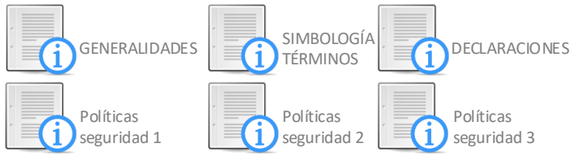
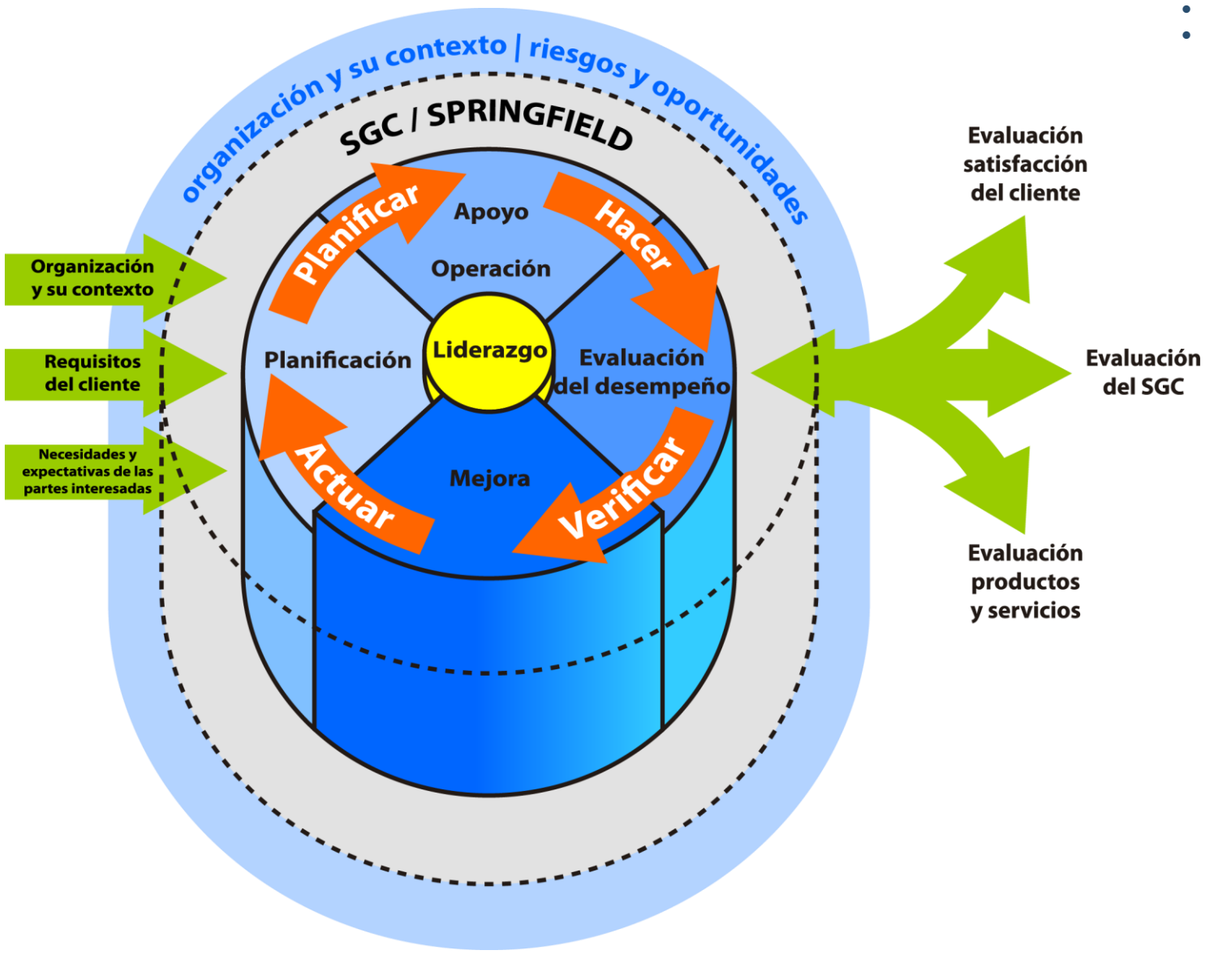
Soluciones Tecnológicas para el Comercio Exterior



MANUAL DE GESTIÓN Y CATÁLOGO DE PROCESOS DEL

SISTEMA SPRINGFIELD

VERSIÓN 13



ALCANCE DEL SISTEMA DE GESTIÓN DE LA CALIDAD Y ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Todos los procesos que afectan el cumplimiento de los requisitos del cliente para los productos:

- Servicio de arriendo de *software*
- Servicio de diseño y desarrollo de *software*
- Servicio de soporte al cliente

ESTÁNDARES

El sistema de gestión Springfield, busca dar conformidad a los estándares certificables ISO 9001, ISO 27001 en sus versiones vigentes.

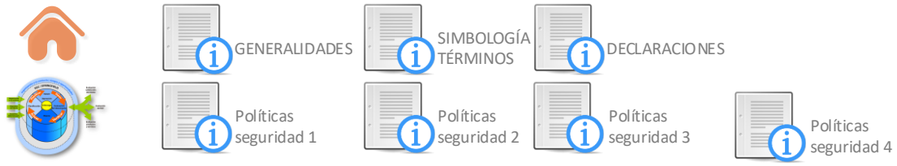
Productos: referidos a Software , cuya trayectoria los ha transformado en productos estandarizados, capaces de asegurar un proceso de instalación e implementación altamente efectiva dentro de cualquier organización.

Diseño y Desarrollo: requerimientos (incluyendo los derivados de los productos), cuyo alcance y complejidad estén fuera de los limites de lo estándar se consideran desarrollos. La metodologías de diseño y desarrollo cuentan con que procesos aseguran resultados eficaces y aseguran el control de los riesgos, tanto operacionales como del negocio.

Control de cambios

1- Se incorporan:
- Modificación Política de teletrabajo
- Modificación de la estructura orgánica
- Corrección Organigrama
- Corrección en proceso de soporte.
- Se agrega Asesor Legal en proceso Gestión Comercial, Compras Criticas, Selección y Desvinculación.
-Se agrega Odoo en los procesos del sistema y en proceso de facturación, cobranza, compras criticas.
- Corrección proceso selección, reclutamiento, contratación.
- Corrección proceso Acciones de aprendizaje.

ASPECTOS GENERALES DEL SISTEMA SPRINGFIELD



OBJETIVO DEL CATÁLOGO DE PROCESOS

Servir como elemento de comunicación y formalización de la operación de Editrade, de manera que facilite el análisis de la misma.

PROCESOS DE LA CADENA DE VALOR

Los procesos de la Cadena de Valor son aquellos que se relacionan directamente con la generación de valor al cliente.

Sobre el Catálogo de Procesos

- La Portada, Introducción, Simbología y Procesos del Sistema, en su conjunto. (su versión corresponde a la vigente del catálogo)

Sobre Procesos

- Los procesos del catálogo son codificados, elaborados, revisados y aprobados de forma individual de manera de asegurar su adecuación antes de su emisión.

Disponibilidad de los procesos

- Los procesos del sistema están disponibles en el catálogo de procesos, en intranet.

PROCESOS SISTEMA DE GESTIÓN

- Los procesos del catálogo incluyen criterios de ejecución y son considerados procedimientos de la organización.
- Los procesos varían en su nivel de profundidad.

PROCESOS DE APOYO

- Los procesos de Apoyo son quienes dan el soporte para que la organización pueda ejecutar los procesos de la cadena de valor.
- Estos procesos dan valor directamente a la organización e indirectamente al cliente.
- En Editrade se han agrupado en dos categorías
- Procesos de apoyo a la Operación: estos procesos son claves para el desarrollo del producto.

- Procesos de apoyo estratégico y de mejora continua:
- Estos procesos buscan revisar, mejorar y/o determinar las grandes directrices de la organización.
- Analizar información para la toma decisiones y planificar.

PUNTOS DE CONTROL

Los puntos de control se identifican en el proceso como una forma de facilitar las labores de comunicación, supervisión, auditoría y otras, dándole énfasis a la actividades que tienen un impacto gravitante en la calidad del servicio, en la consecución de los objetivos del proceso en cuestión y para los estándares de Editrade.

SIMBOLOGÍA Y TÉRMINOS

SIMBOLOGÍA

TERMINOLOGÍAS

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

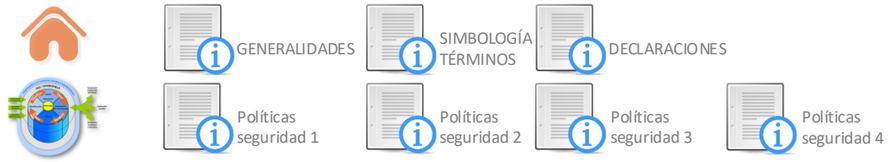
Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Equipos móvil: todo dispositivo con la capacidad de ser portado

Medio removible: Discos duros



POLÍTICAS DE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN

1. Elaborar Soluciones Eficaces, mediante un equipo altamente experimentado y el uso de tecnología de avanzada.

2. Conocer, diagnosticar y tomar decisiones en base a información objetiva, de forma sistemática y participativa.

3. Dar respuestas oportunas a las necesidades de nuestros clientes y usuarios.

4. Revisar regularmente nuestros procesos, políticas, estándares y las necesidades de nuestros clientes, con el objetivo de mejorar continuamente.

5. Mantener una comunicación fluida con nuestros Proveedores, Partners y Stakeholders, propiciando una relación virtuosa para beneficio del negocio y de la satisfacción de nuestros clientes.

6. Gestionar oportuna y eficazmente los activos de la empresa, frente a amenazas internas o externas, con el fin de preservar su confidencialidad, integridad y disponibilidad, proporcionando confianza en nuestras partes interesadas.

7. Revisar continuamente procesos, políticas, estándares y buenas prácticas, tanto internos como de las partes interesadas, con el fin de garantizar la continuidad de los sistemas de información de la organización, por medio de un plan de recuperación ante desastre y un plan de continuidad del negocio.

OBJETIVOS DE LA CALIDAD Y DE SEGURIDAD DE LA INFORMACIÓN

1. Satisfacer de forma eficaz las necesidades de nuestros clientes.

2. Contar con un equipo altamente capacitado.

3. Asegurar la continuidad operacional de los servicios.

4. Contar con proveedores, colaboradores y servicios alineados con los objetivos de nuestra organización y la satisfacción del cliente.

5. Resguardar la información de los clientes y su integridad, de acuerdo a los criterios de seguridad implementados en la organización.

6. Asegurar que la información, esté disponible para los usuarios autorizados, en el momento en que así lo requieran.

PROCESOS DEL SISTEMA

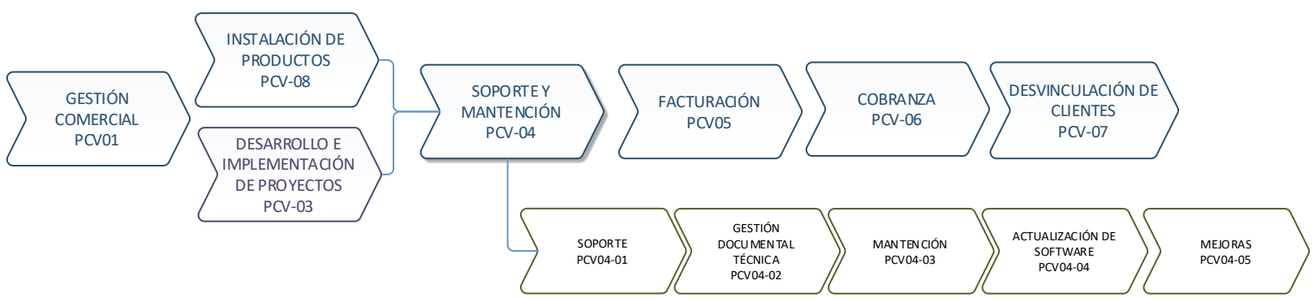
Editrade
Soluciones Tecnológicas para el Comercio Exterior

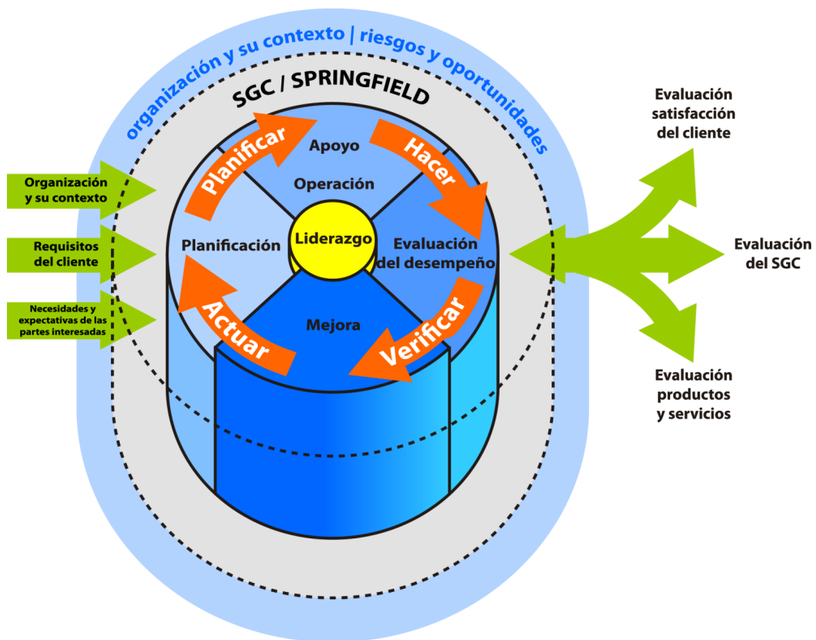
GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Controles Criptográficos
Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

PROCESOS DE APOYO ESTRATÉGICO

- Contexto-Estrategia-Control PAP-16
- Gestión y control de auditoría y mejora
- PROCEDIMIENTO GENERAL AUDITORÍA INTERNA PAP06-PR01
- INFORME DE CASO
- Comunicación al cliente PAP-13
- ACCIONES CORRECTIVAS PAP04-PR01
- GESTIÓN DE RIESGOS PAP-15
- Inventario de Activos y Gestión de Riesgos

CADENA DE VALOR





PROCESOS DE APOYO OPERATIVOS ADMINISTRATIVOS

CLIENTE-SERVICIO

- PERCEPCIÓN DEL CLIENTE PAP09-03
- GESTIÓN DE RECLAMOS DE CLIENTES PAP-12
- PAP08-05 Salida no conforme (Control de servicio no conforme)

Control y Gestión TI

- CONTROL EQUIPOS DE SEGUIMIENTO Y MEDICIÓN PAP02-01
- Enunciado de Aplicabilidad PAP02-15

COMPRAS CRÍTICAS

- COMPRAS CRÍTICAS Y CONTROL DE ACTIVOS TANGIBLES PAP10-01
- SEP-Sistema de Evaluación de Proveedores
- PAP08-05 Procedimiento de control documental

PERSONAS

- GESTIÓN DE PERSONAS PAP08
- SELECCIÓN DE PERSONAS PAP08-01
- DESVINCULACIÓN DEL PERSONAL PAP08-03
- ACCIONES DE APRENDIZAJE PAP08-02
- PAP08-03 Orgánica
- PAP08-05 Organigrama
- PAP08-05 Acuerdo de confidencialidad
- PAP01-D07 Perfiles de cargo/rol
- PAP08-R05 Plan de capacitación

Riesgo Global

Macro riesgo
PERDIDA DE CLIENTES

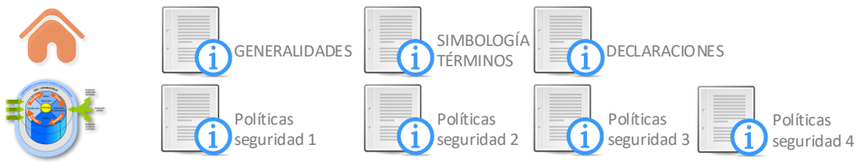
CAUSAS
Mala gestión Comercial.
Mala calidad de desarrollo.
Mala atención de soporte.
No cumplir contratos de respaldos.
Perdida de información.
Acceso no autorizado a la información de un cliente.
No dar continuidad del servicio.
Entrega tardía de requerimientos.

MITIGACIONES
Trabajar en base a procesos y controles.
Incorporar en nuestros procesos, la seguridad de la información
Asignar responsabilidades y compromisos
Hacer constantes mediciones
Ejecutar auditorias
Disponer de personal competente

Devflow | Jira | Monday | Springfield _Drive | SALES FORCE | GLPI | Odoo

POLÍTICAS DE SEGURIDAD 1

Soluciones Tecnológicas para el Comercio Exterior



Responsables: Oficiales de Seguridad
Objetivo: Establecer las directrices generales para gestionar oportuna y eficazmente los activos de la empresa, frente a amenazas internas o externas.

Política general de manejo de activos (Uso aceptable de activos 8.1.3)

Los Activos deben ser Identificados, analizados, catalogados y evaluados periódicamente, para determinar:

1. Las responsabilidades sobre su protección.
2. Evaluar los riesgos asociados.
3. Determinar las restricciones de acceso de los colaboradores según sus roles dentro de la organización.
4. Identificar las respectivas políticas de respaldo de la información y activo.
5. Determinar su uso adecuado.
6. Asegurar que la información cuente con un nivel apropiado de protección.
7. Asegurar que toda entrega y recepción de activos físicos quede registrada.

Política de acceso a la información (9.1.1)

Los accesos a la información deben ser los adecuados según los criterios y permisos establecidos en Gestión de documentos y control de activos.

Los propietarios de la información deben dar los permisos de acceso a la información, así como su registro y desregistro.

Las autoridades de la empresa proporcionan los derechos de acceso y asignación según el rol que ejerce.
Esta entrega o revocación de acceso se debe informar vía email.
El propietario del activo debe hacer revisión periódicas de los usuarios activos.

El **registro y desregistro** en los software, se gestionará según las características del software mismo.

En el caso de acceso a los servidores, se gestionará por el cortafuego y la gestión de usuarios por medio de la gestión de usuarios del sistema operativo de la máquina.

Política de asignación de activos al personal (8.1.3)

Los activos que sean entregados por la empresa a sus colaboradores,

1. Deberán ser usados sólo para los fines establecidos.
2. Cuando corresponda ser registrados
3. Regirse bajo lo establecido en “Gestión de documentos y control de activos”

Política de etiquetado de información (8.2.2)

Todo documento debe ser etiquetado. En base a los criterios establecidos en Gestión de documentos y control de activos.

Criterios generales para la determinación del acceso (8.1.3)

Se espera que los roles ejercidos por el personal de Editrade tengan acceso a los activos de la información.

Es responsabilidad del comité de seguridad de la información realizar el análisis de los accesos a los activos en función de la pertinencia en cuanto a su “Riesgo asociado” y “Uso”.

Para los activos físicos y lógicos se establece una tabla de pertinencia según rol, que se registra en “ACTIVOS, RIESGOS, CONTROLES” fruto del análisis realizado.
Para activos documentales: según su categoría **- INTERNA, CONFIDENCIAL, PÚBLICA-** y la pertinencia de uso según el área y naturaleza de sus funciones.

Política de difusión de contactos de emergencia y servicios básicos

Se deberá dejar disponible la información de contacto de las principales organizaciones de seguridad y servicios básicos para ser utilizados en casos de emergencia

La disposición de la información será preferentemente en

https://sites.google.com/editrade.cl/intranet-editrade/springfield

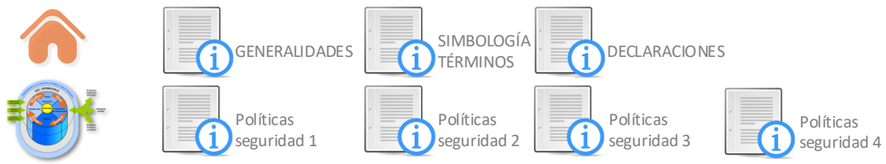
Violación de políticas de seguridad de la información

En el reglamento de “Orden, Higiene y Seguridad“ se declaran las acciones a seguir en los casos que un colaborador viole alguna de las políticas de seguridad de la información.

Política de seguridad para claves de acceso

El cambio de claves para los usuarios de soporte se realizará cada 6 meses, utilizando claves aleatorias.

POLÍTICAS DE SEGURIDAD 2



Responsables: Oficiales de Seguridad
Objetivo: Establecer las directrices generales para gestionar oportuna y eficazmente los activos de la empresa, frente a amenazas internas o externas.

Política de medios removibles (A.8.3.1)

Para la reutilización de un medio, se debe eliminar la información contenida usando el formateo de bajo nivel.

La información contenida en estos medios, se rige bajo las políticas de respaldo del activo asociado, según la Lista de Activos.

La eliminación de medios, previo visto bueno del Oficial de Seguridad de Datacenter, se llevará a cabo por una empresa especializada.

Política de claves

Se recomienda un mínimo de 6 caracteres: números + letras + mayúscula.

Almacenar sus claves en un software seguro como el que proporciona la empresa, en la lista llamada “Lista Blanca de Aplicaciones Corporativas”.

Política de Equipos móviles

Editrade registra y controla de manera física y lógica los equipos móviles que tienen acceso a la red corporativa.
Revisión a todos los equipos que acceden a la red de Editrade, independiente si son de propiedad de Editrade o no.
La revisión debe contemplar los requerimientos de la tabla.

Tipo de Móvil	Requerimiento
Todos los que accedan a la red de Editrade	Catalogados por MAC por el área de Gestión y Control TI.
Celular y Tablet	Colocar pin de seguridad y/o huella digital. Email corporativo con aplicación oficial de Google o aplicación oficial de Android o IOS.
Notebook	Clave BIOS. Clave de sistema operativo. Antivirus. Acceso a la red corporativa por MAC.
Notebook que se sacan de Editrade	OPEN VPN para Windows
	PREY

Actualizar

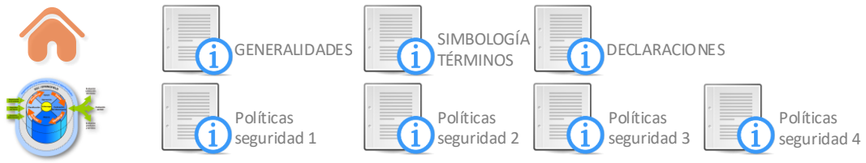
Política de teletrabajo

Editrade establece los lineamientos que regulan el teletrabajo, modalidad a la cual puede optar el colaborador que presta sus servicios para el desempeño de función. Este último debe confirmar con el área de gestión y control TI si el notebook posee las características de seguridad establecidas para trabajo remoto.

Política de Teletrabajo

POLÍTICAS DE SEGURIDAD 3

Soluciones Tecnológicas para el Comercio Exterior



Responsables: Oficiales de Seguridad
Objetivo: Establecer las directrices generales para gestionar oportuna y eficazmente los activos de la empresa, frente a amenazas internas o externas.

Política de acceso a la red y política de red (9.1.2)

Busca limitar el acceso de la información a las instalaciones de procesamiento de la información.

SSH, FW, MAC, VPNs

Política de acceso a redes y servicios de red (A.9.1.2, A.9.2.2)

La gestión de acceso a las redes y servicios de red de la organización, está a cargo del Oficial de Seguridad de Datacenter, quien gestiona, por medio de las **políticas del cortafuego** el acceso según roles, y apoya de la lista de activos.
La validación del acceso, está dada por la MAC del dispositivo.
Para conexiones desde fuera de la red corporativa se deben regir bajo las políticas de trabajo remoto.
Por medio del sistema Nagios, se debe monitorear La Red.

Emplazamiento y Control de Equipo (11.2.1)

Control de Equipamiento:
Se designa como zona segura, el centro de procesamiento de chile, el cual posee acceso por huella digital.

El centro de procesamiento posee, cielo y piso falso, detector de humo, control de temperatura, puerta de acceso, continuidad de energía (generador), extintores, doble enlace internet, ups, alarmas de servidores, termómetro, deshumidificador.

Cableado subterráneo.

Cableado de energía separado y paneles de control especial.

El acceso a las oficinas centrales es por llave más código de alarma.

Los equipos como notebooks, que son activos de la organización tienen la aplicación Prey que permite saber su ubicación.

Se complementa con políticas de trabajo remoto y política de dispositivos móviles.

Política de uso de programas de utilidad privilegiados (9.4.4)

Solo el Oficial de Seguridad de Datacenter, pueden hacer uso de programas que sean capaces de anular los sistemas.

En caso de servidores de producción, deben existir usuarios de mantención asociados a cada software y no realizar estas labores por root.

Políticas y procedimientos de transferencia de la información (A.13.2.1 - A.13.2.3 - **A.14.2.4**)

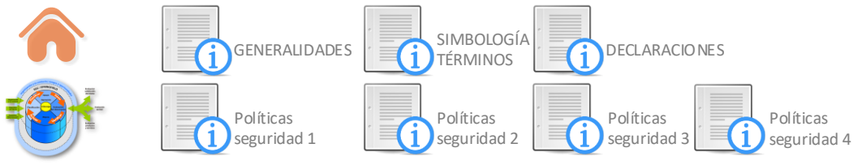
La información corporativa se transfiere por Google (g-suite)
Con externos es encriptado.
Para Orion (Amazon WS) por VPC y servidores externos por VPN.

Mensajes electrónicos (A.13.2.3)
Política de Mensajería Electrónica:
"El uso de otros servicios de mensajería electrónica, debe pedir la aprobación al comité de seguridad."

Restricciones sobre los cambios a paquetes de software (A.14.2.4)
No se modifican paquetes de software externo

POLÍTICA DE SEGURIDAD 4

Soluciones Tecnológicas para el Comercio Exterior



Responsables: Oficiales de Seguridad
Objetivo: Establecer las directrices generales para gestionar oportuna y eficazmente los activos de la empresa, frente a amenazas internas o externas.

Política de ingreso a Datacenter

Todo el personal externo a Editrade que requiera el ingreso al Data Center debe ser registrado y acompañado por responsable del área

El personal de Editrade que no pertenece al área debe ser acompañado por un responsable del área

REGISTRO DE INGRESO DE TERCEROS AL DATA CENTER PAP02-R06

Política de ingreso de terceros

Todo tercero que ingrese a Editrade debe ser registrado (digitalmente)

REGISTRO DE INGRESO DE TERCEROS A EDITRADE PAP02-R05

Acciones en caso de Hurto

El hurto debe ser informado a la brevedad a la jefatura directa y al área de control TI
Acciones de control:
Restricción de acceso
Registro en Lista de Activos, fecha, circunstancias y otros antecedentes

Política de gestión de password (9.4.3)

1. Las características de seguridad, dependerán de las capacidades del sistema a usar.
2. Las passwords de activos corporativos se administran en el sistema TeamPass, el cual, él mismo recomienda contraseñas seguras.
3. Las passwords de cada persona de la organización, las debe almacenar en el software corporativo de claves asignado.(ver lista blanca de aplicaciones corporativas)
4. Complementar con Política de uso de clave: (9.3.1) Ubicada en Personas

GESTIÓN DE PERSONAS PAP08

5. Recordar al personal las buenas prácticas de creación de passwords y de cambios regulares de la clave.

Política de confidencialidad

Todo personal Editrade y terceros que requiera información crítica interna o externa que maneje Editrade o que este bajo su custodia debe suscribir el compromiso de no divulgación correspondiente

ACUERDO DE CONFIDENCIALIDAD PAP02-R02

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE TERCEROS PAP02-R03

Política de propiedad del cliente

1. El resguardo de la propiedad del cliente se establece en los contratos y/ o acuerdos establecidos

2. A través de el área de Control y Gestión TI, se asegurará la comunicación y registro de acciones que resguarden la propiedad del cliente.

Política de Acceso a redes y servicios de Red (9.1.2; 9.2.2)

1. La gestión de acceso a las redes y servicios de red de la organización, está a cargo del Oficial de Seguridad de Datacenter.

2. Son gestionadas por medio de las políticas del cortafuego el acceso según roles, el cual se apoya de la lista de activos.

3. La validación del acceso, está dada por la MAC del dispositivo.

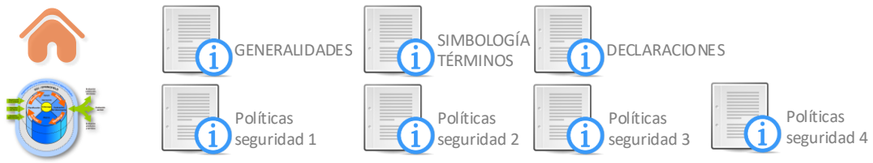
4. Para conexiones desde fuera de la red corporativa, se deben regir bajo las políticas de trabajo remoto.

5. Por medio del sistema Nagios, se debe monitorear la Red.

Procedimiento de inicio de sesión seguros (9.4.2)

Se deben realizar las siguientes prácticas según corresponda:
1. El uso de login y password para acceder a sistemas y servidores.
2. En cuanto a Servidores internos, se aplica el acceso por ssh+llave.
3. Para el Acceso remoto a servidores se utiliza vpn.
4. Utilizar, https cuando el servicio se pueda activar por esa modalidad.
5. Se aplican políticas de acceso por firewall.

CONTROLES DE MALWARE Y CRIPTOGRÁFICO



Responsable: Subgerente de Gestión y Control TI
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información son protegidas contra malware.

Control de MalWare

Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información son protegidas contra malware

Instrumentos:

Políticas del cortafuego
Uso de Antivirus Corporativo
Uso de ssh y vpn
Lista Blanca de Aplicaciones Corporativas

Lista blanca de aplicaciones corporativas

La lista blanca de aplicaciones corporativas se encuentra administrada por el área de TI y se registra en el sistema de inventarios.

GLPI

Política de uso de controles criptográficos (10.1.1)

- Se usarán controles criptográficos dependiendo de la criticidad de la información.
- Se usarán controles criptográficos para:

a)Conexión remota, como lo es el teletrabajo (VPN)
b)Publicar sistemas (HTTPS)
c)Transferir información a otras redes, como Amazon o Servidores de clientes (SSH, VPN)
d)Al usar redes públicas (VPN)
e)Encriptación de discos duros en aquellos notebook que tengan permiso de trabajo remoto.

Política Manejo de llaves (Administración de Claves) (10.1.2)

El uso, la protección y el ciclo de vida de las claves criptográficas, es controlado y manejado por el área de control TI.

Llaves de encriptación para estaciones de trabajo

Las claves criptográficas son manejadas en el gestor de contraseñas y definida al momento de realizar la encriptación. Esta clave es mantenida hasta la eliminación de la encriptación al formatear la unidad de almacenamiento.

Las unidades de almacenamiento son formateadas cuando los equipos presentan fallas y si es necesarario según lo determinado por el equipo de control TI o cuando el equipo es reasignado o dado de baja.

ESTRUCTURA ORGÁNICA

Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerencia de administración y finanzas
Objetivo: Conocer las agrupaciones naturales de trabajo

Área Administración

Objetivo General del Área
Controlar el uso de los recursos económicos de la empresa y ejercer el control financiero y tributario, junto con mantenciones no relacionadas a producción

Gerencia General

Objetivo general
Planificación y proyecciones de la empresa.
Servicios principales:
Formulación y ejecución de planes
Supervisión de actividades de comercialización y ventas.

Administración

Servicios principales:
Labores contables, Informes financieros y contables, seleccionar y coordinar proveedores de servicios generales, Pago a proveedores, Cobranza

Cobranza

Objetivo general del área
El objetivo principal de este servicio personalizado es facilitar el proceso de cobranza a través del fortalecimiento de la relación interpersonal entre cobrador y acreedor así como también el vínculo entre Editrade y el cliente.
Servicios Principales:

- Realizar la cobranza de su cartera de clientes.
- Recuperación de activos.
- Bajar los índices de antigüedad de cuentas por cobrar.
- Fortalecer los vínculos entre el cliente y Editrade a través de un trato personalizado.
- Disponer de información oportuna de soporte para la toma de decisiones por parte de su empresa. La rendición de cuentas se puede adaptar a múltiples formatos como ser medios magnéticos, Internet, papel, etc.

Área Desarrollo y Proyectos

Objetivo General del Área
Planificar y controlar los desarrollos y proyectos de los Software. Gestionar la continuidad operativa.

Área de Ingeniería

Operaciones

Objetivo general del área
Levantar, determinar y establecer requerimientos para el desarrollo de soluciones de tecnologías de la información. Responder a los requerimientos derivados del Desarrollo y arriendo del Software.

Servicio Principales:
Desarrollos asociados al software
Diagnóstico de problemas y propuesta de soluciones al software
Extender o desarrollar nuevas soluciones de software.
Mantención de software
Mejoras del software
Desarrollos asociados al software
Diagnóstico de problemas y propuesta de soluciones al software
Extender o desarrollar nuevas soluciones de software

Área Servicios y Control de Calidad

Objetivo General del Área
Gestionar la seguridad de la información, la continuidad operacional y satisfacción de los clientes mediante el control de la calidad.

Área Gestión de Control y Calidad

Servicio al Cliente

Objetivo general del área
Coordinar los aspectos administrativos y de control para la implementación y mantención integral de las normas de calidad y seguridad de la información al interior de la organización.
Servicios Principales:

- Analizar continuamente los intereses de los clientes y representar a los clientes en la organización.
- Gestionar los reclamos de los clientes, según el sistema de calidad
- Gestionar la central Telefónica y los diferentes canales de comunicación de la empresa.

Calidad

Objetivo general del área
Coordinar los aspectos administrativos y de control para la implementación y mantención integral de las normas de calidad y seguridad de la información al interior de la organización.
Servicios Principales:

- Analizar datos relacionados con la calidad, evaluar hechos, consolidar datos y reportarlos
- Integrar y combinar requisitos de distintas normas de sistemas de gestión y otros requisitos internos y externos
- Actuar como formador interno para cuestiones relacionadas con el sistema de gestión de la calidad y otros sistemas de gestión
- Promover el sistema de gestión de la organización
- Supervisar en forma directa el SGC y SGS en su conjunto, dar apoyo a los responsables de procesos en el desarrollo de sus funciones y coordinar todas las acciones que permitan el normal funcionamiento del SGC y SGS.

Gestión y Control TI

Objetivo general del área
Proporcionar a la administración una guía para el uso idóneo y proyección de los recursos informáticos de Editrade, así como su respectivo control y mantenimiento.
Servicios Principales:
Gestionar la seguridad de la información en los ámbitos de:

- Compromiso del personal
- Seguridad física y ambiental
- Seguridad en las operaciones y comunicaciones
- Control de acceso
- Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica
- Continuidad de los servicios de TI
- Decisiones sobre asuntos estratégicos de TI
- Implementación de tecnologías de información
- Prestación de servicios y mantenimiento
- Seguimiento y evaluación de los procesos de TI

Soporte

Objetivo General del Área
Recibir y gestionar las necesidades de los clientes, asegurando su solución a través de la resolución directa o de la derivación a la area de mantenimiento de software.
Servicios Principales:

- Centralización de la comunicación con el cliente
- Atención al cliente de manera inmediata.
- Planificación capacitaciones formales al cliente de puesta en marcha inicial y mantención de Software en terreno y remotas

Mantenimiento Software

Objetivo General del Área
Recibir y gestionar las necesidades de los clientes, asegurando su solución a través de la resolución directa o de la derivación a el área de Operaciones.
Servicios Principales:

- Actualizaciones e instalaciones de los sistemas.
- Soporte de sistemas.
- Estudiar y analizar mejoras de los softwares para la mejora continua.
- Planificación capacitaciones formales al cliente de puesta en marcha inicial y mantención de Software en terreno y remotas.

Área Comercial

Objetivo General del Área
Servir como canal de comunicación entre Editrade y el cliente, para asegurar correcta recepción y determinación de sus requerimientos. Asegurar, validar y comunicar a los niveles que correspondan los requisitos del cliente y sus modificaciones.

Gestión Comercial

Servicio principales:
Captación de clientes, Comunicación de requerimientos al área correspondiente, Creación de presupuestos

Área Capacitación

Objetivo General del Área
Aumentar las capacidades del personal en comunicación efectiva, para las relaciones interpersonales, de negociación y resolución de problemas para atender correctamente las necesidades de los clientes.

Gestión De Capacitación

Servicio principales:
Captación del personal , Organizar seminarios internos como externos, Desarrollar material educativo digital e impreso, Coordinar programas de tutoría para nuevos representantes de atención al cliente, Evaluar el impacto de los cursos a partir del desempeño del personal y la satisfacción del cliente.

Comité de Seguridad de la Información

Objetivo general
Asegurar el cumplimiento de los requisito normativos del estándar ISO 27001.
Informar sobre el desempeño del sistema de seguridad de la información a la alta dirección y cuando corresponda dentro la organización.

Servicios principales:
Analizar, planificar, comunicar y promover los elementos del sistema de seguridad de la información en los niveles y formas atingentes a cada proceso.
Analizar, informar y tomar acciones en relación al desempeño del sistema de seguridad de la información.

Miembros del comité

- OFICIAL DE SEGURIDAD DE LA INFORMACIÓN DE EDITRADE
- OFICIAL DE SEGURIDAD DE DATACENTER Y COMUNICACIONES
- OFICIAL DE SEGURIDAD DOCUMENTAL Y COMPLIANCE
- OFICIAL DE SEGURIDAD DE SOFTWARE

Perfiles de cargo/rol

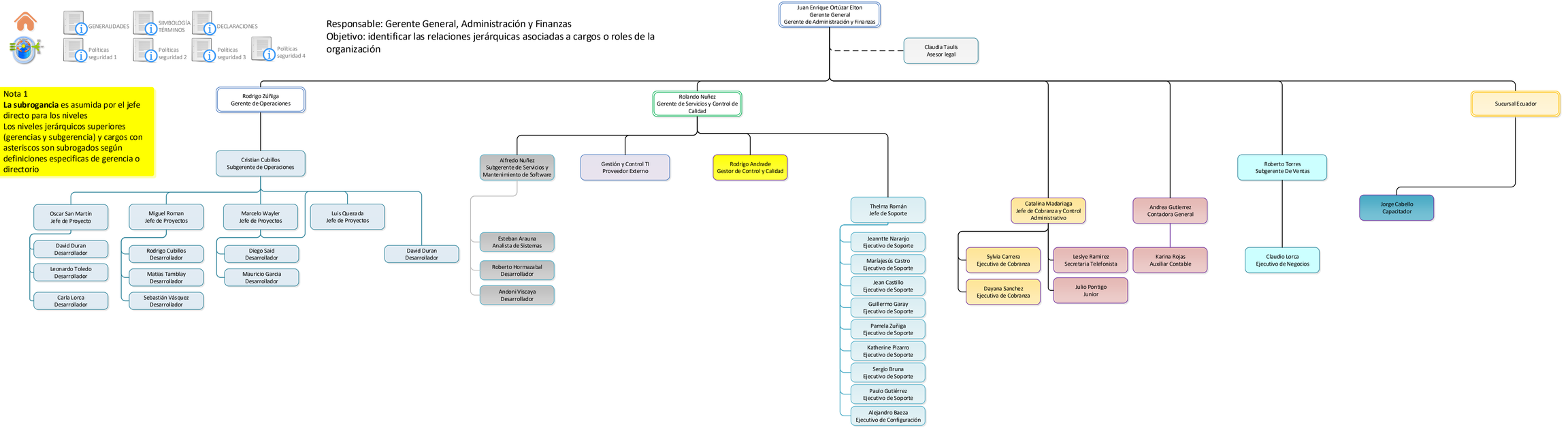
ORGANIGRAMA

Editrade
Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES
Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerente General, Administración y Finanzas
Objetivo: identificar las relaciones jerárquicas asociadas a cargos o roles de la organización

Nota 1
La subrogancia es asumida por el jefe directo para los niveles
Los niveles jerárquicos superiores (gerencias y subgerencia) y cargos con asteriscos son subrogados según definiciones especificas de gerencia o directorio



GESTIÓN COMERCIAL

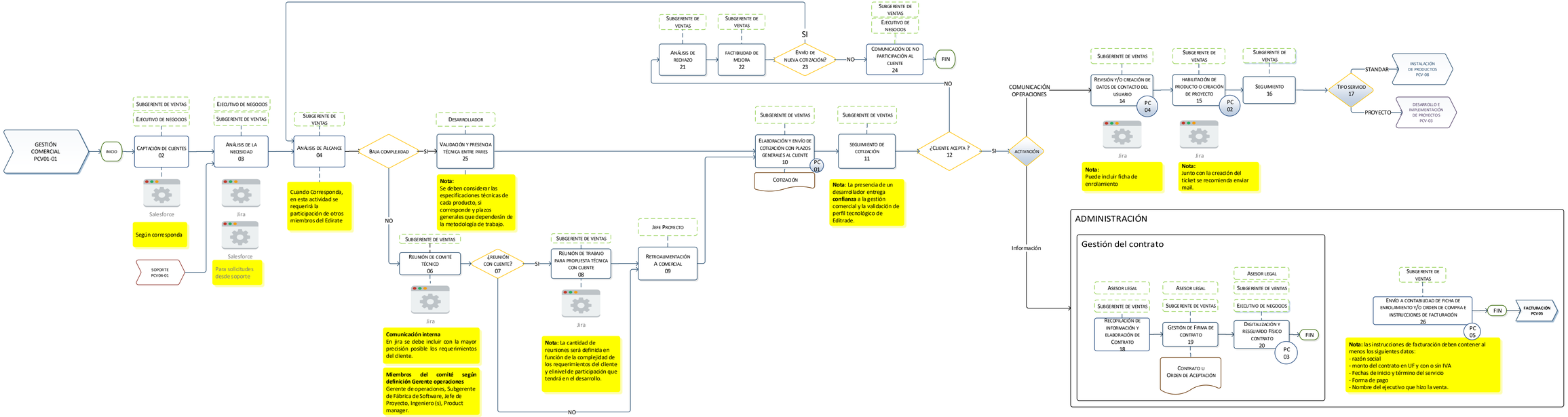
Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de ventas y Ejecutivo de Negocios

Alcance: Todas las actividades asociadas a la Gestión Comercial de productos existentes de Editrade

Objetivo: Gestionar y determinar las necesidades y requerimientos del cliente y aquéllos relacionados con el producto, para entregar la mejor solución posible.
Comunicar correctamente los requerimientos de los clientes al área de operaciones y dar el inicio formal de un proyecto cuando corresponda.



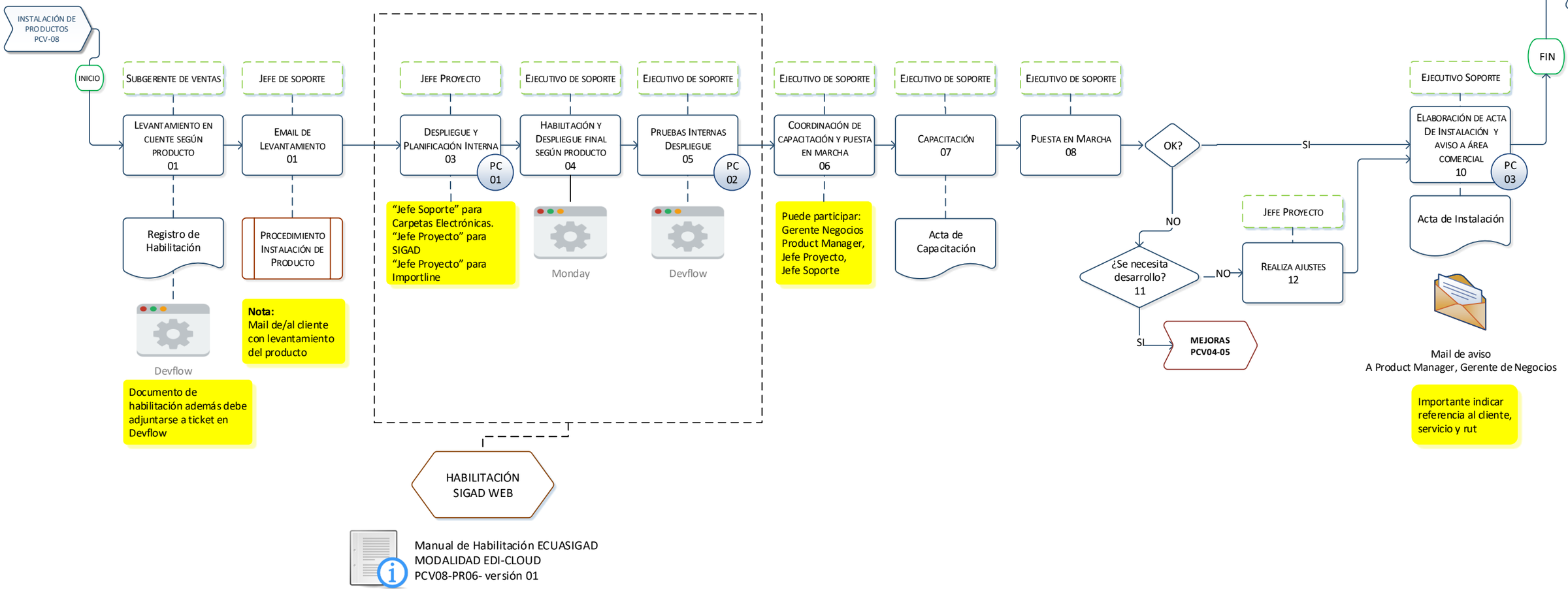
INSTALACIÓN DE PRODUCTO

Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de Servicios y Mantenimiento Software, Jefe de Soporte
Alcance: Instalación de productos de línea
Objetivo: Asegurar la correcta instalación de los productos de línea de Editrade



DISEÑO Y DESARROLLO

14.2.3-14.2.5-14.2.6

Responsable: Jefe de Proyecto
Alcance: Proyectos que comprendan diseño y desarrollo de Proyectos de *Software*.

Objetivo: Asegurar que el diseño y el desarrollo de soluciones de *software* de los proyectos de Editrade cumpla los requisitos del cliente, los legales (si corresponde) y reglamentarios en los plazos y condiciones acordadas.

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Política de acceso a código fuente. (A.9.4.5)

Se debe contemplar lo siguiente:

- La organización establece que **solo el equipo de desarrollo** puede acceder al código fuente de los sistema.
- Este acceso, va de la mano con el control de cambios, el cual solo puede efectuarse por medio de los procesos "Mantención", " Mejora" o "Diseño y Desarrollo Proyectos".
- Las personas deben tener firmado el acuerdo de confidencialidad.

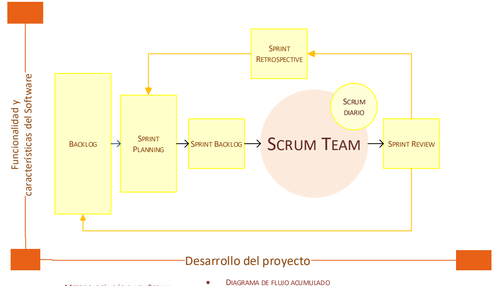
Consideraciones de seguridad de proyecto: 14.1.1

- Acceso por una red segura a los software que se usan de apoyo a este proceso.
- Debe existir el documento project charter para saber los interesados y comunicación
- La documentación debe estar resguardada en el sistema Jira y Monday respectivamente.
- La interacción de mensajería electrónica con el cliente debe ser por medio del email corporativo.
- La creación de usuarios debe ser ejecutada por el dueño del activo "Jira" y "Monday".
- Se debe desarrollar el proyecto con un notebook seguro.

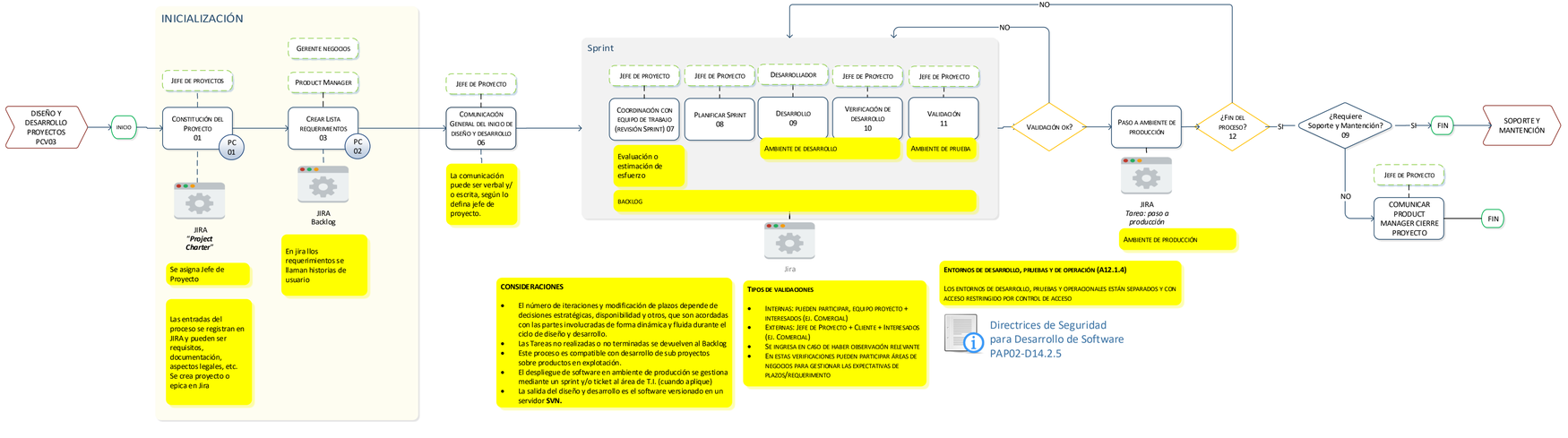
Riesgos

N°	Factor de Riesgo	Riesgo	Impacto	Ocurrencia	Acción de Mitigación
1	Levantamiento de requerimientos	Desalineamiento de información sobre requerimiento del cliente y desarrollo	Alto	Alta	Incorporación de modelo iterativo de diseño y desarrollo con la participación del cliente
2	Cumplimiento de Plazo	Incumplir plazos acordados con el cliente, con la probabilidad de pérdida del negocio	Alto	Alta	Modelo iterativo conlleva el control de plazos de común acuerdo con el cliente Comunicación con área comercial, para controlar expectativas de entrega
3	Información	Pérdida de información del proyecto por ausencia de desarrollador o Jefe de Proyecto	Alto	Baja	Equipo de trabajo Registro de Jira Respaldo de código fuentes y bases de datos

Metodología de Desarrollo



- Metodología basada en Scrum
- Jira como Gestionador de proyectos
- Priorización de actividades
- Épicas: agrupaciones de tareas
- Diagrama de flujo acumulado
- Resguardo de Información del diseño y desarrollo
- Repositorio de Código fuente con control de versiones SVN
- Conocimiento de modelos y metodologías para el desarrollo de software



CONSIDERACIONES

- El número de iteraciones y modificación de plazos depende de decisiones estratégicas, disponibilidad y otros, que son acordadas con las partes involucradas de forma dinámica y fluida durante el ciclo de diseño y desarrollo.
- Las Tareas no realizadas o no terminadas se devuelven al Backlog
- Este proceso es compatible con desarrollo de sub proyectos sobre productos en explotación.
- El despliegue de software en ambiente de producción se gestiona mediante un sprint y/o ticket al área de T.I. (cuando aplique)
- La salida del diseño y desarrollo es el software versionado en un servidor **SVN.**

TIPOS DE VALIDACIONES

- Internas: pueden participar, equipo proyecto + interesados (ej. Comercial)
- Externas: Jefe de Proyecto + Cliente + Interesados (ej. Comercial)
- Se ingresa en caso de haber observación relevante
- En estas verificaciones pueden participar áreas de negocios para gestionar las expectativas de plazos/requerimiento

Entornos de desarrollo, pruebas y de operación (A12.1.4)

Los entornos de desarrollo, pruebas y operacionales están separados y con acceso restringido por control de acceso

Directrices de Seguridad para Desarrollo de Software PAP02-D14.2.5

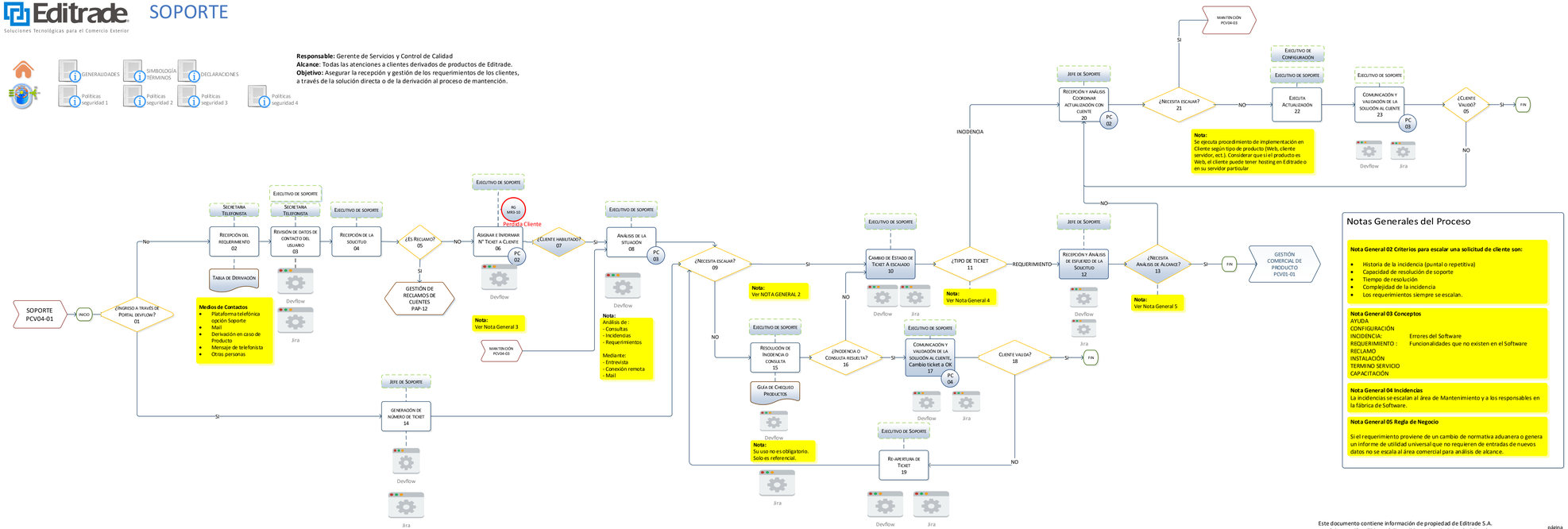
SOPORTE

Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerente de Servicios y Control de Calidad
Alcance: Todas las atenciones a clientes derivados de productos de Editrade.
Objetivo: Asegurar la recepción y gestión de los requerimientos de los clientes, a través de la solución directa o de la derivación al proceso de mantención.



Notas Generales del Proceso

Nota General 02 Criterios para escalar una solicitud de cliente son:

- Historia de la incidencia (puntal o repetitiva)
- Capacidad de resolución de soporte
- Tiempo de resolución
- Complejidad de la incidencia
- Los requerimientos siempre se escalan.

Nota General 03 Conceptos

AYUDA
CONFIGURACIÓN
INCIDENCIA: Errores del Software
REQUERIMIENTO : Funcionalidades que no existen en el Software
RECLAMO
INSTALACIÓN
TERMINO SERVICIO
CAPACITACIÓN

Nota General 04 Incidencias

La incidencias se escalan al área de Mantenimiento y a los responsables en la fábrica de Software.

Nota General 05 Regla de Negocio

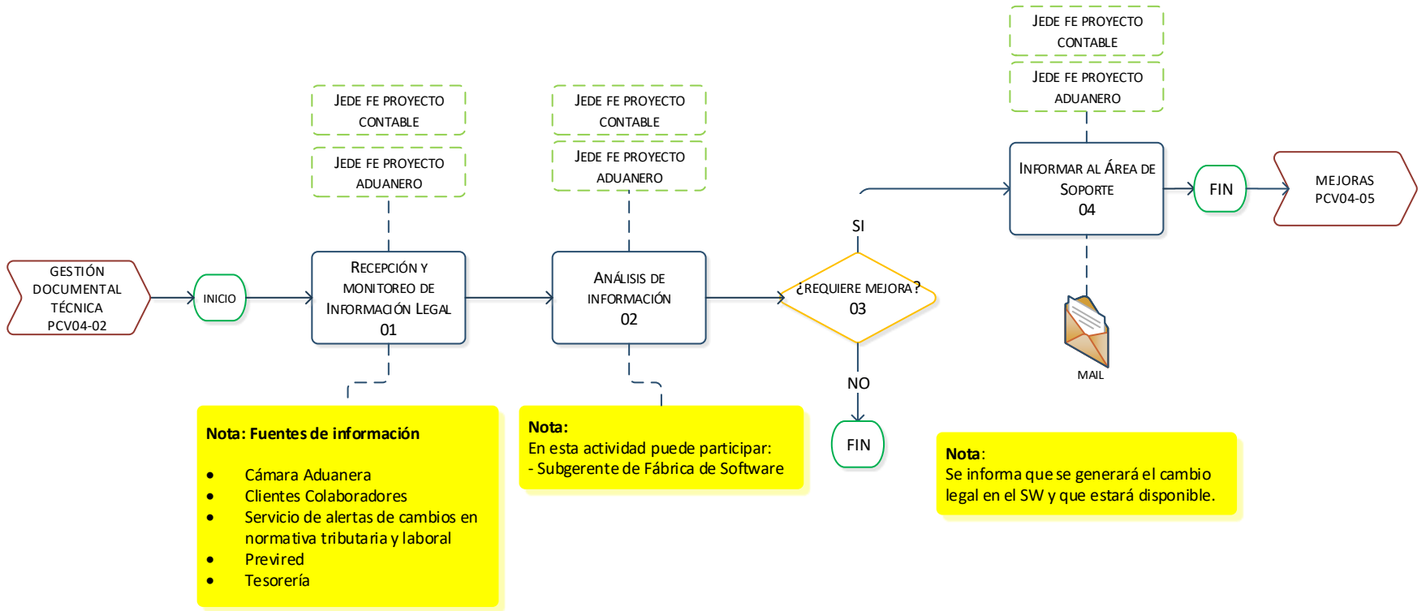
Si el requerimiento proviene de un cambio de normativa aduanera o genera un informe de utilidad universal que no requieren de entradas de nuevos datos no se escala al área comercial para análisis de alcance.

GESTIÓN TÉCNICA DOCUMENTAL

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

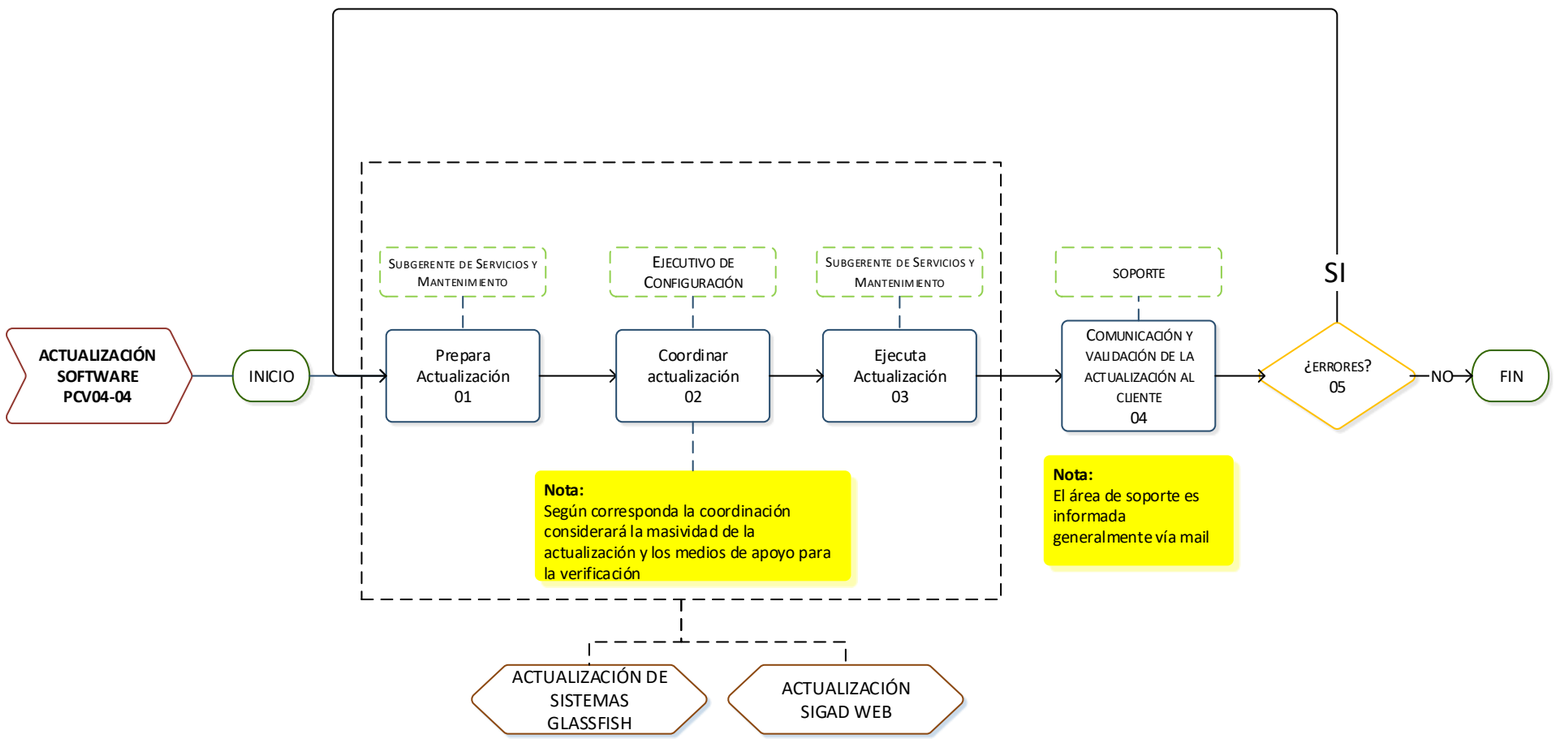
Responsable: Jefe de proyecto
Alcance: Actualizaciones legales, aduaneras y contables de SIGAD.
Objetivo: Mantener el sistema actualizado con la normativa vigente. Informar al cliente de las actualizaciones efectuadas en el Software.



ACTUALIZACIÓN DE SOFTWARE

Soluciones Tecnológicas para el Comercio Exterior

Responsable: Subgerente de Servicios y Mantenimiento de Software
Alcance: Disponer a los clientes de una versión actualizada del sistema
Objetivo: Realizar en nuestros clientes periódicas actualizaciones del sistema.



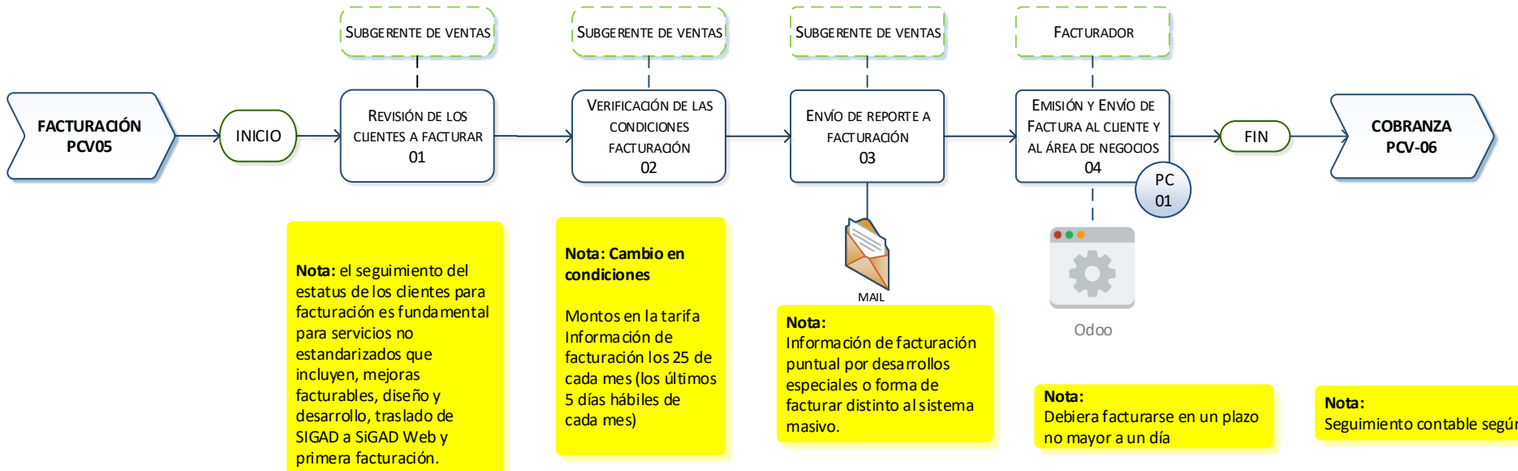
FACTURACIÓN

Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

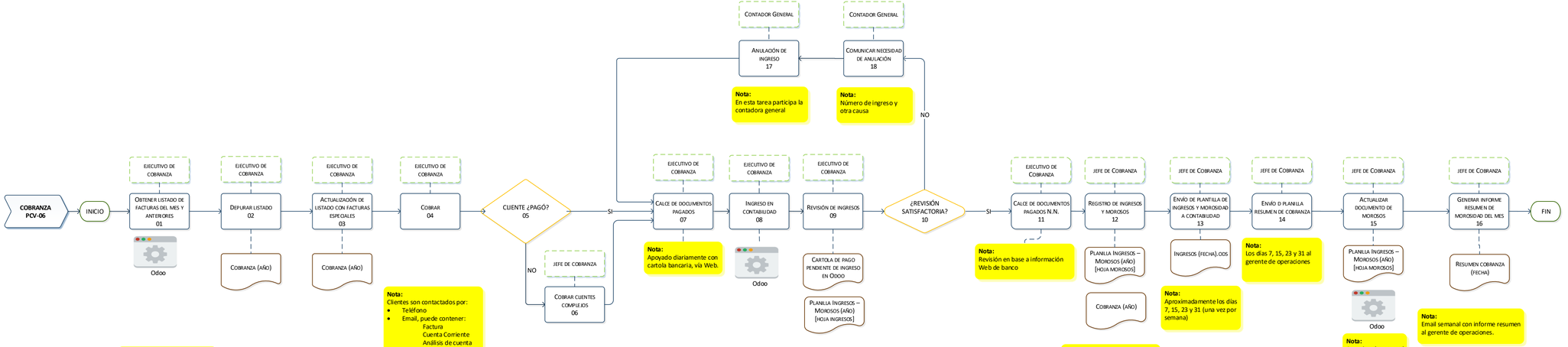
Responsable: Contador General
Alcance: Factura a clientes con arriendo y mantención de productos.
Objetivo: Asegurar que los productos sean facturados según lo acordado con el cliente.



COBRANZA

Soluciones Tecnológicas para el Comercio Exterior

Responsable: Contador General
Alcance: Factura a clientes con arriendo y mantención de productos.
Objetivo: Asegurar que los productos sean facturados según lo acordado con el cliente.



Política de corte y reposición de servicios

Determinación de Corte
- La principal causa de corte de servicio total o parcial es comportamiento de pago del cliente
- La determinación de corte es acompañada por un proceso de negociación determinado por la gerencia general cuyo resultado puede ser el corte parcial, total o el pago de la deuda.
- La determinación de corte total o parcial de un servicio es tomada por la gerencia general a la luz de información histórica de la relación con el cliente en cuanto al comportamiento de pago y consistencia en los servicios prestados por parte de Editrade y el resultado del proceso de negociación

Reposición del Servicio
- La determinación de reposición del corte es tomada por el gerente general

Acción a tomar con el cliente
El cliente es informado del corte o reposición vía mail, dejando copia oculta a:
- Gerente de operaciones

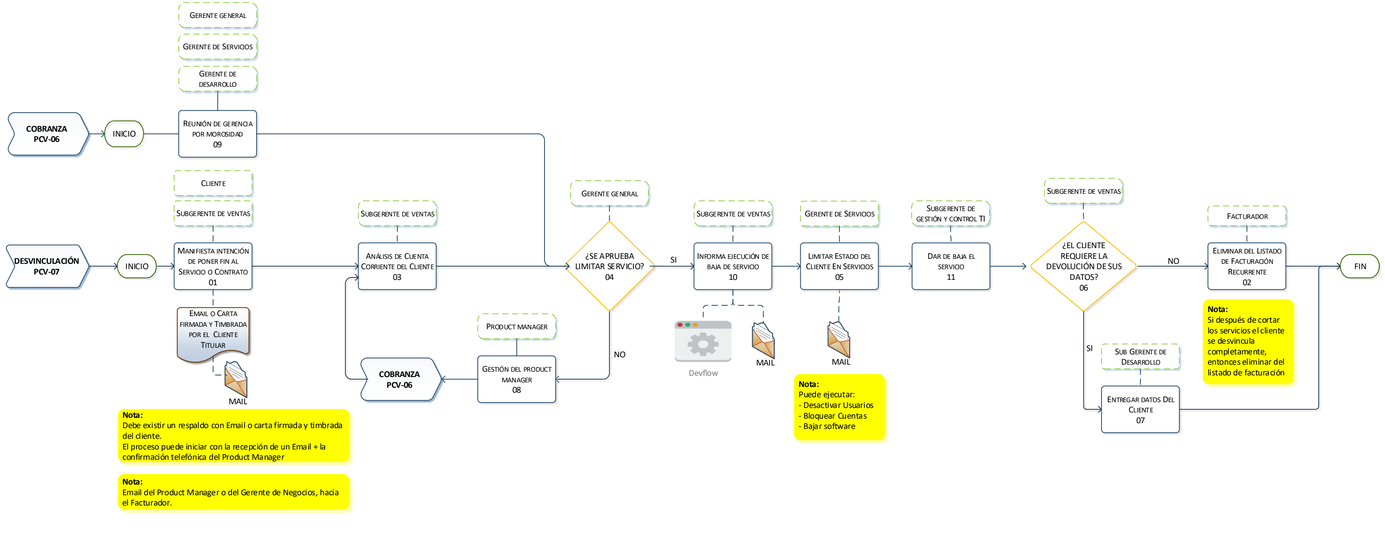
Ejecución del Corte
La ejecución del corte dependerá de la gerencia de operaciones con apoyo de la subgerencia TI

DESVINCULACIÓN DE CLIENTE

Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerente General
Alcance: Clientes que pongan fin a uno o varios servicios o corte de servicios por deuda.
Objetivo: Asegurar el termino de los servicios al cliente, verificar deudas pendientes y entrega de los datos que sean de propiedad del cliente.

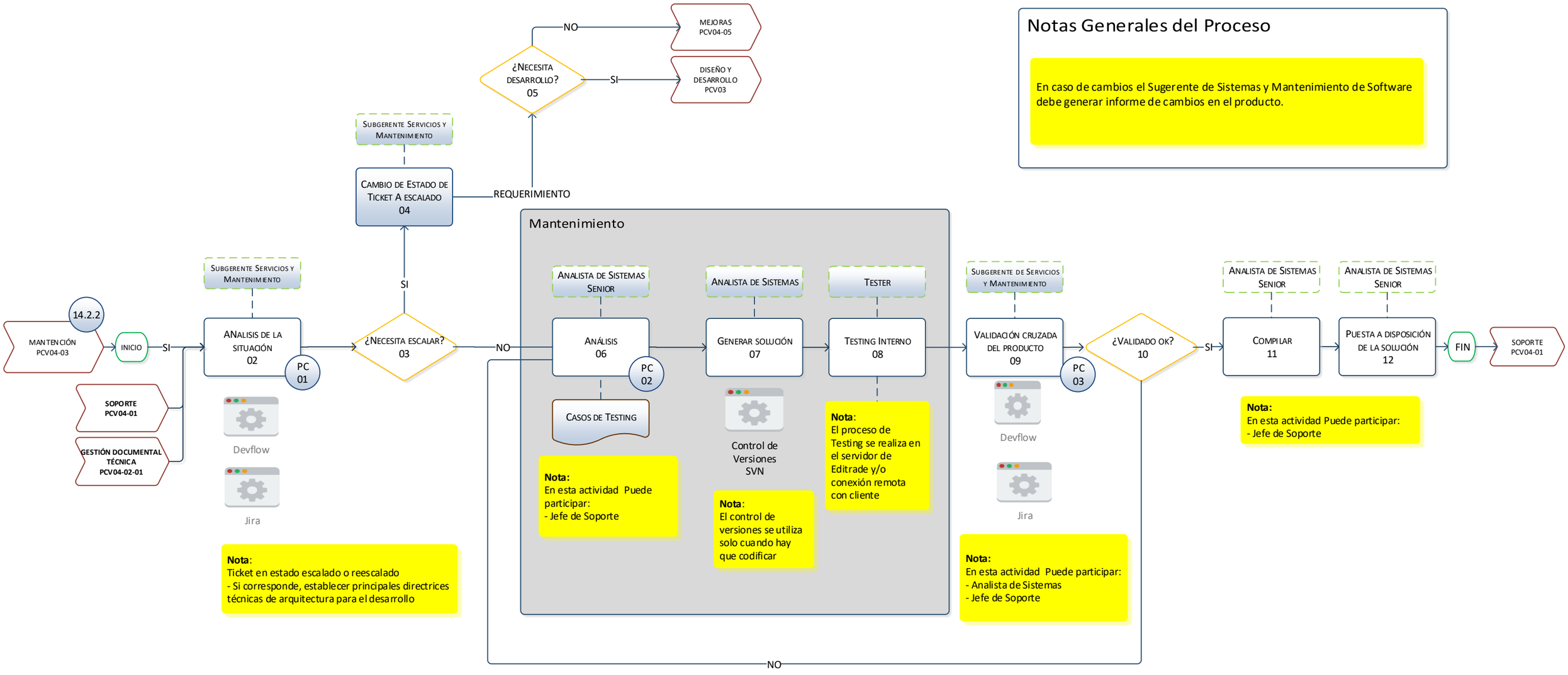


MANTENCIÓN

14.2.2-14.2.3-14.2.8-14.2.9

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de Servicios y Mantenimiento de Software
Alcance: Mantenimiento de productos existentes o proyectos
Objetivo:
Planificar y gestionar soluciones de productos existentes bajo condiciones controladas, mantenciones, relacionados con un producto o proyecto.



Notas Generales del Proceso

En caso de cambios el Sugerente de Sistemas y Mantenimiento de Software debe generar informe de cambios en el producto.

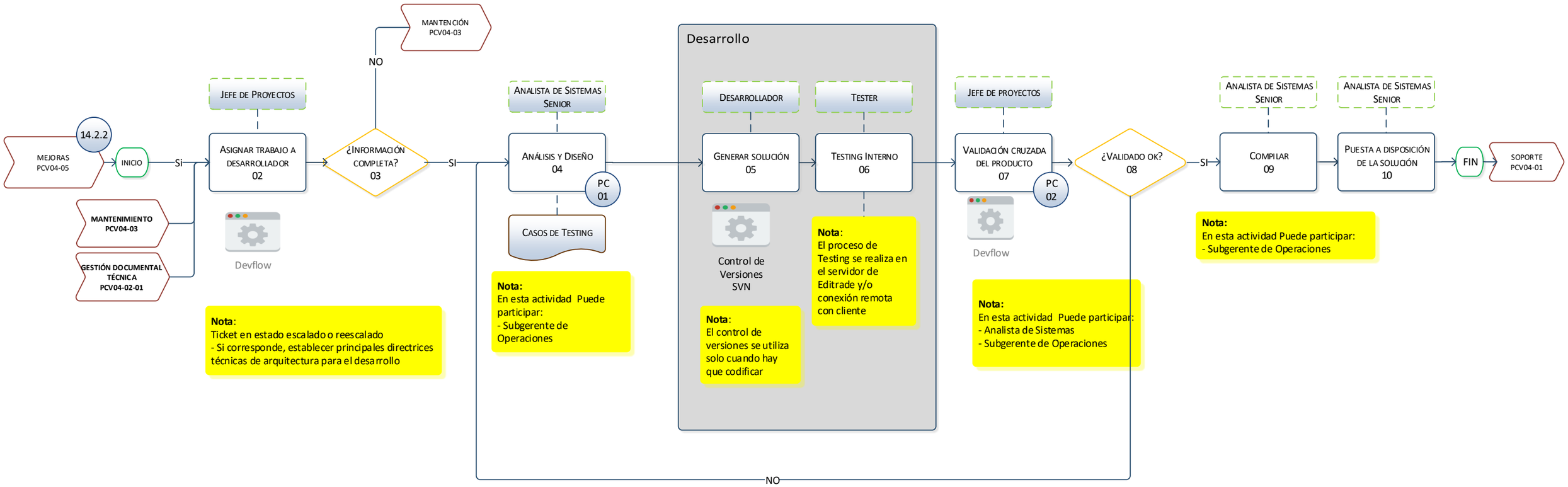
MEJORAS

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de Desarrollo
Alcance: Desarrollos y actualizaciones de productos existentes o proyectos
Objetivo:
Planificar y desarrollar soluciones particulares y universales de productos existentes bajo condiciones controladas, mejoras o actualizaciones, relacionados con un producto o proyecto.

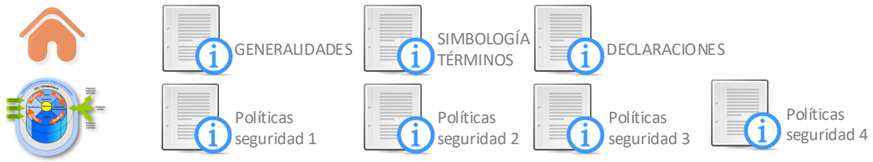
Notas Generales del Proceso

En caso de cambios el Jefe de Proyecto debe generar informe de cambios en el producto.



COMUNICACIÓN AL CLIENTE

CÓDIGO: PAP-13



Responsable: Gestor de Calidad
Alcance: Grupos objetivos de cada producto o servicio
Objetivo: Asegurar instancias de comunicación con el cliente

Solicitante Gerente Operaciones

	Periodicidad	Tema	Criterio	Medio
1	anual	Mejoras a los sistemas actualizaciones	Todas las actualizaciones son comunicadas	Mail base de datos segmentada
				Masivo: Twitter
2	Excepciones	x Sistema	Lentitud, inestabilidad y otro	Grupo: Mail
		x Transmisiones a la aduana	Retraso entre 30 a 60 min	Twitter + Login SIGAD
			Mayor a 60 min	Mail base de datos segmentada

Políticas Generales:

- Editrade se compromete a buscar siempre una comunicación fluida y eficaz que permita tener relaciones de mutuo beneficio, entendiendo que su rol es gravitante para el servicio que presta al cliente.

SALIDA NO CONFORME (CONTROL SERVICIO NO CONFORME)

PAP08-05

Responsable: Gestor de Calidad

Objetivo: asegurar de que las salidas que no sean conformes con los requisitos son identificadas, controladas y corregidas.

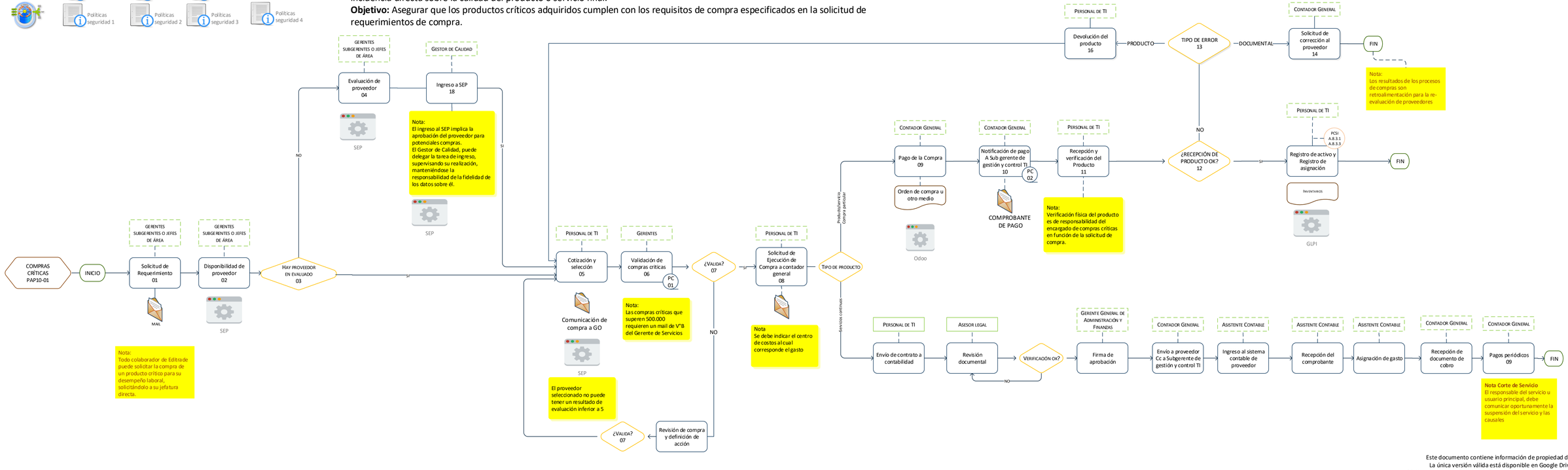
#	área	Proceso	Medio de detección	Tipo de Producto no conforme	Descripción	RESPONSABLE	Acciones preliminares	Acciones - posibles	registro y control	Excepciones
1	DISEÑO Y DESARROLLO	PCV03-02 IMPLEMENTACIÓN y PUESTA EN MARCHA DE SOFTWARE	**Actividades 07 , 08 1. ¿acciones efectivas? (Actividad 07) 2. Análisis de la situación (Actividad 08)**	**Inviabilidad de proyecto**	Error en la definición del alcance del proyecto, no identificado en los controles anteriores del proceso global de diseño y desarrollo que deriva en la inviabilidad del proyecto	Subgerente de Fábrica de Software	1.- Verificar el criterio utilizado para definir la magnitud del ajuste. Desde la actividad 07 del proceso en cuestión 2.- Análisis de la situación en conjunto con gerencia de operaciones, comercial y gerencia general según sea necesario	1.- Suspensión o continuidad del proyecto con costo a empresa 2.- Suspensión o continuidad del proyecto con costo a cliente 3.- Determinación de otras medidas compensatorias según disposición de gerencia general	Informe de caso	
2	PRODUCTO ESTÁNDAR	GESTIÓN Y CONTROL TI PAP-02	**Monitoreo de continuidad operacional del servicio**	**Suspensión del servicio**	Suspensión del servicio, que genere la llamada del cliente informando que no pueden acceder a un sistema alojado en los servidores controlados por Editrade y/o a su información alojada en dichos servidores. Nota: La fábrica de software debe declarar que la caída es de responsabilidad de Editrade. Se excluyen: los servicios alojados parcial o totalmente en los servidores del cliente. caídas del enlace del cliente.	Gerente de Operaciones	1.- Identificación del origen del corte 2.- Determinación del alcance 3.- Impacto en la propiedad del cliente	Comunicado interno de solución y tiempo estimado de reposición a soporte y central telefónica Nota: Las acciones específicas de control, contención y solución dependerán del equipo técnico especialista	Informe de caso	Suspensiones programadas e informadas al cliente con antelación, según acuerdos del SLA.

COMPRAS CRÍTICAS Y CONTROL DE ACTIVOS TANGIBLES

Editrade
Soluciones Tecnológicas para el Comercio Exterior

GENERALIDADES | SIMBOLOGÍA TERMINOS | DECLARACIONES
Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

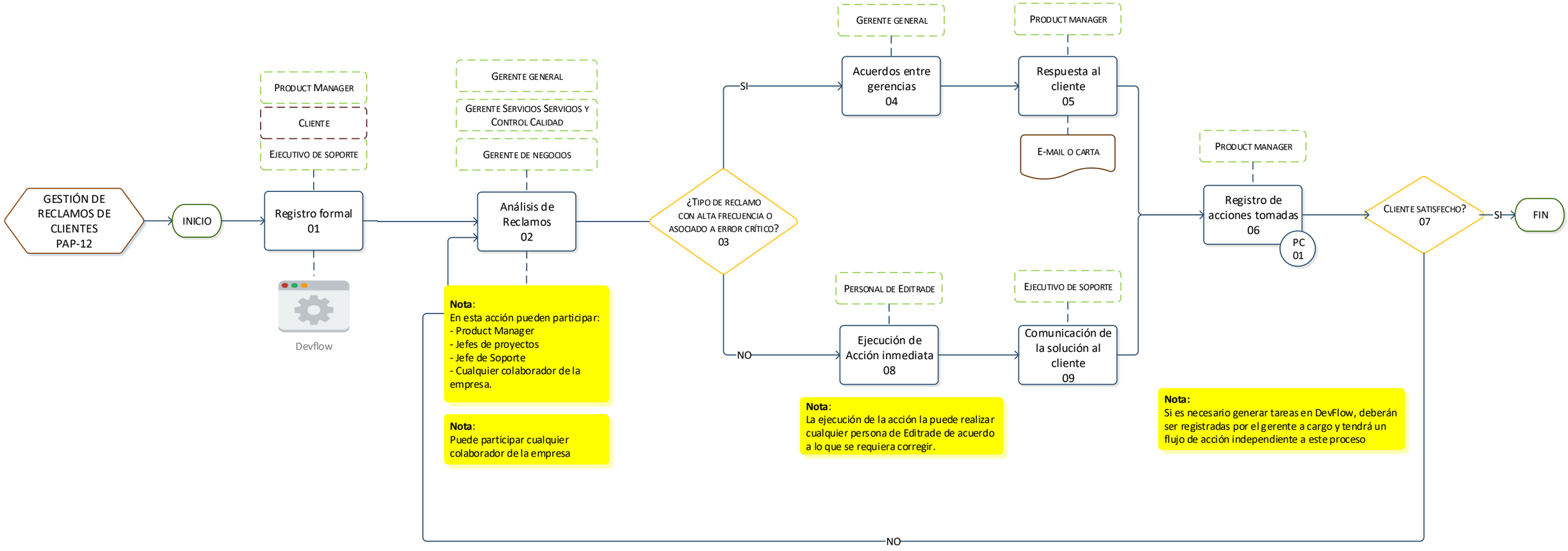
Responsable: Gerente General
Alcance: Este procedimiento es aplicable a todos los insumos y servicios críticos, adquiridos por Editrade que tienen una incidencia directa sobre la calidad del producto o servicio final.
Objetivo: Asegurar que los productos críticos adquiridos cumplen con los requisitos de compra especificados en la solicitud de requerimientos de compra.



GESTIÓN DE RECLAMOS DE CLIENTES

PAP-12

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4



PROCEDIMIENTO ACCIONES CORRECTIVAS

Soluciones Tecnológicas para el Comercio Exterior

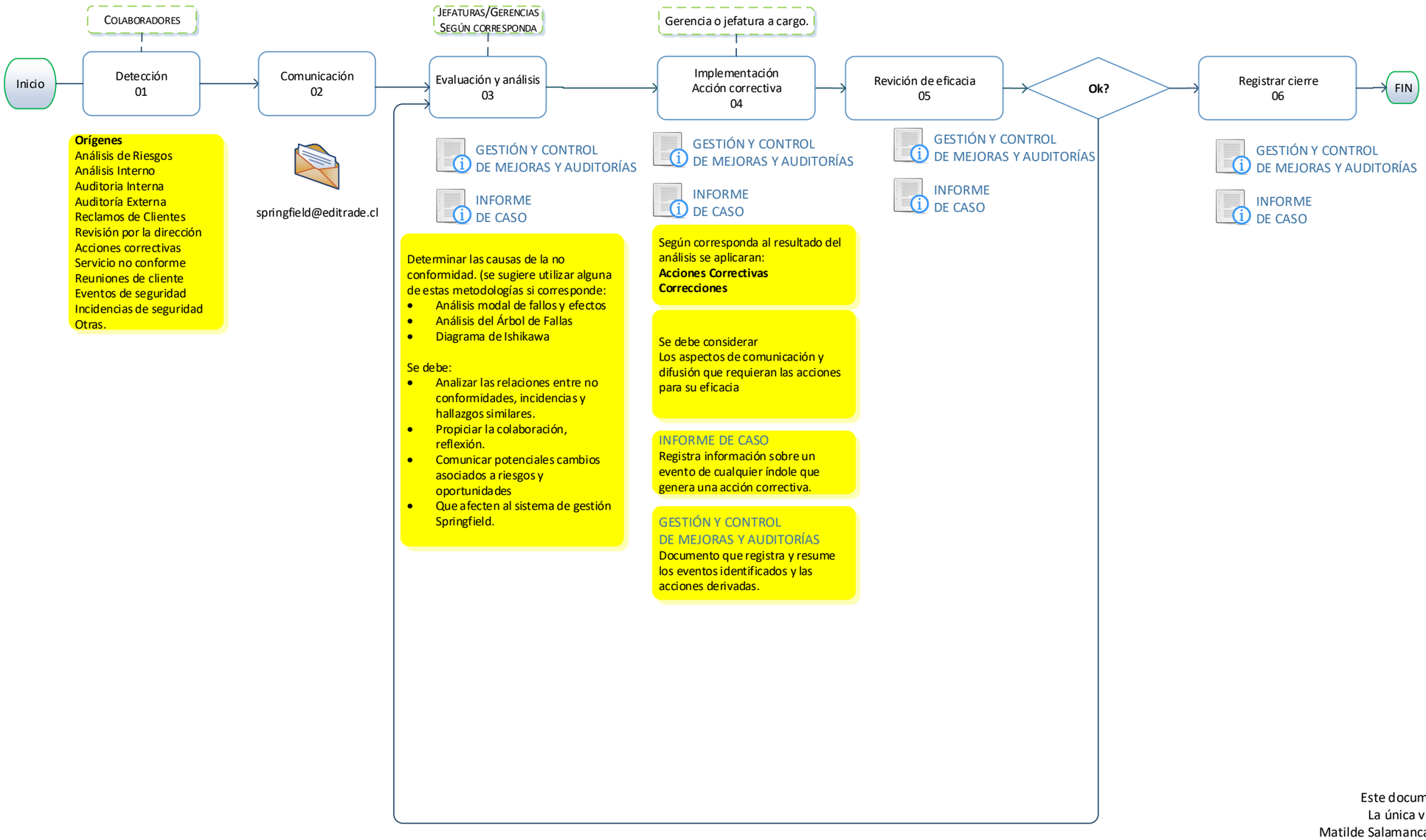
PAP04-PR01

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gestor de Control y Calidad

Objetivo: Asegurar la toma de acciones apropiadas frente a una no conformidad detectada, incidente de seguridad o producto no conforme, reaccionando oportunamente y tomando acciones pertinentes. Buscando mejorar el desempeño y la eficacia del sistema de gestión de la calidad.

Alcance:
Personas y procesos necesarios para entregar los servicios comprometidos por Editrade.



TÉRMINOS

1. **No Conformidad:** No cumplimiento de un requisito.
2. **Acción Inmediata:** Son acciones a realizar una vez detectada una no conformidad que permitan aminorar un impacto perjudicial en el cliente o en Editrade.
3. **Acción Correctiva:** Son las acciones necesarias para corregir la causa raíz de una no conformidad.
5. **Hallazgo para la mejora:** cualquier situación que tiene el potencial de convertirse en un problema o un área con potencial de mejora.
6. **Análisis:** Método utilizado para identificar las causas de una no conformidad o hallazgo, están divididos en causa y efecto. Este análisis es utilizado para recomendar acciones preventivas o correctivas.
7. **Causa:** Es el origen de una no conformidad o hallazgo para la mejora, la cual puede detectarse con el método de los cinco ¿Por qué? Se puede comenzar con un planteamiento sencillo del problemas que explique cuál es el asunto y, desde ahí, comenzar a trabajar hacia atrás
8. **Efecto:** Es el impacto o problema detectado que genera una no conformidad, real o potencial. La identificación del efecto aporta las evidencias con que se podrá identificar la causa.
9. **Incidente de seguridad de la información**: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

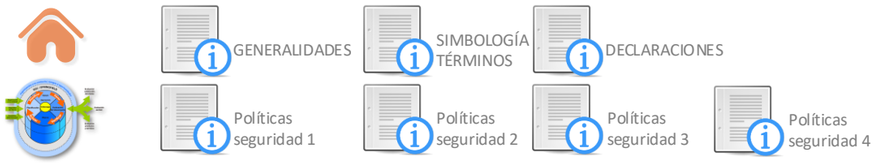
10. Producto o Servicio no conforme:

Nota general 2
Los análisis de causa raíz o cualquier otro tipo de metodología que apoye el proceso reflexivo

Puede aplicarse en cualquier etapa que corrija el daño real o potencial al cliente. Por ejemplo corregir un dato o corregir el algoritmo que genera el dato.

GESTIÓN DE PERSONAS

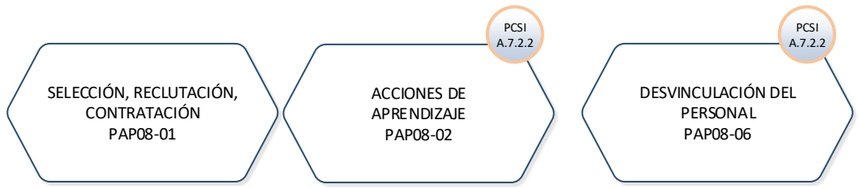
CÓDIGO: PAP08

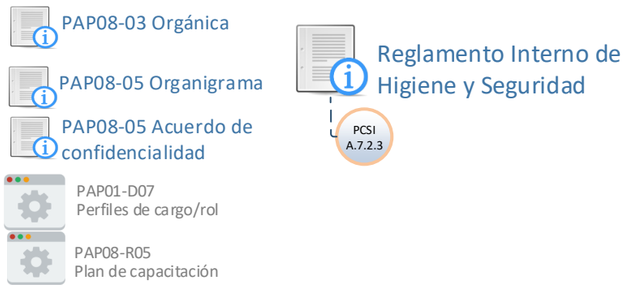


Responsable: Gestor de Control y Calidad

Objetivo: Asegurar la toma de acciones apropiadas frente a una no conformidad detectada, reaccionando oportunamente y tomando acciones pertinentes, buscando mejorar el desempeño y la eficacia del sistema de gestión de la calidad.

Alcance:
Nuestra organización busca analizar y reflexionar buscando mejorar los productos y servicios, la convivencia, la reducción de riesgos, el para cumplimientos de requisitos y requerimientos, así como considerar las necesidades y expectativas futuras;





PCSI A.7.2.1

Responsabilidad de la Gerencia en la gestión de personas

Los recursos humanos son gestionados por cada gerencia, para su contratación, gestión y desvinculación. Los registros son administrados por el gerente de administración y finanzas para dar cumplimiento a la normativa legal.

Editrade se asegura de contar con los recursos humanos adecuados a través de las siguientes actividades:

Funciones principales del gerente del área en relación a sus recursos humanos

- Debe asegurar el cumplimiento de la normativa legal vigente relativa a las personas.
- Mantener y resguardar la información obligatoria de los trabajadores, para lo cual mantiene carpetas de personal que incluye entre otros su perfil de cargo debidamente firmado y la información de sus competencias y habilidades. Comunicación de funciones y tareas a través de la inducción al trabajador, ejecutada al ingresar a la organización.
- Coordinar y gestionar acciones de aprendizaje al personal.
- Coordinación y registro de la evaluación de la eficacia de las acciones de aprendizaje tomadas: la evaluación de la eficacia es determinada por la gerencia y la Jefatura que corresponda.

Política de uso de clave (A.9.3.1)

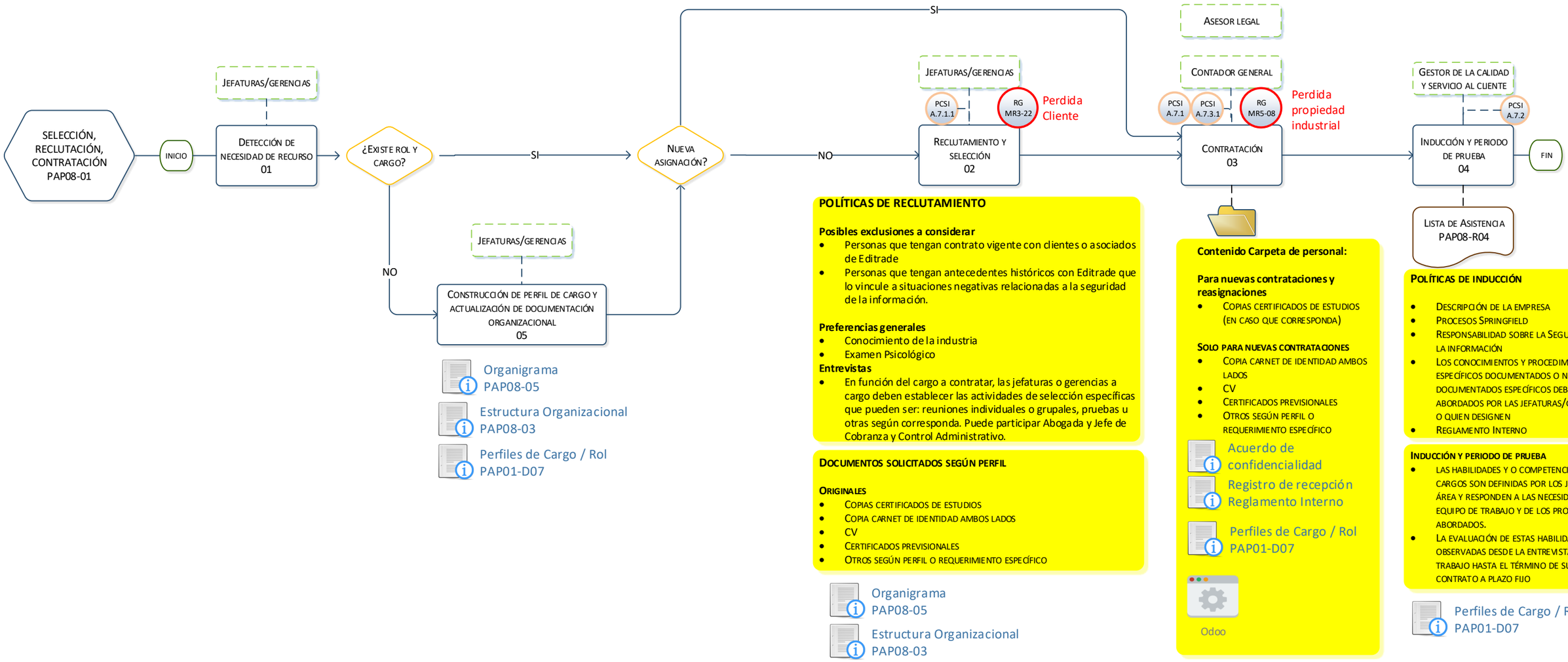
Toda persona de la organización a la cual se le entregue una clave de acceso, debe hacer buen uso de ella y resguardada adecuadamente, según lo firmado en el acuerdo de confidencialidad.

SELECCIÓN, RECLUTAMIENTO, CONTRATACIÓN

PAP08-01

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerente General
Alcance: Todos los procesos de reclutamiento de colaboradores para cubrir plazas del sistema de gestión Springfield.
Objetivo: Asegurar la selección reclutamiento y contratación de personal competente que afecte la conformidad de los requisitos de los servicios prestados.



Organigrama PAP08-05
Estructura Organizacional PAP08-03
Perfiles de Cargo / Rol PAP01-D07

POLÍTICAS DE RECLUTAMIENTO

Posibles exclusiones a considerar
- Personas que tengan contrato vigente con clientes o asociados de Editrade
- Personas que tengan antecedentes históricos con Editrade que lo vincule a situaciones negativas relacionadas a la seguridad de la información.

Preferencias generales
- Conocimiento de la industria
- Examen Psicológico

Entrevistas
- En función del cargo a contratar, las jefaturas o gerencias a cargo deben establecer las actividades de selección específicas que pueden ser: reuniones individuales o grupales, pruebas u otras según corresponda. Puede participar Abogada y Jefe de Cobranza y Control Administrativo.

DOCUMENTOS SOLICITADOS SEGÚN PERFIL

ORIGINALES
- COPIAS CERTIFICADOS DE ESTUDIOS
- COPIA CARNET DE IDENTIDAD AMBOS LADOS
- CV
- CERTIFICADOS PREVISIONALES
- OTROS SEGÚN PERFIL O REQUERIMIENTO ESPECÍFICO

Organigrama PAP08-05
Estructura Organizacional PAP08-03

Contenido Carpeta de personal:

Para nuevas contrataciones y reasignaciones
- COPIAS CERTIFICADOS DE ESTUDIOS (EN CASO QUE CORRESPONDA)

SOLO PARA NUEVAS CONTRATACIONES
- COPIA CARNET DE IDENTIDAD AMBOS LADOS
- CV
- CERTIFICADOS PREVISIONALES
- OTROS SEGÚN PERFIL O REQUERIMIENTO ESPECÍFICO

Acuerdo de confidencialidad
Registro de recepción Reglamento Interno
Perfiles de Cargo / Rol PAP01-D07
Odoo

POLÍTICAS DE INDUCCIÓN
- DESCRIPCIÓN DE LA EMPRESA
- PROCESOS SPRINGFIELD
- RESPONSABILIDAD SOBRE LA SEGURIDAD DE LA INFORMACIÓN
- LOS CONOCIMIENTOS Y PROCEDIMIENTOS ESPECÍFICOS DOCUMENTADOS O NO DOCUMENTADOS ESPECÍFICOS DEBEN SER ABORDADOS POR LAS JEFATURAS/GERENCIAS O QUIEN DESIGNEN
- REGLAMENTO INTERNO

INDUCCIÓN Y PERIODO DE PRUEBA
- LAS HABILIDADES Y O COMPETENCIAS DE LOS CARGOS SON DEFINIDAS POR LOS JEFES DE ÁREA Y RESPONDEN A LAS NECESIDADES DEL EQUIPO DE TRABAJO Y DE LOS PROYECTOS ABORDADOS.
- LA EVALUACIÓN DE ESTAS HABILIDADES SON OBSERVADAS DESDE LA ENTREVISTA DE TRABAJO HASTA EL TÉRMINO DE SU PRIMER CONTRATO A PLAZO FIJO

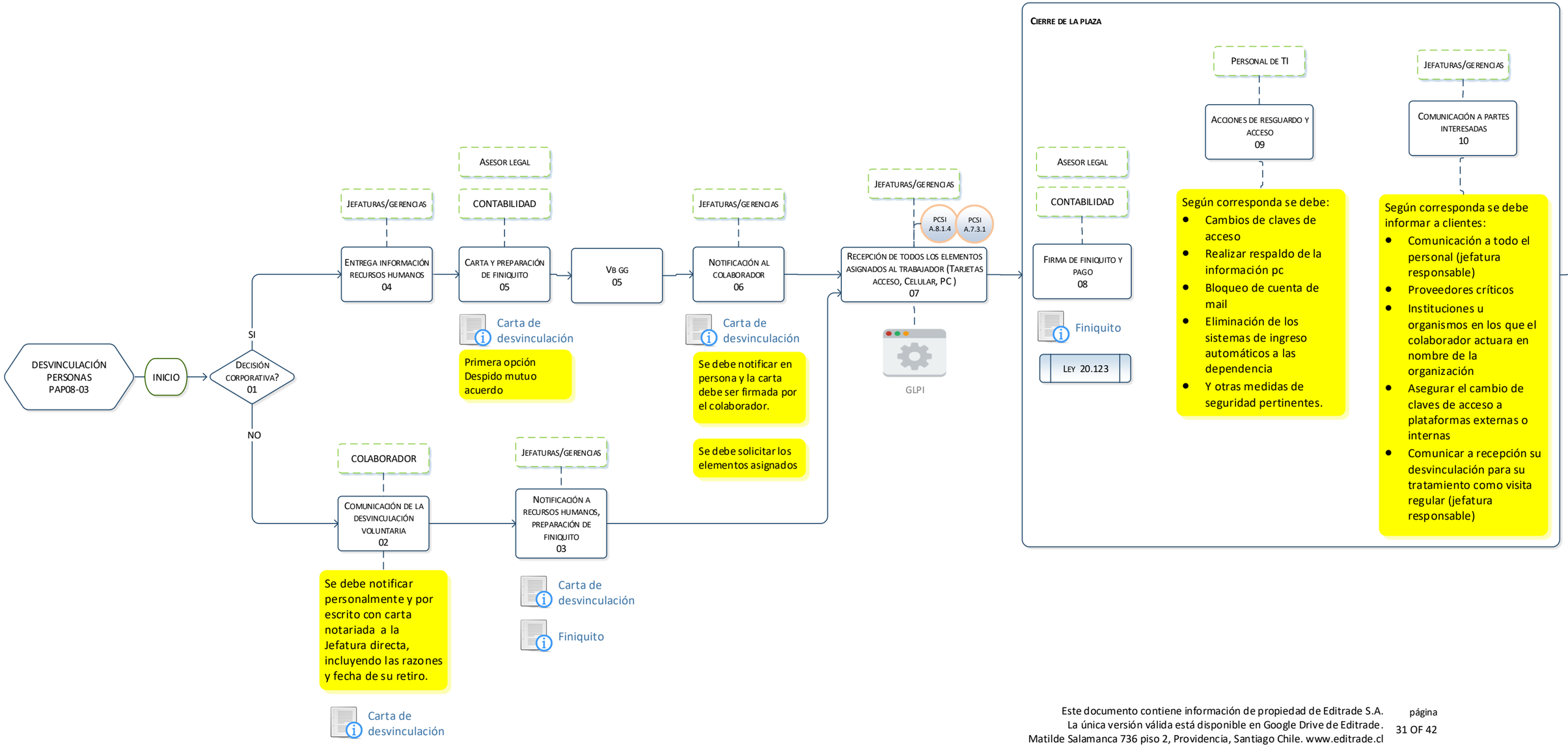
Perfiles de Cargo / Rol PAP01-D07

DESVINCULACIÓN PERSONAS

PAP08-03

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerente General
Alcance: Colaborares contratados por Editrade
Objetivo: Asegurar el cumplimiento de la normativa legal vigente y minimizar el impacto de la desvinculación en los procesos.

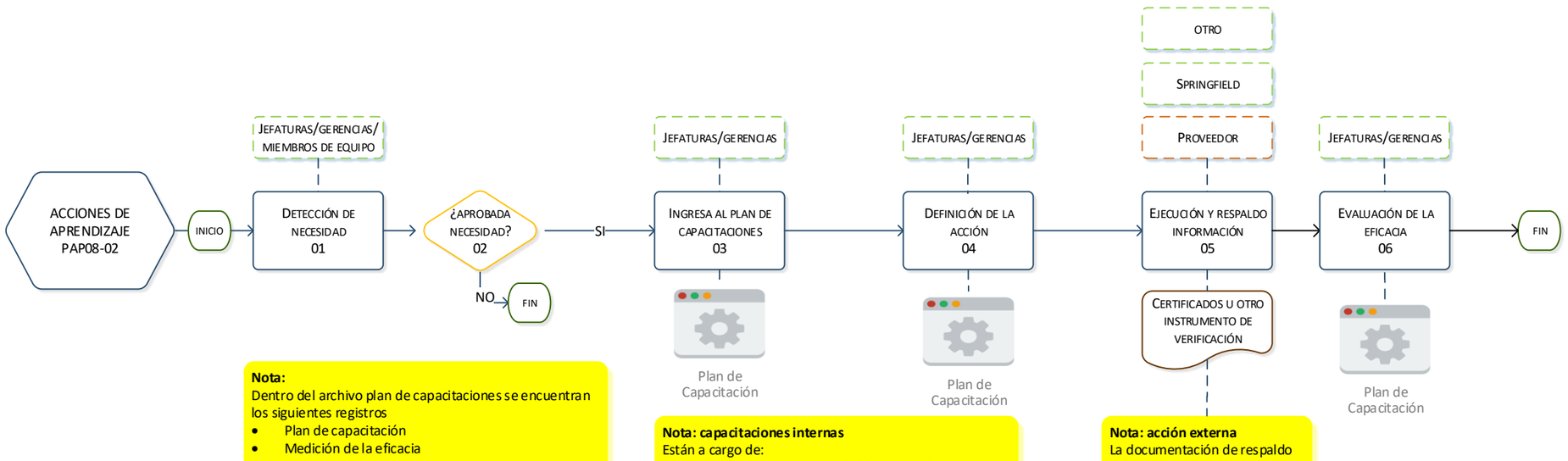


ACCIONES DE APRENDIZAJE

PAP08-02

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Capacitador
Alcance: Todos los requerimientos de personas que son acogidos.
Objetivo: Asegurar que la entrega de formación al personal con énfasis en aquellos que afectan la calidad del servicio prestado.



Nota:
Dentro del archivo plan de capacitaciones se encuentran los siguientes registros

- Plan de capacitación
- Medición de la eficacia

Nota:
La revisión y actualización del plan es permanente.
Y se establece su revisión general una vez al año, normalmente durante la revisión por la dirección .

Nota: capacitaciones internas
Están a cargo de:

- escuelita primaria Springfield y responden a necesidades específicas de proyectos o habilidades propias de la organización.
- Líderes funcionales: responden a acciones asociadas a prácticas, políticas internas o proceso propios de la cultura de la organización

Nota: capacitaciones externas

- Los proveedores externos son definidos y seleccionados por el responsable de la actividad.

Nota: acción externa
La documentación de respaldo debe resguardarse en la carpeta de personal y puede ser una fotocopia simple.

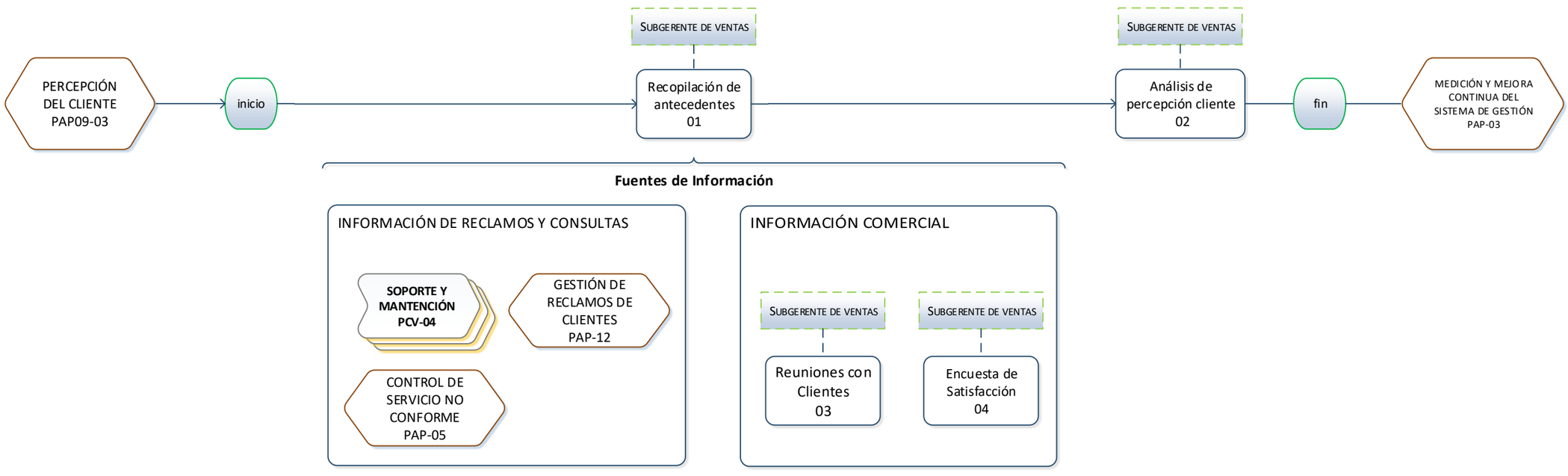
PERCEPCIÓN DE CLIENTE

PAP09-03

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de ventas
Alcance: Procesos que involucren actividades donde su correcto desempeño depende del manejo de las expectativas del cliente
Objetivo: Obtener evidencia de la percepción del cliente a través de los distintos procesos y analizar la misma en pos de una mejora continua



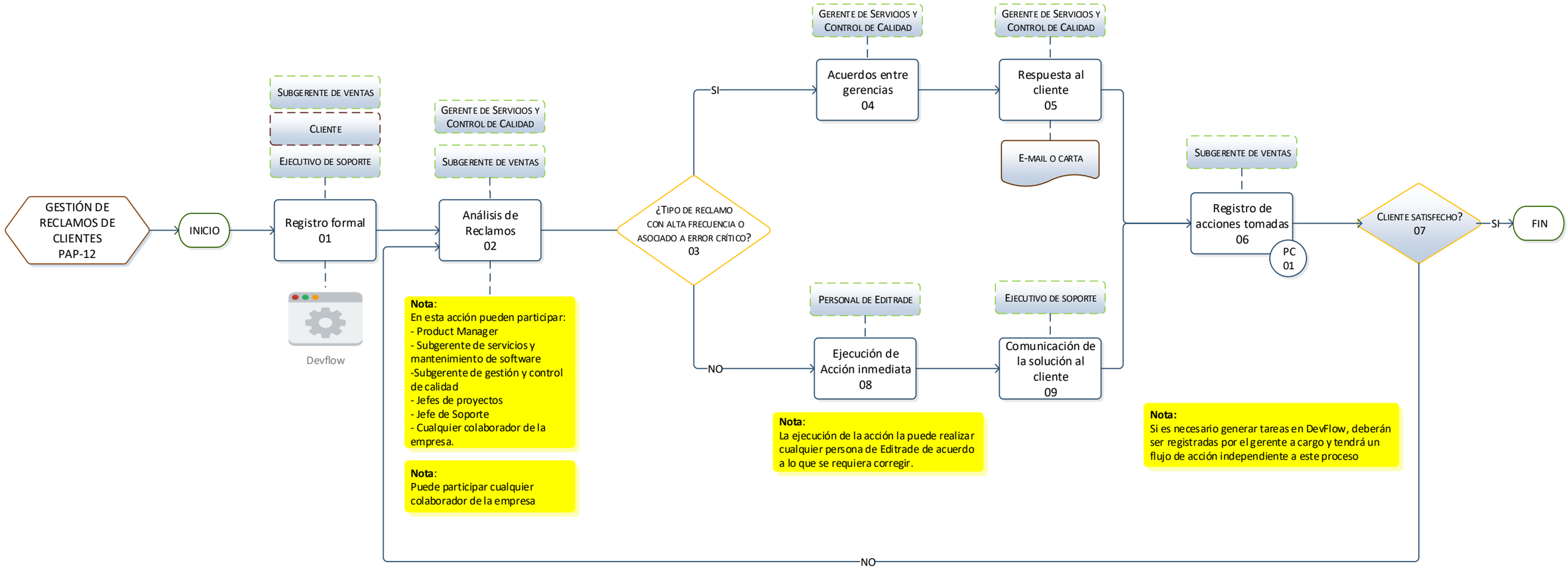
GESTIÓN RECLAMOS DE CLIENTES

PAP-12

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gerente De Servicios y Control de Calidad
Alcance: Activos, información, personal de Editrade, personal externo y visitas
Objetivo: Asegurar una evaluación y gestión adecuada para el tratamiento de los riesgos a los que están expuestos los activos de la Empresa, ya sean incidencias, fallas o manejo de la información confidencial de manera de asegurar continuidad operacional



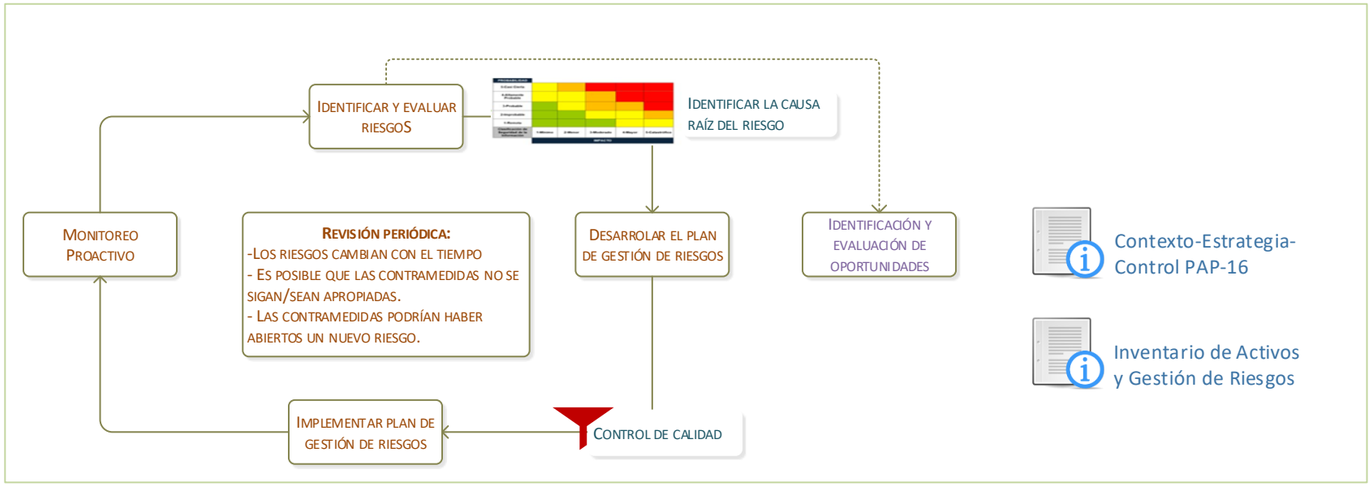
METODOLOGÍA GESTIÓN DE RIESGOS

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Gestor de Control y Calidad
Alcance: Procesos de la cadena de valor

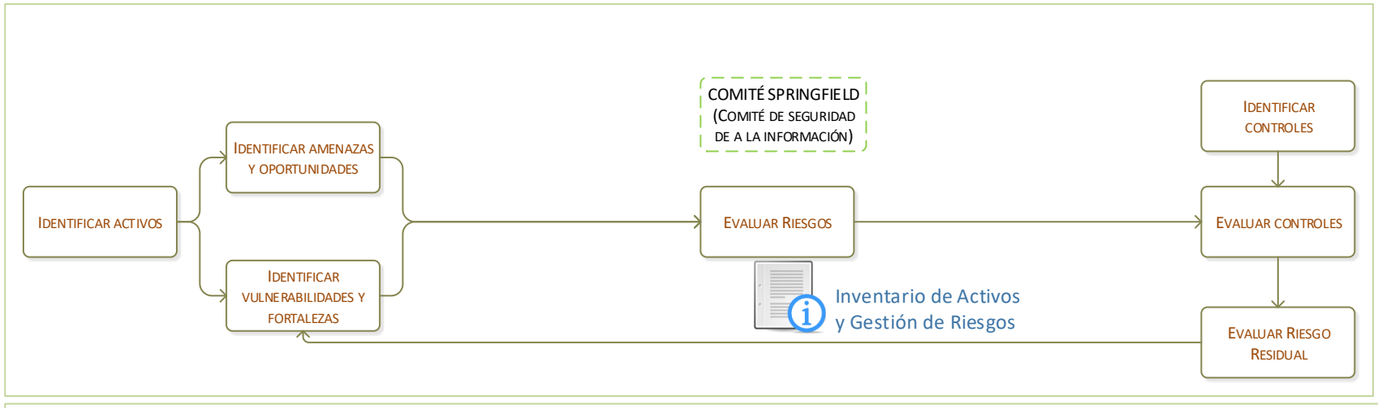
Objetivo
Identificar los activos principales de la empresa. Identificar los procesos críticos de la empresa. Levantar los riesgos de los activos principales de la empresa. Definir el Tiempo Objetivo de Recuperación(RTO). Definir el Punto Objetivo de Recuperación(RPO). Desarrollar la estrategia de recuperación
Identificar los procesos a ejecutar por las distintas áreas para mantener este plan.

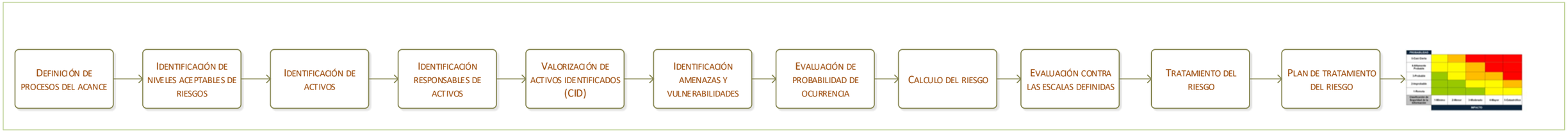


Definiciones

Evaluación: Proceso de análisis del entorno de la amenaza y las vulnerabilidades de los activos de información para determinar si la organización está expuesta. El análisis resultante se utiliza como base para identificar los controles adecuados y rentables para reducir el riesgo identificado.

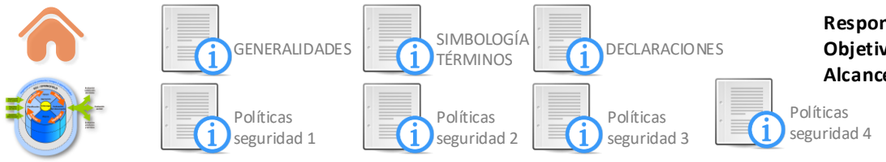
Análisis: Proceso de combinar la información de la vulnerabilidad recopilada durante una evaluación y la información de amenaza recolectada de otras fuentes para determinar el riesgo de compromiso, tanto en términos de frecuencia como de magnitud potencia (puede concluir cálculos estadísticos como VAR, ALE o ROSI).





CONTROL EQUIPOS DE SEGUIMIENTO Y MEDICIÓN

CÓDIGO: PAP04-PR01



Responsable: Gerente de Servicios
Objetivo: Asegurar el correcto funcionamiento de los equipos de seguimiento y medición
Alcance: Equipos de seguimiento y medición críticos para la prestación de servicios

#	Equipo de seguimiento y medición	Descripción	Seguimiento	Responsable
1	Equipo *split* muro marca Gree	Sistema de climatización de temperatura controlada entre 18° y 24°, 2 ubicado en DataCenter y 1 ubicado a un costado del DataCenter equipo de contingencia.	Se realizan mantenciones periódicas según especificaciones técnicas del fabricante.	subgerente de gestión y control TI
2	Grupo Electrógeno de 20KVA	Continuidad eléctrica de Editrade.	Se realizan mantenciones periódicas según especificaciones técnicas del fabricante.	subgerente de gestión y control TI
3	UPS	UPS a PC de 3k, 5k y 6k	Se realizan mantenciones en base a las alarmas que arroja el equipo	subgerente de gestión y control TI
4	NAGIOS	Seguimiento de servicios solicitados por otras áreas	Verificación visual de que el equipo esté operativo.	subgerente de gestión y control TI

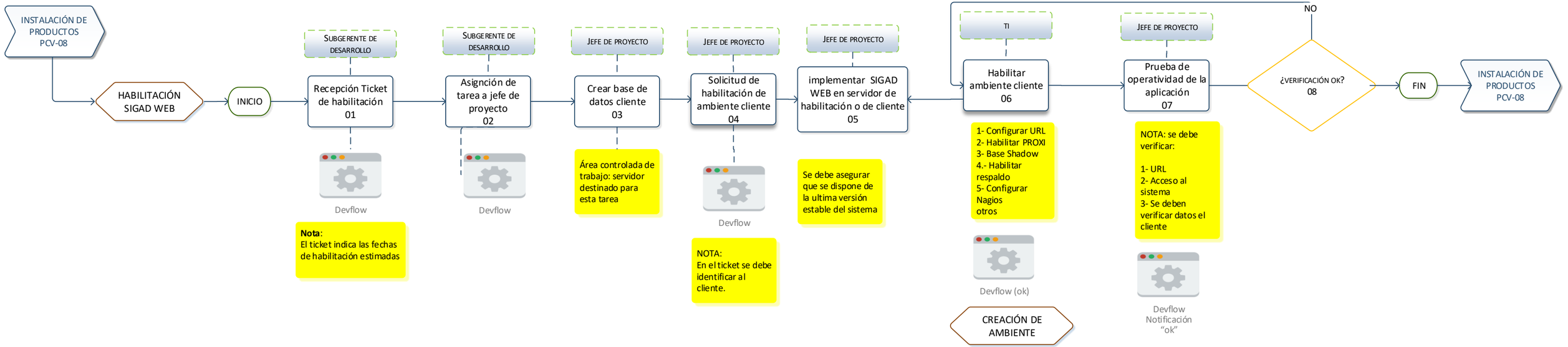
HABILITACIÓN DE SIGAD WEB

CÓDIGO: PCV0 8-01

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de Desarrollo
Objetivo: Asegurar la correcta habilitación de Sigad web
Alcance: Clientes Sigad Web

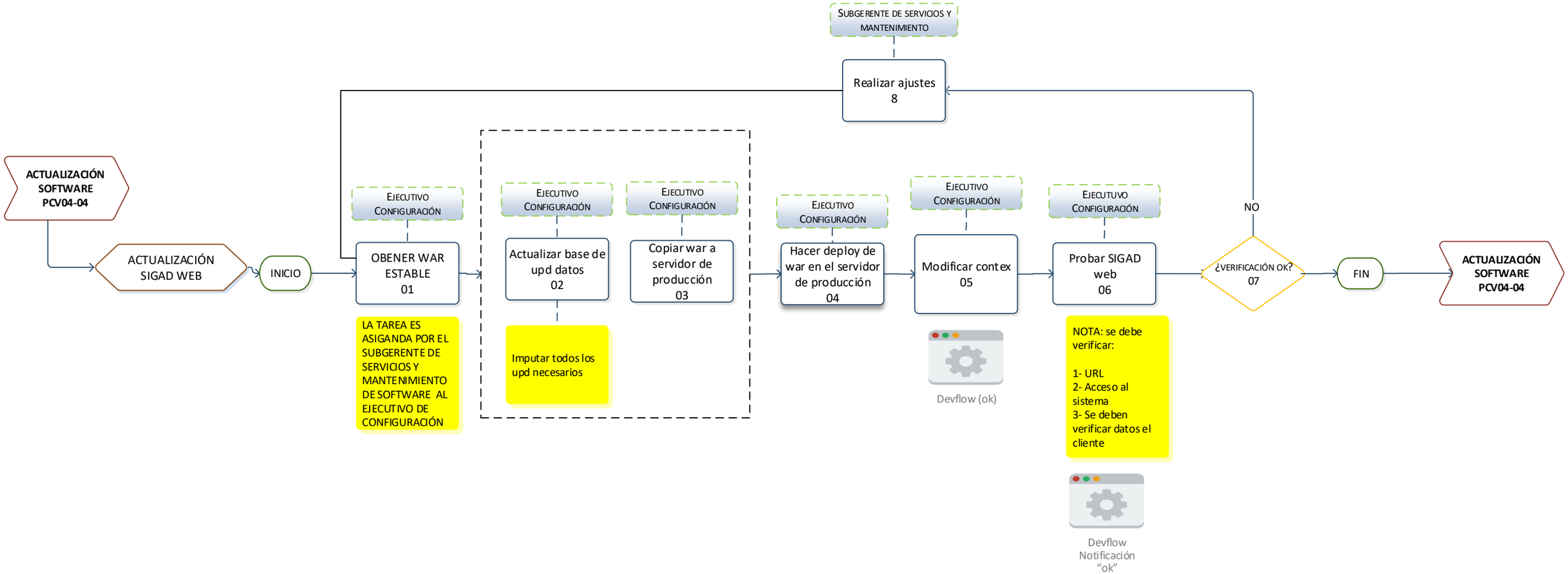


ACTUALIZACIÓN SIGAD WEB

CÓDIGO: PCV0 404-02

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de Servicios y Mantenimiento de Software
Objetivo: Asegurar la correcta habilitación de Sigad web
Alcance: Clientes Sigad Web



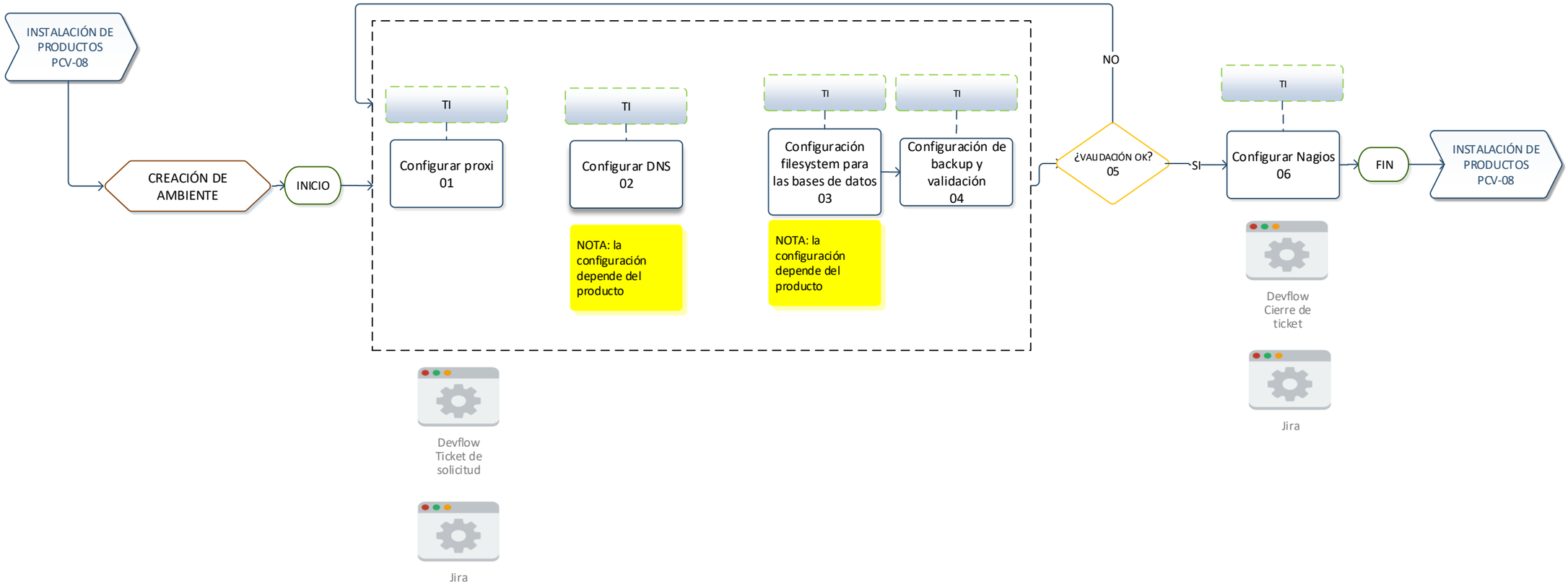
CREACIÓN AMBIENTE

CÓDIGO: PCV0 8-03

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES

Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: TI
Objetivo: Asegurar la correcta creación del ambiente SIGAD WEB o ECUASIGAD
Alcance: SIGAD WEB o ECUASIGAD

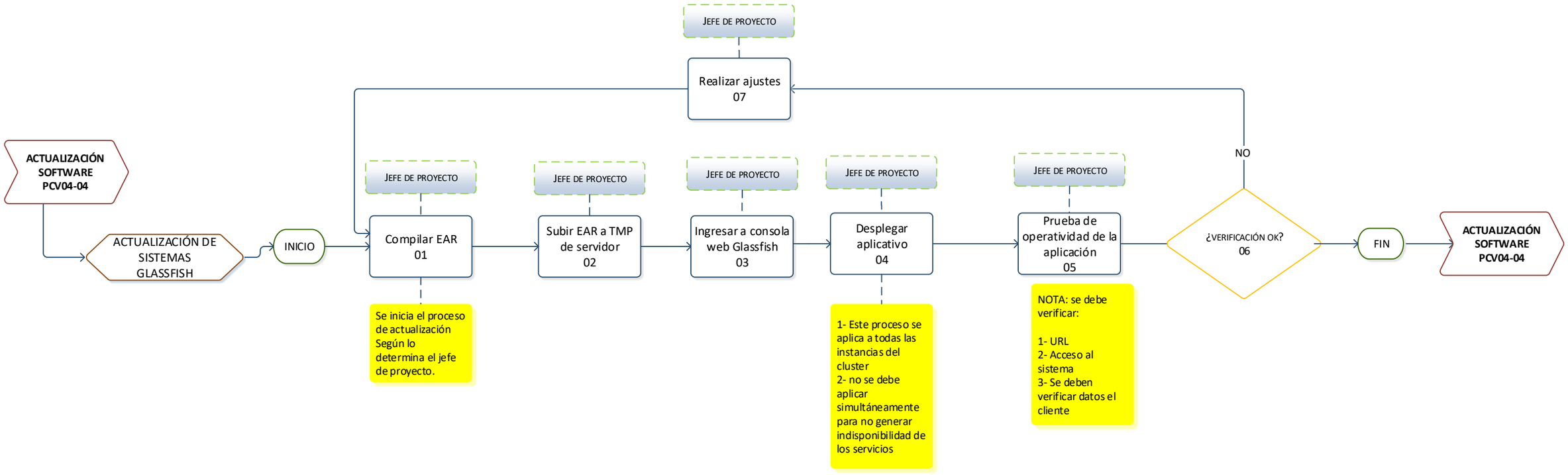


ACTUALIZACIÓN DE SISTEMAS GLASSFISH

CÓDIGO: PCV04-04 01

GENERALIDADES | SIMBOLOGÍA TÉRMINOS | DECLARACIONES | Políticas seguridad 1 | Políticas seguridad 2 | Políticas seguridad 3 | Políticas seguridad 4

Responsable: Subgerente de Servicios
Objetivo: Asegurar la correcta y oportuna actualización de sistemas
Alcance: Sistemas que estén sobre servidores Glassfish



INFRAESTRUCTURA

Responsable: Gerencia de Servicios y Control de Calidad y TI
Objetivo: Establecer las directrices bases para la gestión de la infraestructura.

CONTROL DE SEGURIDAD
Editrade busca evitar el acceso físico no autorizado, os daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.
Zona Segura

-Se establece como zona segura, el centro de procesamiento de Chile, el cual posee acceso por huella digital.

-El centro de procesamiento posee, cielo y piso falso, detector de humo, control de temperatura, puerta de acceso con control biométrico, continuidad de energía(generador), extintores, doble enlace internet, ups, alarmas de servidores.

-Cableado subterráneo.

-Cableado de energía separado y paneles de control especial.

-El acceso a las oficinas centrales es por llave más código de alarma.

-Los equipos como notebooks, que son activos de la organización tienen la aplicación Prey que permite saber su ubicación.

11.1.1 "Perímetro de seguridad física"
Editrade establece perímetros de seguridad para proteger las áreas que contienen información y a las instalaciones de procesamiento de información sensible o crítica.
Acceso físico a las instalaciones y seguridad a catástrofes.
Editrade cuenta con:

Área Segura: Datacenter
Puerta de seguridad, cámaras, alarmas, la zona segura posee laminas de acero por el perímetro entre capas de vulcanita, posee puerta con control biométrico, con acceso restringido, ventanas con láminas de seguridad y triple seguro

Accesos permitidos:
Equipo Gerencial
Equipo de TI

Perímetro de del edificio

Puerta de seguridad, cámaras, alarmas, posee puerta con control biométrico, con acceso restringido, ventanas con láminas de seguridad y triple seguro

11.1.2 "Controles de entrada físicos"
-Portería entrada edificio.
-Recepción en oficina
-Huella biométrica
-Puerta blindada.
-Alarma
-Llave
11.1.3 "Asegurando oficinas, salas e instalaciones"
Los dos puntos anteriores.
A.11.1.4 "Protección contra las amenazas externas y ambientales"
-Prevencionista ACHS
-Piso Falso
-Generador
-Extintores
-Sensores de humo
-Sensores de incendio
11.1.5 "Trabajando en áreas seguras"
-Registro de personas internas por huella digital.
-Control de personas externas se anotan en planilla.
-Personas externas acceden con personal autorizado de Editrade a Datacenter.

11.1.6 "Accesos públicos, despacho y áreas de descarga"
-El acceso público es la entrada principal.
-No hay acceso al área segura desde fuera.
Crear política en Infraestructura:

11.2.1 "Protección y ubicación de los equipos"
Enfocado al área segura.
Crear política en Infraestructura:
11.2.2 "Servicios de soporte"
-UPS
-Aire acondicionado
-Alarma
-Grupo electrógeno
-Extintor
-Sensor de humedad
11.2.3 "Seguridad del cableado"
Enfocado al área segura.
-Cableado independiente de electricidad e independiente de comunicaciones.
-Redundancia de ISP.
-Pasan por piso falso, cables entregados por el proveedor de internet.
-Cajas de electricidad tienen caja y seguridad por llave.
-Acceso al panel eléctrico del área segura, se rige por el control a área segura.
-Complementar con control A.11.2.1

11.2.4 "Mantenimiento de equipos"
-Registro de Mantención de equipos del área segura.
-UPS
-Aire acondicionado
-Alarma
-Grupo electrógeno
-Extintor
-Limpieza de sala
-Sensor de humedad
[evidencia de las mantenciones]

Crear política
"11.2.8 Uso de equipamiento desatendido":
-Bloqueo de pantalla con clave
-Sistema operativo con contraseña

[agregar esta política en el catálogo]
En catálogo en sección Infraestructura.
"La sincronización del reloj de los servidores, se hace por NTP hacia el SHOA"

13.1.1 "Controles de red"
Políticas de acceso por cortafuego
-está en el catálogo de respaldo
Crear en infraestructura:
"13.1.2 Seguridad de los servicios de red"
-SLA por contrato
-monitoreo Nagios
-Evaluación de proveedores (Reevaluación)

"13.1.3 Segregación de redes"
-lan
-wifi visita
-wifi corporativa
-Usuarios vs red en el siguiente Link
-Reglas de cortafuego

13.2.3 Política de Mensajería Electrónica:
Los mensajes Electrónicos actuales son:
-Email (GSuite usa HTTPS)
-Se dispone de mensajería electrónica con:
-SII (Firma Electrónica).
-S.N. Aduana (Firma Electrónica).
-Hacienda (Firma Electrónica).
-Redes Sociales (usuario y clave)

"El uso de otros servicios de mensajería electrónica, debe pedir la aprobación al comité de seguridad."

"14.1.2 Asegurar los servicios sobre redes públicas"
-Los servicios públicos entregados por Editrade se hacen por HTTPS.
-El servicio de VAN se entrega por VPN + firma electrónica.
-Otras interacciones con terceros se hace por HTTPS + firma electrónica

"14.1.3 Protección de las aplicaciones de servicios transaccionales"
-transacción son por https
-la comunicación entre app y base de datos es confiable porque está dentro de la misma red aislada.
-Seguridad de los activos y control de acceso.