componentes que integran la arquitectura de la solución, a continuación un diagrama de red que los ilustra antes de describir los posibles escenarios de fallos:

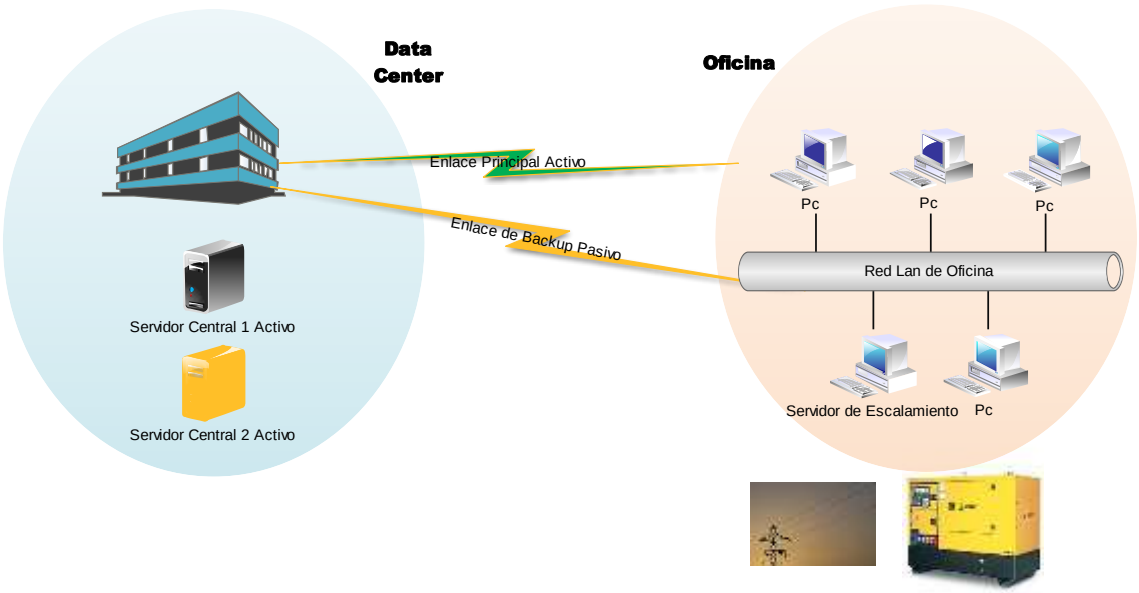


Figura 5.5 Diagrama de red

Data center.

El centro de datos deberá adoptar medidas de restauración de servicios básicos a través de un adecuado manejo y provisión de energía eléctrica alterna (grupo electrógeno).

La calidad de la energía eléctrica que llegue a la sensible infraestructura que llegue al data center debe estar estabilizada y protegida por sistemas redundantes de UPS's que a la vez cumplan el rol preventivo en caso de suspensión total de energía eléctrica y garanticen una adecuado apagado controlado de todos los equipos.

Las condiciones adecuadas de climatización que garanticen la temperatura correcta para todos los equipos que en el resida debe estar soportada por un sistema de aire acondicionado de precisión que cubra la disipación de calor actual y la proyectada.

El sistema de detección y extinción de incendios es obligatorio implementar protegiendo las áreas críticas como son las de servidores, monitoreo, cintoteca y UPS's.

Es mandatorio cubrir el control adecuado del nivel de acceso a las áreas críticas del data center para lo cual se debe contar con un sistema de control de accesos con tarjeta de aproximación y en las áreas más criticas un sistema mixto con lectura biométrica.

El monitoreo del estado de la infraestructura así como el movimiento permanente del área de monitoreo debe ser registrado en un CCTV que permita mantener históricos de los eventos suscitados y que además esté conectado al área del seguridad central del edificio.

Teniendo en cuenta que toda la información que se genera y procesa en la institución está sujeta a una política de respaldo solicitada y definida por el usuario o dueño de la misma, es responsabilidad de la

Gerencia Nacional de Sistemas como custodio del estado de esta información reducir al mínimo la posibilidad de pérdida total a través de un servicio de resguardo de la información fuera de la institución. De la misma manera se garantiza por este medio disponer de un punto de restauración de las configuraciones tanto a nivel de sistema operativo como de aplicaciones para toda la infraestructura tecnológica que soporta los servicios que oferta la institución. Hoy en día existen instituciones que ofertan este servicio y garantizan la correcta custodia de los dispositivos de almacenamiento entregados guardando altos esquemas de seguridad en el traslado de la información.

Herramienta para distribución de software.

El concepto de clusterización para el servidor que soporta el servicio que permite automatizar la distribución de software debe ser adoptado en función de la capacidad financiera y de infraestructura que disponga la organización. Actualmente la virtualización es un concepto que ha tomado mucha fuerza y que no permite desperdiciar recursos de los servidores asignados, balaceando la carga que manejan y estando en la capacidad de absorber en uno solo el nivel de procesamiento si uno de ellos sufre una degradación o indisponibilidad.

Enlace de comunicación.

Desde el punto de vista del negocio, garantizar la permanente comunicación de la oficina con el data center principal requiere una doble inversión que únicamente se ve justificada con los réditos financieros que la localidad reporte. Sin embargo desde el punto de vista tecnológico la disponibilidad del servicio no tiene precio y muchas veces obliga a tener componentes pasivos que siendo un gasto, reportan ganancias intangibles como la imagen, reputación y calidad del servicio. Un adecuado SLA debe ser contratado y exigido al proveedor del sistema de comunicación.

Oficina.

El servicio de energía eléctrica al ser provisto por un tercero y no depender de la institución de forma directa debe ser garantizado a través de un grupo electrógeno que provea energía eléctrica continua y un UPS que garantice un apagado controlado de todas la infraestructura tecnológica que soporta a la oficina.

La red interna de datos y los dispositivos de comunicación que la habilitan son susceptibles de fallos o interrupciones que pueden significar la indisponibilidad de todos los servicios para la localidad; por lo tanto es necesario en la medida de lo posible de contar con procedimientos de mantenimiento preventivo y correctivo que garanticen el buen estado de los dispositivos y de ser necesario su reemplazo en tiempos de respuesta adecuados en sitio.

CAPITULO VI

6.1 PLAN DE IMPLEMENTACION DEL PROCESO DE RELEASE MANAGEMENT EN EL BNF

Programa	Líneas de acción	Productos / resultados esperados	Actividades	Responsable	Plazo
1. Estructura organizacional del área de Release					
Conformación administrativa del área de Release	Recurso Humano	Unidad de Release estructurada	Definir la estructura organizacional a nivel de Dirección, que dentro de la Gerencia Nacional de Sistemas, tendrá a cargo el proceso Seleccionar personal de acuerdo al perfil del cargo descrito mínimo un administrador de Versionamiento y dos especialistas de despliegue y Versionamiento Entrenamiento e inducción al personal en el proceso a cargo Integración de la unidad organizacional dentro de la Gerencia Nacional de Sistemas	Gerente Nacional de Sistemas	Diciembre 2009
2. Infraestructura Tecnológica para el proceso de Release					
Infraestructura tecnológica	Software	Herramienta de Control de Fuentes Herramienta de Despliegue	Analizar herramientas existentes en el mercado informático Iniciar proceso de adquisición de la herramienta elegida Implementar la herramienta en ambiente de Producción Capacitar al responsable de Control de Fuentes definido	Administrador de Despliegue y Versionamiento	Marzo 2010

			Implementar el proceso en la herramienta en ambiente de Producción		
	Hardware	Servidor que soporte las herramientas para control de fuentes y despliegue	Analizar el hardware requerido de acuerdo a las necesidades de las herramientas adquiridas Iniciar proceso de adquisición del hardware Implementar el hardware en ambiente de Producción Implementar la herramienta en el hardware adquirido Desarrollar los planes de contingencia que garanticen alta disponibilidad del servicio en concordancia con la criticidad del mismo	Director de Infraestructura	Marzo 2010
3. Subproceso de Definición de Políticas de Release					
Definición de Políticas de Release	Normativa Interna	Políticas, Estándares y Procedimientos para el proceso de Release, definidos, aprobados y difundidos	Diseñar y definir la política Elaborar, revisar y corregir la Política Aprobar la Política Solicitar la inclusión de la política en el Manual de Sistema de Gestión de Seguridad de la Información Difundir las políticas a las áreas operativas	Director de Producción	Marzo 2010
4. Subproceso de Control de Fuentes					
Control de Fuentes	Documentación	Estándares y normativa para el proceso	Definir la norma para el Control de Fuentes. Determinar el estándar de Versionamiento para el control de versiones	Director de Producción	Marzo 2010
5. Diseño y Configuración del Roll-Out					
Diseño y Configuración del Roll-Out	Infraestructura	Ambiente de compilación seguro	Documentación a nivel de CI's actualizada (Gestión de Configuración) para crear los ambientes requeridos	Administrador de Despliegue y	

			dependiendo de cada aplicación	Versionamiento Especialista de Configuración Analista de Service Desk	
	Documentación	Generación eficaz y eficiente de paquete de distribución	Procedimiento para documentación de Requerimiento de Cambio y Estándar de Ejecución RFC	Administrador de Control de Cambios	Diciembre de 2009
6. Planificación del Roll-Out					
Planificación del Roll-Out	Documentación	Procedimiento de implantación de una nueva versión adecuada	Levantamiento y actualización de catálogo de servicios de la institución Levantamiento y revisión de los acuerdos de niveles de servicio para los servicios de misión crítica y no crítica Definición de dueños de la información	Director de Producción Especialista de Configuración Seguridad de la Información	Marzo 2010
7. Certificación Unitaria previa al Roll-Out masivo					
Certificación Unitaria	Infraestructura	Ambiente confiable para la certificación con los valores de CI's validados	Ambientes de pre-producción, Back-End y Front-End controlados y similares a producción Elementos de configuración actualizados	Director de Producción Especialista de Configuración	Marzo 2010
	Documentación	Proceso de certificación unitaria eficaz y eficiente	Procedimiento para documentación de Requerimiento de Cambio especificando el rol y la responsabilidad del usuario certificador	Especialista de Control de Cambios	
8. Logística para el Roll-Out masivo					
Logística	Infraestructura	Alto porcentaje de éxito de la distribución	Definir la infraestructura operacional de la distribución (infraestructura, equipos de escritorio, personas, proveedores) Establecer planes preventivos correctivos sobre la	Administrador de Despliegue y Versionamiento	Marzo 2010

			infraestructura del servicio de despliegue y Versionamiento		
	Comunicación	Minimizar el impacto de la liberación de una nueva versión	Comunicar eficientemente a los usuarios sobre el despliegue de una nueva versión de software Establecer planes de manejo de incidencias personalizados para cada liberación de una nueva versión	Administrador de Despliegue y Versionamiento Administrador de Service Desk	Marzo 2010
9. Ejecución del Roll-Out masivo					
Ejecución de Roll-Out	Infraestructura	Ejecutar eficaz y eficientemente el roll-out del release probado	Disponer de un plan de continuidad y alta disponibilidad para la infraestructura que soporta el software de despliegue Disponer de un soporte 7x24 para la infraestructura y el software de despliegue Disponer de un acuerdo de niveles de servicios con proveedores de enlace que garantice la disponibilidad del servicio en un alto porcentaje (aceptable 99.5%)	Administrador de Infraestructura Administrador de Despliegue Administrador de Comunicaciones	Marzo de 2010
	Documentación	Garantizar la correcta ejecución del Roll-Out	Obtener y revisar dentro de un proceso de mejora continua el Documento de planificación del Roll-Out	Administrador de Despliegue	
10. Gestión de Niveles de Servicio					
OLA	Documentación	Acuerdo de Niveles Operacionales con las áreas relacionadas al proceso de release	Identificar las áreas internas relacionas con el proceso Establecer el objetivo de operación del servicio Identificar los servicios y los tiempos de entrega de los mismos Confirmar con las áreas involucradas Formalizar el acuerdo establecido con las firmas de los responsables de las áreas involucradas	Gestión de Disponibilidad	Marzo de 2010

SLA	Documentación	Acuerdos de Niveles de Servicio con los proveedores que soportan técnicamente la infraestructura tecnológica de release	Identificar los proveedores externos de la infraestructura tecnológica de release Describir las características del servicio Definir los horarios de misión crítica Describir el tipo de soporte técnico y tipificar las incidencias Definir tiempos de respuesta adecuados dentro del horario de misión crítica y fuera de él Establecer las acciones preventivas para garantizar el correcto estado del servicio Definir las penalidades por incumplimiento de los niveles establecidos	Gestión de Disponibilidad	Marzo de 2010

6.2 ANALISIS COSTO BENEFICIO DE LA PROPUESTA DE IMPLEMENTACION DEL PROCESO DE RELEASE MANAGEMENT PARA BNF

El Banco Nacional de Fomento en su afán de mejorar cada vez más su infraestructura operativa; debe realizar esfuerzos permanentes para adoptar nuevas tecnologías que ofrezcan ventajas competitivas, que cumplan con los estándares de disponibilidad, seguridad y soporte.

La institución necesita optimizar los procesos de inventario de software y equipos físicos, como también distribuir software de forma calendarizada y automática, lo mismo que permitir al personal de Service Desk, controlar una estación de trabajo para identificar de forma rápida y eficaz las posibles causas de un incidente y de esta manera brindar sistemas más manejables y automatizar operaciones que se llevan a cabo de forma manual o semiautomática. Con ello se consigue importantes reducciones de costos, se mejora la disponibilidad de las aplicaciones y se puede brindar un mejor servicio. La infraestructura de equipos de escritorio que dispone el BNF en todas las oficinas a nivel nacional es de 3100 equipos.

Desde Marzo 26 de 2009, hasta la presente fecha, se han realizado más de 800distribuciones categorizadas como lo describe la tabla 6.1:

Tabla 6.1 - Detalle distribuciones de software

Categoría del despliegue	Número de Paquetes	Número de distribuciones realizadas
Software de Aplicaciones	215	1.086
Software Core Bancario	520	19.606
Utilitarios	100	1.093
Total general	**835**	**31.432**

Beneficios Relevantes y optimización de tiempo y recursos

El Proyecto de implementación del Core Bancario, por su arquitectura de aplicación requiere que tanto en el servidor central, como en cada uno de los equipos que se conectan para hacer uso cada uno de los módulos; deba ser actualizado sus programas ejecutables, librerías, archivos, scripts, etc., simultáneamente.

Con este antecedente, en la tabla 6.2 se describe el cálculo del tiempo de una distribución manual, tomando como ejemplo una distribución real que consta de cuatro paquetes de software, con un peso de 34.7 MB;el destino de la distribución son la totalidad de equipos del banco agrupados en nueve zonales; se cuenta con recursos técnicos, los cuales ejecutan sus labores de analistas de Service Desk y para este caso, realizan el proceso de actualización en un tiempo promedio de 26 minutos, en un escenario ideal, con enlaces 100% operativos y con ocho horas laborables ininterrumpidas de trabajo.

Tabla 6.2 - Calculo de tiempo en distribución Manual

Zonal BNF	Número de Analistas de Service Desk por Zonal	Número de equipos por Analista	Tiempo por equipos en minutos	Tiempo por equipos en horas	Tiempo por equipos en días
Cuenca	1	153	3978	66	8
Guayaquil	5	543	2824	47	6
Loja	1	222	5772	96	12
Machala	1	157	816	14	2
Portoviejo	1	264	6864	114	14
Puyo	1	245	6370	106	13
Quito	6	916	3969	66	8
Riobamba	1	267	6942	116	14
Santo Domingo	1	263	1140	19	2
Total	**18**	**3030**	**38675**	**645**	

Los cálculos indican que trabajando en paralelo, interrumpiendo las labores de atención al público, este trabajo podría ser concluido en un tiempo de 14 días (laborables), es decir alrededor de tres semanas calendario. Trabajar un mayor número de horas o, en días no laborables, implica para el BNF, pago de horas extras al personal involucrado. Incluir mayor personal en la tarea, significa contratar más recursos permanentes, lo cual no es coherente con la política de racionalización de personal impuesta para toda institución pública.

Implementando Release Managementcomo se ha propuesto a lo largo del presente trabajo, se evidencia que:

1. El número de recursos técnicos necesarios para la ejecución de la misma tarea, es de 3.
2. El tiempo de distribución, al ser el despliegue masivo y asíncrono,se reduce a horas de ejecución en el total de equipos solicitado.
3. No es necesario efectuar interrupciones de la aplicación que está siendo actualizada, por lo tanto es factible programar la distribución fuera de horario de atención al público.
4. Se tiene un control centralizado de las incidencias que se pudieran generar producto de la distribución para atenderlas de forma eficaz y eficiente.

La tabla6.3 permite visualizar en forma numérica lo comentado:

Tabla 6.3Calculo de tiempo en distribución Automática

Zonal BNF	Número técnicos de Release en Casa Matriz	Número de equipos por Analista	Tiempo por equipos en minutos	Tiempo por equipos en horas	Tiempo por equipos en días
Cuenca	3	153	90	1:14	0,05
Guayaquil		543			
Loja		222			
Machala		157			
Portoviejo		264			
Puyo		245			
Quito		916			
Riobamba		267			
Santo Domingo		263			
Total	**3**	**3030**	**90**	**1,14**	**0,05**

Consideraciones para la implementación de Release Management

Recursos Humanos

Actualmente el proceso de distribución de software se lo ejecuta a través de 18 recursos contratados cuya actividad esencial no es la de ejecutar distribuciones masivas de software. Con la implementación de esta propuesta, como se observa en la tabla 6.4, se debe disponer únicamente de un administrador del proceso y dos técnicos que cumplan con el perfil adecuado y realicen las actividades descritas en cada subproceso establecido.

Tabla 6.4 - Cuadro comparativo desde el punto de vista de Recursos Humanos

Sin Release Management	Con Release Management
18 Recursos: Analistas de Service Desk, cuya función principal es dar soporte de primer nivel a los requerimientos e incidencias ingresadas por la herramienta de Service Desk, dedicados a tiempo completo en caso de distribuciones a ejecutar procesos manuales de instalación y desinstalación de software de aplicaciones del Banco.	3 Recursos: 1 Administrador de despliegue y versionamiento, responsable de gestionar el proceso de Release y de interactuar con las áreas involucradas 2 Especialistas de Despliegue y versionamiento, responsables de la ejecución de los planes de despliegue certificados y probados.

Procesos

Al implementar todos los subprocesos planteados, se optimizaran los tiempos de ejecución, se logrará un adecuado nivel de reutilización para los procedimientos conocidos; los niveles de responsabilidad y autorización adecuados garantizaran la disponibilidad e integridad de las versiones liberadas en producción, así como también se logrará cumplir con los acuerdos de niveles de servicio establecidos para los usuarios finales. La inexistencia de subprocesos definidos antes de implementar release en forma óptima, se evidencia claramente en la tabla 6.5

Tabla 6.5 - Cuadro comparativo desde el punto de vista de Procesos

Sin Release Management	Con Release Management
Existe un proceso de Control de Fuentes definido que permite únicamente llevar un historial de cambios en las versiones de los programas para las diferentes aplicaciones	Se definen siete subprocesos que permiten gestionar y controlar la liberación de nuevas versiones en producción de una manera integral considerando los riesgos inherentes, definiendo políticas, planificando las actualizaciones, certificando la distribución en ambientes de pre-producción, desarrollando planes de apoyo a la distribución, comunicando adecuadamente los cambios esperados y manejando en forma eficaz los incidentes post-producción.

Infraestructura

La automatización del proceso de Release permite ofertar tiempos óptimos de ejecución de la distribución, tanto en condiciones normales como emergentes, manteniendo la continuidad del servicio para los productos que ofrece la institución a sus clientes.

La inversión a este nivel, tanto de software (Herramienta para despliegue y versionamiento) como de hardware (servidor principal, servidor de backup, servidores de oficina, almacenamiento para los datos) sobre el cual soportar el servicio; debe estar apoyada por un plan de alta disponibilidad, así como medidas de contingencia para la infraestructura provista por terceros; además de contar con estrictos acuerdos de niveles de servicio que se deben establecer para todos los componentes del servicio de Release. La tabla 6.6, ilustra la inversión en infraestructura que se requiere para viabilizar el plan de implementación propuesto.

Tabla 6.6 - Cuadro comparativo desde el punto de vista de Infraestructura Tecnológica

Sin Release Management	Con Release Management
Herramienta de Control de Fuentes Servidor de aplicaciones para herramienta de control de fuentes Normativa para el versionamiento Plan de respaldos para la Base de datos de control de fuentes	• Herramienta de Despliegue y Versionamiento • Servidor de aplicaciones para la Herramienta de despliegue y Versionamiento • Librería de Software Definitivo (DSL) • CMDB • Almacenamiento para la (DSL) y la CMDB • Plan de contingencia tecnológico para la Herramienta de despliegue y versionamiento • SLA´s con proveedores • OLA´s con áreas internas de la Gerencia Nacional de Sistemas. • Planes de Respaldo de los datos

Costo Beneficio

A continuación, en la tabla 6.7, se compara el costo beneficio evidenciado en tiempo y salario de un técnico que ejecuta las mismas tareas de la herramienta que apoya el proceso de distribución, siguiendo un estándar de ejecución, con un nivel de riesgo bastante alto por la omisión involuntaria de lo especificado en el estándar de ejecución; contra la funcionalidad de una herramienta, correctamente administrada y parametrizada, con un proceso definido en constante mejora, que optimiza tiempos y remuneraciones de recursos humanos, minimiza tiempos de indisponibilidad de servicios críticos, con un nivel controlable de fallas que está en función de los componentes externos como enlaces de comunicación, energía eléctrica, entre otros.

Tabla 6.7 - Análisis desde el punto de vista de Tiempo y Costo

	Sin Release Management	Con Release Management
Tiempo en horas para una distribución	645 Horas	1:14 Horas
Número de Recursos involucrados	18 personas (analistas de Service Desk)	3 personas:1 administrador y dos especialistas
Valor de las 31.432 distribuciones realizadas en función del salario de un técnico (*)	645 Horas x USD 4,19 = USD 2702,55	1,14 Horas x USD 4,19 x 3 = USD 14,32

(*) El cálculo del valor de una hora de trabajo está en función de la denominación del cargo y la escala salarial asignada

La relación costo beneficio, justifica financiera y operativamente la implementación de esta propuesta por parte de la Gerencia Nacional de Sistemas.

CONCLUSIONES

1. Se ha logrado identificar y determinar la adecuada gestión de recursos en la administración del proceso de Release Management, que permita controlar y monitorear la exposición a cierto tipo de riesgo que pudiese causar un alto impacto en la disponibilidad del servicio que soporta la infraestructura tecnológica del Banco Nacional de Fomento.

2. El marco de referencia ITIL aplicado por la Gerencia Nacional de Sistemas ha permitido identificar las áreas involucradas en el proceso de Release Management así como el perfil técnico de sus actores y el nivel de responsabilidad requerido.

3. La arquitectura del Core Bancario adquirido por el Banco Nacional de Fomento requiere de un estricto control de versión entre el cliente y el servidor central, por lo tanto, se ha establecido que hay una relación directamente proporcional entre, el nivel de complejidad de la solución bancaria y la importancia de la administración eficaz del proceso de Release Management.

4. Se ha identificado la importancia de contar con una herramienta que permita automatizar el proceso de Release Management en concordancia con la gran cobertura geográfica del Banco Nacional de Fomento y la complejidad de sus operaciones.

5. Es necesaria la aplicación de una metodología para la identificación de los riesgos inherentes a cada subproceso y obtener una medida sobre el impacto de cada uno de ellos en el objetivo final, de tal manera que se establece la necesidad de definir controles adecuados para que estos riesgos sean gestionados en base a lo estipulado en la normativa de la entidad de supervisión.

6. El enfoque del levantamiento del proceso de Release Management desde el punto de vista técnico de la Gerencia Nacional de Sistemas y del punto de vista de riesgo operativo de la Gerencia Nacional de Riesgos, permitió construir un proceso eficaz, eficiente y viable de implementar en el contexto de una Institución Financiera Pública.

RECOMENDACIONES

1. Al implementar el proceso de Release Management es necesario otorgar un alto nivel de importancia en la selección del recurso humano, la tecnología que soporte el servicio, la implementación de cada uno de los subprocesos definidos y los adecuados y probados planes de contingencia que garanticen la disponibilidad del servicio que provee este proceso.

2. La administración del proceso de Release Management debe ser formalizado a través de las instancias autorizadas para garantizar el compromiso y apoyo antes, durante y posterior a su implementación.

3. La administración del proceso de Release Management debe ser socializada a través de los canales disponibles a fin de garantizar el total conocimiento de las acciones y responsabilidades de sus actores.

4. La permanente gestión de riesgo operativo que toda institución financiera controlada está obligada a cumplir, debe verse como un proceso de mejora continua y no como el establecimiento de controles estáticos que nunca evolucionarán.

5. La pertenencia de la institución financiera a un sector (público o privado), no debe condicionar la implementación del proceso de Release Management dentro de la organización, tomando en cuenta que el objetivo de calidad en la entrega de servicio es en la actualidad un termómetro de efectividad y eficiencia de toda institución.

ANEXOS

ANEXO 2.1 ADMINISTRADOR DE DESPLIEGUE Y VERSIONAMIENTO

Sección 1: DATOS DE IDENTIFICACIÓN

Institución: Banco Nacional de Fomento	**Unidad: Producción**
Puesto: Administrador de Despliegue y Versionamiento	**Código:**
Nivel: Profesional	**Puntos: 675**
Grupo Ocupacional: Servidor Público 4	**Grado:**
Rol del Puesto: Ejecución y supervisión de procesos	

Sección 2: MISIÓN DEL PUESTO

Establecer una política de implementación de nuevas versiones de hardware y software.

Implementar las nuevas versiones de software y hardware en el entorno de producción tras su verificación en un entorno realista de pruebas.

Garantizar que se mantengan debidamente protegidas y archivadas copias idénticas del software en producción, así como de toda su documentación asociada.

Sección 3: ACTIVIDADES DEL PUESTO

Se definen las actividades relevantes que permanentemente se llevan a cabo y que además serán las consideradas para la evaluación del desempeño del cargo que la institución ejecuta dos veces al año.

Actividades del Puesto	F	CO	CM	Total
Planificar la distribucion de software de las aplicaciones centralizadas de la institucion	4	4	4	20
Planificar las pruebas de validación de la distribución de software a través de herramienta	4	3	4	16
Garantizar la confiabilidad de la versión de los programas fuentes en la herramienta para control de versionamiento Visual Source Safe	4	4	4	20
Realizar durante el período de implementación, la distribución para los diferentes ambientes tecnológicos de: pruebas y capacitación de los diferentes módulos del sistema integrado bancario	2	4	4	18
Certificar con el usuario en ambiente de pre-producción la distribución planificada.	4	4	4	20
Implementar los planes de roll-back para minimizar el posible impacto negativo sobre el servicio y la integridad del sistema TI después de una	4	4	3	16

distribución.				
Administrar los recursos humanos y técnicos necesarios para llevar a cabo la implementación de la nueva versión con garantías de éxito.	4	4	3	16
Desarrollar los planes de comunicación y/o formación para que los usuarios estén puntualmente informados y puedan percibir la nueva versión como una mejora.	4	4	4	20
Evaluar el impacto que puede tener el proceso de lanzamiento de una nueva versión en la calidad del servicio.	4	4	4	20

Donde:

F = frecuencia de la actividad

CO = consecuencias por omisión de la actividad

CM = complejidad de la actividad

Total = F + (CO x CM)

Sección 4: INTERFAZ DEL PUESTO

Especifica por cada actividad relevante, el/los beneficiarios de la ejecución de esa tarea

Actividades Esenciales	Interfaz Nombres de las unidades, puestos, clientes, usuarios o beneficiarios directos de la actividad.
Planificar la distribución de software de las aplicaciones centralizadas de la institucion	**Clientes** **Usuarios de sistemas informáticos**
Planificar las pruebas de validación de la distribución de software a través de herramienta	**Clientes** **Usuarios de sistemas informáticos**
Certificar con el usuario en ambiente de pre-producción la distribución planificada.	**Clientes** **Usuarios de sistemas informáticos**
Implementar los planes de roll-back para minimizar el posible impacto negativo sobre el servicio y la integridad del sistema TI después de una distribución.	**Clientes** **Usuarios de sistemas informáticos**
Desarrollar los planes de comunicación y/o formación para que los usuarios estén puntualmente informados y puedan percibir la nueva versión como una mejora.	**Clientes** **Usuarios de sistemas informáticos**

Sección 5: CONOCIMIENTOS REQUERIDOS

Define los conocimientos técnicos (adquiridos a través de la formación académica) indispensables para la ejecución de las actividades relevantes especificadas para el cargo

Actividades esenciales	Conocimientos

Planificar la distribución de software de las aplicaciones centralizadas de la institucion	Ingeniería en Procesos Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco
Planificar las pruebas de validación de la distribución de software a través de herramienta	Ingeniería en Procesos Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco
Certificar con el usuario en ambiente de pre-producción la distribución planificada.	Ingeniería en Procesos Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco
Implementar los planes de roll-back para minimizar el posible impacto negativo sobre el servicio y la integridad del sistema TI después de una distribución.	Ingeniería en Procesos Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco
Desarrollar los planes de comunicación y/o formación para que los usuarios estén puntualmente informados y puedan percibir la nueva versión como una mejora.	Ingeniería en Procesos Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco

Sección 6: INSTRUCCIÓN FORMAL REQUERIDA

Nivel de Instrucción Formal	Especifique el número de años de estudio o los diplomas / títulos requeridos	Indique el área de conocimientos formales (ejemplo, administración, economía, etc.).
Ingeniería	**5 años**	**Sistemas / Procesos**

Sección 7: EXPERIENCIA LABORAL REQUERIDA

Dimensiones de Experiencia	Detalle
Tiempo de experiencia	**2-5 años**

Especificidad de la experiencia	Actividades de informática
Contenido de la experiencia	Ingeniería en Procesos
	Seguridad de la Información
	Redes y Comunicación
	Manejo de equipos
	Inglés Técnico nivel medio

Sección 8: DESTREZAS TÉCNICAS (ESPECÍFICAS) REQUERIDAS

Sujetas al Catálogo de Competencias Técnicas del Ministerio de Relaciones Laborales

Destrezas	Definición	Relevancia		
		Alta	Media	Baja
Recopilación de información	Conocer cómo localizar e identificar información esencial.		X	
Selección de equipos	Determinar el tipo de equipos, herramientas e instrumentos necesarios para realizar un trabajo.		X	
Comprensión oral	Es la capacidad de escuchar y comprender información o ideas presentadas.	X		
Expresión oral	Es la capacidad de comunicar información o ideas en forma hablada de manera clara y comprensible.	X		
Comprensión escrita	La capacidad de leer y entender información e ideas presentadas de manera escrita.	X		
Administración del Desempeño	La Administración del Desempeño es un enfoque sistemático aplicado a la administración de personal –del día a día– en el ambiente de trabajo, orientado a evaluar los resultados esperados en la ejecución de un proceso; utilizando el "acompañamiento" como recurso principal para optimizar los resultados.	X		
Educación y capacitación	Es la educación tendiente a ampliar, desarrollar y perfecciona los conocimientos que permita un crecimiento profesional para que se vuelva más eficiente y productivo en su cargo.	X		

Sección 9: DESTREZAS / HABILIDADES CONDUCTUALES (GENERALES)

Sujetas al Catálogo de Competencias Conductuales del Ministerio de relaciones Laborales

Destrezas	Definición	Relevancia		
		Alta	Media	Baja
Trabajo en equipo	Es el interés de cooperar y trabajar de manera coordinada con los demás.	X		
Orientación de servicio	Implica un deseo de ayudar o de servir a los demás satisfaciendo sus necesidades. Significa focalizar los esfuerzos en el descubrimiento y la satisfacción de las necesidades de los clientes, tanto internos como externos.	X		
Orientación a los resultados	Es el esfuerzo por trabajar adecuadamente tendiendo al logro de estándares de excelencia.	X		
Actitud al cambio	Es la predisposición a generar, desarrollar y promover cambios positivos acorde a los objetivos y metas organizacionales.	X		
Relaciones Humanas	Es la habilidad de construir y mantener relaciones cordiales con personas internas o externas a la organización.	X		
Conocimiento del entorno organizacional	Es la capacidad para comprender e interpretar las relaciones de poder e influencia en la institución o en otras instituciones, clientes o proveedores, etc. Incluye la capacidad de prever la forma en que los nuevos acontecimientos o situaciones afectarán a las personas y grupos de la institución.	X		
Iniciativa	Es la predisposición para actuar proactivamente. Los niveles de actuación van desde concretar decisiones tomadas en el pasado hasta la búsqueda de nuevas oportunidades o soluciones a problemas.	X		
Aprendizaje continuo	Es la habilidad para buscar y compartir información útil, comprometiéndose con el aprendizaje. Incluye la capacidad de aprovechar la experiencia de otros y la propia.	X		

Sección 10: REQUERIMIENTOS DE SELECCIÓN Y CAPACITACIÓN

Conocimientos / Destrezas	Requerimiento de Selección	Requerimiento de Capacitación
Conocimientos		
Seguridad de la Información	X	
Redes y Comunicación	X	
Manejo de equipos	X	
Sistemas Operativos	X	
Sistemas informáticos del Banco		**X**

Inglés Técnico nivel medio	X	
Instrucción Formal		
Ingeniería en Sistemas / Procesos	X	
Contenido de la Experiencia		
Desarrollo de sistemas informáticos	X	
Operación de equipos de cómputo	X	
Análisis y diseño de sistemas	X	
Destrezas Técnicas y Conductuales		
Recopilación de información	X	
Selección de equipos	X	
Comprensión oral	X	
Expresión oral	X	
Comprensión escrita	X	
Administración del Desempeño		**X**
Educación y capacitación	X	
Trabajo en equipo	X	
Orientación de servicio	X	
Orientación a los resultados	X	
Actitud al cambio	X	
Relaciones Humanas	X	
Conocimiento del entorno organizacional		**X**
Iniciativa	X	
Aprendizaje continuo	**X**	

Sección 11: VALORACIÓN DEL PUESTO

Corresponde al resultado del cálculo del puesto, basado en la tabla establecida por el Ministerio de Relaciones Laborales para el efecto.

COMPETENCIAS				COMPLEJIDAD DEL PUESTO		RESPONSABILIDAD	
Instrucción formal	Experiencia	Habilidades		Condiciones de trabajo	Toma de decisiones	Rol del puesto	Control de resultados
		Gestión	Comunicación				

Profesional	2 años	Nivel 4	Nivel 4	Nivel 1	Nivel 3	Supervisión	**Nivel 4**
155	50	80	80	20	60	150	**80**
675 puntos							

ANEXO 2.2 ESPECIALISTA DE DESPLIEGUE Y VERSIONAMIENTO

Sección 1: DATOS DE IDENTIFICACIÓN

Institución: Banco Nacional de Fomento	**Unidad: Producción**
Puesto: Especialista de Despliegue y Versionamiento	**Código:**
Nivel: Profesional	**Puntos: 475**
Grupo Ocupacional: Servidor Público de Apoyo 4	**Grado:**
Rol del Puesto: Ejecución de procesos de apoyo y tecnológico	

Sección 2: MISIÓN DEL PUESTO

Diseñar e implementar procedimientos eficientes para la distribución y la instalación de los cambios de los sistemas TI.

Asegurar que el hardware y el software que son cambiados sean revisables, seguros y que sólo las versiones correctas, autorizadas y probadas sean instaladas.

Comunicar y manejar las expectativas del cliente durante la planificación y despliegue de nuevas versiones de los sistemas informáticos.

Asegurar que las copias maestras de todo el software estén aseguradas en la biblioteca definitiva del software.

Sección 3: ACTIVIDADES DEL PUESTO

Se definen las actividades relevantes que permanentemente se llevan a cabo y que además serán las consideradas para la evaluación del desempeño del cargo que la institución ejecuta dos veces al año.

Actividades del Puesto	F	CO	CM	Total
Desplegar agentes de herramienta para distribución de software de los equipos de escritorio de toda la organización	4	4	3	16
Actualizar el estado de la distribución de los agentes de la herramienta de distribución de software a nivel nacional	5	4	3	17
Obtener el paquete de distribución del software centralizado para su envío a través de la herramienta	4	4	4	20
Ejecutar las pruebas de validación de la distribución de software a través de herramienta	4	3	4	16
Brindar soporte técnico durante el período de implementación a todos los funcionarios del Comité de implementación del sistema integrado bancario	2	4	4	18
Administrar los programas fuentes en la herramienta para control de versionamiento Visual Source Safe	5	4	4	21
Realizar durante el período de implementación, la instalación y	2	4	4	18

configuración de ambientes tecnológicos para pruebas, capacitación y producción de los diferentes módulos del sistema integrado bancario				
Archivar documentos que respalden las entregas/ recepciones de programas fuentes realizadas, aprobadas, rechazadas o en proceso	5	3	3	14
Establecer los derechos de acceso de los usuarios, mantenimiento y permisos para el sistema.	4	4	4	20
Planificar horarios para cubrir actividades de desarrollo en fin de semana o feriados	2	4	4	18
Garantizar el uso de fuentes actualizados y concordantes con las versiones liberadas en producción	5	4	4	21

Donde:

F = frecuencia de la actividad

CO = consecuencias por omisión de la actividad

CM = complejidad de la actividad

Total = F + (CO x CM)

Sección 4: INTERFAZ DEL PUESTO

Especifica por cada actividad relevante, el/los beneficiarios de la ejecución de esa tarea

Actividades Esenciales	Interfaz Nombres de las unidades, puestos, clientes, usuarios o beneficiarios directos de la actividad.
Desplegar agentes de herramienta para distribución de software de los equipos de escritorio de toda la organización	**Clientes** **Usuarios de sistemas informáticos**
Actualizar el estado de la distribución de los agentes de la herramienta de distribución de software a nivel nacional	**Clientes** **Usuarios de sistemas informáticos**
Obtener el paquete de distribución del software centralizado para su envío a través de la herramienta	**Clientes** **Usuarios de sistemas informáticos**
Administrar los programas fuentes en la herramienta para control de versionamiento Visual Source Safe	**Clientes** **Usuarios de sistemas informáticos**
Garantizar el uso de fuentes actualizados y concordantes con las versiones liberadas en producción	**Clientes** **Usuarios de sistemas informáticos**
Archivar documentos que respalden las entregas/ recepciones de programas fuentes realizadas, aprobadas, rechazadas o en proceso	**Clientes** **Usuarios de sistemas informáticos**

Sección 5: CONOCIMIENTOS REQUERIDOS

Define los conocimientos técnicos (adquiridos a través de la formación académica) indispensables para la ejecución de las actividades relevantes especificadas para el cargo

Actividades esenciales	Conocimientos
Desplegar agentes de herramienta para distribución de software de los equipos de escritorio de toda la organización	Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco Herramientas de administración de versiones
Actualizar el estado de la distribución de los agentes de la herramienta de distribución de software a nivel nacional	Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco Herramientas de administración de versiones
Obtener el paquete de distribución del software centralizado para su envío a través de la herramienta	Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco Herramientas de administración de versiones
Administrar los programas fuentes en la herramienta para control de versionamiento Visual Source Safe	Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco Herramientas de administración de versiones
Garantizar el uso de fuentes actualizados y concordantes con las versiones liberadas en producción	Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco Herramientas de administración de versiones
Archivar documentos que respalden las entregas/ recepciones de programas fuentes realizadas, aprobadas, rechazadas o en proceso	Seguridad de la Información Redes y Comunicación Manejo de equipos Sistemas informáticos del Banco Herramientas de administración de versiones

Sección 6: INSTRUCCIÓN FORMAL REQUERIDA

Nivel de Instrucción Formal	Especifique el número de años	Indique el área de conocimientos

	de estudio o los diplomas / títulos requeridos	formales (ejemplo, administración, economía, etc.).
Ingeniería	6 años	Sistemas / Procesos

Sección 7: EXPERIENCIA LABORAL REQUERIDA

Dimensiones de Experiencia	Detalle
Tiempo de experiencia	2 años
Especificidad de la experiencia	Actividades de informática
Contenido de la experiencia	Desarrollo de sistemas informáticos Manejo de bases de datos

Sección 8: DESTREZAS TÉCNICAS (ESPECÍFICAS) REQUERIDAS

Sujetas al Catálogo de Competencias Técnicas del Ministerio de Relaciones Laborales.

Destrezas	Definición	Relevancia		
		Alta	Media	Baja
Recopilación de información	Conocer cómo localizar e identificar información esencial.		X	
Selección de equipos	Determinar el tipo de equipos, herramientas e instrumentos necesarios para realizar un trabajo.		X	
Comprensión oral	Es la capacidad de escuchar y comprender información o ideas presentadas.		X	
Expresión oral	Es la capacidad de comunicar información o ideas en forma hablada de manera clara y comprensible.		X	
Comprensión escrita	La capacidad de leer y entender información e ideas presentadas de manera escrita.		X	
Administración del Desempeño	La Administración del Desempeño es un enfoque sistemático aplicado a la administración de personal –del día a día– en el ambiente de trabajo, orientado a evaluar los resultados esperados en la ejecución de un proceso; utilizando el “acompañamiento” como recurso principal para optimizar los resultados.		X	
Educación y capacitación	Es la educación tendiente a ampliar, desarrollar y perfecciona	X		

	los conocimientos que permita un crecimiento profesional para que se vuelva más eficiente y productivo en su cargo.

Sección 9: DESTREZAS / HABILIDADES CONDUCTUALES (GENERALES)

Sujetas al Catálogo de Competencias Conductuales del Ministerio de Relaciones Laborales.

Destrezas	Definición	Relevancia		
		Alta	Media	Baja
Trabajo en equipo	Es el interés de cooperar y trabajar de manera coordinada con los demás.	X		
Orientación de servicio	Implica un deseo de ayudar o de servir a los demás satisfaciendo sus necesidades. Significa focalizar los esfuerzos en el descubrimiento y la satisfacción de las necesidades de los clientes, tanto internos como externos.	X		
Orientación a los resultados	Es el esfuerzo por trabajar adecuadamente tendiendo al logro de estándares de excelencia.	X		
Actitud al cambio	Es la predisposición a generar, desarrollar y promover cambios positivos acorde a los objetivos y metas organizacionales.	X		
Relaciones Humanas	Es la habilidad de construir y mantener relaciones cordiales con personas internas o externas a la organización.	X		
Conocimiento del entorno organizacional	Es la capacidad para comprender e interpretar las relaciones de poder e influencia en la institución o en otras instituciones, clientes o proveedores, etc. Incluye la capacidad de prever la forma en que los nuevos acontecimientos o situaciones afectarán a las personas y grupos de la institución.		X	
Iniciativa	Es la predisposición para actuar proactivamente. Los niveles de actuación van desde concretar decisiones tomadas en el pasado hasta la búsqueda de nuevas oportunidades o soluciones a problemas.	X		
Aprendizaje continuo	Es la habilidad para buscar y compartir información útil, comprometiéndose con el aprendizaje. Incluye la capacidad de aprovechar la experiencia de otros y la propia.	X		

Sección 10: REQUERIMIENTOS DE SELECCIÓN Y CAPACITACIÓN

Conocimientos / Destrezas	Requerimiento de Selección	Requerimiento de Capacitación
Conocimientos		
Manejo de Bases de Datos	X	
Procesos bancarios	X	
Sistemas Operativos	X	
Sistema Bancario del BNF		**X**
Herramientas de Versionamiento		**X**
Instrucción Formal		
Tecnología en Sistemas	X	
Experiencia		
Desarrollo de sistemas informáticos	X	
Manejo de bases de datos	X	
Liste las Destrezas Técnicas y Conductuales		
Recopilación de información	X	
Selección de equipos	X	
Comprensión oral	X	
Expresión oral	X	
Comprensión escrita	X	
Administración del Desempeño	X	
Educación y capacitación	X	
Trabajo en equipo	X	
Orientación de servicio	X	
Orientación a los resultados	X	
Actitud al cambio	X	
Relaciones Humanas	X	
Conocimiento del entorno organizacional		**X**
Iniciativa	X	
Aprendizaje continuo	**X**	

Sección 11: VALORACIÓN DEL PUESTO

Corresponde al resultado del cálculo del puesto, basado en la tabla establecida por el Ministerio de Relaciones Laborales para el efecto.

COMPETENCIAS				COMPLEJIDAD DEL PUESTO		RESPONSABILIDAD	
Instrucción formal	Experiencia	Habilidades		Condiciones de trabajo	Toma de decisiones	Rol del puesto	Control de resultados
		Gestión	Comunicación				
Tecnología	2 años	Nivel 2	Nivel 3	Nivel 1	Nivel 2	Apoyo	**Nivel 2**
125	50	40	60	20	40	100	**40**
475 Puntos							

ANEXO 2.3 ESPECIFICACIONES TECNICAS SERVIDOR CENTRAL

Componentes	Requisitos
Equipo y procesador	Servidor con velocidad de procesador de 2,5 gigahercios (GHz) o superior; procesador dual, se recomienda 3 GHz o superior
Memoria	4 gigabyte (GB) de RAM; se recomienda 8 GB
Disco duro	100 GB mínimo de disco duro disponible. El total de espacio requerido depende del número y tamaño de los paquetes a almacenar.
Unidad	Unidad de CD-ROM o DVD, local o en la red
Pantalla	Monitor con una resolución de 1024 x 768 o superior
Sistema operativo	• Microsoft Windows Server 2003 (Enterprise Edition, Standard Edition) SP1 and SP2 • Microsoft Windows 2000 (Advanced Server, Server) SP4.
Otros	Microsoft SQL Server 2005 SP1 and SP2 o Microsoft SQL Server 2000 SP4, se necesita una conexión de 100 megabits por segundo (Mbps) para la implementación en un conjunto de servidores y 56 kilobits por segundo (Kbps) para la conexión de cliente a servidor. Para las notificaciones por correo electrónico se necesita el protocolo simple de transferencia de correo de Internet y el protocolo de oficina postal (SMTP/POP3), el protocolo de acceso a mensajes de Internet 4 (IMAP4) o un software de mensajería compatible con MAPI.
Explorador	• Microsoft Internet Explorer 6 o superior • Mozilla 1.6 • Firefox 1.0 o superior

ANEXO 2.4 ESPECIFICACIONES TECNICAS SERVIDOR DE ESCALAMIENTO

Componentes	Requisitos
Equipo y procesador	Servidor o Desktop con velocidad de procesador de 2,5 gigahercios (GHz) o superior; procesador dual, se recomienda 3 GHz o superior
Memoria	1 gigabyte (GB) de RAM; se recomienda 2 GB
Disco duro	Mínimo 3 GB de disco duro disponible. El total de espacio requerido depende del número y tamaño de los paquetes a almacenar.
Unidad	Unidad de CD-ROM o DVD, local o en la red
Pantalla	Monitor con una resolución de 1024 x 768 o superior
Sistema operativo	• Microsoft Windows Server 2003 (Enterprise Edition, Standard Edition, Web Edition) SP1 and SP2 • Microsoft Windows 2000 (Advanced Server, Server, Professional) SP4 • Microsoft Windows XP Professional SP2 • Microsoft Windows Vista (Enterprise, Business, Ultimate) (32- and 64-bit)
Otros	Se necesita una conexión de 100 megabits por segundo (Mbps) para la implementación en un conjunto de servidores y 56 kilobits por segundo (Kbps) para la conexión de cliente a servidor. Para las notificaciones por correo electrónico se necesita el protocolo simple de transferencia de correo de Internet y el protocolo de oficina postal (SMTP/POP3), el protocolo de acceso a mensajes de Internet 4 (IMAP4) o un software de mensajería compatible con MAPI.
Explorador	• Microsoft Internet Explorer 6 o superior • Mozilla 1.6 • Firefox 1.0 o superior

ANEXO 2.5 ESPECIFICACIONES TECNICAS CONSOLA DE EXPLORACION

Componentes	Requisitos
Equipo y procesador	Servidor con velocidad de procesador de 2,5 gigahercios (GHz) o superior; procesador dual, se recomienda 3 GHz o superior
Memoria	1 gigabyte (GB) de RAM; se recomienda 2 GB.
Disco duro	200 MB de disco duro disponible
Unidad	Unidad de CD-ROM o DVD, local o en la red
Pantalla	Monitor con una resolución de 1024 x 768 o superior
Sistema operativo	• Microsoft Windows Server 2003 (Enterprise Edition, Standard Edition, Web Edition) SP1 and SP2 • Microsoft Windows 2000 (Advanced Server, Server, Professional) SP4 • Microsoft Windows XP Professional SP2 • Microsoft Windows Vista (Enterprise, Business, Ultimate) (32- and 64-bit)
Otros	Se necesita una conexión de 100 megabits por segundo (Mbps) para la implementación en un conjunto de servidores y 56 kilobits por segundo (Kbps) para la conexión de cliente a servidor. Para las notificaciones por correo electrónico se necesita el protocolo simple de transferencia de correo de Internet y el protocolo de oficina postal (SMTP/POP3), el protocolo de acceso a mensajes de Internet 4 (IMAP4) o un software de mensajería compatible con MAPI.
Explorador	• Microsoft Internet Explorer 6 o superior • Mozilla 1.6 • Firefox 1.0 o superior
Adicional	Consulte el documento de programación de capacidad para obtener requisitos específicos para cada equipo.

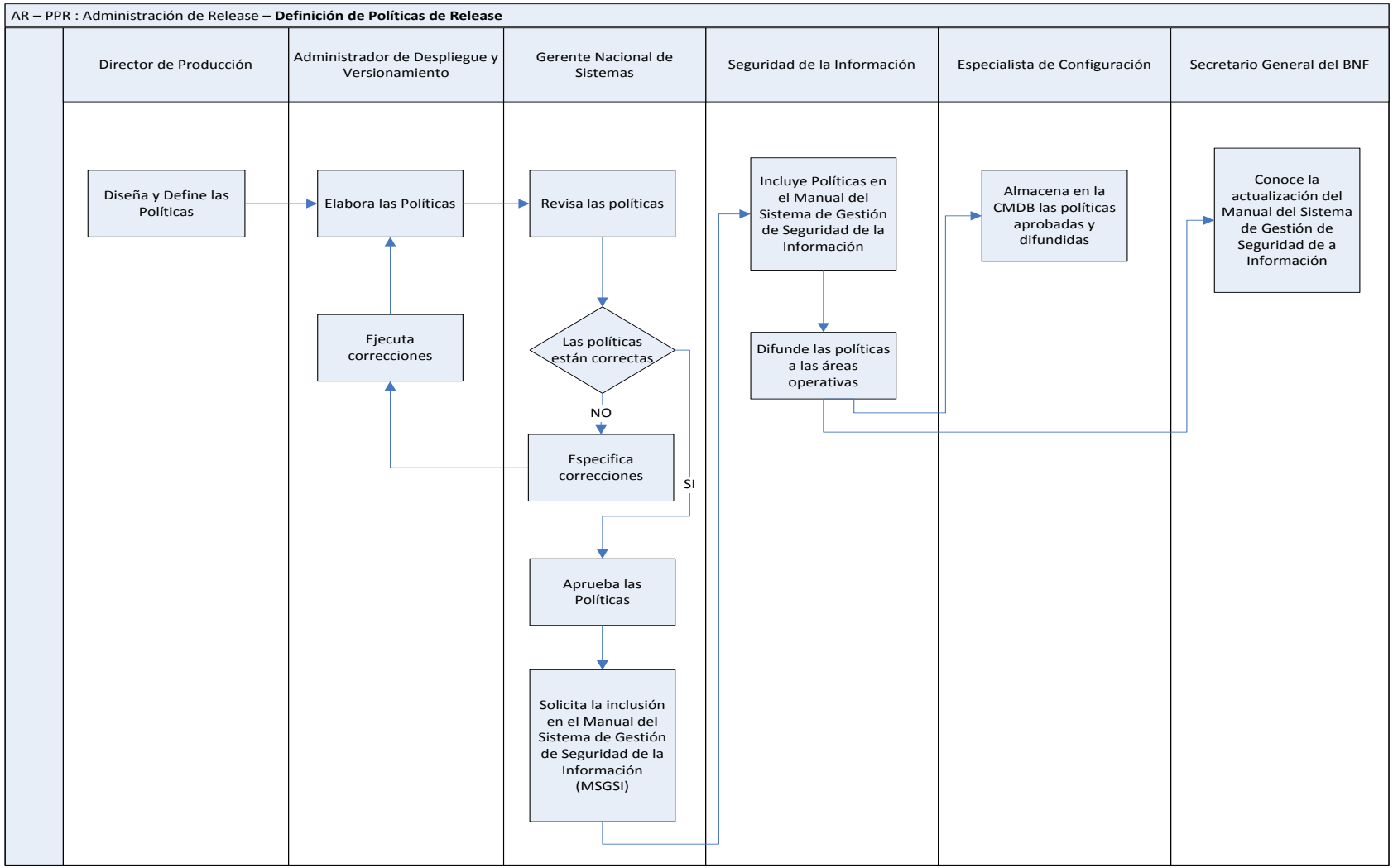
ANEXO 2.6 ESPECIFICACIONES TECNICAS EQUIPO DE ESCRITORIO

Componentes	Requisitos
Equipo y procesador	Servidor con velocidad de procesador de 200 MHZ, se recomienda 1 GHz o superior
Memoria	256 megabyte (MB) de RAM; se recomienda 512 MB.
Disco duro	200 MB de disco duro disponible
Unidad	Unidad de CD-ROM o DVD, local o en la red[2]
Pantalla	Monitor con una resolución de 1024x768 o superior
Sistema operativo	• Microsoft Windows Server 2008 (Enterprise Edition and Standard Edition) SP1 (32- and 64-bit) (Not a Packager platform. No OSIM support available.) • Microsoft Windows Server 2003 (Enterprise Edition, Standard Edition, Web Edition) SP1 and SP2 • Microsoft Windows Server 2003 R2 (Enterprise Edition) SP2 • Microsoft Windows Server 2003 R2 (Standard Edition) SP2 • Microsoft Windows Server 2003 x64 (Enterprise Edition, Standard Edition) SP2 • Microsoft Windows 2000 (Advanced Server, Server, Professional) SP4 • Microsoft Windows XP (Professional, Home) SP2 • Microsoft Windows XP (Professional) SP3 • Microsoft Windows XP Professional x64 • Microsoft Windows XP Embedded SP2 • Microsoft Windows XP Embedded Point of Service (WEPOS) SP2 • Microsoft Windows Vista (Enterprise, Business, Ultimate) (32- and 64-bit) (Not a Packager platform) • Microsoft Windows NT 4.0 (Workstation and Server) SP6a • Microsoft Windows Me • Microsoft Windows 98 SE • Microsoft Windows 95 OSR 2.5
Otros	Se necesita una conexión de 100 megabits por segundo (Mbps) para la implementación en un conjunto de servidores y 56 kilobits por segundo (Kbps) para la conexión de cliente a servidor. Para las notificaciones por correo electrónico se necesita el protocolo simple de transferencia de correo de Internet y el protocolo de oficina postal (SMTP/POP3), el protocolo de acceso a mensajes de Internet 4 (IMAP4) o un software de mensajería compatible con MAPI.[3]
Explorador	• Microsoft Internet Explorer 6 o superior • Mozilla 1.6 • Firefox 1.0 o superior

ANEXO 3.1 DIAGRAMA SIPOC – DEFINICION DE POLITICAS DE RELEASE

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Definición de Políticas de Release		
PROVEEDORES	**ENTRADAS**	**PROCESO**	**SALIDAS**	**CLIENTES**
Gerente Nacional de Sistemas	Políticas de la Gerencia Nacional de Sistemas	Definición de Políticas de Release	Políticas Generales de Release	Administrador de Configuración
Oficial de Seguridad de Seguridad de la Información	Manual del Sistema de Gestión de Seguridad de la Información		Procedimiento de Planificacion del roll-out	Administrador de despliegue y versionamiento
Secretario General	Políticas Y Reglamentos del BNF		Estándar de Versionamiento	Secretario General
Director de Producción	Diseño y mantenimiento de Políticas		Norma para el Control de Fuentes	Área de Release
Gerente Nacional de Riesgos	Normativa para Gestión de Riesgo Operativo		Procedimiento de Diseño de roll-out y roll-back	Administrador de Control de Cambios
Contraloría General del Estado	Normas de Control Interno Entidades del Sector Público		Procedimiento de Logística para roll-out masivo	Gerente Nacional de Sistemas
Office of Government Commerce OGC	Fundamentos ITIL		Procedimiento de Notificación del roll-out	Oficial de Seguridad de Seguridad de la Información
Information Systems Audit and Control Association (ISACA) IT Governance Institute (ITGI)	Fundamentos COBIT			
International Organization Standard	Dominios y Controles ISO 27002			

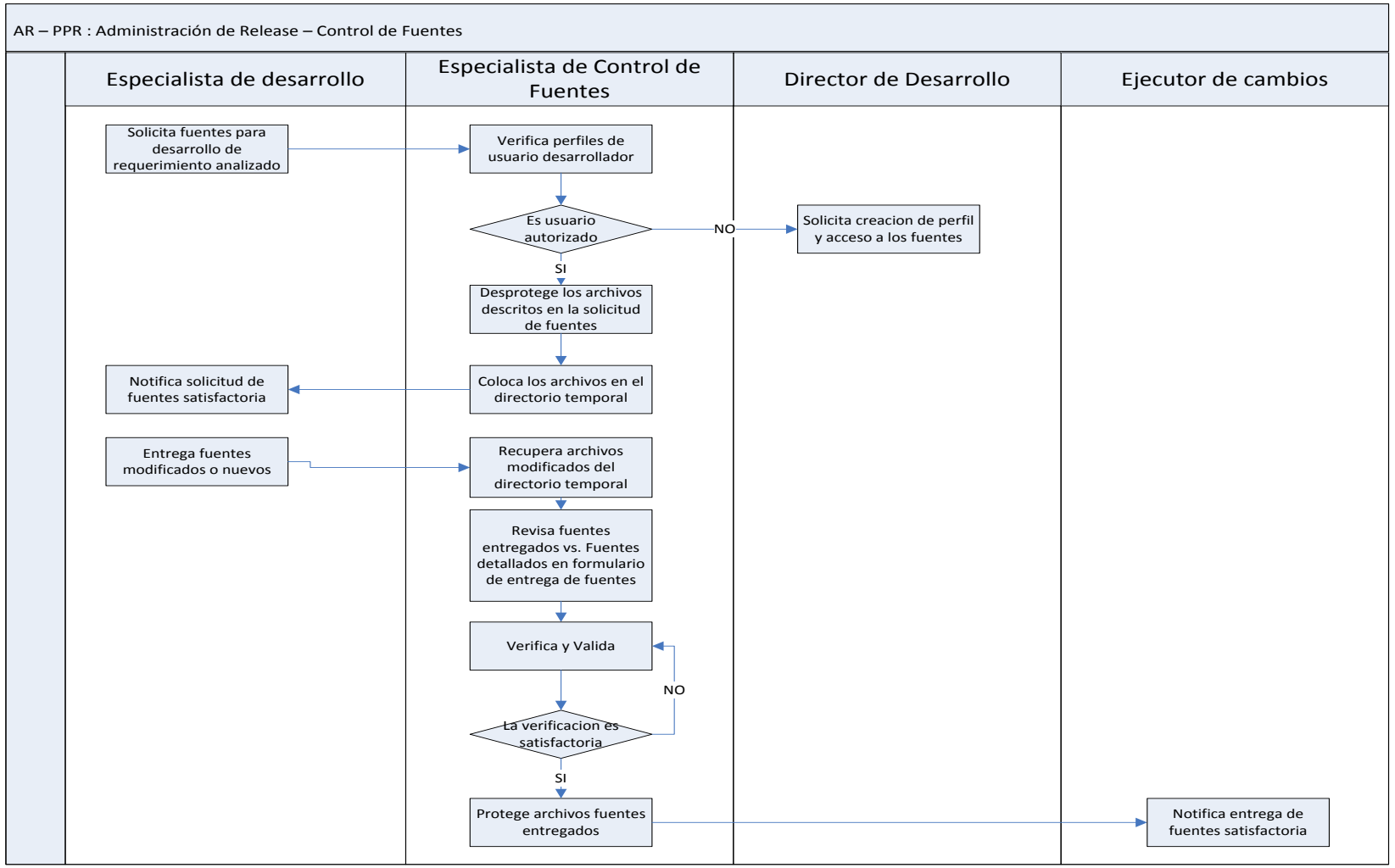
ANEXO 3.2 DIAGRAMA DE FLUJO – DEFINICION DE POLITICAS DE RELEASE



ANEXO 3.3 DIAGRAMA SIPOC – CONTROL DE FUENTES

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Control de Fuentes		
PROVEEDORES	**ENTRADAS**	**PROCESO**	**SALIDAS**	**CLIENTES**
Especialista de Desarrollo	Formulario de Solicitud de Fuentes Procedimiento de llenado de formulario de solicitud o entrega de fuentes Request For Change (RFC) Formulario de Entrega de Fuentes Estandar de Versionamiento Historial de desproteccion - proteccion de fuentes Base de Datos de Control de Fuentes (DSL)	Solicitud de Fuentes para Desarrollo Entrega de Fuentes nuevos y/o modificados	Directorio temporal para desproteccion de archivos Notificacion de confirmacion para puesta en Produccion	Especialista de Desarrollo Especialista de Control de Cambios Ejecutores de Cambios Especialista de despliegue y Versionamiento Director de Desarrollo Ingeniero de Procesos

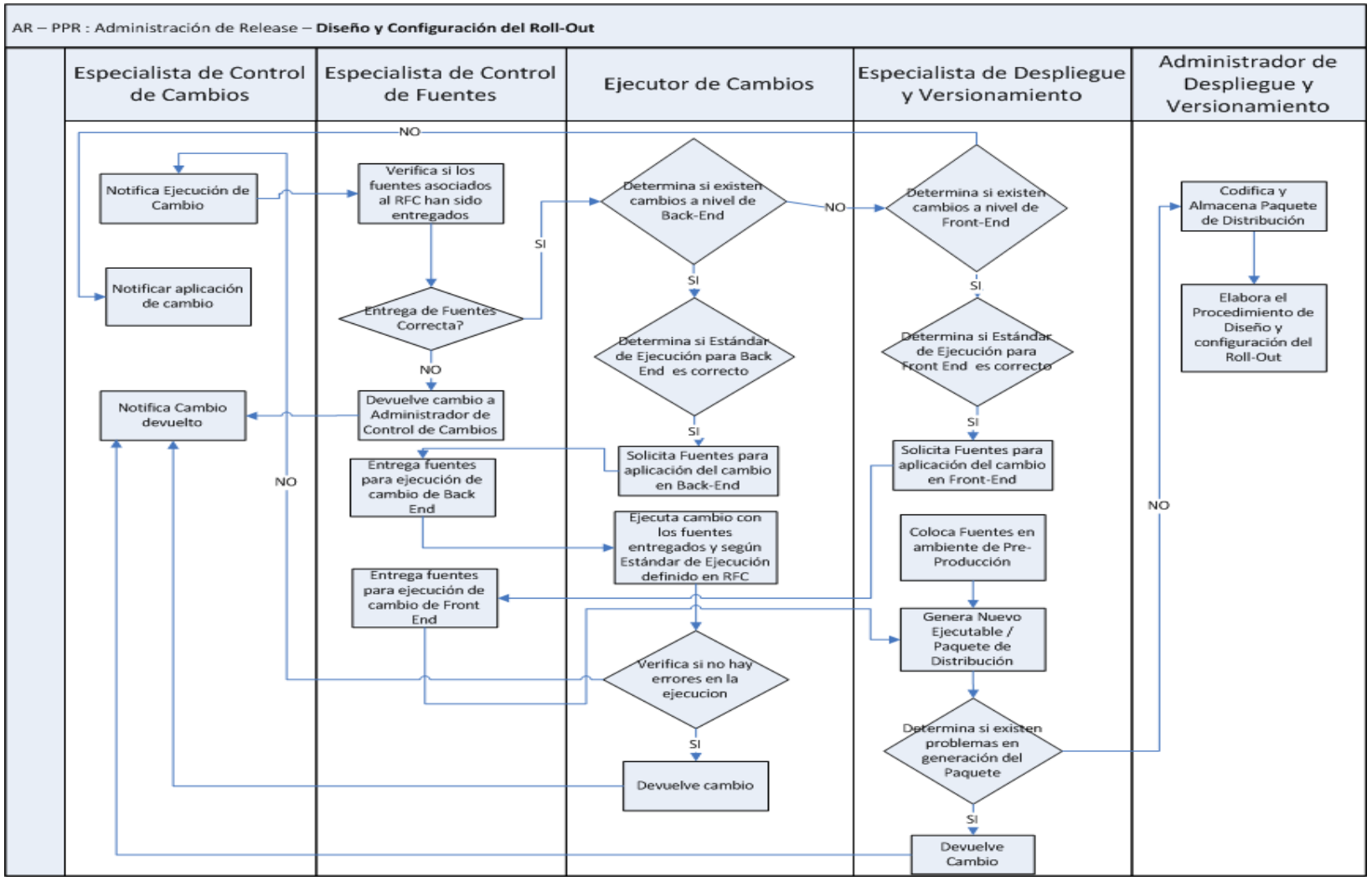
ANEXO 3.4 DIAGRAMA DE FLUJO – CONTROL DE FUENTES



ANEXO 3.5 DIAGRAMA SIPOC – DISEÑO Y CONFIGURACION DE ROLL-OUT

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Diseño y Configuración de roll-out		
PROVEEDORES	**ENTRADAS**	**PROCESO**	**SALIDAS**	**CLIENTES**
Especialista de Control de Cambios	Formulario de Solicitud de Fuentes	Revision de Estandar de Ejecucion	Devolucion de Cambio no aplicado	Especialista de Desarrollo
Especialista de Control de Fuentes	Request For Change (RFC)	Aplicacion de cambio en Back End	Notificacion de aplicación de cambio Back End exitoso	Especialista de Control de Cambios
Especialista de desarrollo	Estándar de Ejecución	Aplicacion de cambio en Front End	Nuevo paquete de distribucion para Front End almacenado y codificado	Ejecutores de Cambios
Especialista de Despliegue y Versionamiento	Base de Datos de Control de Fuentes (DSL)	Solicitud de Fuentes	Procedimiento de Diseño y Configuracion del Roll Out	Especialista de despliegue y Versionamiento
Ejecutor de cambios	Directorio de entrega de fuentes	Devolucion de Cambio		Director de Desarrollo
Administrador de Despliegue y Versionamiento		Generacion de nuevo ejecutable		Ingeniero de Procesos
		Elaborar procedimiento de Diseño y Configuración del Roll Out		

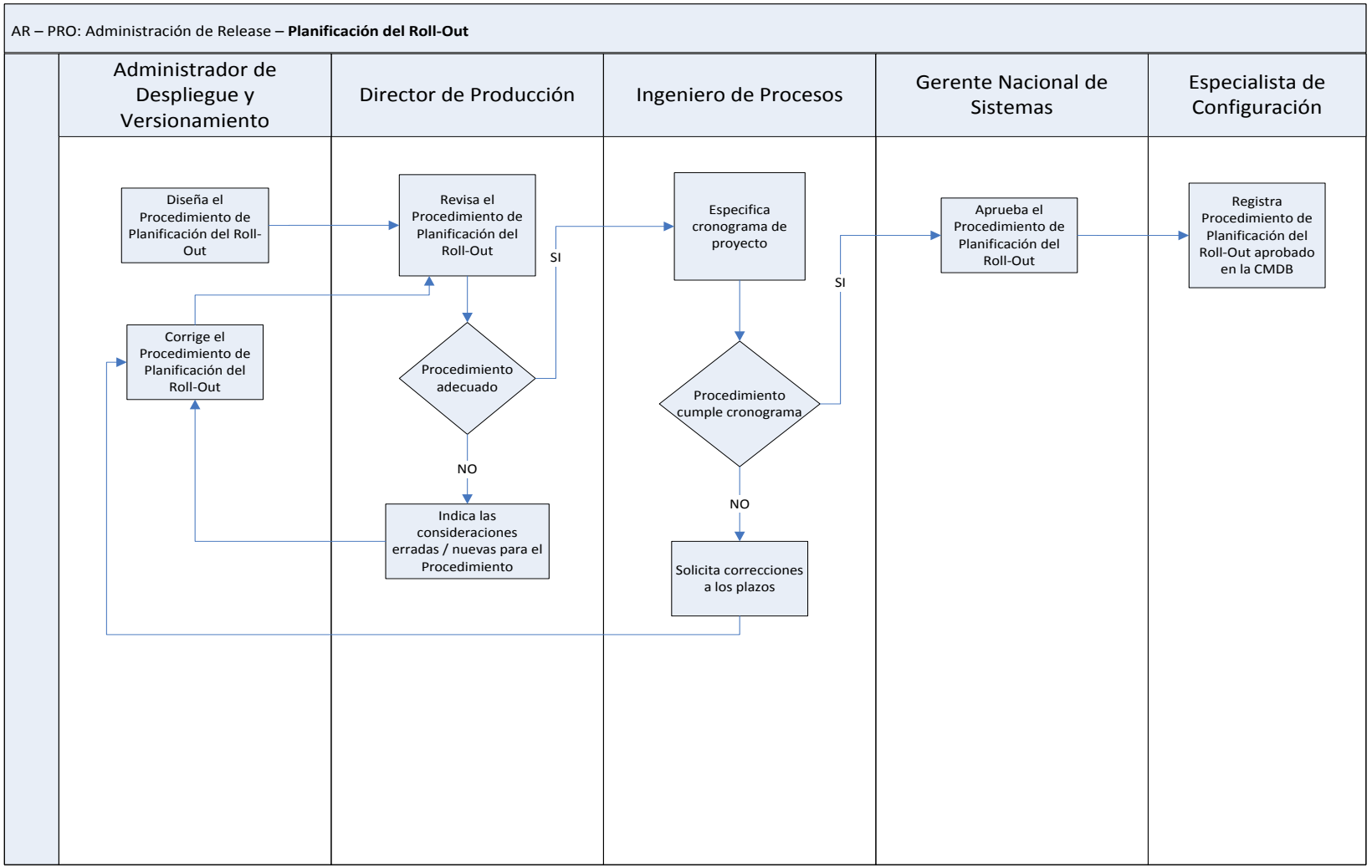
ANEXO 3.6 DIAGRAMA DE FLUJO – DISEÑO Y CONFIGURACION DE ROLL-OUT



ANEXO 3.7 DIAGRAMA SIPOC – PLANIFICACION DE ROLL-OUT

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Planificacion del Roll Out		
PROVEEDORES	**ENTRADAS**	**PROCESO**	**SALIDAS**	**CLIENTES**
Ingeniero de Procesos Administrador de despliegue y versionamiento Director de Produccion	Procedimiento de Diseño y Configuracion de roll-out CMDB	Diseñar el Procedimiento Revisar el procedimiento Corregir el procedimiento Aprobar el procedimiento Almacenar el procedimiento	Procedimiento de planificacion del Roll Out	Especialista de despliegue y versionamiento Director de Produccion Ingeniero de Procesos Gerente Nacional de Sistemas Especialista de Configuracion

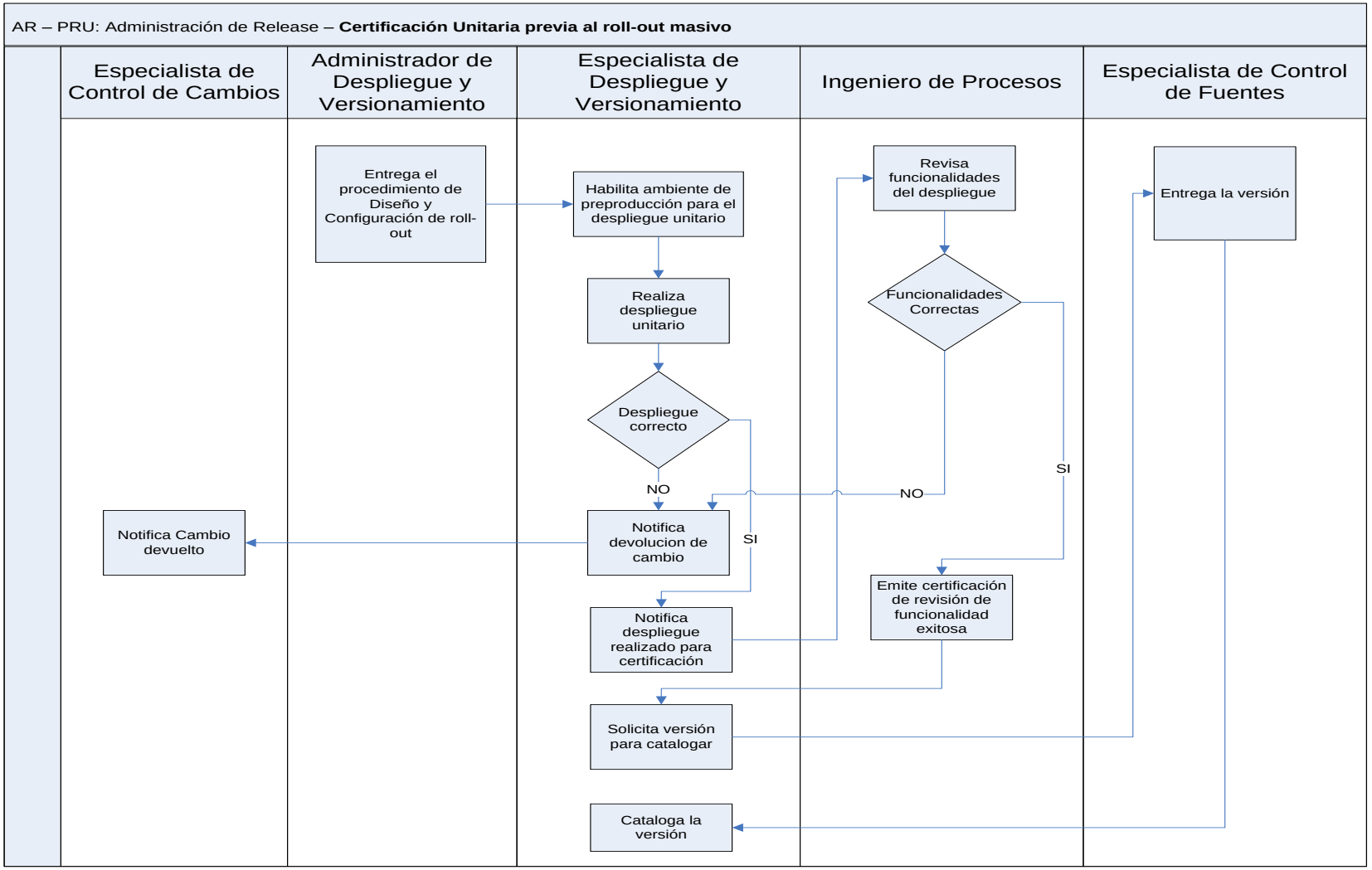
ANEXO 3.8 DIAGRAMA DE FLUJO – PLANIFICACION DEL ROLL-OUT



ANEXO 3.9 DIAGRAMA SIPOC – CERTIFICACION UNITARIA PREVIA AL ROLL-OUT MASIVO

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Certificación unitaria previa al roll-out masivo		
PROVEEDORES	ENTRADAS	PROCESO	SALIDAS	CLIENTES
Ingeniero de Procesos	Procedimiento de Diseño y Configuración de roll-out	Realizar el despliegue Unitario	Certificación de distribución unitaria	Ingeniero de Procesos
Administrador de despliegue y versionamiento	DSL	Revisar la ejecucion del despliegue unitario	Certificación de nuevas funcionalidades	Especialista de Control de Cambios
Especialista de Control de Fuentes		Revisar la funcionalidad del cambio despues del despliegue unitario	Version para catalogar	Especialista de despliegue y versionamiento
		Certificar la funcionalidad correcta del despliegue unitaria		Especialista de Control de Fuentes
		Solicitar version para catalogar		Administrador de Despliegue y Versionamiento
		Catalogar distribucion con version entregada		
		Notificar cambio devuelto		

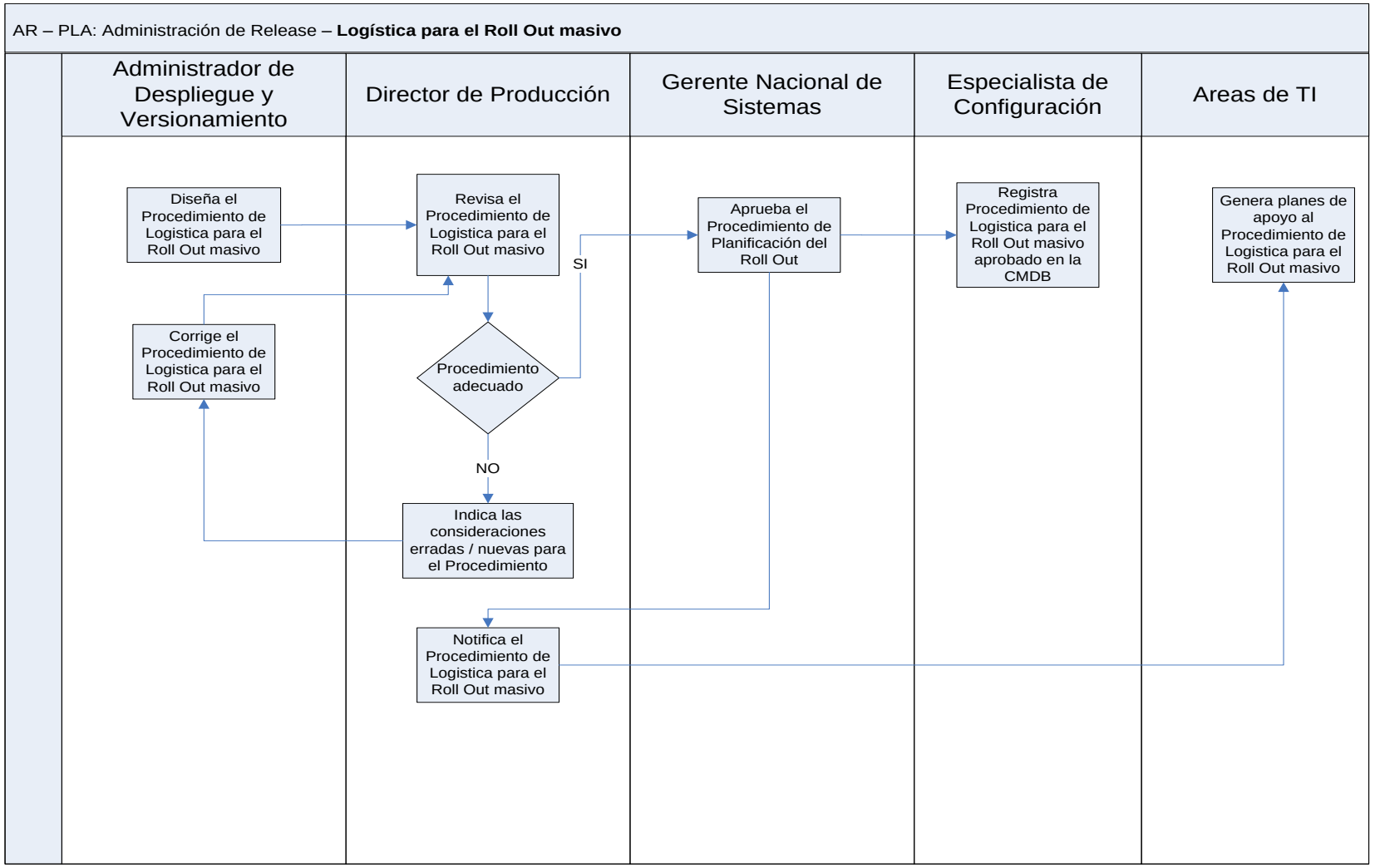
ANEXO 3.10 DIAGRAMA DE FLUJO – CERTIFICACION UNITARIA PREVIA AL ROLL-OUT MASIVO



ANEXO 3.11 DIAGRAMA SIPOC – LOGISTICA PARA EL ROLL-OUT MASIVO

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Logistica para el Roll Out masivo		
PROVEEDORES	**ENTRADAS**	**PROCESO**	**SALIDAS**	**CLIENTES**
Administrador de despliegue y versionamiento Director de Produccion	Procedimiento de Planificacion del Roll-Out Procedimiento de Diseño y Configuracion del Roll Out RFC Estandar de Ejecucion	Diseñar el Procedimiento Revisar el procedimiento Corregir el procedimiento Aprobar el procedimiento Almacenar el procedimiento	Procedimiento de logistica del Roll Out masivo	Especialista de despliegue y versionamiento Director de Produccion Ingeneiro de Procesos Gerente Nacional de Sistemas Especialista de Configuracion Director de Infraestructura Administrador de Service Desk Administrador de Telecomunicaciones Adminsitrador de Disponibilidad y Continuidad

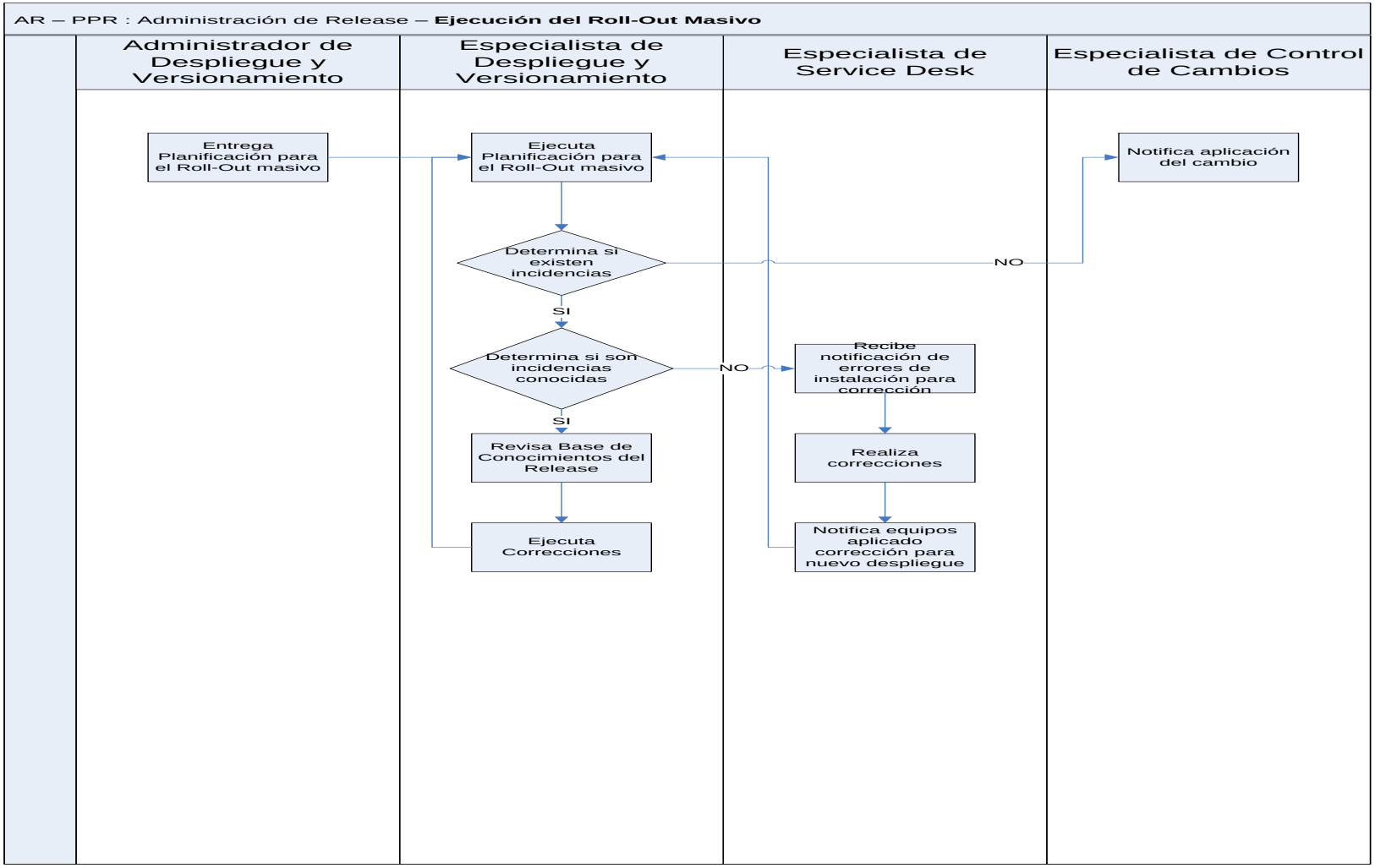
ANEXO 3.12 DIAGRAMA DE FLUJO – LOGISTICA PARA EL ROLL-OUT MASIVO



ANEXO 3.13 DIAGRAMA SIPOC – EJECUCION DEL ROLL-OUT MASIVO

DIAGRAMA SIPOC				
PROCESO: RELEASE		**Subproceso:** Ejecucion del Roll-Out masivo		
PROVEEDORES	ENTRADAS	PROCESO	SALIDAS	CLIENTES
Administrador de despliegue y versionamiento	RFC	Ejecutar Planificación para el Roll-Out masivo	Estadísticas de la distribución	Administrador de despliegue y versionamiento
	Procedimiento de Diseño y Configuracion del Roll Out	Notifica la ejecución del Roll-Out masivo	Manejo de Incidencias de la distribución	Especialista de despliegue y versionamiento
	Procedimiento de Planificacion del Roll-Out	Determina incidencias	Notificación del cambio	Especialista de Service Desk
		Notifica las incidencias	Notificación de las incidencias	Especialista de Control de Cambios

ANEXO 3.14 DIAGRAMA DE FLUJO – EJECUCION DEL ROLL-OUT MASIVO



ANEXO 5.1 PLANTILLA PARA EVALUACION DE RIESGOS

BANCO NACIONAL DE FOMENTO
IDENTIFICACION Y VALORACION DE ACTIVOS DE INFORMACION
GERENCIA NACIONAL DE SISTEMAS
PROCESO DE RELEASE

SUBPROCESO:			TASACION				Amenazas			Vulnerabilidades					
			C	I	D	TOTAL	CATEGORIA	DESCRIPCION	PROBABILIDAD	DESCRIPCION	PROBABILIDAD	IMPACTO	CALIF. RIESGO DE VULNERABILIDAD	CALIF. RIESGO DE AMENAZA	RIESGO DEL ACTIVO

Documento	D	C CONFIDENCIALIDAD
Recurso Humano	R	I INTEGRIDAD
Tecnología	T	D DISPONIBILIDAD

3	Alto
2	Medio
1	Bajo

Alto > 2,2
Medio > 1,6
Bajo < 1,7

GLOSARIO

Activos de Información	Ficheros y bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, información archivada, software de aplicación, software del sistema, herramientas y programas de desarrollo, equipo de tratamiento (procesadores, monitores, portátiles, módems), equipo de comunicaciones (routers, centrales digitales, máquinas de fax), medios magnéticos (discos y cintas), otro equipo técnico (suministro de energía, unidades de aire acondicionado), muebles, etc.
Amenaza	Es un evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas a sus activos
AR	Administración de Release
Back-end	Es la parte que procesa la entrada desde el front-end
BNF	Banco Nacional de Fomento
CAIR	Comité de Administración Integral de Riesgos
CA IT Client Manager	Es un nuevo producto que reúne diversos productos existentes, como CA Asset Management, CA Asset Intelligence, CA Software Delivery, CA Remote Control, CA Patch Management y CA Desktop Migration Manager. Ayuda a simplificar la administración de todos los dispositivos informáticos de los usuarios finales, desde laptops y desktops, hasta dispositivos móviles y PDA
CI	(Configuration Items) Elementos de configuración
CMDB	(Configuration Management Database) Base de Datos que registran componentes, sus estructuras y contenidos
COBIT	(Control Objetives for Information Systems and Related Technology) Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA)

Confidencialidad	Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información
Control	Puede ser utilizado en el contexto organizacional para evaluar el desempeño general frente a un plan u objetivo estratégico
Core Bancario	Solución integral bancaria que administran y controlan los procesos y actividades bancarias de una entidad financiera
CUPRON	Certificación Unitaria Previa al Roll-Out Masivo
DHS	(Definitive Hardware Storage) Librería Definitiva de Hardware
Directorio	Junta Directiva conformada por cinco miembros con poder de decisión en la estrategia de manejo y administración del BNF
Disponibilidad	Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones
DSL	(Definitive Software Library- DSL) Librería de Software Definitivo
Estándar	Lineamientos construidos a partir de políticas sólidas
Front-end	Es la parte del software que interactúa con el o los usuarios
Integridad	Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas
ISO 27002	Es un estándar internacional de buenas prácticas sobre la gestión de Seguridad de la Información
ITIL	(Information Technology Infraestructure Library) Es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información
Máquina Virtual	Equipo instalado y configurado con un propio sistema operativo y software virtual utilizado frecuentemente para pruebas y ambientes de desarrollo
MSGSI	Manual del Sistema de Gestión de Seguridad de la Información

PDCA	El ciclo PDCA, también conocido como "Círculo de Deming" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos
PNUD	Programa para las Naciones Unidas
Política	Consta de unas directrices, las cuales nos imponemos cumplir
Proceso	Es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) con un fin determinado
Release	Término que hace referencia a toda la descripción de cambios autorizados para los servicios TI
RFC	(Request for Change) Documento formal con el Requerimiento de Cambio
Riesgo	Es el potencial de una amenaza dada que explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a los mismos
RO	Riesgo Operativo
Roll-Out	Despliegue final
Scalability Server	Servidor o Desktop con velocidad de procesamiento alto y procesador de alta prestación
SGSI	(ISMS) Sistema de Gestión de Seguridad de la Información
SIPOC	(Suppliers, inputs, process, outputs, customers) Es una herramienta utilizada por un equipo para identificar todos los elementos relevantes de un proyecto de mejora de proceso antes de comenzar el trabajo. Metodología Seis Sigma
Software Delivery	Distribución de Software
Stakeholders	Cualquier persona o entidad que es afectada por las actividades de una organización
Subproceso	Un Subproceso es un proceso en sí mismo, cuya funcionalidad es parte de un proceso más grande

TCO	(Total Cost OwnerShip) es un método de cálculo diseñado para ayudar a los usuarios y a los gestores empresariales a determinar los costes directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos
TI	Tecnologias de la Información
Versionamiento	Cada versión importante de un producto pasa generalmente a través de una etapa en la que se agregan las nuevas características (etapa alfa), después una etapa donde se eliminan errores activamente (etapa beta), y finalmente una etapa en donde se han quitado todos los bugs importantes (etapa estable)
Vulnerabilidad	Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo

BIBLIOGRAFIA

- Banco Nacional de Fomento. Departamento de Organización y Métodos. Estatuto Orgánico por Procesos.

- PricewaterhouseCoopers. Informe de la consultoría al Banco Nacional de Fomento sobre Estructura Organizacional y su clasificador de puestos.

- OSIATIS. Gestión de Servicios de TI. Fundamentos de la Gestión de TI. Disponible en WWW: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

- iSEC INFORMATION SECURITY INC. (2010). Curso de Análisis de Riesgo en Seguridad de la Información.

- iSEC INFORMATION SECURITY INC. (2010). Sistema de Gestión de Seguridad de la Información.

- SCALAR CONSULTING. OCTUBRE 2007. Diplomado de Gestión y Administración Integral de Riesgos. Material Bibliográfico.

- Superintendencia de Bancos y Seguros. Normativa de Gestión y Administración de Riesgo Operativo JB-834-2005.

- Fundamentos de ITIL Introducción a la Gestión del Servicio IT. Rodríguez, M. Marlon, Madrid, 2006

- Seguridad Informática para empresas y particulares. Gonzales Alvarez Marañón, Pedro Pablo Pérez García. McGraw-Hill, 2004

- Seminario – Taller Internacional “Gestión del Riesgo Operativo en Bancos e Instituciones Financieras”. Santo Domingo, República Dominicana -2009

REFERENCIAS

http://www.monografias.com/trabajos14/control/control.shtml

http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/

http://www.tecnoav.com/index.php/gestion-de-servicios-it/ca-itcm

http://www.nasoft.com/site/Home/Soluciones/Portecnolog%C3%ADa/CoreBancario/tabid/97/Default.aspx

http://es.wikipedia.org/wiki/Est%C3%A1ndar

http://www.ca.com/us/client-automation.aspx

http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

http://www.monografias.com/trabajos27/implantacion-sistemas/implantacion-sistemas.shtml

http://wiki.bizagi.com/es/index.php?title=Subproceso

http://iso27000.wik.is/Area_Normas/ISO%2f%2fIEC_27002/10._Gesti%c3%b3n_de_Comunicaciones_y_Operaciones/10.10._Monitorizaci%c3%b3n

http://es.wikipedia.org/wiki/Seis_Sigma

http://www.gestiopolis.com/recursos/experto/catsexp/pagans/ger/no12/6sigma.htm

http://www.elprisma.com/apuntes/ingenieria_industrial/conceptodeseissigma/

http://www.tecnoav.com/index.php/gestion-de-servicios-it/ca-service-desk

http://es.wikipedia.org/wiki/Fases_del_desarrollo_de_software

http://wiki.es.it-processmaps.com/index.php/Glosario_ITIL

http://www.acens.com