TRATAMIENTO DE RIESGOS												5 de 7
N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox	Tiempo Aprox	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia					
Amenazas a los Activos Físicos												
7	Servidor de Dominio Zonal	Daño físico de equipos	3.333	2.834	4	3.389	Crítico	Utilizar correctamente el servidor y realizar respaldos de acuerdo a un cronograma	**10.1.1** Documentación de procesos operativos **10.5.1** Recuperación de la información	**2** De S/. 15,000 a S/. 30,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir
		Incongruencia de fecha y hora	3	3.334	4	3.444	Crítico	Revisar que el reloj del servidor esté sincronizados con los demás servidores	**10.8.3** Sincronización del Reloj	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir
8	Servidor de Keyfile	Daño físico de equipos	3.333	2.834	4	3.389	Crítico	Utilizar correctamente el servidor y realizar respaldos de acuerdo a un cronograma	**10.1.1** Documentación de procesos operativos **10.5.1** Recuperación de la información	**2** De S/. 15,000 a S/. 30,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir
		Incongruencia de fecha y hora	3	3.334	4	3.444	Crítico	Revisar que el reloj del servidor esté sincronizados con los demás servidores	**10.8.3** Sincronización del reloj	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir

TRATAMIENTO DE RIESGOS											6 de 7
N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox	Tiempo Aprox	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia					
Amenazas a los Activos Físicos												
9	Servidor de Base de Datos	Daño físico de equipos	3.333	2.834	4	3.389	Crítico	Utilizar correctamente el servidor y realizar respaldos de acuerdo a un cronograma	**10.1.1** Documentación de procesos operativos **10.5.1** Recuperación de la información	**2** De S/. 15,000 a S/. 30,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir
		Incongruencia de fecha y hora	3	3.334	4	3.444	Crítico	Revisar que el reloj del servidor esté sincronizados con los demás servidores	**10.8.3** Sincronización del reloj	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir
10	Servidor de Replicación	Incongruencia de fecha y hora	3	3.334	4	3.444	Crítico	Revisar que el reloj del servidor esté sincronizados con los demás servidores	**10.8.3** Sincronización del reloj	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir

TRATAMIENTO DE RIESGOS												7 de 7
N°	**Activo**	**Amenaza**	**Riesgo Efectivo**					**Control Propuesto**	**Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007**	**Costo Aprox**	**Tiempo Aprox**	**Opción para el Tratamiento**
			Nivel de Impacto	**Probabilidad de Ocurrencia del Riesgo**	**Valor del Activo**	**Nivel de Exposición al Riesgo**	**Nivel de Tolerancia**					
Amenazas a los Activos Físicos												
11	Cintas de Backup DLT	Robo de cintas	4	3	5	4	Crítico	Mantener las cintas en un lugar seguro	**10.8.3** Medios físicos en tránsito	**2** De S/. 15,000 a S/. 30,000	**M** Mediano plazo (De 3 a 12 meses)	**T** Transferir **R** Reducir
		Daño físico de cintas	3.333	2.834		3.722	Crítico	Generar los respaldos y backups correctamente siguiendo procedimientos estandarizados	**10.1.1** Documentación de procesos operativos **10.5.1** Recuperación de la información	**2** De S/. 15,000 a S/. 30,000	**M** Mediano plazo (De 3 a 12 meses)	**R** Reducir

Tabla N°6 - *Tratamiento de Riesgos de la UTI*

Fuente: *Elaboración Propia*

4.2.2. Implementar los controles.-

El proceso para la implementación de cada control, se llevará a cabo en 4 partes: la explicación del control y objetivos de control (objetivo y guía de implementación mencionados en la NTP ISO/IEC 17799:2007), el diagrama de actividades que proponemos, el diagrama de procesos que proponemos (de acuerdo a la guía de implementación) y los formularios correspondientes para llevar a cabo cada implementación de ser necesarios.

4.2.2.1. Procedimientos y responsabilidades de operación.-

Objetivo: Asegurar la operación correcta y segura de los recursos de tratamiento de información.
Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.
Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

4.2.2.1.1. Documentación de procedimientos operativos.-

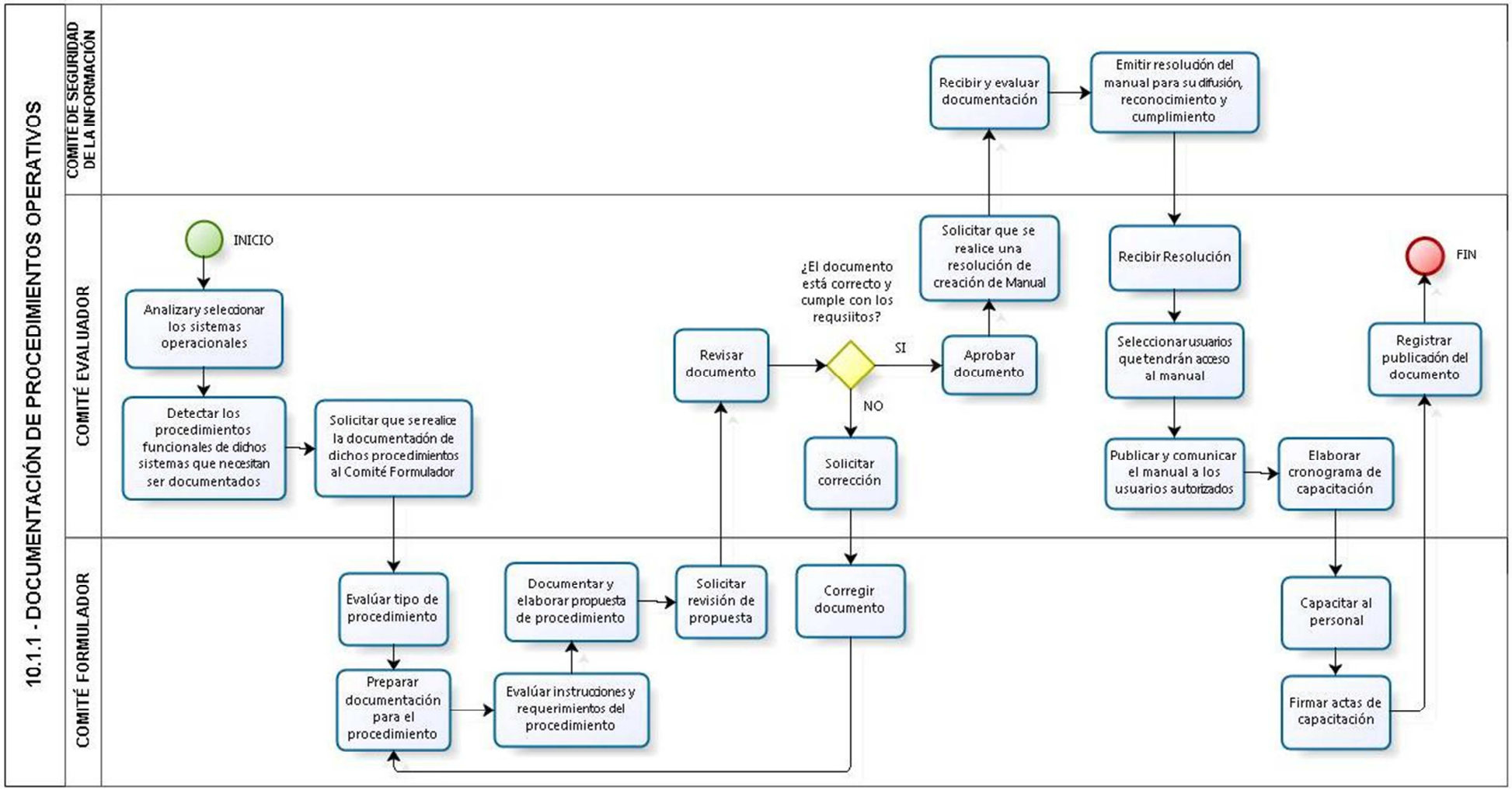
Control: Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.

Guía de Implementación: Se debe de preparar los procedimientos documentados para actividades del sistema asociados con el procesamiento de información y los recursos de comunicación, como los procedimientos de prendido y apagado de la computadora, backups, mantenimiento de equipos, manipulación de medios, ambientes de cómputo y manipulación de correos, y seguridad

Diagrama de Actividades N°1 - Documentación de procedimientos operativos (10.1.1)

1. El Comité Evaluador analiza y selecciona aquellos sistemas operacionales que cuenten con procedimientos funcionales que necesitan ser documentados. Una vez identificados, solicita al Comité Formulador que realice la documentación respectiva para cada uno de los procedimientos.
2. El Comité Formulador evalúa y clasifica cada procedimiento, para luego preparar la documentación respectiva evaluando las instrucciones y requerimientos que necesita dicho procedimiento. Documenta la propuesta de procedimiento, convirtiéndolo en un manual y solicita al Comité Evaluador la revisión respectiva.
3. El Comité Evaluador revisa el documento/manual creado por su personal, si le parece que está correcto y que cumple con los requisitos, aprueba el documento y solicita al Comité de Seguridad de la Información que se realice una resolución de creación de manual de dicho procedimiento. Si el documento no le parece correcto, solicita al Comité Formulador, la corrección respectiva.
4. Una vez que el documento esté aprobado, el Comité de Seguridad de la Información recibe la documentación y la evalúa para luego poder aprobar y emitir una resolución del manual de procedimiento, para su difusión, reconocimiento y cumplimiento en la UTI.
5. El Comité Evaluador recibe resolución y elabora una lista de los usuarios que tendrán acceso al manual. Publica y comunica el manual a los usuarios autorizados. Una vez realizado ello, elabora cronogramas de capacitación para dar a conocer y explicar el proceso estudiado al personal que lo necesite.
6. El Comité Formulador capacita al personal según cronograma y elabora actas para registrar las capacitaciones.
7. Finalmente, el Comité Evaluador registra la publicación del documento.

Diagrama de Procesos N°1 - Documentación de procedimientos operativos (10.1.1)



Formulario N°1 - Documentación de procedimientos operativos (10.1.1)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.1.1 – DOCUMENTACIÓN DE PROCEDIMIENTOS OPERATIVOS**	**Código:** [FRM - 10.1.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **87** de **1**

1 DEL PROCEDIMIENTO OPERATIVO: **Fecha:** [dd/mm/aaaa]

Sistema Operacional: [Indicar el nombre del Sistema Operacional]

Procedimiento: [Indicar el nombre del procedimiento a documentar]

Tipo de Procedimiento: [Indicar el tipo de procedimiento]

- Base de Datos [ ] - Técnico [ ] - Operativo [ ]

Descripción del Procedimiento: [Indicar una breve descripción del procedimiento a documentar]_____

_____

Instrucciones y requerimientos del Procedimiento: [Listar las instrucciones, requerimientos y secuencia de pasos que se necesitan documentar del procedimiento] _____

Documentación elaborada: [Indicar el nombre de la documentación elaborada para el procedimiento funcional]

Usuarios con autorización al documento:
[Listar usuarios que tendrán acceso al manual/documentación]

- [Usuario 1] – [Perfil N]
- [Usuario 2] – [Perfil N]

Fechas de Capacitación:
[Indicar las fechas de capacitación en las que se instruirá al personal sobre la documentación]

- [Fecha 1 – Hora – Lugar – Capacitador]
- [Fecha 2 – Hora – Lugar – Capacitador]

**** Número de Resolución de aprobación de la documentación del procedimiento***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró documentación del proceso operativo]	**Nombre:** [Nombre de la persona que revisó la documentación del proceso operativo]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación de la documentación]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.1.2. Gestión de cambios.-

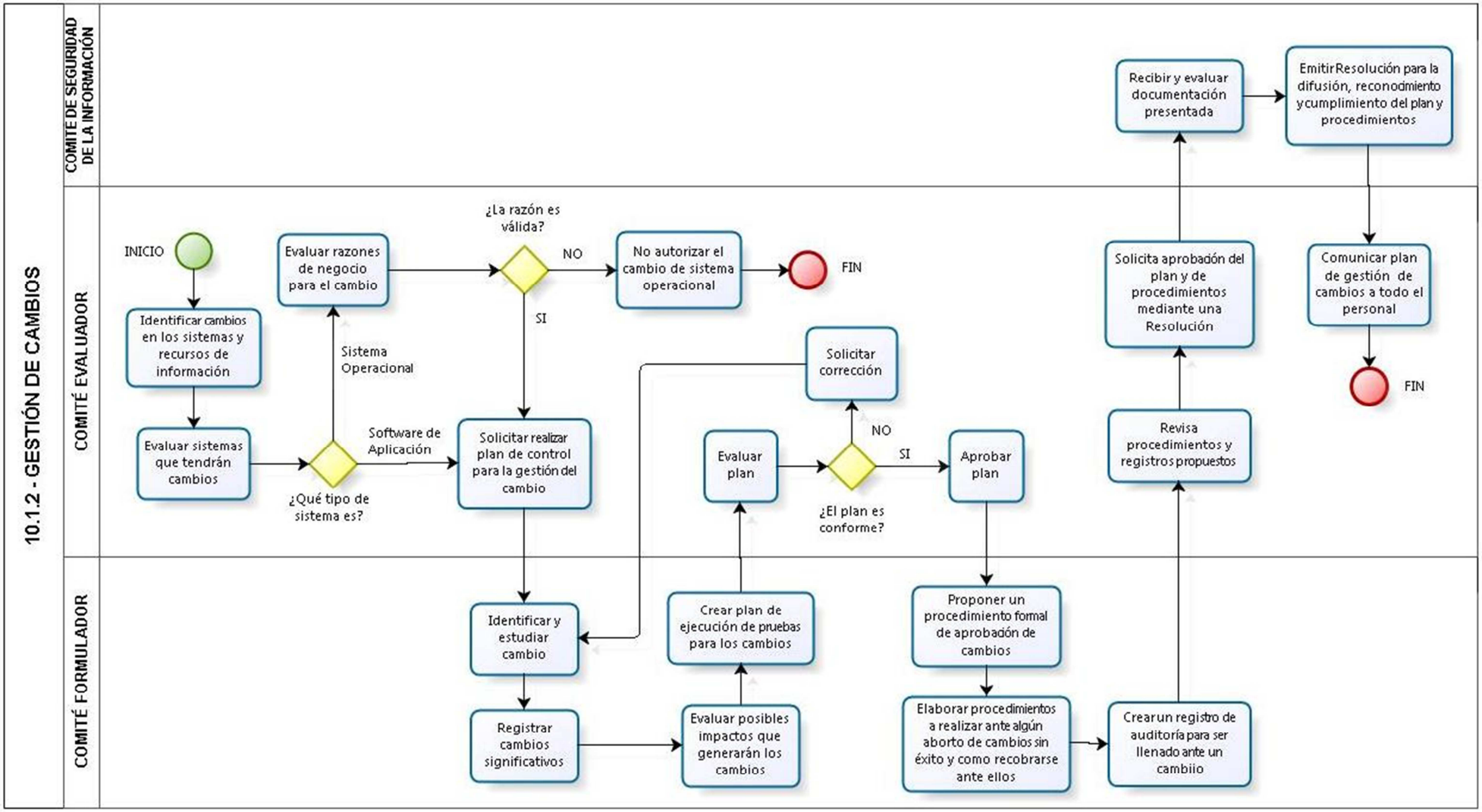
Control: Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información

Guía de Implementación: Los sistemas operacionales y los softwares de aplicación deben ser sujetos a un estricto control de la gestión de cambios

Diagrama de Actividades N°2 - Gestión de cambios (10.1.2)

1. El Comité Evaluador identifica los cambios en los sistemas y recursos de información que se han dispuesto desde la sede central y evalúa los sistemas operacionales y software de aplicación que se verán afectados con el cambio. Si el cambio afecta a un Sistema Operacional, debe de evaluar si existen razones de negocio válidas para el cambio, de no existir ninguna, no autoriza el cambio del sistema operacional, caso contrario si existe una razón válida, solicita al Comité Formulador que realice un plan de control estricto para gestionar dicho cambio.
   Si el cambio afecta a un software de aplicación, no necesita evaluar razones y solicita al Comité Formulador que realice el mismo plan de control para gestionar el cambio.
2. El Comité Formulador identifica y estudia el cambio a realizar, registrando los cambios/movimientos significativos y los impactos que conllevará este proceso al sistema operacional u software de aplicación. Crea y elabora un plan de ejecución de pruebas para los cambios, indicando posibles fechas y activos a usar para ejecutar dicho plan.
3. El Comité Evaluador recibe informe sobre el plan de ejecución de pruebas y lo evalúa, si está conforme con el plan, lo aprueba y si no está conforme con el plan, solicita al Comité Formulador que lo corrija.
4. El Comité Formulador recibe la aprobación del plan de ejecución de pruebas y propone los procedimientos formales a realizar para la aceptar los cambios, además de ello elabora una lista o manual de procedimientos a realizar ante un caso de aborto de cambios y cómo recobrarse ante ellos que no tuvieron éxito. Finalmente crea un registro de auditoría para ser llenado ante cada cambio, terminando así de elaborar el proceso de Gestión de Cambios.
5. Una vez recibido dichos registros y manuales, el Comité Evaluador solicita al Comité de Seguridad de la Información, la aprobación del Plan y de los procedimientos de la Gestión de Cambios mediante una Resolución.
6. El Comité de Seguridad de la Información recibe y evalúa documentación presentada y procede a emitir la respectiva resolución para la difusión, reconocimiento y cumplimiento del plan y de los procedimientos.
7. Finalmente, recibida dicha resolución, el Comité Evaluador comunica el Plan de Gestión de Cambios a todo el personal.

Diagrama de Procesos N°2 - Gestión de cambios (10.1.2)



Formulario N°2 - Gestión de cambios (10.1.2)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.1.2 – GESTIÓN DE CAMBIOS**	**Código:** [FRM - 10.1.2 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **91** de **1**

1 DEL CAMBIO: **Fecha:** [dd/mm/aaaa]

Sistema Operacional: [Indicar el nombre del Sistema que será afectado al cambio]
Tipo de Sistema: [Indicar el tipo de sistema]
- ❖ Sistema Operacional [ ] - Software de Aplicación [ ]

Cambio realizado: [Indicar el nombre del cambio y/o actualización realizado]
Versión del Cambio: [Indicar la versión del cambio y/o actualización]
Cambios significativos: [Listar los cambios puntuales que presentará el sistema con la actualización]
Impactos a generarse: [Listar los posibles impactos que se generarán con los cambios en el sistema]

DE LAS PRUEBAS REALIZADAS:

Documento del Plan de Ejecución de Pruebas: [Indicar y describir brevemente plan de ejecución de pruebas para el cambio] _____ **Fecha de documento:** [dd/mm/aaaa]

Ambiente de pruebas: [Indicar el ambiente utilizado para realizar las pruebas de los cambios y/o actualizaciones]

Pruebas realizadas en fecha: [dd/mm/aaaa]

Documento del Procedimiento para la Aprobación del Cambio: [Indicar y describir brevemente el procedimiento planteado que se debe de realizar, para la aprobación de cada cambio]_____ **Fecha de documento:** [dd/mm/aaaa]

**** Número de Resolución de aprobación del plan de Gestión del Cambios***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró el Plan de Gestión del Cambio]	**Nombre:** [Nombre de la persona que revisó el Plan de Gestión del Cambio]	**Nombre:** [Nombre de la persona que emitió la Resolución de Aprobación para el Plan de Gestión del Cambio]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.1.3. Segregación de tareas.-

Control: Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un al uso de los archivos de la organización.

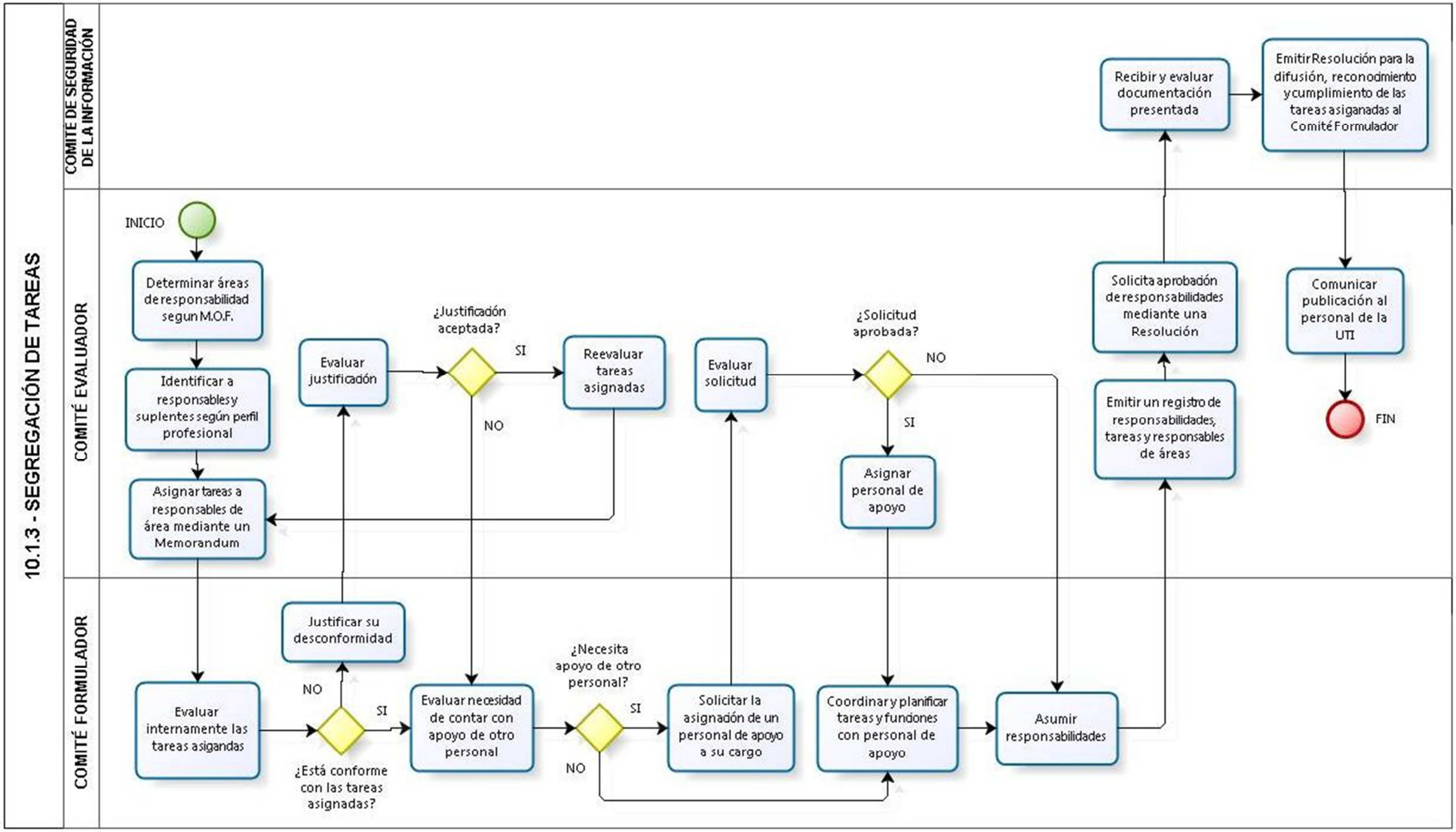
Guía de Implementación: La segregación de tareas es un método para reducir el riesgo de mal uso accidental o deliberado de un sistema. Se debe tener cuidado de que cualquier persona puede acceder, modificar o utilizar los activos sin autorización o sin ser detectado. La iniciación de un evento debe estar separado de su autorización. La posibilidad de confabulación debe ser considerada en el diseño de los controles.

Las organizaciones pequeñas pueden considerar que este método de control es difícil de lograr, pero el principio debería aplicarse en la medida en que sea posible y practicable. Cuando la segregación sea difícil, se considerarán otros controles como la monitorización de las actividades, las pista de auditoría y la supervisión de la gestión. Es importante que la auditoría de seguridad permanezca independiente.

Diagrama de Actividades N°3 - Segregación de tareas (10.1.3)

1. El Comité Evaluador evalúa y estudia el Manual de Organizaciones y Funciones (M.O.F.) de su unidad y según ello determina cuáles son las áreas de responsabilidad, luego de eso identifica y determina de entre sus trabajadores, quienes son los responsables y suplentes de cada área tomando en cuenta el perfil profesional de cada uno de ellos. Mediante memorándums asigna las tareas a realizar a cada responsable de área dentro del Comité Formulador
2. El Comité Formulador evalúa internamente las tareas que se le han sido asignadas en el memorándum. Si no está conforme con las tareas, justifica y presenta su disconformidad al Comité Evaluador.
3. El Comité Evaluador recibe y evalúa la justificación, si la acepta, corrige las tareas que le asignó al Comité Formulador y vuelve a presentar memorándums con los cambios realizados. Si no acepta justificación, comunica que no se realizarán cambios.
4. Una vez que el Comité Formulador esté conforme con las tareas que se le asignaron, procede a evaluar si es que necesita que se le asigne un personal de apoyo. Si es que no necesita ningún personal, procede a coordinar y planificar las tareas y funciones a realizar, para finalmente asumir las responsabilidades que se le han sido asignadas. Si es que necesita un apoyo, lo solicita al Comité Evaluador.
5. El Comité Evaluador recibe y evalúa solicitud, si aprueba la solicitud, procede a seleccionar y a asignar un personal de apoyo a cargo del Comité Formulador. Si no aprueba solicitud, comunica dicha decisión.
6. Una vez que el Comité Formulador esté conforme y cuente con un personal de apoyo, procede a coordinar y planificar las tareas y funciones con su personal. Finalmente asume las responsabilidades que se le han sido asignadas.
7. Luego de ello, el Comité Evaluador emite un registro de los responsables de cada área indicando las responsabilidades y tareas asignadas y solicita la aprobación de las mismas mediante una Resolución.
8. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada para luego emitir una resolución para la difusión, reconocimiento y cumplimiento de las tareas asignadas al Comité Formulador.
9. Finalmente el Comité Evaluador, recibe resolución y comunica la publicación al personal de la UTI.

Diagrama de Procesos N°3 - Segregación de tareas (10.1.3)



Formulario N°3 - Segregación de tareas (10.1.3)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.1.3 – SEGREGACIÓN DE TAREAS**	**Código:** [FRM - 10.1.3 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **95** de **1**

1 DE LA ASIGNACIÓN DE TAREAS: **Fecha:** [dd/mm/aaaa]

Área de Responsabilidad: [Indicar el área de responsabilidad del M.O.F. a evaluar]

Responsable de área: [Nombre de la persona responsable del área de responsabilidad a evaluar]

Cargo actual del responsable: [Indicar el cargo actual del responsable del área]
- Operador [ ] - Especialista en Base de Datos [ ] - Técnico de Sistemas [ ]

Suplente de área: [Nombre de la persona suplente del área de responsabilidad a evaluar]

Cargo actual del suplente: [Indicar el cargo actual del suplente de área]
- Operador [ ] - Especialista en Base de Datos [ ] - Técnico de Sistemas [ ]

Personal de Apoyo: [Nombre de la persona que les apoyará con el cumplimiento de las tareas]

Tareas Asignadas: [Listar y describir las tareas que se asignaron al responsable de área]
- Tarea N°1
- Tarea N°2
- Tarea N°3

Memorando de Asignación: [Indicar el N° de Memorando con el que se determinó al responsable y suplente del área y las tareas que se les asignaron]

**** Número de Resolución de aprobación del plan de Gestión del Cambios***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona a la que se le asignaron dichas tareas para realizar]	**Nombre:** [Nombre de la persona que asignó área y tareas al personal del Comité Formulador]	**Nombre:** [Nombre de la persona que emitió la Resolución de Aprobación para el cumplimiento de las tareas asignadas]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.1.4. Separación de los recursos para desarrollo y producción.-

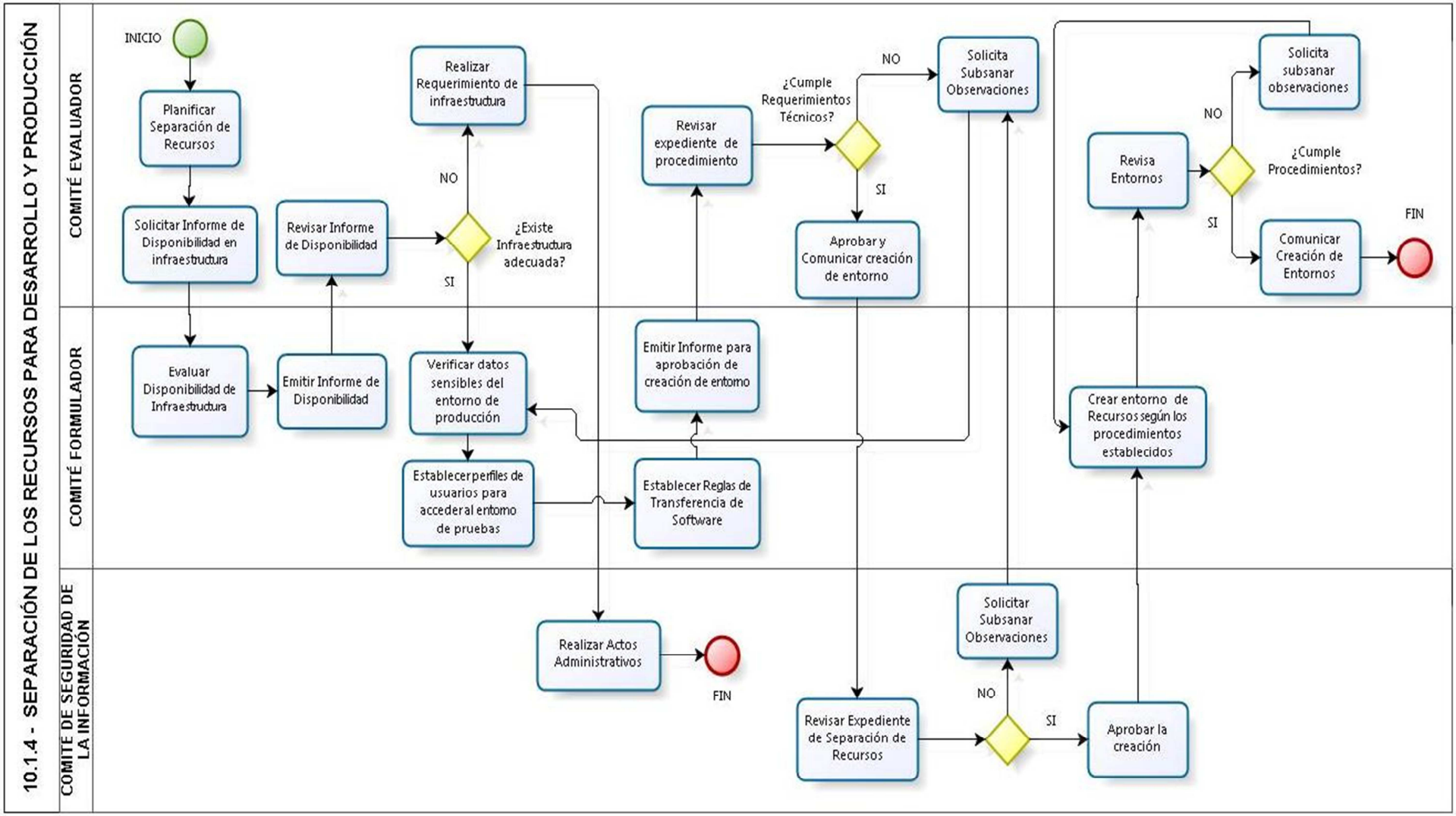
Control:
La separación de los recursos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional

Guía de Implementación:
Se debería identificar e implementar controles adecuados para el nivel de separación entre los entornos de desarrollo, prueba y producción que es necesario para evitar problemas operacionales.

Diagrama de Actividades N°4 - Separación de los recursos para desarrollo y producción (10.1.4)

1. El Comité Evaluador planifica la Separación de los recursos que existen en la Unidad de Tecnologías de la Información, luego encarga al Comité Formulador, la evaluación de disponibilidad de la infraestructura.
2. El Comité Formulador recibe documentación, evalúa disponibilidad de infraestructura y luego emite informe de disponibilidad.
3. El Comité Evaluador evalúa el Informe de Disponibilidad emitida por el Comité Formulador. Si existe disponibilidad de infraestructura, solicita al Comité Formulador continuar con los procedimientos, caso contrario realiza el requerimiento al Comité de Seguridad de la Información, la falta de infraestructura, para que realicen los actos administrativos correspondientes.
4. El Comité Formulador verifica los datos sensibles de los recursos de producción para poder establecer perfiles de usuario para el acceso al entorno de prueba, a continuación establece reglas de transferencia de Software, luego de ello emite informe para aprobación de creación de entorno de pruebas.
5. El Comité Evaluador revisa expediente de procedimientos. Si cumple los requerimientos técnicos, aprueba y comunica al Comité de Seguridad de la Información la creación de entornos. Caso contrario devuelve al Comité Formulador para subsanar observaciones.
6. El Comité de Seguridad de la Información emite opinión de separación de recursos, si es favorable aprueba la creación de entorno, caso contrario devuelve al Comité Evaluador para subsanar observaciones.
7. El Comité Formulador crea entorno según procedimiento aprobado e informa dicha creación al Comité Evaluador.
8. El Comité Evaluador revisa creación de entornos, si cumple con los procedimientos establecidos, informa al Comité de Seguridad de la Información sobre la creación del entorno, caso contrario, solicita subsanar observaciones.

Diagrama de Procesos N°4 - Separación de los recursos para desarrollo y producción (10.1.4)



Formulario N°4 - Separación de los recursos para desarrollo y producción (10.1.4)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.1.4 - SEPARACIÓN DE LOS RECURSOS PARA DESARROLLO Y PRODUCCIÓN**	**Código:** [FRM - 10.1.4 – 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **99** de **1**

1 DEL RECURSO: **Fecha:** [dd/mm/aaaa]

Recurso: [Descripción del Recurso a ser separado]

Nombre: [Nombre del Servidor] **Tipo:** [Tipo de Servidor (Base de Datos, Producción, Otros)]

Host Name: [Host name del Equipo] **Dirección IP:** [Indicar la dirección IP del Recurso a Separar]

Perfil de Acceso: [Indicar el tipo de perfiles de accesos autorizado para el acceso al Recurso]

DEL PROCESO:

Datos Sensibles: [Descripción de los datos sensibles, indicando la ubicación de resguardo]

_____

_____

_____

Reglas de Transferencia: [Descripción de las reglas de transferencia]

_____

_____

_____

[Numero de Resolución de Aprobación de la Separación de Recursos]

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró plan de separación de recursos]	**Nombre:** [Nombre de la persona que revisó el plan de separación de recursos]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del plan de separación de recursos]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.2. Planificación y aceptación del sistema.-

Objetivo:
Minimizar el riesgo de fallos de los sistemas.
Son necesarios una planificación y preparación para asegurar la disponibilidad de capacidad y de recursos adecuados para entregar el sistema de funcionamiento requerido
Deberían realizarse proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema.
Se debería establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los sistemas nuevos.

4.2.2.2.1. Planificación de la capacidad.-

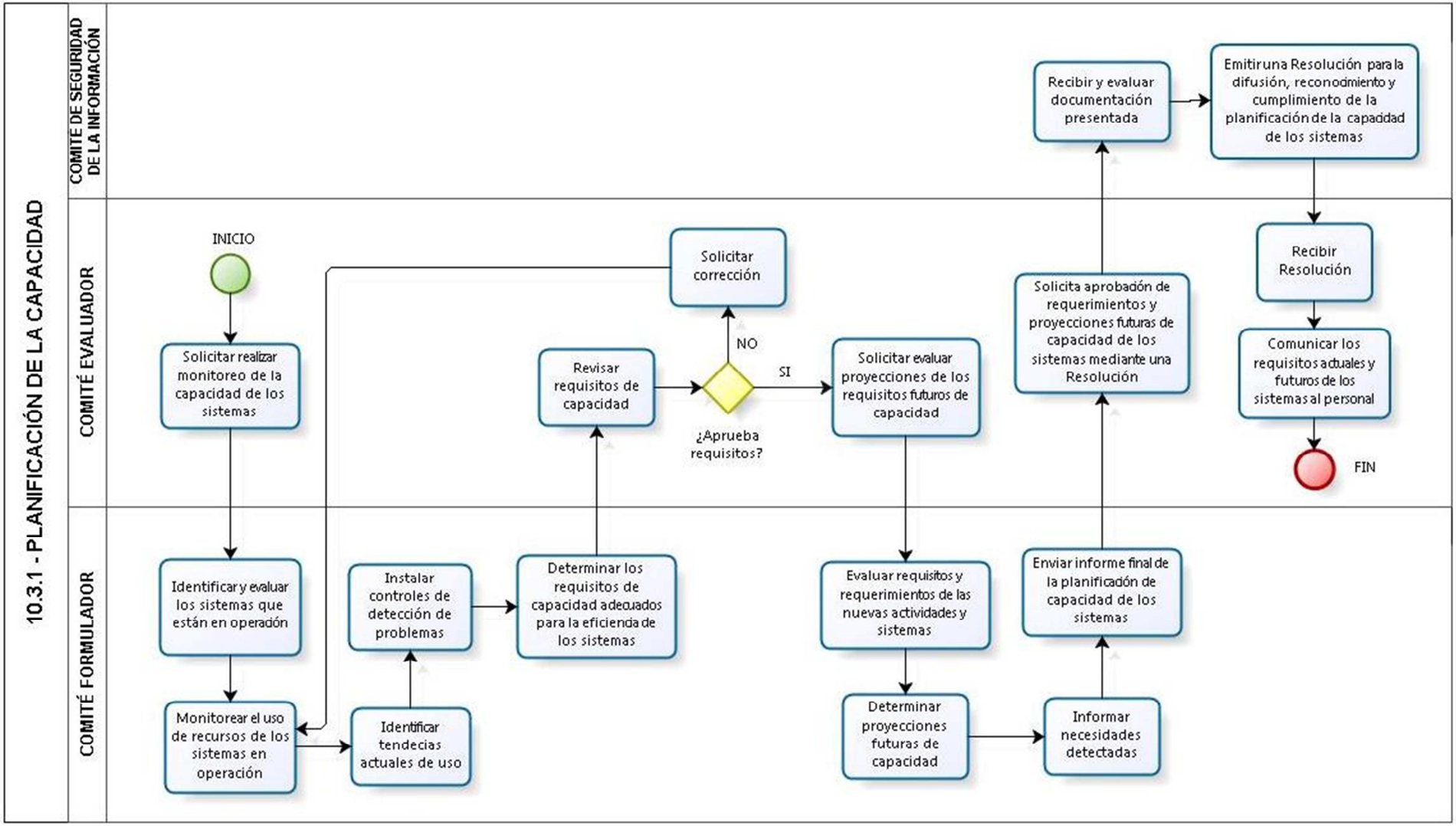
Control:
El uso de recursos debe ser monitoreado y las proyecciones hechas de requisitos de capacidades futuras para el sistema de funcionamiento requerido.

Guía de Implementación:
Para cada actividad que se esté llevando a cabo o para una actividad nueva, los requisitos de capacidad deben ser identificados. Se debe aplicar el monitoreo de los sistemas con el fin de asegurar, y donde sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. Controles de detección deben ser instalados para detectar los problemas en un tiempo debido. Las proyecciones deberían tener en cuenta los requisitos de las nuevas actividades y sistemas, así como la tendencia actual y proyectada de tratamiento de la información en la organización.
Se requiere poner particular atención a cualquier recurso con tiempo de llegada largo o con costos altos; por esto, la gerencia debe monitorear la utilización de los recursos claves del sistema. Se deberían identificar las tendencias de uso, particularmente relativas a las aplicaciones del negocio o a las herramientas de administración de sistemas de información.
Los administradores deberían usar esta información para identificar y evitar posibles cuellos de botella que pueden representar una amenaza a la seguridad del sistema o a los servicios al usuario, y para planificar la acción correctora apropiada.

Diagrama de Actividades N°5 - Planificación de la capacidad (10.3.1)

1. El Comité Evaluador solicita al Comité Formulador que realice un monitoreo de la capacidad con la que cuentan todos los sistemas que utilizan.
2. El Comité Formulador recibe solicitud y procede a identificar y evaluar todos los sistemas que se encuentran actualmente en operación, para luego monitorear el uso de los recursos de cada sistema e identificar las tendencias actuales de uso que cada uno presenta. Terminado ello, instala controles de detección de problemas para cada sistema y finalmente con todo lo evaluado anteriormente, determina cuales son los requisitos de capacidad adecuados para la eficiencia de los sistemas en operación.
3. El Comité Evaluador revisa los requisitos de capacidad elaborados por el Comité Formulador, si no aprueba los requisitos, solicita la corrección de ellos, pero por el contrario si los aprueba, solicita la evaluación de las proyecciones de los requisitos futuros de capacidad de todos los sistemas.
4. El Comité Formulador evalúa los requisitos y requerimientos que cuentan las nuevas actividades y nuevos sistemas a ser utilizados en la UTI, para así determinar cuáles son las proyecciones futuras de capacidad de cada una de ellas. Finalmente, informa las necesidades detectadas al Comité Evaluador.
5. Una vez recibido el informe final de la planificación de capacidad de los sistemas, el Comité Evaluador solicita la aprobación del mismo mediante una Resolución.
6. El Comité de Seguridad de la Información, recibe y evalúa la documentación presentada, una vez realizado ello, emite una Resolución para la difusión, reconocimiento y cumplimiento de la planificación de la capacidad de los sistemas.
7. El Comité Evaluador recibe resolución y comunica al personal, los requisitos actuales y futuros de todos los sistemas en operación.

Diagrama de Procesos N°5 - Planificación de la capacidad (10.3.1)



Formulario N°5 - Planificación de la capacidad (10.3.1)

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**FORMULARIO 10.3.1 - PLANIFICACIÓN DE LA CAPACIDAD**	**Código:** [FRM - 10.3.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **103** de **1**

1 DE LOS REQUISITOS DE CAPACIDAD:

Fecha: [dd/mm/aaaa]

Sistema y/o actividad a monitorear: [Indicar el sistema o actividad a monitorear para determinar sus requisitos de capacidad]

Estado del sistema y/o actividad: [Indicar estado del sistema y /o actividad según corresponda]

Se encuentra Operativo [ ]	**Es una proyección para futuro [ ]**
Tendencia de uso actuales del sistema o actividad en operación: [Determinar tendencias de uso actuales del sistema o actividad monitoreado] ❖ Tendencia de uso 1 ❖ Tendencia de uso 2 ❖ Tendencia de uso 3	**Requisitos y requerimientos de los nuevos sistemas y actividades:** [Determinar requisitos y requerimientos futuros para nuevos sistemas y actividades] ❖ Requisito 1 ❖ Requisito 2 ❖ Requisito 3
Requisitos de capacidad adecuados para la eficiencia del sistema o actividad: [Listar los requisitos de capacidad del sistema o actividad monitoreado] ❖ Requisito de Capacidad 1 ❖ Requisito de Capacidad 2 ❖ Requisito de Capacidad 3	**Proyecciones futuras de capacidad:** [Listar las proyecciones futuras a necesitar para los sistemas y/o actividades] ❖ Proyección 1 ❖ Proyección 2 ❖ Proyección 3

Documentación elaborada: [Indicar el nombre de la documentación elaborada para el procedimiento funcional]

**** Número de Resolución de aprobación de la documentación del procedimiento***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona encargada de elaborar los requisitos de capacidad del sistema a evaluar]	**Nombre:** [Nombre de la persona que revisó los requisitos de capacidad propuestos del sistema evaluado]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento de la planificación de capacidad del sistema]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.2.2. Aceptación del sistema.-

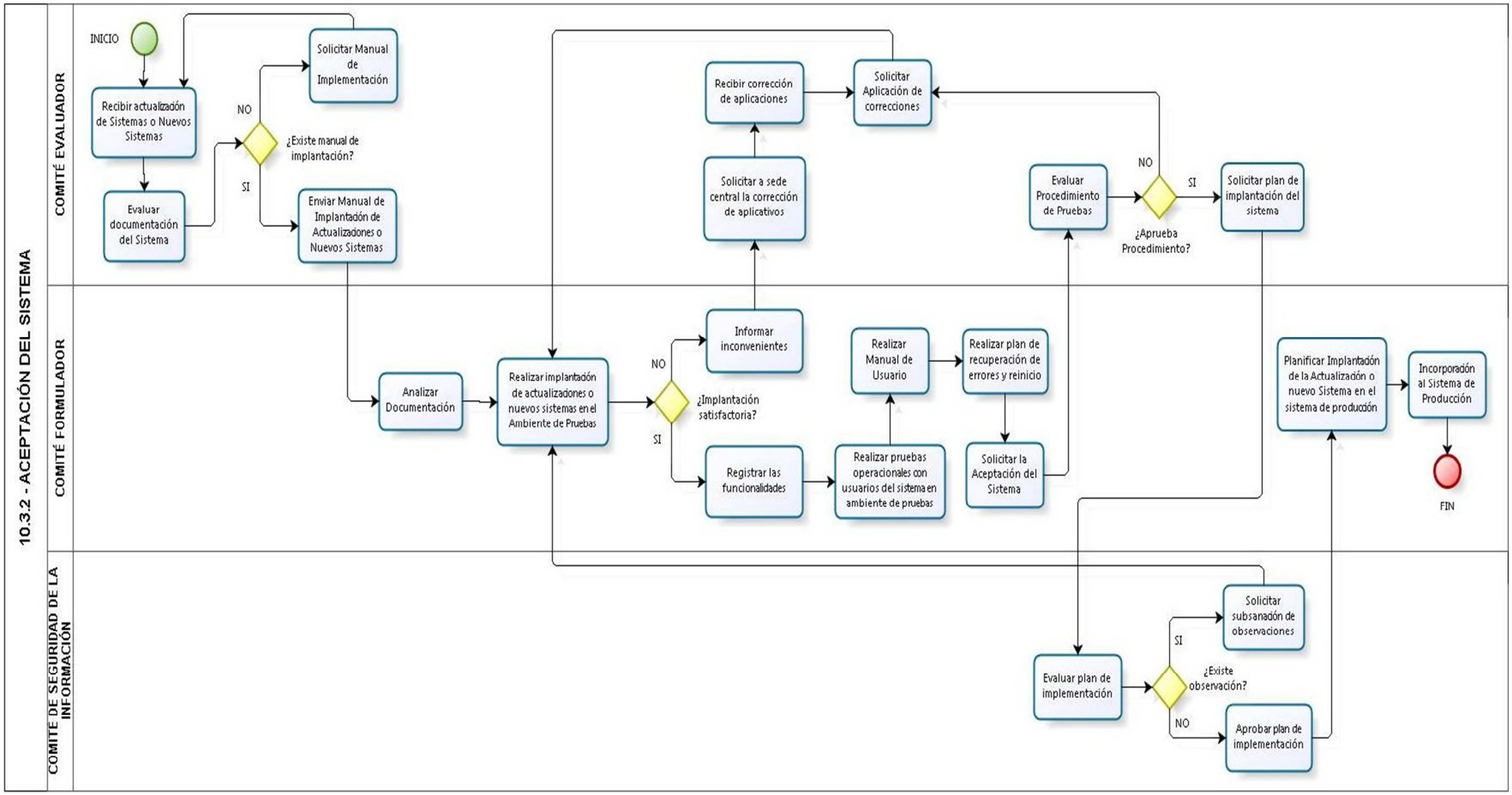
Control:
Se deberían implementar criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deberían desarrollar con ellos las pruebas adecuadas antes de su aceptación.

Guía de Implementación:
Los administradores se deberían asegurar que los requisitos y criterios de aceptación de los nuevos sistemas estén claramente definidos, acordados, documentados y probados. Los nuevos sistemas de información, actualizaciones y nuevas versiones deben ser migradas a producción solamente después de obtener una aceptación formal.

Diagrama de Actividades N°6 - Aceptación del sistema (10.3.2)

1. El Comité Evaluador recibe comunicado para aplicar actualizaciones y/o nuevos Sistemas por parte de Sede Central, luego evalúa documentación del sistema. Si existe manual de implantación y/o implementación, remite documentación al Comité Formulador, para su aplicación. Caso contrario, solicita documentación a OGTI Sede Central.
2. El Comité Formulador analiza documentación, luego realiza implantación de actualizaciones o nuevos sistemas en un ambiente de pruebas, según el manual de la documentación. Si las pruebas de implementación no generan inconvenientes, se procede a registrar las funcionalidades de las actualizaciones o características de los nuevos sistemas. Luego de ello se realiza pruebas operacionales con usuarios del sistema en el ambiente de pruebas, a continuación realiza manual del usuario, luego de ello desarrollan un plan de recuperación de errores y reinicio de los nuevos cambios y solicita al Comité Evaluador la aceptación del sistema. Caso sea que la implantación en el ambiente de pruebas no fue satisfactoria, informa al Comité Evaluador los inconvenientes presentados para que sea elevado mediante su persona a OGTI Sede Central, para su corrección.
3. El Comité Evaluador evalúa los procedimientos que se realizaron para las pruebas; si no cumple los requisitos, solicita al Comité Evaluador las correcciones respectivas, caso contrario solicita el plan de implantación de la actualización o nuevo sistema.
4. El Comité Formulador realiza el plan de implantación del sistema para su puesta en producción.
5. El Comité Evaluador autoriza la implantación de actualización o nuevo sistema y comunica dicha implantación al Comité de Seguridad de la Información.
6. Finalmente el Comité Formulador realiza la implantación del sistema o actualización del sistema.

Diagrama de Procesos N°6 - Aceptación del sistema (10.3.2)



Formulario N°6 - Aceptación del sistema (10.3.2)

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**FORMULARIO 10.3.2 - ACEPTACIÓN DEL SISTEMA**	**Código:** [FRM - 10.3.2 – 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **107** de **1**

1 DEL SISTEMA: **Fecha:** [dd/mm/aaaa]

Nombre del Sistema: [Descripción del Nombre del Sistema]
Versión del Sistema: [Indicar la Versión del Sistema]
Fecha de Recepción: [Fecha de Recepción del Sistema]
Tipo del Sistema: [Describir el Tipo de Sistema]

- Registral [ ] - Administrativo [ ]
  Otro [ ] _____

DEL PROCEDIMIENTO:

Pruebas de Implantación:	[Indicar el Informe de las pruebas de Implantación]	**Fecha:** [dd/mm/aaaa]
Pruebas Operacionales:	[Indicar el Informe de las pruebas Operacionales]	**Fecha:** [dd/mm/aaaa]
Informe de Implantación:	[Informe de Implantación del Sistema]	**Fecha:** [dd/mm/aaaa]

**** N°de Resolución de aprobación del plan de acepta ción del sistema***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró el plan de aceptación del sistema]	**Nombre:** [Nombre de la persona que revisó el plan de aceptación del sistema]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del plan de aceptación del sistema]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.3. Protección contra software malicioso.-

Objetivo:
Proteger la integridad del software y de la información.
Se requieren ciertas precauciones para prevenir y detectar la introducción del software malicioso.
El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, "gusanos de la red", "caballos de Troya" y bombas lógicas. Los usuarios deberían conocer los peligros que pueden ocasionar el software malicioso o no autorizado, y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.

4.2.2.3.1. Medidas y controles contra software malicioso.-

Control:
Se deberían implementar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios.

Guía de Implementación:
La protección contra el software malicioso debería basarse en la conciencia de la seguridad, en sistemas adecuados de acceso y en controles de gestión de los cambios.

Diagrama de Actividades N°7 - Medidas y controles contra software malicioso (10.4.1)

1. El Comité Evaluador establece 2 políticas:
   La **PRIMERA** es sobre la protección contra riesgos asociados a la obtención de archivos y software por redes externas. Solicita al Comité de Seguridad de la Información la aprobación inicial de la política mediante una Resolución.
2. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para el cumplimiento de la política.
3. El Comité Evaluador recibe Resolución y comunica dicha política al Comité Formulador para su cumplimiento.
4. El Comité Formulador analiza política y planifica revisiones para controlar que todas las computadoras cuenten con antivirus actualizados.
5. El Comité Evaluador revisa la planificación; si no la aprueba, solicita al Comité Formulador que se corrija. Si aprueba planificación, lo comunica al Comité Formulador para su ejecución.
6. Una vez que el plan ha sido aprobado, el Comité Formulador ejecuta las revisiones en cada computadora. Si existe alguna computadora o servidor que no tenga antivirus, procede a verificar que existan licencias de antivirus disponibles para dicha computadora, si es que hay licencias disponibles, instala antivirus en la computadora/servidor que lo necesitaba; si no existen licencias, lo informa al Comité Evaluador.
7. El Comité Evaluador, revisa informe y solicita la compra/renovación de las licencias al área de administración.
8. Si todas las computadoras cuentan con antivirus, el Comité Formulador procede a revisar que todas las licencias estén al día y actualiza el antivirus a las que lo necesiten. Así procede a realizar pruebas del funcionamiento del antivirus, si es que encuentra algún problema o incidencia, lo informa al Comité Evaluador.
9. El Comité Evaluador reporta las incidencias a la empresa proveedora del antivirus.
10. Si no existen problemas al realizar las pruebas, el Comité Formulador registra las revisiones realizadas, propone un plan de contingencia ante incidentes con antivirus y recolecta información sobre nuevos virus para mantenerse actualizado. Finalmente capacita al personal sobre la detección de virus.

11. La **SEGUNDA** política establecida por el Comité Evaluador es sobre el cumplimiento de licencias de software. Solicita al Comité de Seguridad de la Información la aprobación inicial de la política mediante una Resolución.

12. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para el cumplimiento de la política.

13. El Comité Evaluador recibe la Resolución y comunica dicha política al Comité Formulador para su cumplimiento.

14. El Comité Formulador analiza política y revisa el inventario de software para poder identificar las licencias actuales con las que la UTI cuenta. Una vez revisado ello, planifica revisiones regulares para controlar el cumplimiento de las licencias de software y la no existencia de software no autorizado.

15. El Comité Evaluador revisa la planificación; si no la aprueba, solicita al Comité Formulador que se corrija. Si aprueba planificación, lo comunica al Comité Formulador para su ejecución.

16. Una vez que el plan ha sido aprobado, el Comité Formulador ejecuta las revisiones regulares de licencias en cada computadora. Si existe alguna computadora que tenga alguna licencia caducada, procede a evaluar si dicho software es aún útil para la oficina; de ser el caso que si sea útil, informa al Comité Evaluador sobre la licencia caducada y recomienda su renovación, si el software ya no es útil, informa el desuso del software y recomienda darle de baja. Registra revisión de licencias realizada

17. Tal sea el caso, el Comité Evaluador solicita la compra o la baja de dicho software al área de administración.

18. Si no existen licencias caducadas, el Comité Formulador registra revisión realizada y evalúa si encontró algún software no autorizado que esté instalado en alguna computadora. Si no encontró ningún software no autorizado, procede a registrar e informar la revisión realizada al Comité Evaluador. De ser el caso que si haya encontrado alguno, informa la existencia de software no autorizado al Comité Evaluador.

19. El Comité Evaluador revisa informe y evalúa la funcionalidad del software encontrado; si éste es útil, solicita su compra al área de abastecimientos y junto con el Comité Formulador, actualiza el inventario una vez adquirido el software. Si no es útil, aprueba la eliminación y desinstalación del software encontrado.

20. El Comité Formulador procede a la desinstalación del software, además recomienda y concientiza al personal sobre el cumplimiento de la prohibición de software no autorizado en la institución. Finalmente registra revisión realizada.

Diagrama de Procesos N°7 - Medidas y controles contra software malicioso (10.4.1) – Proceso N°1

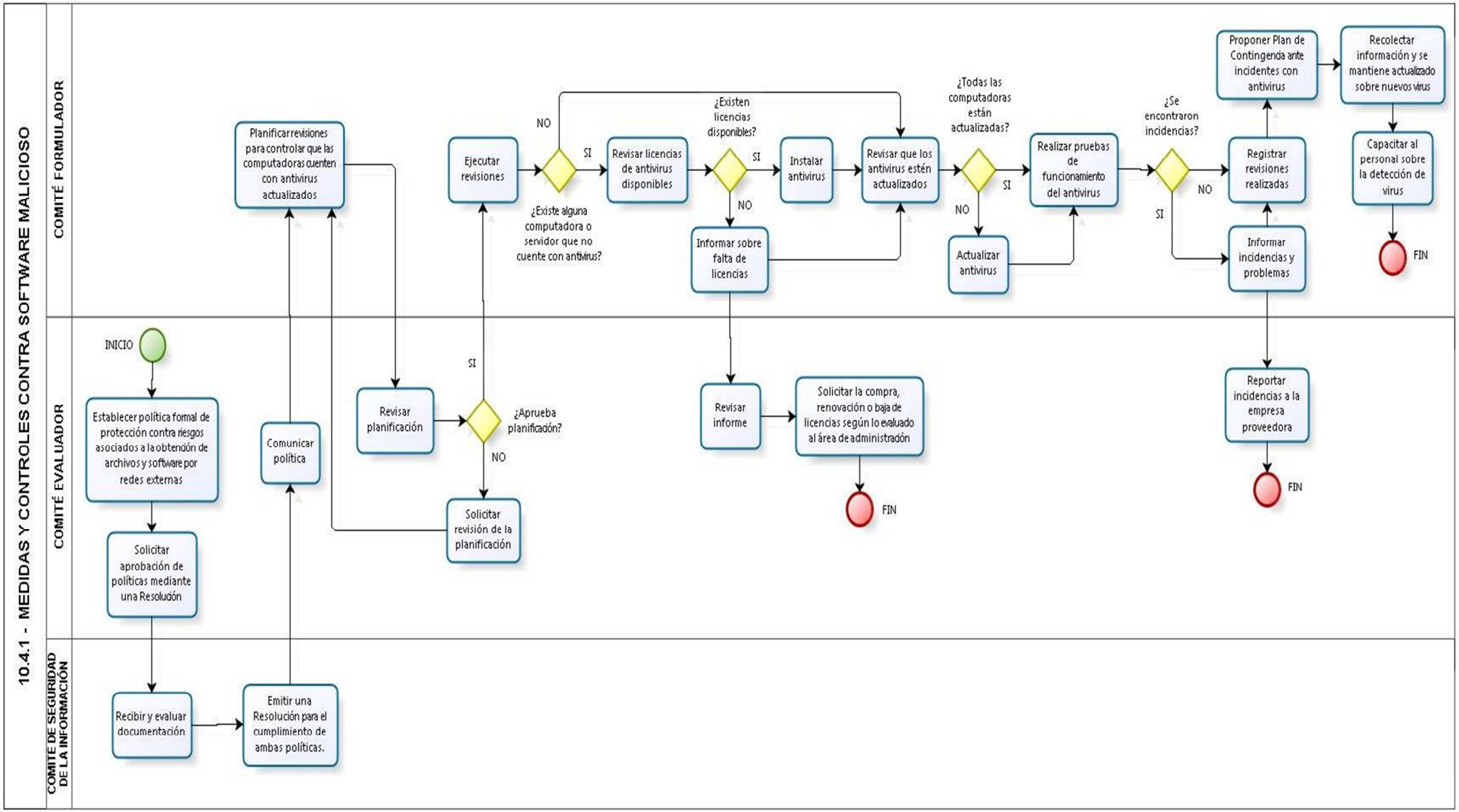
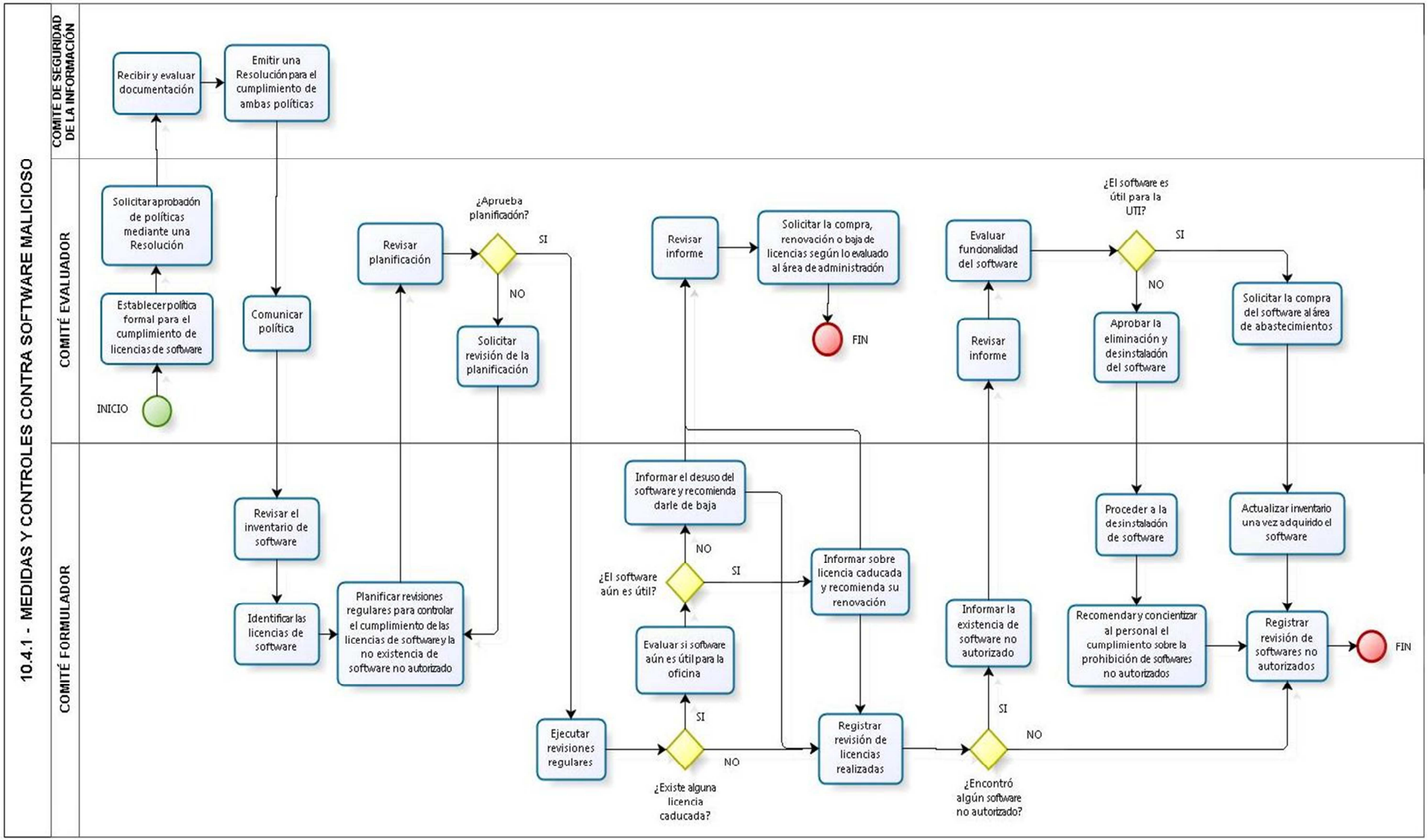


Diagrama de Procesos N°8 - Medidas y controles contra software malicioso (10.4.1) – Proceso N°2



Formulario N°7 - Medidas y controles contra software malicioso (10.4.1)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.4.1 - MEDIDAS Y CONTROLES CONTRA SOFTWARE MALICIOSO (Form 01)**	**Código:** [FRM - 10.4.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **113** de **1**

1 DE LA POLÍTICA ESTABLECIDA:

Fecha: [dd/mm/aaaa]

Política establecida: [Nombre de la Política establecida para la protección contra riesgos asociados a la obtención de archivos y software por redes externas]
Antivirus utilizado: [Indicar el nombre del antivirus utilizado en la Institución]
Versión del Antivirus: [Indicar la versión actual del antivirus utilizado en la Institución]

DE LAS REVISIONES REALIZADAS:

Revisión N°: [Indicar el número de revisión realizada y la fecha en la que se realizó]
N°de computadoras sin antivirus: [Indicar cantidad de computadoras encontradas sin antivirus]
N°de computadoras con antivirus desactualizado: [Indicar cantidad de computadoras encontradas con antivirus desactualizado]
N°de licencias de antivirus disponibles: [Indicar cantidad de licencias de antivirus disponibles encontradas]

DE LAS ACTUALIZACIONES REALIZADAS:

N°de computadoras a las que se les instaló el antivirus: [Indicar cantidad de computadoras a las que se les instaló el antivirus]
N°de computadoras a las que se les actualizó el antivirus: [Indicar cantidad de computadoras a las que se les actualizó el antivirus]
Pruebas de funcionamiento: [Detallar las pruebas realizadas para verificar el correcto funcionamiento del antivirus instalado/actualizado]
Incidencias presentadas: [Detallar las incidencias presentadas durante las pruebas realizadas]

**** Número de Resolución de aprobación de la política establecida***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona encargada de realizar el monitoreo del antivirus]	**Nombre:** [Nombre de la persona que revisó el monitoreo del antivirus realizado]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento de la política contra riesgos]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**FORMULARIO** **10.4.1 - MEDIDAS Y CONTROLES CONTRA SOFTWARE MALICIOSO** **(Form 02)**	**Código:** [FRM - 10.4.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **114** de **1**

1 DE LA POLÍTICA ESTABLECIDA: **Fecha:** [dd/mm/aaaa]

Política establecida: [Nombre de la Política establecida para el cumplimiento correcto de las licencias de software]

DE LA REVISIÓN DE LICENCIAS DE SOFTWARE NO VIGENTES:

Revisión N°:	[Indicar el número de revisión realizada y la fecha en la que se realizó]
N° de licencias de software no vigentes:	[Indicar cantidad de licencias de software no vigentes encontradas en la revisión realizada]
Software no vigente:	[Indicar y describir el software no vigente encontrado]
Acción a realizar:	[Indicar si se dará de baja o se renovará la licencia de software]
Motivo de la Acción a realizar:	[Indicar el motivo de la **Baja**: Vigencia Tecnológica, Fuera de Mantenimiento, Desuso, o el motivo de la **Renovación**: Necesidad o Garantía]

DE LA REVISIÓN DE SOFTWARE NO AUTORIZADO:

Cantidad de software no autorizado:	[Indicar cantidad de licencias de software encontradas y que no están autorizadas]
Software no autorizado:	[Indicar y describir el software no autorizado que se ha encontrado]
Acción a realizar:	[Indicar si se procederá a Desinstalar o a Adquirir software]
Motivo de la Acción a realizar:	[Indicar el motivo de la **Desinstalación**: Software no útil, Software prohibido, o indicar el motivo de la **Adquisición**: Software útil, Software necesario]

**** Número de Resolución de aprobación de la política establecida***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona encargada de realizar el monitoreo de las licencias de software]	**Nombre:** [Nombre de la persona que revisó el monitoreo de las licencias de software realizado]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento de la política del el uso de licencias de software]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.3.2. Medidas y controles contra código móvil

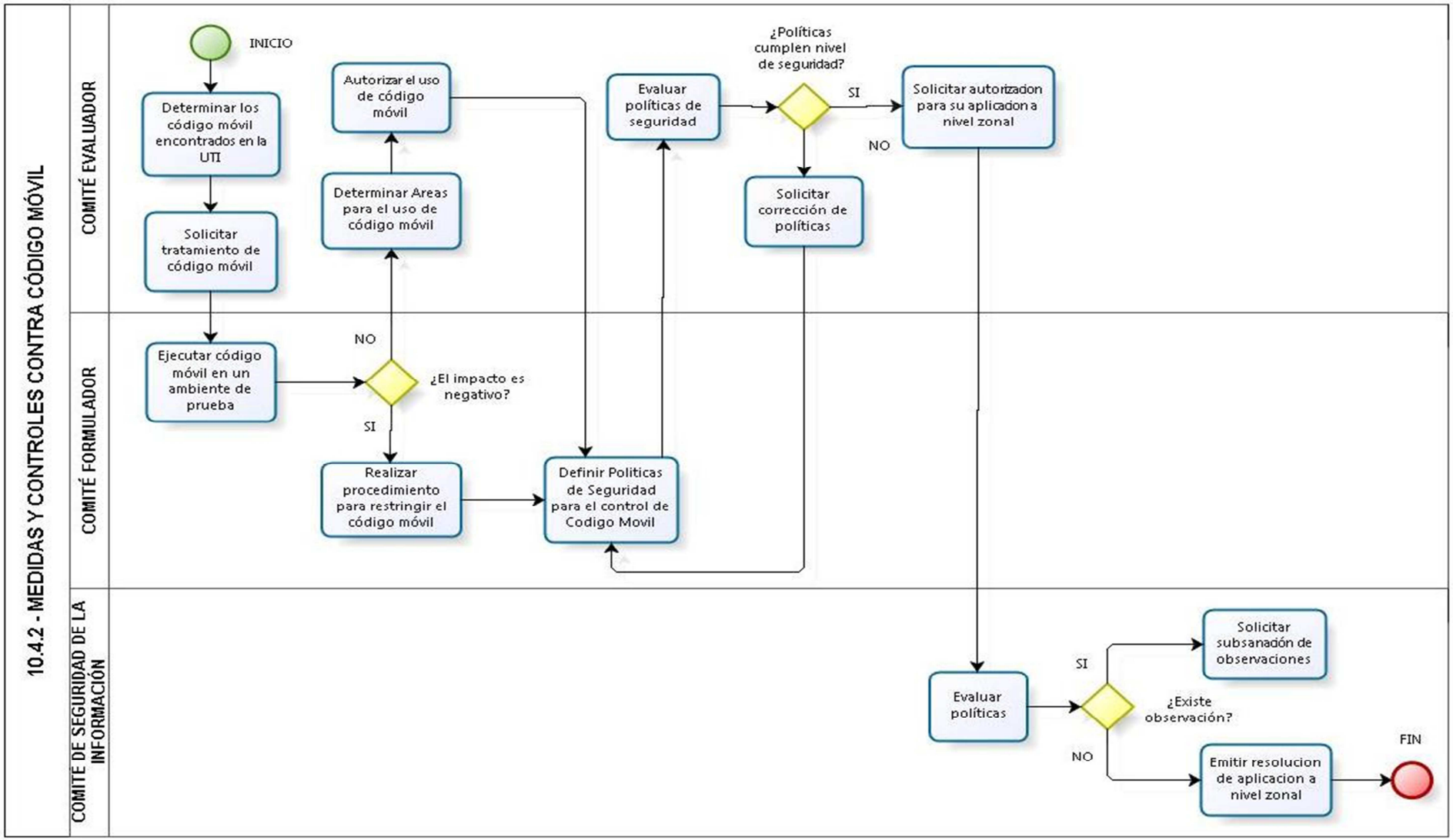
Control:
Donde el uso de código móvil es autorizado, la configuración debe asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y que se debe prevenir que este sea ejecutado.

Guía de Implementación:
Se debe ejecutar código móvil en un ambiente aislado, bloquear cualquier el recibo y uso de código móvil, activar medidas técnicas para asegurar que el código móvil este manejado, controlar los recursos de código móvil y controlar criptográficamente para autentificar individualmente un código móvil.

Diagrama de Actividades N°8 - Medidas y controles contra código móvil (10.4.2)

1. El Comité Evaluador determina los códigos móviles de la Unidad de Tecnologías de Ia Información y solicita al Comité Evaluador el tratamiento de código móvil.
2. El Comité Formulador ejecuta el código en un ambiente de pruebas y determina el impacto que éste causa dentro de la UTI. Si la ejecución genera un impacto negativo, define políticas de seguridad para el control de código móvil, caso contrario solicita al Comité Evaluador determinar áreas autorizadas para el uso de código móvil, para definir políticas de seguridad para el control del mismo.
3. Luego de ello el Comité Evaluador evalúa procedimiento y políticas de seguridad, si las políticas cumple el nivel de seguridad para el control de código móvil, aprueba las políticas y solicita al Comité de Seguridad de la Información la autorización para su aplicación a nivel zonal. Caso contrario solicita la corrección de políticas.
4. Finalmente el Comité de Seguridad de la Información procede a evaluar políticas, si realiza alguna observación, solicita levantar observaciones, caso contrario emite resolución para su aplicación.

Diagrama de Procesos N°9 - Medidas y controles contra código móvil (10.4.2)



Formulario N°8 - Medidas y controles contra código móvil (10.4.2)

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**FORMULARIO 10.1.2 – MEDIDAS Y CONTROLES CONTRA CÓDIGO MÓVIL**	**Código:** [FRM - 10.4.2 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **118** de **1**

1 DEL CÓDIGO MÓVIL: **Fecha:** [dd/mm/aaaa]

Código Móvil:	[Descripción del Código Móvil]
Pruebas de Código Móvil:	[Número de Informe donde determine las pruebas de ejecución de código móvil]
Ambiente de Pruebas:	[Indicar la infraestructura donde se realizó el ambiente de pruebas]
Impacto de Código Móvil:	Negativo [ ] Positivo [ ] [Indicar el impacto de la ejecución del código móvil]
Políticas de Control:	[Descripción de políticas de seguridad para el control de código móvil e indicar el número de informe con el cual estas fueron presentadas y aprobadas]
Acceso de código móvil:	Autorizado[ ] Restringido [ ] [Indicar el acceso del código móvil]

*** SOLO SI EL ACCESO DEL CÓDIGO MÓVIL AUTORIZADO ES NEGATIVO**

Unidad Organizativa:	[Nombre de la Unidad Organizativa donde está permitido el código móvil]
Responsable:	[Nombre de la persona responsable de la Unidad Organizativa]
Fecha de Aprobación:	[Fecha en el que el código móvil es autorizado para la unidad organizativa]

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró plan de medidas y controles contra código móvil]	**Nombre:** [Nombre de la persona que revisó el plan de medidas y controles contra código móvil]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del plan de medidas y controles contra código móvil]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.4. Gestión de respaldo y recuperación.-

Objetivo:
Mantener la integridad y disponibilidad de los servicios de tratamiento de información y comunicación.
Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo haciendo copias de seguridad y ensayando su oportuna recuperación.

4.2.2.4.1. Recuperación de la información.-

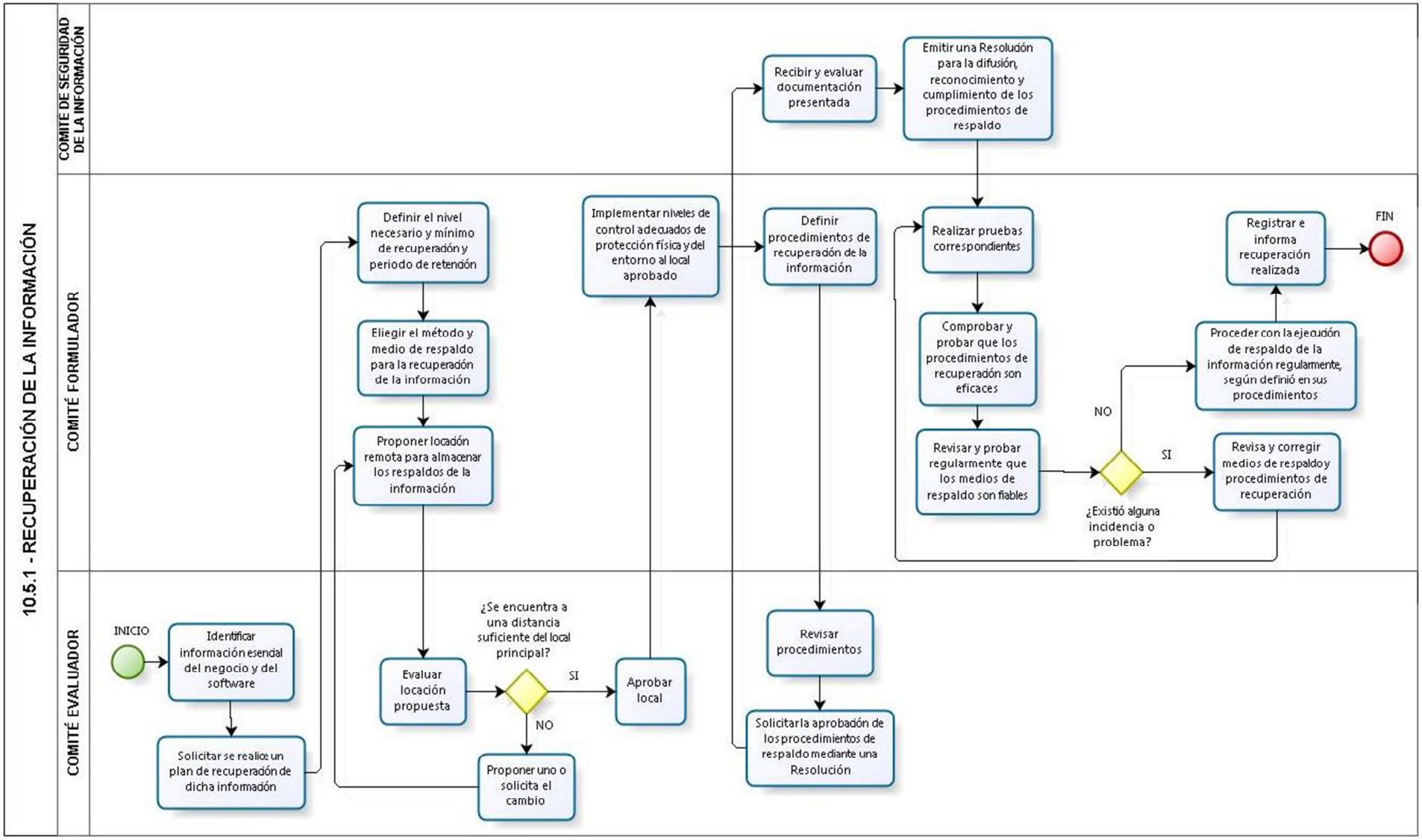
Control:
Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.

Guía de Implementación:
Adecuados servicios de respaldo deben ser provistos para asegurar que toda la información esencial del negocio pueda recuperarse tras un desastre o un fallo de los medios.
Deben probarse regularmente arreglos individuales de las copias de seguridad de los sistemas para asegurar que estos reúnen los requisitos de los planes de continuidad del negocio. Para los sistemas críticos, los arreglos auxiliares deben cubrir toda la información de los sistemas, aplicaciones y datos necesarios de recuperarse del sistema complemento en caso de un desastre.
El periodo de retención para la información esencial del negocio, y también cualquier requisito permanente para las copias de los archivos debe determinarse.

Diagrama de Actividades N°9 - Recuperación de la información (10.5.1)

1. El Comité Evaluador identifica la información esencial del negocio y del software y solicita al Comité Formulador que realice un plan de recuperación de dicha información.
2. El Comité Formulador estudia la información a recuperar y define el nivel necesario/mínimo de recuperación y período de retención de la información. Elije además, el método de respaldo para la recuperación de la información y propone locación remota segura para almacenar los respaldos de la información.
3. El Comité Evaluador evalúa locación remota propuesta, y verifica que dicho local se encuentre a una distancia suficiente del local principal. Si el local cumple con lo establecido, aprueba el local, si no cumple, propone un nuevo local o solicita el cambio al Comité Formulador.
4. Una vez que se tiene el local aprobado, el Comité Formulador implementa niveles de control adecuados de protección física y del entorno para el local elegido y define procedimientos de recuperación de la información
5. El Comité Evaluador revisa los procedimientos propuestos y solicita la aprobación de los mismos mediante una Resolución.
6. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento de los procedimientos de respaldo.
7. Una vez obtenida la Resolución, el Comité Formulador realiza las pruebas correspondientes utilizando dichos procedimientos. Comprueba que los procedimientos de recuperación sean eficaces y revisa regularmente que los medios de respaldo sean fiables. Si es que existen incidencias o problemas, revisa y corrige los medios de respaldo y procedimientos de recuperación, para luego volver a realizar las pruebas correspondientes. Si no existieron inconvenientes, procede con la ejecución de respaldo de la información regularmente según lo definido en sus procedimientos. Finalmente registra e informa la recuperación de información realizada.

Diagrama de Procesos N°10 - Recuperación de la información (10.5.1)



Formulario N°9 - Recuperación de la información (10.5.1)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.5.1 - RECUPERACIÓN DE LA INFORMACIÓN**	**Código:** [FRM - 10.5.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **122** de **1**

1 DEL PLAN DE RECUPERACIÓN DE LA INFORMACIÓN: **Fecha:** [dd/mm/aaaa]

Plan de Recuperación: [Indicar el nombre del Plan de Recuperación de la información elaborado]
Plan documentado con: [Número de informe con el que se documentó el plan de recuperación]

DE LA INFORMACIÓN A RECUPERAR:

Tipo de Información a recuperar: [Indicar el tipo de información a recuperar]
- ❖ Keyfile [ ] Base de Datos [ ]

Nivel de Recuperación: [Indicar el nivel necesario y mínimo de recuperación a obtener]
Método de Recuperación: [Indicar el método elegido para realizar la recuperación]
Medio de Recuperación: [Indicar el medio de recuperación a utilizar]
Periodo de retención: [Indicar el tiempo de retención de la información recuperada]
Locación remota de almacenaje: [Indicar el lugar elegido para almacenar la información recuperada]

DE LAS PRUEBAS Y LA RECUPERACIÓN:

Pruebas de respaldos realizadas por: [Indicar el nombre de la persona que realizó las pruebas de los respaldos obtenidos y la fecha en la que las realizó]
Incidencias encontradas: [Indicar las incidencias o problemas presentados durante las pruebas]
Recuperación elaborada por: [Indicar el nombre de la persona que recuperó la información]
En fecha: [Indicar la fecha en la que se realizó la recuperación de la información]

**** Número de Resolución de aprobación del Plan de Recuperación de la Información***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona encargada de elaborar el plan de recuperación de la información]	**Nombre:** [Nombre de la persona que revisó el plan de recuperación de la información]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento del plan de recuperación de la información]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.5. Gestión de seguridad en redes.-

Objetivo:
Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
La gestión de la seguridad de las redes que cruzan fronteras de la organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles por las redes públicas.
Controles adicionales pueden ser requeridos también con el fin de proteger información sensible pasando sobre redes públicas.

4.2.2.5.1. Controles de red.-

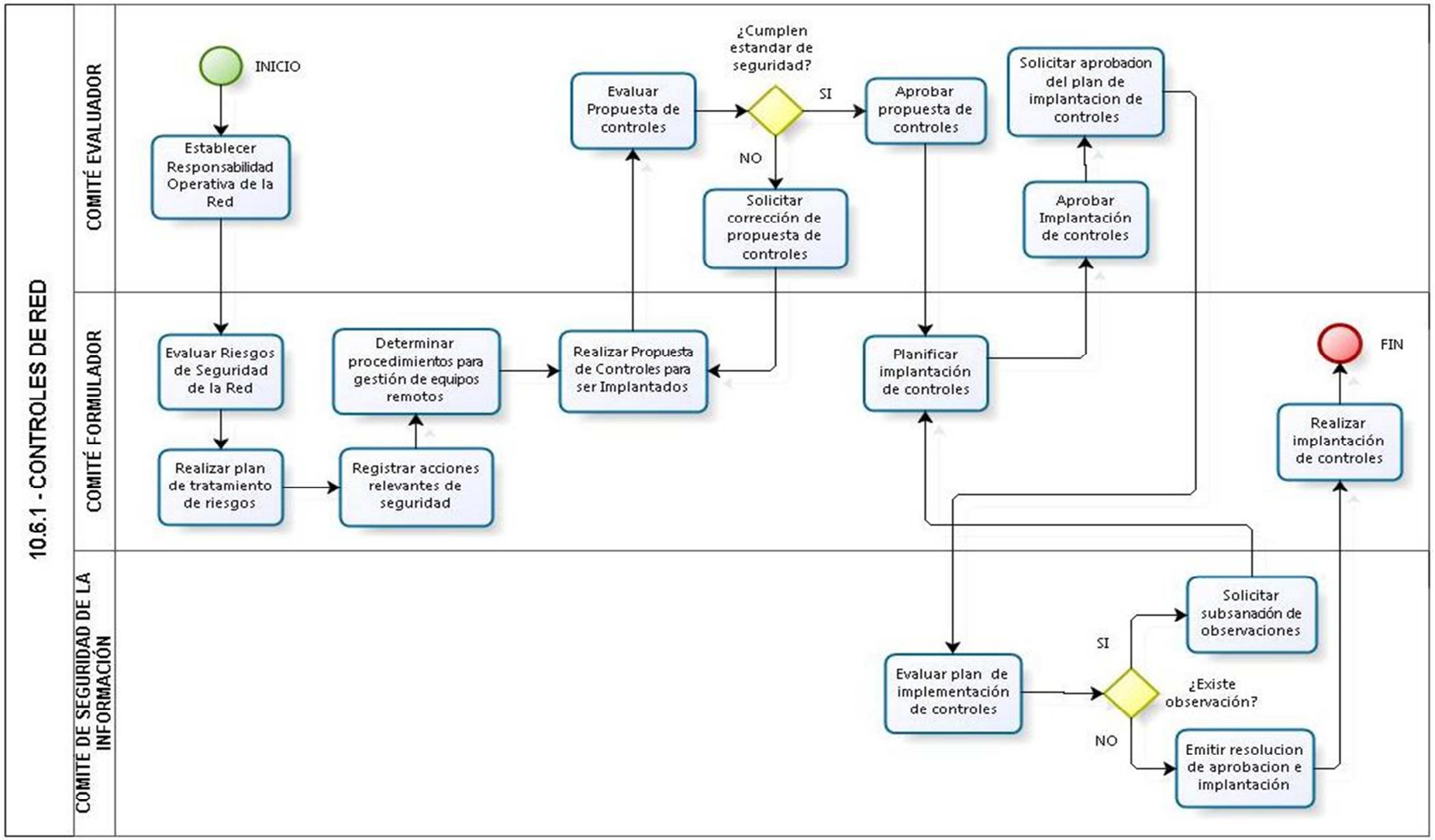
Control:
Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito.

Guía de Implementación:
Los administradores de redes deberían implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de las computadoras, así como la protección de los servicios conectados contra accesos no autorizados.

Diagrama de Actividades N°10 - Controles de red (10.6.1)

1. El Comité Evaluador establece responsabilidades operativas de la red y determina responsable.
2. El Comité Formulador evalúa los riesgos de seguridad existentes en la red, para luego realizar un plan para tratamiento de dichos riesgos. Luego de ello procede a registrar las acciones relevantes de seguridad y determina los procedimientos de gestión de los equipos remotos. A continuación, realiza una propuesta de controles para ser implantados y presentados al Comité evaluador.
3. El Comité Evaluador recibe y evalúa si la propuesta de controles cumple estándares de seguridad establecidos, si es que no los cumple, solicita corrección al Comité Evaluador; caso contrario, aprueba controles.
4. Una vez aprobado los controles, el Comité Formulador procede a planificar la implantación de los controles.
5. Luego de ello el Comité Evaluador revisa el plan de implantación y lo aprueba, solicitando así su aplicación al Comité de Seguridad mediante resolución.
6. El Comité de Seguridad de la Información evalúa los controles y el plan de implantación, si realiza alguna observación, solicita levantar observaciones, caso contrario emite resolución para su implantación.
7. El Comité Formulador realiza la implantación de los controles según el plan de implantación, finalmente registra los controles realizados.

Diagrama de Procesos N°11 - Controles de red (10.6.1)



Formulario N°10 - Controles de red (10.6.1)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.6.1 – CONTROLES DE RED**	**Código:** [FRM - 10.6.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **126** de **1**

1 DEL CONTROL DE RED: **Fecha:** [dd/mm/aaaa]

Responsable de la Red:	[Nombre de la persona asignada como responsable de la Red]
Riegos de Red:	[Riesgo determinado luego de la evaluación de riesgos]
Tratamiento de Riesgos:	[Indicar el informe del Plan de Tratamiento de Riesgos de Red]
Acciones Relevantes:	[Descripción de las acciones relevantes a los riesgos de Red]
Controles de Red:	[Informe con el cual se presenta los controles de red para el riesgo de red encontrado]
Gestión de Equipos Remotos:	[Detalle sobre el procedimiento para la gestión de equipos remotos]
Plan de Implantación:	[Indicar el Informe de las pruebas Operacionales] **Fecha:** [dd/mm/aaaa]

* ***Resolución con el cual aprueban el procedimiento de controles de red***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró plan de controles de red]	**Nombre:** [Nombre de la persona que revisó el plan de controles de red]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del plan de controles de red]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.5.2. Seguridad en los servicios de redes.-

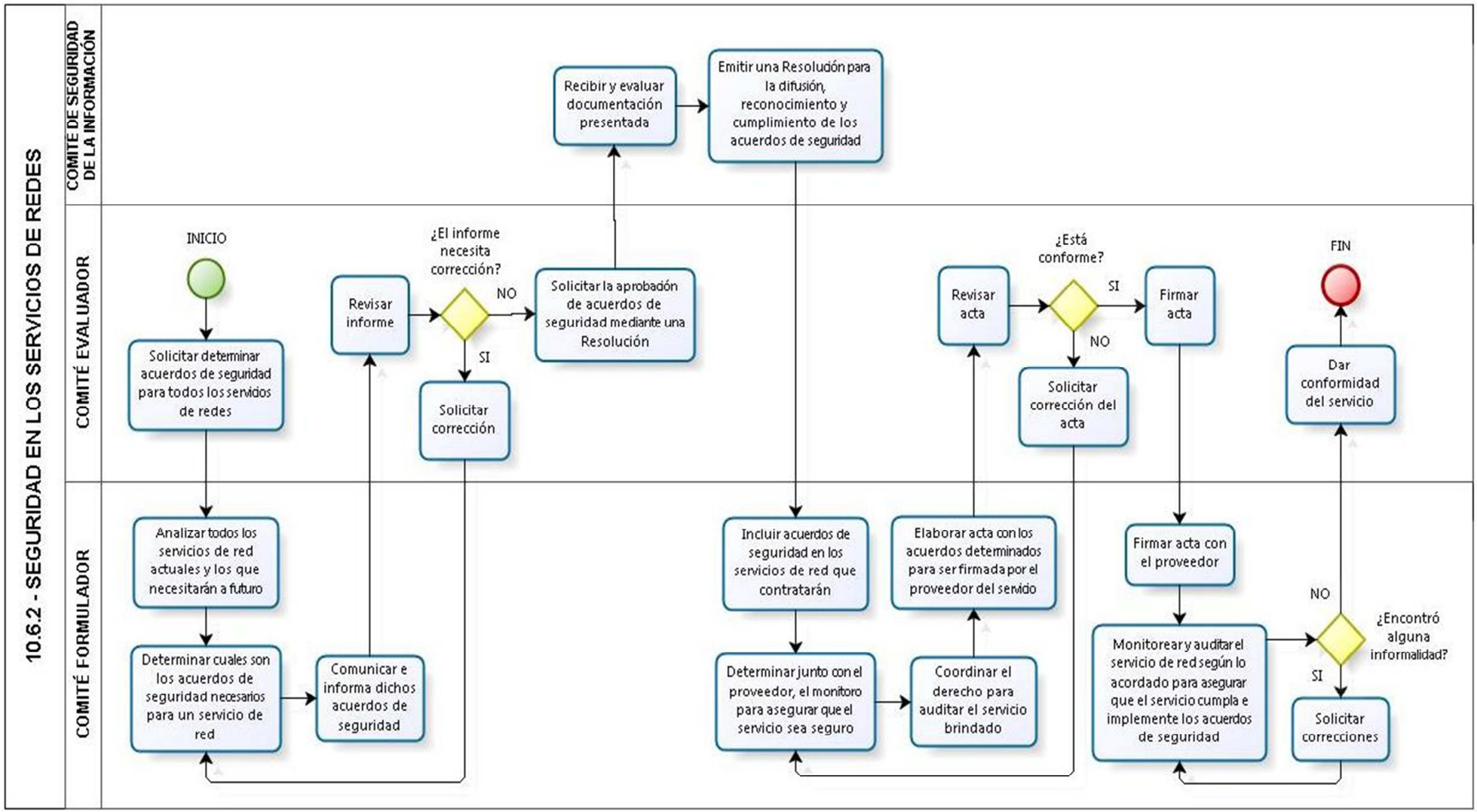
Control:
Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización.

Guía de Implementación:
La habilidad del proveedor del servicio de red para manejar servicios acordados de una manera segura debe ser determinado y monitoreado regularmente, y el derecho para auditar debe ser acordado.
Los acuerdos de seguridad necesarios para servicios particulares, como características de seguridad, niveles de servicio y los requisitos de gestión, deben ser identificados. La organización debe asegurarse que los proveedores de servicio de red implementen estas medidas.

Diagrama de Actividades N°11 - Seguridad en los servicios de redes (10.6.2)

1. El Comité Evaluador solicita determinar los acuerdos de seguridad a tomar para todos los servicios de redes que se realizan, dicha tarea lo asigna al Comité Formulador.
2. El Comité Formulador recibe asignación y analiza todos los servicios de red actuales y los que necesitarán a futuro, una vez hecho el análisis, determina cuales son los acuerdos de seguridad necesarios que se debe de cumplir para contratar un servicio de red. Dichos acuerdos los comunica e informa al Comité Evaluador.
3. El Comité Evaluador, revisa el informe y lo evalúa, si es que encuentra disconformidades, solicita al Comité Formulador que las corrija, de otro modo si es que no encuentra problemas, solicita que se realice la aprobación de los acuerdos de seguridad mediante una Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento de los acuerdos de seguridad.
5. Una vez que los acuerdos de seguridad han sido aprobados, el Comité Formulador los incluye en los servicios de red a contratar: para ello determina junto con el proveedor, el proceso de monitoreo al servicio para asegurar que éste sea seguro, coordina el derecho para auditar el servicio brindado y elabora acta inicial con los acuerdos determinados para ser firmada por el proveedor del servicio.
6. El Comité Evaluador revisa el acta realizada por el Comité Formulador, si es que no está conforme con dicha acta, solicita la corrección inmediata; si es que está conforme procede a firmar el acta.
7. El Comité Formulador firma acta con el proveedor y procede a monitorear y a auditar e servicio de red brindado según lo acordado, para asegurar que el servicio cumpla e implemente los acuerdos de seguridad. Si es que el Comité Formulador encuentra alguna informalidad, solicita las correcciones respectivas al proveedor. Si es que no encontró ningún problema, lo informa al Comité Evaluador para la conformidad del servicio.
8. Finalmente el Comité Evaluador procede a dar conformidad junto con el Comité Formulador, el servicio brindado por el proveedor.

Diagrama de Procesos N°12 - Seguridad en los servicios de redes (10.6.2)



Formulario N°11 - Seguridad en los servicios de redes (10.6.2)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.6.2 - SEGURIDAD EN LOS SERVICIOS DE REDES**	**Código:** [FRM - 10.6.2 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **130** de **1**

1 DEL ACUERDO DE SEGURIDAD: **Fecha:** [dd/mm/aaaa]

Acuerdo de Seguridad: [Indicar el acuerdo de seguridad para los servicios de redes a utilizar]
Acuerdo documentado con: [Número de informe con el que se documentaron los acuerdos de seguridad]

DEL SERVICIO DE RED:

Servicio de Red: [Indicar el nombre del Servicio de Red]
Descripción del Servicio de Red: [Indicar una breve descripción del Servicio de Red] _____
_____
Nombre del proveedor: [Indicar el nombre del proveedor que brinda el Servicio de Red]
Nombre de la empresa: [Indicar el nombre de la empresa que brinda el Servicio de Red]

DE LOS ACUERDOS PARA EL SERVICIO DE RED:

Fechas de monitoreo: [Indicar las fechas acordadas con el proveedor para el monitoreo del servicio]
Fechas de auditoría: [Indicar las fechas acordadas con el proveedor para auditar el servicio de red]
Acta inicial de acuerdos: [Indicar el N° de acta en la que se acuerdan las fechas de monitoreo y auditoría además de la Fecha en la que se firma dicha Acta inicial]
Conformidad del Servicio: [**Si se da la conformidad**, indicar el N° de documento con el que se da conformidad del servicio además de incluir la Fecha en la que se firma dicha conformidad. **Si no se da la conformidad**, indicar NO CONFORME]
Conformidad brindada por: [Nombre de la persona que dio la conformidad del Servicio de Red]

**** Número de Resolución de aprobación para el cumplimiento de los acuerdos de seguridad***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona encargada de elaborar los acuerdos de seguridad para los servicios de redes]	**Nombre:** [Nombre de la persona que revisó los acuerdos de seguridad para los servicios de redes]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento de los acuerdos de seguridad]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.6. Utilización de los medios de información.-

Objetivo:
Prevenir acceso no autorizado, modificaciones, evitar daños a los activos e interrupciones de las actividades de la organización.
Los medios deben ser controlados y físicamente protegidos.
Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado.

4.2.2.6.1. Gestión de medios removibles.-

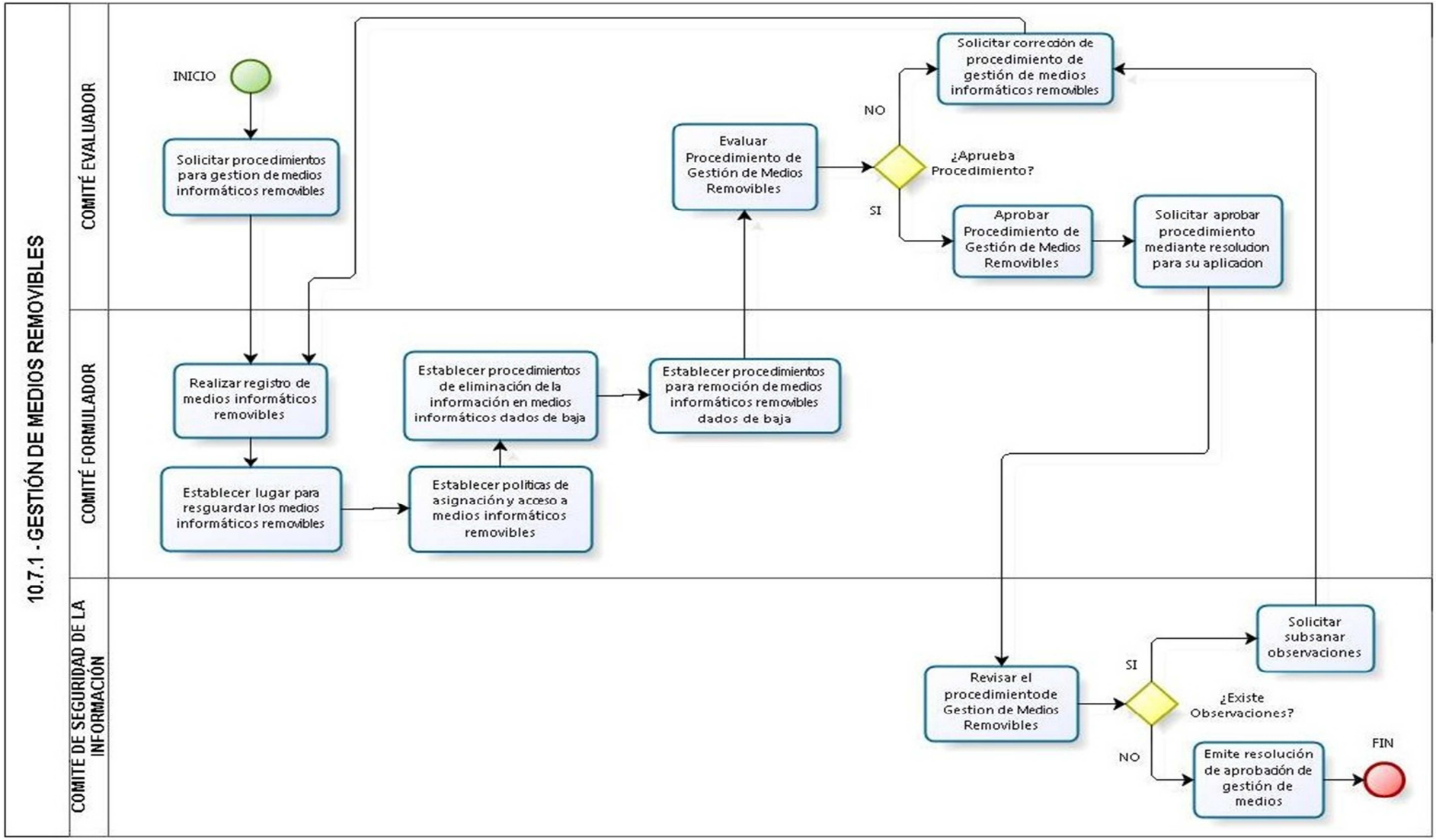
Control:
Debería haber procedimientos para la gestión de los medios informáticos removibles.

Guía de Implementación:
Se deberían borrar los contenidos previos de todo medio reutilizable cuando no se necesiten más, todo medio desechado por la organización debería requerir autorización y se debería guardar registro de dicha remoción para guardar una posta de auditoría, todos los medios se deberían almacenar en un entorno seguro, la información almacenada en el medio debe ser también guardada con el fin de no perder dicha información debido al deterioro del medio, el registro de medios removibles debe ser considerado para limitar la oportunidad de pérdida de datos, los medios removibles deben ser solo activados si existe una razón de negocio para hacerlo.

Diagrama de Actividades N°12 - Gestión de medios removibles (10.7.1)

1. El Comité Evaluador solicita al Comité Formulador procedimientos para la gestión de medios removibles de la UTI.
2. El Comité Formulador realiza un análisis y registra todos los medios informáticos removibles de la UTI, determinando procedimientos para resguardar los medios en un lugar seguro. Luego de ello, establece políticas de asignación y de acceso a los medios informáticos removibles. A continuación establece procedimientos de remoción de los medios informáticos removibles dados de baja, así como también procedimientos para la eliminación de la información contenida en dichos medios.
3. El Comité Evaluador evalúa los procedimientos creados para la gestión de medios removibles, si cumple con lo requerido, solicita al Comité de Seguridad de la Información, aprobar dicho procedimiento mediante resolución, caso contrario, solicita la corrección del procedimiento.
4. Finalmente el Comité de Seguridad de la Información evalúa los procedimientos, si realiza alguna observación, solicita la respectiva corrección, caso contrario emite resolución de aprobación de procedimiento de gestión de medios removibles.

Diagrama de Procesos N°13 - Gestión de medios removibles (10.7.1)



Formulario N°12 - Gestión de medios removibles (10.7.1)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.7.1 – GESTIÓN DE MEDIOS REMOVIBLES**	**Código:** [FRM - 10.7.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **134** de **1**

1 DEL MEDIO REMOVIBLE: **Fecha:** [dd/mm/aaaa]

Nombre del Medio Removible:	[Descripción del Medio Informático Removible]
Tipo de Medio Removible:	[Descripción del Tipo de Medio Informático Removible]
Ubicación:	[Descripción del Lugar de Resguardo del Medio Informático Removible]
Acceso y Asignación de Medios:	[Informe con el cual fue presentado las políticas de acceso y asignación de Medios Removibles]
Eliminación de Información:	[Informe con el cual se presenta los procedimientos de eliminación de información de los medios informáticos removibles dados de baja]
Remoción de Medios:	[Informe con el cual se presenta procedimientos de remoción de medios removibles]

**** Resolución con el cual aprueban el procedimiento de Gestión de Medios Removibles.***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró plan de gestión de medios removibles]	**Nombre:** [Nombre de la persona que revisó el plan de gestión de medios removibles]	**Nombre**: [Nombre de la persona que emitió Resolución de aprobación del plan de gestión de medios removibles]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.6.2. Eliminación de medios.-

Control:
Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales.

Guía de Implementación:
Se deberían establecer procedimientos formales para minimizar el riesgo de filtro de información sensible a personas externas con la eliminación segura de los medios. Los procedimientos para la seguridad de los medios que contienen información sensible deben ser conmensurados con la sensibilidad de dicha información.
Se debería considerar el efecto de acumulación de medios a la hora de eliminar, ya que puede suceder que una gran cantidad de información no clasificada sea más sensible que una pequeña cantidad de información clasificada.

Diagrama de Actividades N°13 - Eliminación de medios (10.7.2)

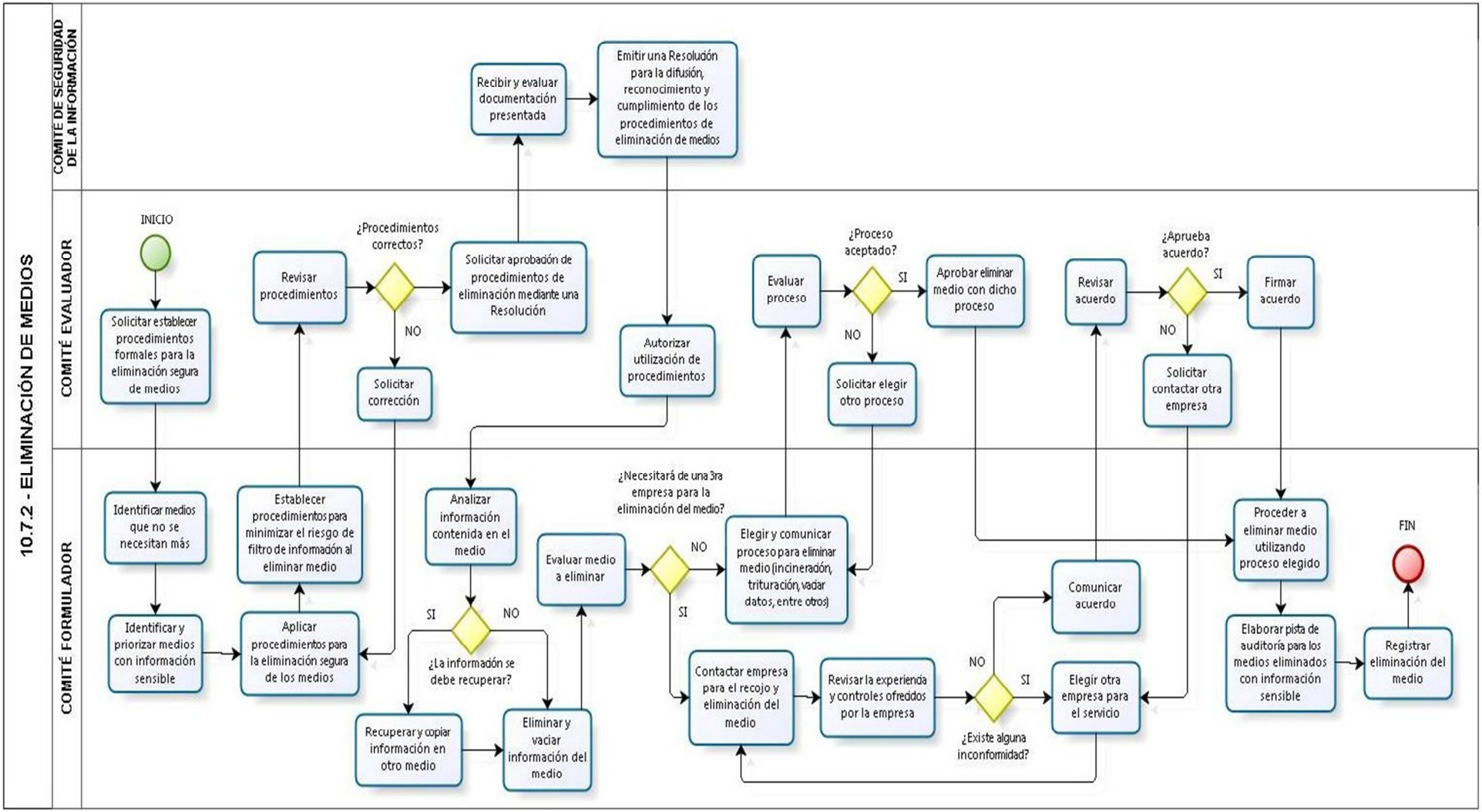
1. El Comité Evaluador solicita que se establezcan procedimientos formales para la eliminación segura de los medios, ésta tarea lo asigna al Comité Formulador.
2. El Comité Formulador identifica medios informáticos que no se necesitan más y prioriza los medios que cuenten con información sensible. Aplica los procedimientos ya determinados en el Control 10.7.1 Gestión de medios removibles para la eliminación segura de los medios y establece procesos para minimizar el riesgo de filtro de información al eliminar el medio.
3. El Comité Evaluador revisa y evalúa los procedimientos, si no le parece que sean correctos, solicita la corrección de los mismos; si los procedimientos le parecen correctos, solicita la aprobación de los mismos mediante Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento de los procedimientos de eliminación de medios.
5. Una vez recibida la Resolución, el Comité Evaluador autoriza la utilización de los procedimientos.
6. El Comité Formulador analiza la información contenida en el medio. Si la información se debe de recuperar, procede a recuperarla y a copiarla en otro medio que no será eliminado, pero si la información ya no es necesaria elimina y vacía la información del medio. Luego de cerciorarse de que el medio a eliminar no cuenta con información, procede a evaluar el medio a eliminar.
7. Si se necesita que una tercera empresa elimine el medio, el Comité Formulador contacta a una empresa ya elegida para el recojo y la eliminación correspondiente. Revisa la experiencia y controles ofrecidos por parte de la empresa y si es que no existen inconvenientes, comunica el acuerdo al Comité Evaluador, pero si es que los hubiera, elige otra empresa para el servicio de eliminación

9. Si es que el medio no necesita de una tercera empresa para ser eliminado, el Comité Formulador elige y comunica al Comité Evaluador el proceso para eliminar el medio, entre ellos está la incineración, trituración, vacío de datos, entre otros que vea convenientes.

10. El Comité Evaluador evalúa el proceso elegido, si no lo aprueba, solicita al Comité Formulador que elija otro proceso para eliminar medio. Caso contrario, comunica y aprueba continuar con la eliminación del medio.

11. Una vez aprobado, el Comité Formulador procede con la eliminación del medio utilizando el proceso elegido, luego de ello elabora una pista de auditoría para los medios eliminados con información sensible. Finalmente registra la eliminación del medio realizada.

Diagrama de Procesos N°14 - Eliminación de medios (10.7.2)



Formulario N°13 - Eliminación de medios (10.7.2)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.7.2 - ELIMINACIÓN DE MEDIOS**	**Código:** [FRM - 10.7.2 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **139** de **1**

1 DE LA ELIMINACIÓN DEL MEDIO:

Fecha: [dd/mm/aaaa]

Medio a eliminar: [Indicar el medio a eliminar]

Descripción del medio: [Indicar una breve descripción del medio a eliminar]

Información contenida en el medio: [Indicar una breve descripción de la información contenida en el medio] _____

Información recuperable: [Indicar si es que la información contenida en el medio será recuperada]

- SI [ ] NO [ ]

Fecha de recuperación: [Indicar fecha de recuperación de la información contenida en el medio]

Nueva ubicación de la información recuperada: [Indicar el lugar físico o lógico en el que se recuperó la información contenida en el medio a eliminar]

Proceso elegido para la eliminación del medio: [Indicar el proceso elegido para eliminar el medio una vez recuperada la información que contenía]

- Incineración [ ] Trituración [ ] Vacío de Datos [ ]
  Tercerización [ ] Otros [ ] _____

Descripción del proceso de eliminación del medio: [Indicar una breve descripción del proceso elegido para eliminar el medio]

Fecha de eliminación del medio: [dd/mm/aaaa]

**** Número de Resolución de aprobación para el cumplimiento de los procesos de eliminación del medio***

2 DE LA ELABORACIÓN: **Personal del Comité Formulador**	3 DE LA REVISIÓN: **Personal del Comité Evaluador**	4 DE LA APROBACIÓN: **Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona encargada de la eliminación del medio]	**Nombre:** [Nombre de la persona que revisó los procesos de eliminación de medios]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento de los procesos de eliminación de medios]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.6.3. Procedimientos de manipulación de la información.-

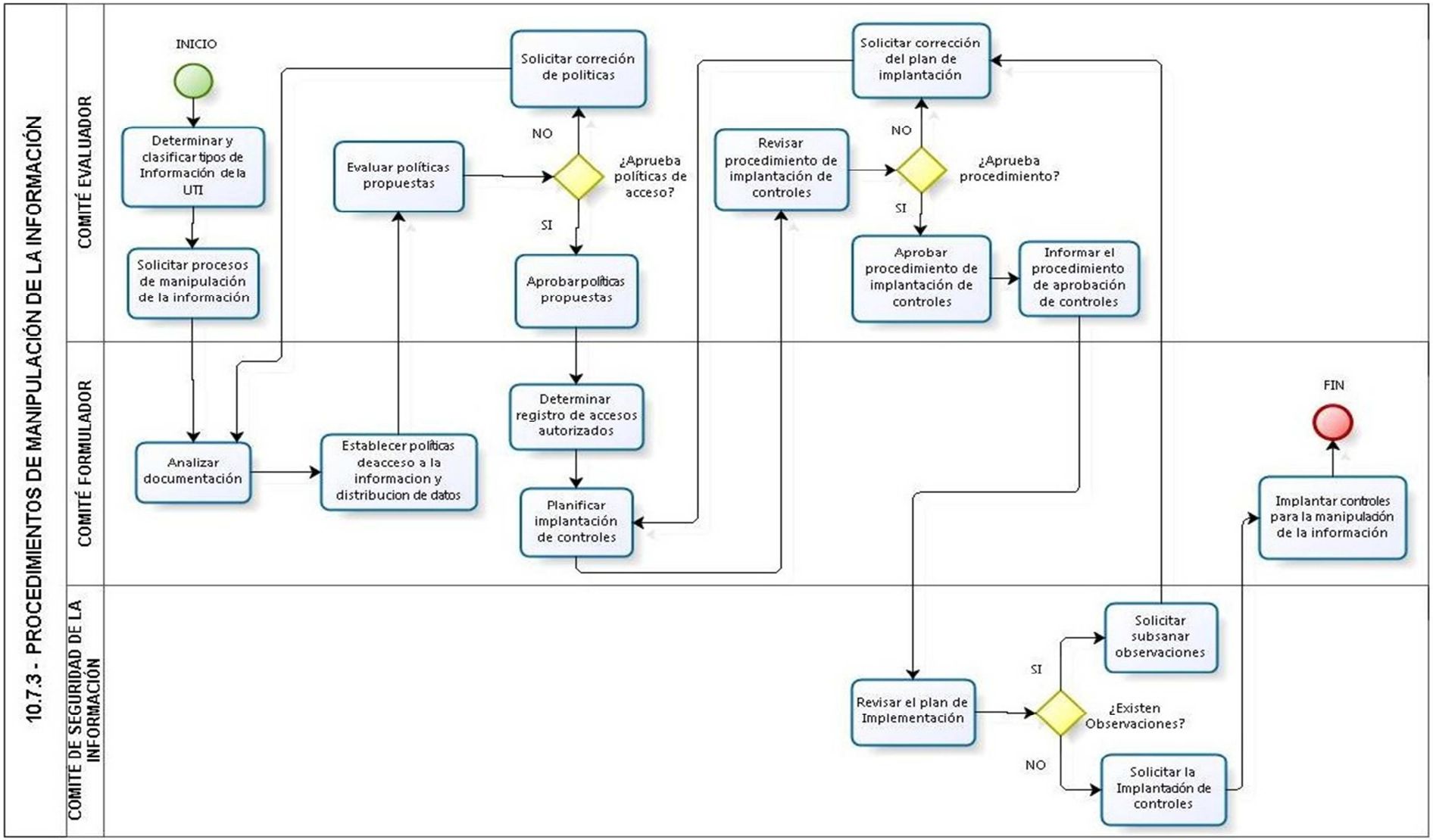
Control:
Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados.

Guía de Implementación:
Se deberían establecer procedimientos de manipulación y almacenamiento de la información de forma coherente con su clasificación.

Diagrama de Actividades N°14 - Procedimientos de manipulación de la información (10.7.3)

1. El Comité Evaluador determina los tipos de información de la Unidad de Tecnologías de la Información y los clasifica por tipo, luego de ello solicita al Comité Formulador procesos de manipulación de información.
2. El Comité Formulador realiza un análisis de la documentación establecida y establece políticas de acceso a dicha información, políticas de distribución de controles y políticas de distribución de datos para presentar al Comité Evaluador.
3. El Comité Evaluador procede a evaluar políticas propuestas, si no cumplen el nivel de seguridad adecuado, solicita la corrección de las mismas, caso contrario, las aprueba y da el visto bueno para su aplicación.
4. Una vez que las políticas han sido aprobadas, el Comité Formulador determina un registro de accesos autorizados, luego de ello desarrolla un plan de implantación de controles.
5. El Comité Evaluador revisa el procedimiento de implantación de controles, si cumple lo establecido, solicita a Comité de Seguridad de la Información la aprobación del plan de implantación de controles.
6. El Comité de Seguridad de Información revisa el plan de implantación, si realiza alguna observación, solicita las correcciones respectivas, caso contrario da el visto bueno y solicita la implantación de controles.
7. Una vez emitida la aprobación de plan de implantación, el Comité Formulador procede a implantar los controles de acuerdo al plan aprobado.

Diagrama de Procesos N°15 - Procedimientos de manipulación de la información (10.7.3)



Formulario N°14 - Procedimientos de manipulación de la información (10.7.3)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.7.3 – PROCEDIMIENTO DE MANIPULACIÓN DE INFORMACIÓN**	**Código:** [FRM - 10.7.3 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **143** de **1**

1 DE LA INFORMACIÓN: **Fecha:** [dd/mm/aaaa]

Tipo de Información: [Descripción del Medio Informático Removible]

Clasificación: [Descripción del Tipo de Medio Informático Removible]

DEL PROCEDIMIENTO:

Acceso a la Información: [Informe con el cual se presenta las Políticas de Acceso a la Información]

Distribución de Datos: [Informe con el cual se presenta las políticas de distribución de datos]

Registro de Accesos Autorizados: [Ruta donde se guarda el registro de acceso autorizados a la información]

Plan de Implantación de Controles: [Informe con el cual se presenta el plan de Implantación de controles]

**** Resolución con el cual aprueban el procedimiento de Gestión de Medios Removibles.***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró el procedimiento de manipulación de información]	**Nombre:** [Nombre de la persona que revisó el procedimiento de manipulación de información]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del procedimiento de manipulación de información]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.6.4. Seguridad de la documentación de sistemas.-

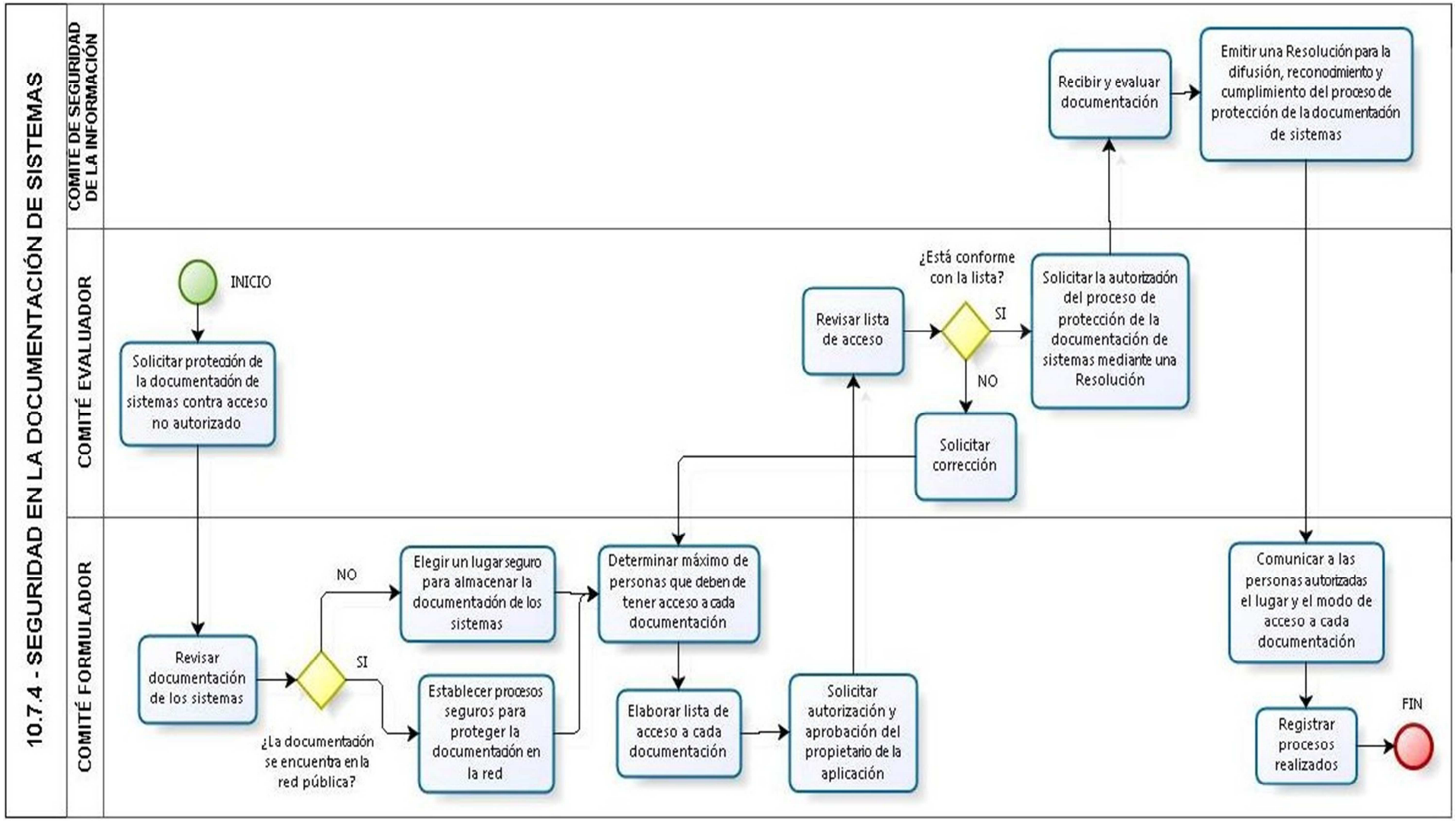
Control:
Los documentos de sistemas deben ser protegidos contra accesos no autorizados.

Guía de Implementación:
La documentación de sistemas se debería almacenar con seguridad, la lista de acceso a dicha documentación se debería limitar al máximo y ser autorizada por el propietario de la aplicación, si ésta documentación es mantenida en una red pública, o suministrada vía una red pública, se debería proteger adecuadamente.

Diagrama de Actividades N°15 - Seguridad de la documentación de sistemas (10.7.4)

1. El Comité Evaluador solicita que la documentación de los sistemas sea protegido contra acceso no autorizado, asigna esta tarea al Comité Formulador.
2. El Comité Formulador revisa toda la documentación existente de los sistemas incluyendo la ubicación en la que se encuentran: si es que está ubicada dentro de la red púbica, elige un directorio seguro y establece procesos para proteger la documentación en la red; si es que no está en la red, elige un lugar físico seguro para almacenar dicha documentación. Una vez ubicada la documentación, determina un número máximo de personas que deben de tener acceso a ella y elabora una lista con sus nombres para cada documentación.
3. El Comité Evaluador revisa lista de acceso, si es que no está conforme con ella, solicita la corrección; si es que está conforme, solicita la autorización del proceso de protección de la documentación de sistemas mediante una Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento del proceso de protección de la documentación de sistemas.
5. Una vez que la lista de acceso ha sido aprobada, el Comité Formulador comunica a cada una de las personas autorizadas cual es la ubicación y el modo de acceso a cada documentación. Finalmente registra los procesos realizados y concluye con el proceso de protección de la documentación de sistemas.

Diagrama de Procesos N°16 - Seguridad de la documentación de sistemas (10.7.4)



Formulario N°15 - Seguridad de la documentación de sistemas (10.7.4)

sunarp Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**FORMULARIO 10.7.4 - SEGURIDAD EN LA DOCUMENTACIÓN DE LOS SISTEMAS**	**Código:** [FRM - 10.7.4 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **147** de **1**

1 DEL SISTEMA:

Fecha: [dd/mm/aaaa]

Sistema a documentar: [Indicar el nombre del sistema que será documentado]
Versión del sistema: [Indicar la versión del sistema a documentar]
Descripción del sistema: [Indicar una breve descripción del sistema a documentar]
Propietario del sistema: [Indicar el nombre del propietario de la aplicación/sistema si lo hubiera]

DE LA DOCUMENTACIÓN:

Código de documentación: [Indicar el código o identificador de la documentación del sistema]
Versión de documentación: [Indicar la versión de la documentación del sistema]
Elaborada por: [Indicar el nombre de la persona que elaboró la documentación del sistema]
Fecha de documentación: [dd/mm/aaaa]
Ubicación lógica elegida: [Indicar ruta lógica de la red en donde se procedió a guardar documentación]
Ubicación física elegida: [Indicar el lugar físico en donde se procedió a asegurar la documentación]
Seguridad establecida: [Describir los procesos de seguridad establecidos para proteger la documentación del sistema en cada ubicación] _____
N°máximo de personas con acceso autorizado: [Indicar el número máximo acordado de usuarios que deben de tener acceso a la documentación]
Usuarios con acceso autorizado: [Listar usuarios que cuenten con de acceso autorizado a la documentación]

- Usuario 1 - Perfil de Acceso

**** Núm. de Resolución de aprobación para el cumplimiento del proceso de protección de documentación de los sistemas***

2 DE LA ELABORACIÓN:

Personal del Comité Formulador

Fecha: [dd/mm/aaaa]

Nombre: [Nombre de la persona encargada de elaborar el proceso de protección de la documentación de los sistemas]

Cargo: [Indicar el cargo que ocupa en la institución]

_____
Firma y Sello

3 DE LA REVISIÓN:

Personal del Comité Evaluador

Fecha: [dd/mm/aaaa]

Nombre: [Nombre de la persona que revisó el proceso de protección de la documentación de los sistemas]

Cargo: [Indicar el cargo que ocupa en la institución]

_____
Firma y Sello

4 DE LA APROBACIÓN:

Personal del Comité de Seguridad de la Información

Fecha: [dd/mm/aaaa]

Nombre: [Nombre de la persona que emitió Resolución de aprobación para el cumplimiento del proceso de protección de la documentación de los sistemas]

Cargo: [Indicar el cargo que ocupa en la institución]

_____
Firma y Sello

4.2.2.7. Intercambio de información.-

Objetivo:
Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.
Se deberían realizar los intercambios sobre la base de acuerdos formales. Se deberían controlar los intercambios de información y software entre organizaciones, que deberían cumplir con toda la legislación correspondiente.
Se deberían establecer procedimientos y normas para proteger la información de los medios en tránsito.

4.2.2.7.1. Políticas y procedimientos para el intercambio de información y software.-

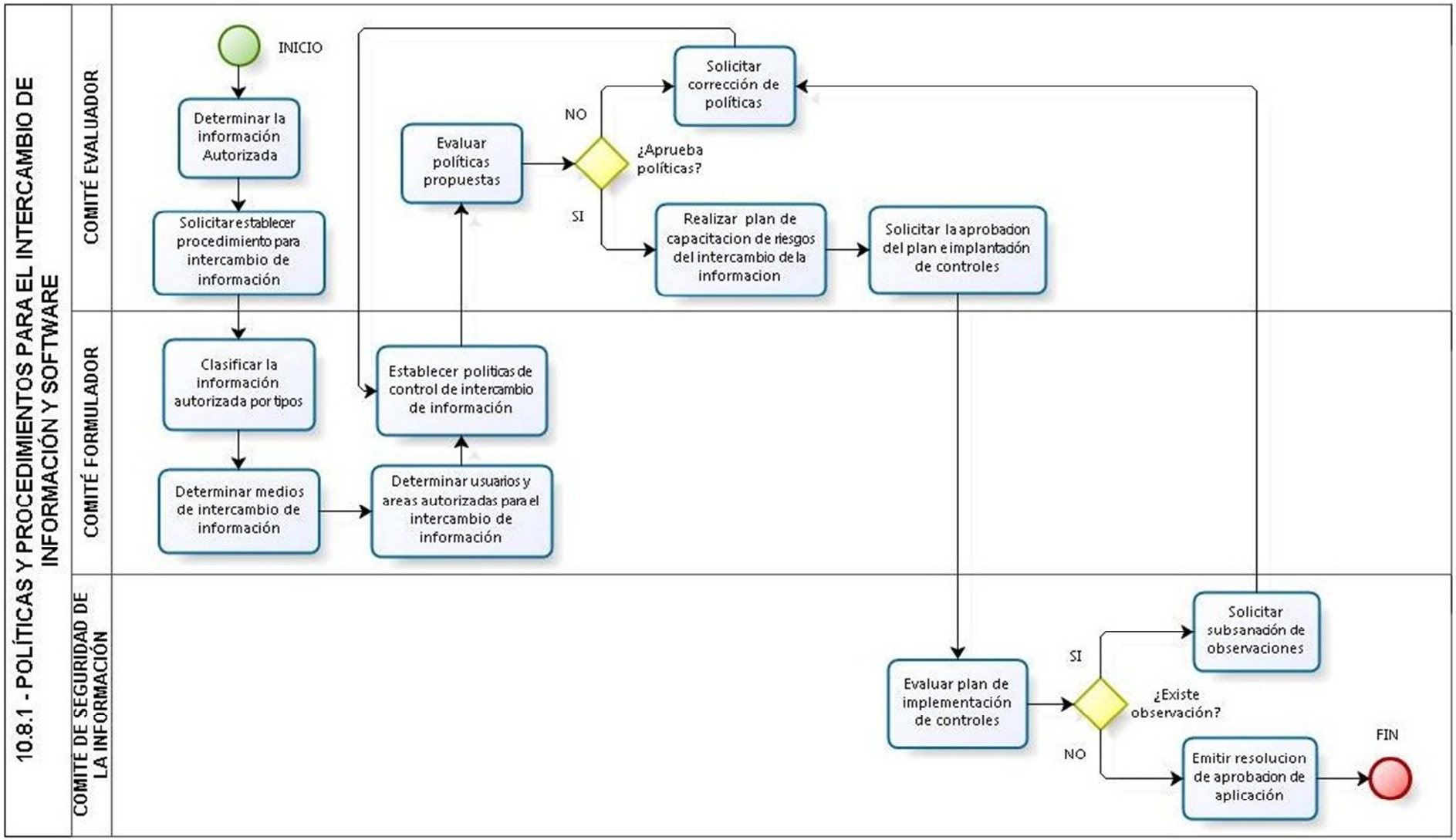
Control:
Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación.

Guía de Implementación:
Los procedimientos y controles a ser seguidos cuando se utilice instalaciones electrónicas de comunicación para el intercambio de información deben considerar: los procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta y destrucción, los procedimientos para la detección y protección contra código malicioso que puede ser transmitido a través del uso de comunicación electrónica, los procedimientos para proteger información electrónica sensible que está en forma de archivo adjunto, entre otros.

Diagrama de Actividades N°16 - Políticas y procedimientos para el intercambio de información y software (10.8.1)

1. El Comité Evaluador determina que información de la Unidad de Tecnologías de la Información es permitida para poder realizar un intercambio, y solicita al Comité Formulador establecer procedimiento para intercambio de información.
2. El Comité Formulador clasifica la información por tipos determinando límites de tamaño para el intercambio de información, luego determina medios, usuarios y áreas autorizadas para el intercambio de información revisando sus respectivos Formato de Accesos, terminado ello realiza políticas para el control del intercambio de la información y lo presenta al Comité Evaluador para su revisión y aprobación.
3. El Comité Evaluador evalúa las políticas propuestas, si no las aprueba, solicita su corrección, caso contrario, solicita la aprobación de las políticas de control al Comité de Seguridad de la Información, adicionando un plan de charlas al personal sobre los riesgos que existen en el intercambio de información.
4. El Comité de Seguridad de la Información revisa el procedimiento, si realiza una observación, solicita correcciones, caso contrario emite la resolución de aprobación respectiva.
5. Una vez recibida la resolución, el Comité Evaluador solicita al Comité Formulador el cumplimiento de procedimiento de intercambio de información.

Diagrama de Procesos N°17 - Políticas y procedimientos para el intercambio de información y software (10.8.1)



Formulario N°16 - Políticas y procedimientos para el intercambio de información y software (10.8.1)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.8.1 – POLÍTICAS Y PROCEDIMIENTOS PARA EL INTERCAMBIO DE LA INFORMACIÓN**	**Código:** [FRM - 10.8.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **151** de **1**

1 DEL PROCEDIMIENTO DE INTERCAMBIO: **Fecha:** [dd/mm/aaaa]

Información: [Descripción de la información, para el intercambio de información] *
Tipo de Información: [Describir el tipo de Información]

**** Informe con el cual determinan la información autorizada para el intercambio***

Medios de Intercambio: [Determinar el Tipo de Intercambio de Información]
- ❖ [ ] Red [ ] Correo [ ] Físico [ ] Courier
- ❖ [ ] Otro _____

Nombre de usuario: [Nombre del usuario responsable del intercambio de información]
Unidad : [Dependencia del usuario responsable del intercambio de información]
Cargo: [Cargo del usuario responsable]
Políticas de Control : [Informe con el cual se presenta el plan de Implantación de controles]

**** Resolución con el cual aprueban el procedimiento de Gestión de Medios Removibles.***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró plan de políticas y procedimientos para el intercambio de información]	**Nombre:** [Nombre de la persona que revisó el plan de políticas y procedimientos para el intercambio de información]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación de políticas y procedimientos para el intercambio de información]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.7.2. Medios físicos en tránsito.-

Control:
Los medios conteniendo información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

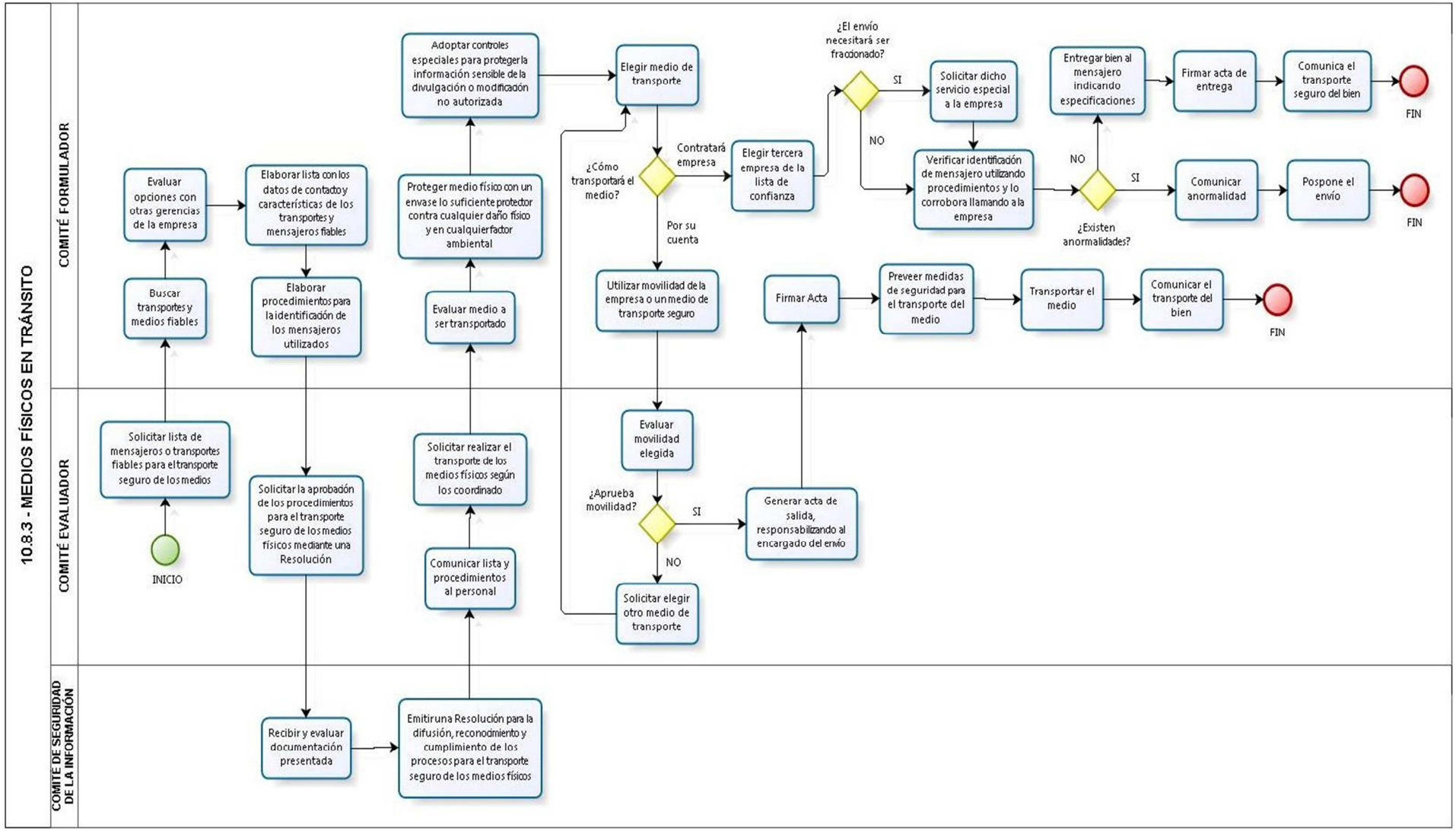
Guía de Implementación:
La información puede ser vulnerable a accesos no autorizados, a mal uso o a corrupción durante su transporte físico. Se deberían aplicar los siguientes controles y medidas para salvaguardar los medios informáticos transportados entre sedes: deberían usarse transportes o mensajeros fiables, debería convenirse entre las gerencias una lista de mensajeros autorizados, se debería realizar un procedimiento para comprobar la identificación de los mensajeros utilizados, el envase debería ser suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito, deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizada, entre otros.

Diagrama de Actividades N°17 - Medios físicos en tránsito (10.8.3)

1. El Comité Evaluador solicita que se cree una lista de mensajeros o empresa de transportes fiables para el transporte seguro de los medios, dicha tarea se la asigna al Comité Formulador.
2. El Comité Formulador busca transportes y medios fiables evaluando y comparando dichas opciones con otras oficinas y gerencias de la Sunarp. Luego de ello, elabora una lista con los datos de contacto y características principales de las empresas de transporte y mensajeros fiables, además elabora procedimientos para la identificación de los mensajeros utilizados.
3. El Comité Evaluador solicita al Comité de Seguridad de la Información, la aprobación de los procedimientos para el transporte seguro de los medios físicos mediante una Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento de los procesos para el transporte seguro de los medios físicos.
5. Una vez recibida a Resolución, el Comité Evaluador comunica la lista de empresas y los procedimientos propuestos a todo el personal, luego de ellos solicita que se utilicen los procedimientos coordinados para cada transporte de medios físicos que se realice.
6. Cada vez que haya un medio físico para transportar, el Comité Formulador evalúa dicho medio, lo protege con un envase lo suficiente protector contra daños físicos y factores ambientales y adopta controles especiales para proteger la información sensible de la divulgación o modificación no autorizada. Una vez realizado ello, procede a elegir el medio de transporte a utilizar, si es que lo enviará por su cuenta, utilizará movilidad de la empresa o un transporte seguro a su cargo.

7. El Comité Evaluador evalúa movilidad elegida, si es no lo aprueba, solicita que se elija otro medio de transporte, y en el caso de que lo aprueba, genera acta de salida responsabilizando el medio al encargado del envío (personal del Comité Formulador).
8. Una vez que se aprobó el envío del medio, el Comité Formulador procede a firmar acta y a prever medidas de seguridad para el transporte seguro del medio. Finalmente transporta el medio y comunica lo realizado al Comité Evaluador
9. En el caso en el que el Comité Formulador elija contratar una empresa de confianza para el envío del medio, procede a evaluar si el envío necesitará ser fraccionado. Si es que si lo necesita, solicitará servicio especial a la empresa, y si es que no lo necesita, continúa con la verificación de la identificación del mensajero enviado utilizando los procedimientos establecidos anteriormente y lo corrobora llamando a la empresa contratada. Si es que encuentra alguna anormalidad con la empresa de transporte antes de realizar el envío, comunica inmediatamente la anormalidad y pospone el envío del medio físico.
10. Finalmente, en el caso de que no existan anormalidades, el Comité Formulador entrega bien al mensajero indicando especificaciones, firman acta de entrega y comunica el transporte seguro del bien.

Diagrama de Procesos N°18 - Medios físicos en tránsito (10.8.3)



Formulario N°17 - Medios físicos en tránsito (10.8.3)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.8.3 – MEDIOS FÍSICOS EN TRÁNSITO**	**Código:** [FRM - 10.8.3 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **156** de **1**

1 DEL MEDIO FÍSICO: **Fecha:** [dd/mm/aaaa]

Medio físico transportado:	[Indicar el medio físico que se ha transportado]
Descripción del medio físico:	[Describir brevemente el medio físico que se ha transportado]

DEL TRANSPORTE DEL MEDIO:

Encargado del transporte del medio:	[Indicar el nombre de la persona encargada de realizar el transporte del medio físico]
Origen / Fecha de envío:	[Indicar el lugar de origen del envío] / [dd/mm/aaaa]
Destino / Fecha de llegada:	[Indicar el lugar de destino del envío] / [dd/mm/aaaa]
Medio de transporte elegido:	[Especificar el transporte elegido para el medio físico]
Envase utilizado para transporte:	[Indicar la protección que fue utilizada para el transporte seguro del medio físico]
Acta de entrega y/o envío del medio:	[Indicar el N° de acta con el que se hace entrega y/o envío del medio a ser transportado]
Empresa encargada del transporte del medio:	[Indicar los datos de la empresa contratada para realizar el transporte] ✓ Nombre de la empresa ✓ Encargado de la empresa ✓ Teléfonos y correo electrónico de contacto, entre otros.

**** Número de Resolución de aprobación de los procedimientos a realizar para el transporte seguro de los medios físicos***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró los procedimientos a realizar para el transporte seguro de los medios físicos]	**Nombre:** [Nombre de la persona que q revisa los procedimientos a realizar para el transporte seguro de los medios físicos]	**Nombre:** [Nombre de la persona que emitió la Resolución de Aprobación de los procedimientos a realizar para el transporte seguro de los medios físicos]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.7.3. Sistemas de información de negocios.-

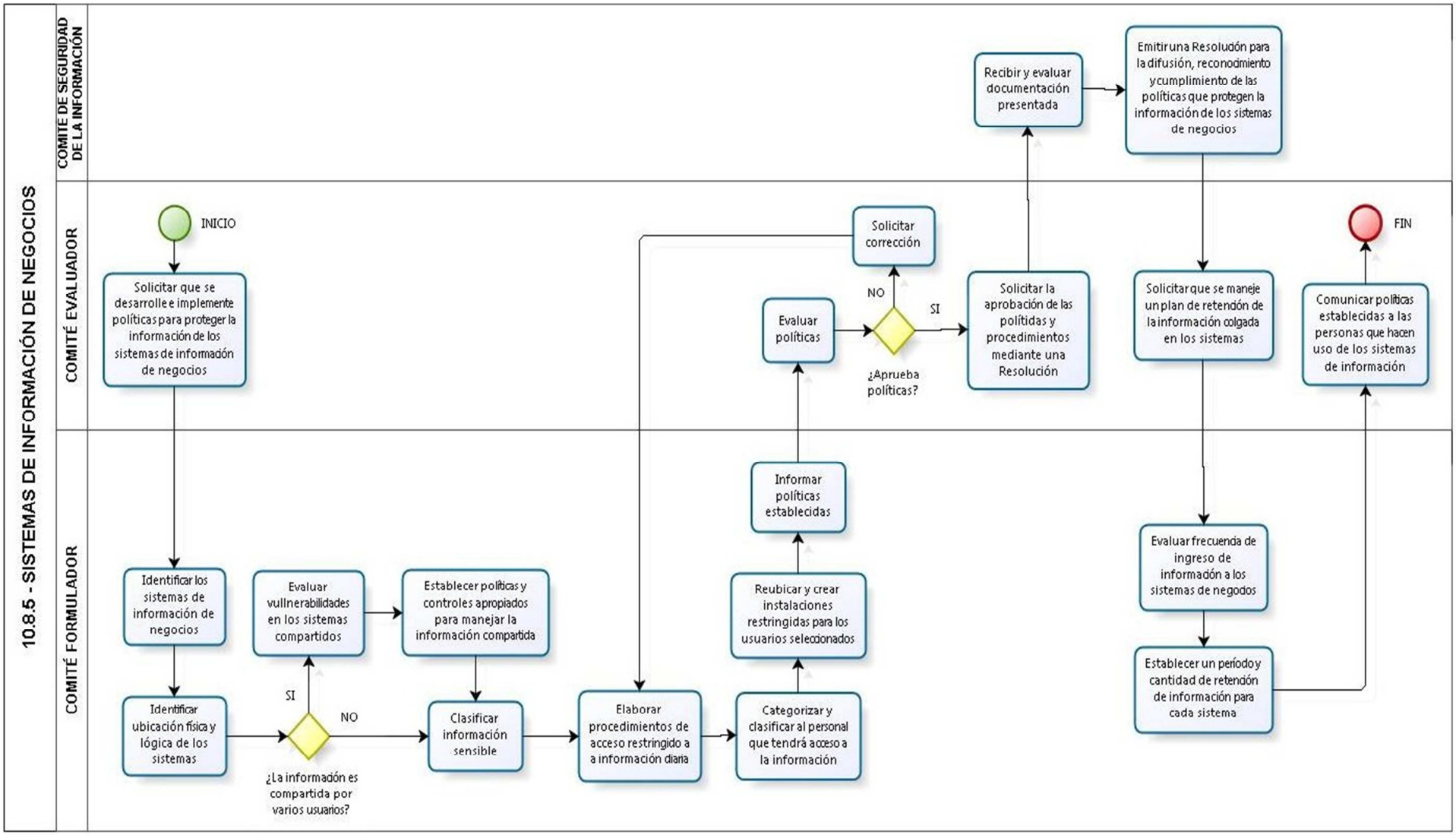
Control:
Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios.

Guía de Implementación:
Las consideraciones dadas a la seguridad e implicaciones de seguridad de interconectar dichas instalaciones, debe incluir: vulnerabilidades conocidas en los sistemas de administración y contabilidad donde la información es compartida por diferentes partes de la organización, vulnerabilidades de información en sistema de comunicación de negocios, políticas y controles apropiados para manejar información compartida, excluir categorías de información de negocios sensible y clasificar documentos si los sistemas no proveen un nivel apropiado de protección, acceso restringido a la información diaria relacionado con los individuos selectos, entre otros.

Diagrama de Actividades N°18 - Sistemas de información de negocios (10.8.5)

1. El Comité Evaluador solicita que se desarrolle e implementen políticas para proteger la información de los sistemas de información de negocios, dicha tarea lo asigna al Comité Formulador.
2. El Comité Formulador identifica todos los sistemas de información de negocios incluyendo su ubicación lógica y evalúa si la información contenida en los sistemas está compartida por varios usuarios. Si es que lo está, evalúa las vulnerabilidades que la información en los sistemas compartidos presenta y establece políticas/controles apropiados para manejarla. Si no está compartida, procede a clasificar la información sensible y elabora procedimientos de acceso restringido a la información de los sistemas que se usa a diario. Terminado ello, categoriza y clasifica al personal que tendrá acceso a la información, reubica y crea las instalaciones restringidas para los usuarios seleccionados anteriormente. Informa sobre el avance realizado.
3. El Comité Evaluador revisa y evalúa políticas propuestas por el Comité Formulador, si es que no le parecen adecuadas, solicita su corrección, en cambio si es que le parecen que son correctas, solicita al Comité de Seguridad de la Información, la aprobación de las políticas y procedimientos mediante una Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento de las políticas que protegen la información de los sistemas de negocio.
5. Una vez recibida la Resolución, el Comité Evaluador solicita que se maneje un plan de retención de información almacenada en los sistemas.
6. Para ello, el Comité Formulador evalúa la frecuencia de uso y de ingreso de información a los sistemas de negocios, para luego establecer un período y cantidad de retención de información para cada sistema. A su término, informa lo avanzado al Comité Evaluador.
7. Por último, el Comité Evaluador recibe informe y comunica las políticas establecidas a las personas que hacen uso de los sistemas de información de negocios.

Diagrama de Procesos N°19 - Sistemas de información de negocios (10.8.5)



Formulario N°18 - Sistemas de información de negocios (10.8.5)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.8.5 – SISTEMAS DE INFORMACIÓN DE NEGOCIOS**	**Código:** [FRM - 10.8.5 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **160** de **1**

1 DEL SISTEMA DE INFORMACIÓN DE NEGOCIOS:

Fecha: [dd/mm/aaaa]

Nombre del Sistema: [Indicar el nombre del Sistema de Información de Negocios]
Descripción del Sistema: [Describir brevemente el Sistema de Información de Negocios]
Ubicación lógica del Sistema: [Indicar la ubicación lógica en donde se encuentra el Sistema]

DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA:

Descripción de la Información: [Breve descripción de la información contenida en el sistema]
Información compartida: [¿La información es compartida por varios usuarios?] [SI] [NO]
Vulnerabilidades: [De ser la información compartida, listar las vulnerabilidades encontradas por dicho atributo, caso contrario, no aplica este campo]
Información sensible: [¿La información es de carácter sensible?] [SI] [NO]
Procesos y políticas de acceso restringido: [Listar los procesos creados para proteger y brindar acceso restringido a la información del sistema]
- ✓ Proceso de acceso restringido N°1
- ✓ Proceso de acceso restringido N°2

Personal con acceso: [Categoriza y lista a las personas que contarán con acceso a la información]
Frecuencia de ingreso: [Indicar la frecuencia de ingreso de información al sistema]
Cantidad de retención: [Indicar la cantidad de retención de información del sistema]

**** Núm. de Resolución de aprobación de procedimientos de seguridad para los Sistemas de Información de Negocios.***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró los procedimientos de seguridad para la información contenida en los sistemas de información de negocios]	**Nombre:** [Nombre de la persona que revisó los procedimientos de seguridad para la información contenida en los sistemas de información de negocios]	**Nombre:** [Nombre de la persona que emitió la Resolución de Aprobación de los procedimientos de seguridad para la información contenida en los sistemas de información de negocios]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.8. Monitoreo.-

Objetivo:
Detectar las actividades de procesamiento de información no autorizadas.
Los sistemas deben ser monitoreados y los eventos de la seguridad de la información deber ser grabadas. El registro de los operadores y el registro de averías deben ser usados para asegurar que los problemas del sistema de información sean identificados.
Una organización debe cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades.
El monitoreo del sistema debe ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad de un acceso a un modelo de política

4.2.2.8.1. Registro de la auditoría.-

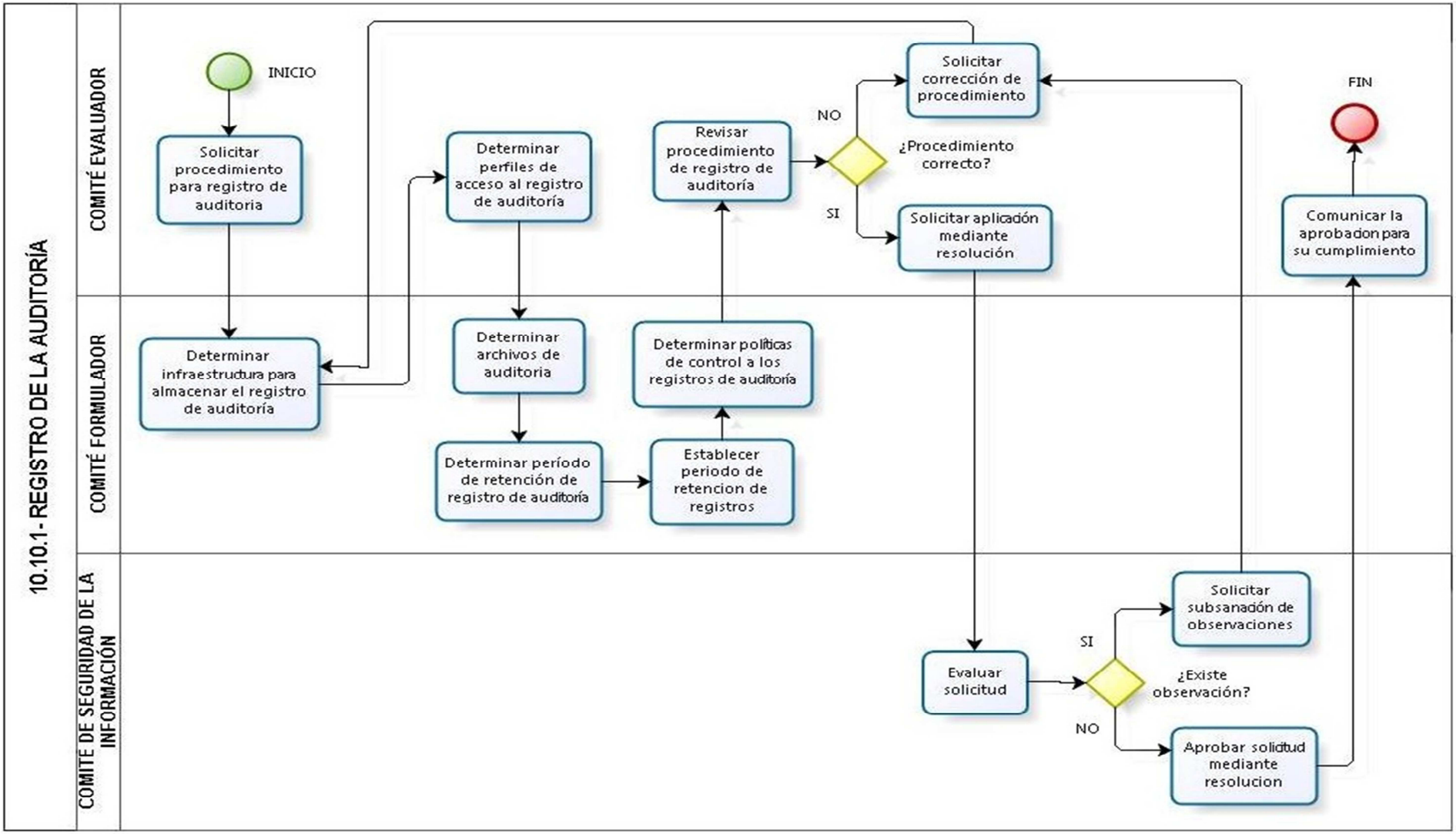
Control:
Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de la información deben ser producidos y guardados para un periodo acordados con el fin de que asistan investigaciones futuras y en el monitoreo de los controles de acceso.

Guía de Implementación:
Los registros de auditoría deben incluir, cuando sea relevante: identificación de usuarios, fecha y hora de conexión y desconexión, identidad del terminal o locación si es posible, registro de éxito y fracaso de los intentos de acceso al sistema, registro de éxito o fracaso de datos y de otros intentos de acceso a recursos, cambios en la configuración del sistema, uso de privilegios, uso de las instalaciones y aplicaciones del sistema, archivos accesados y el tipo de acceso, direcciones de red y protocolos, las alarmas realizadas por el sistema de control de accesos, activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusos

Diagrama de Actividades N°19 - Registro de la auditoría (10.10.1)

1. El Comité Evaluador solicita al Comité Formulador, crear un procedimiento para el registro de auditoría.
2. El Comité Formulador determina la infraestructura para almacenar los registros de auditoria.
3. Una vez establecida la infraestructura, el Comité Evaluador determina los perfiles de acceso a los registros de auditoría.
4. El Comité Formulador determina que tipos de archivos contendrá el registro de auditoría, para luego establecer el periodo de retención de los registros de auditoría, luego de ello determinan políticas de control a los registros de auditoría, a continuación envían el procedimiento del registro de auditoría para su revisión.
5. El Comité Evaluador revisa y evalúa procedimiento de registro de auditoría, si el procedimiento no es el adecuado, solicita la corrección, caso contrario, lo aprueba y solicita su aplicación mediante resolución por parte del Comité de Seguridad de la Información.
6. El Comité de Seguridad de la Información evalúa el procedimiento, si realiza alguna observación, solicita levantar observaciones, caso contrario emite resolución para su aprobación.
7. El Comité Evaluador recibe la resolución de aprobación y lo comunica al Comité Formulador para su cumplimiento.

Diagrama de Procesos N°20 - Registro de la auditoría (10.10.1)



Formulario N°19 - Registro de la auditoría (10.10.1)

sunarp Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.10.1 – REGISTRO DE AUDITORIA**	**Código:** [FRM - 10.10.1 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **164** de **1**

1 DEL PROCESO DE REGISTRO DE AUDITORIA: **Fecha:** [dd/mm/aaaa]

Infraestructura: [Descripción de la infraestructura donde se almacena el archivo de auditoría]

PERFILES DE ACCESO:

Nombre: [Nombre de la persona que accede al registro de auditoría]

Cargo: [Cargo del personal que accede al registro de auditoría]

Nivel de Acceso: [Descripción del nivel de acceso al registro de auditoría]

ARCHIVOS DE AUDITORIA:

Log de Auditoría: [Descripción de donde se guarda el log de auditoría]

Tipo: [Descripción del Tipo de Archivo para auditoría]

Tiempo de Retención: [Determinar el tiempo de retención de los archivos de auditoría]

Políticas de Control: [Informe con el cual se presenta el plan de Implantación de controles]

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró registro de auditoría]	**Nombre:** [Nombre de la persona que revisó el registro de auditoría]	**Nombre:** [Nombre de la persona que emitió la Resolución de aprobación del registro de auditoría]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.8.2. Monitoreando el uso del sistema.-

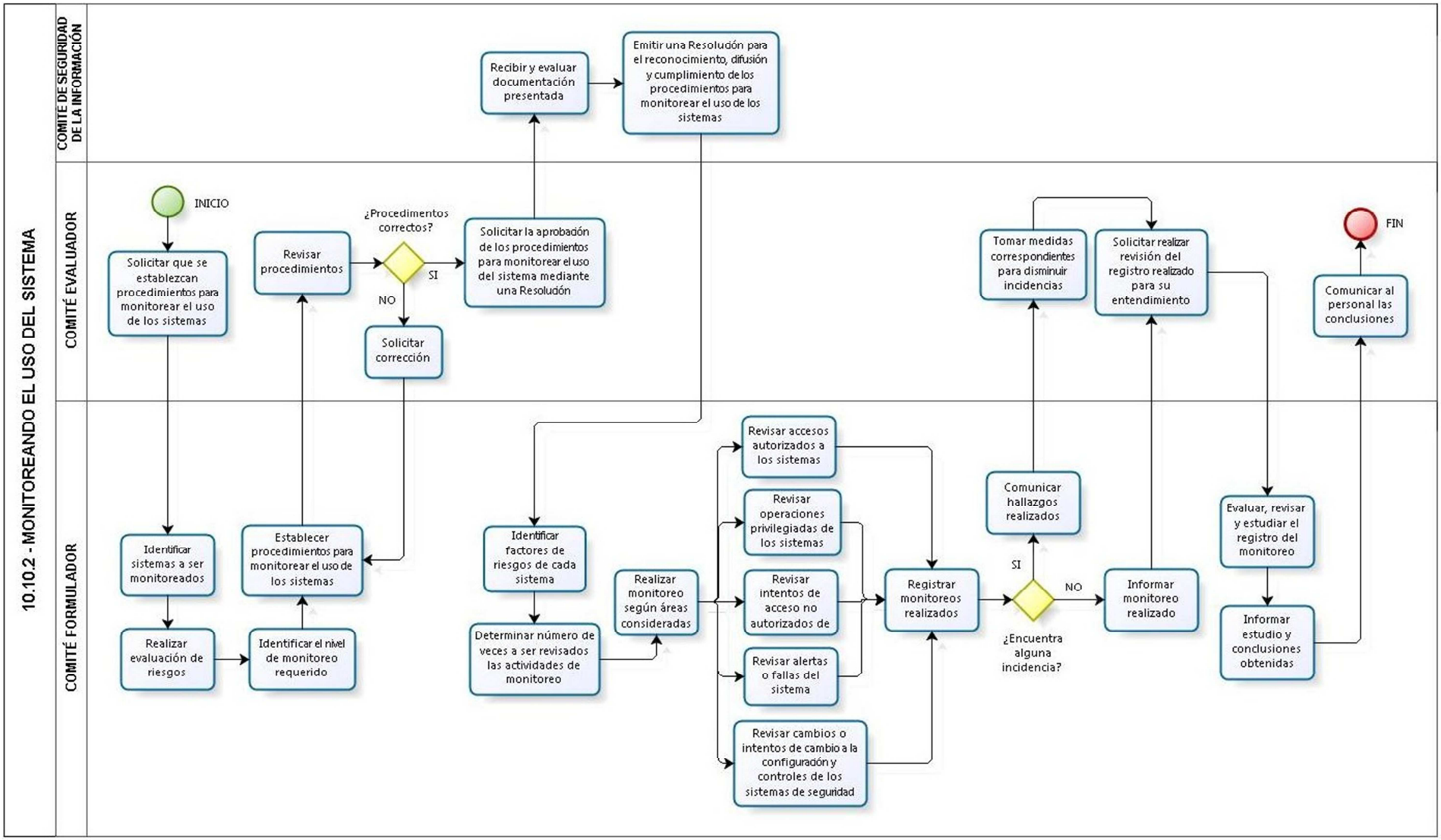
Control:
Los procedimientos para el uso del monitoreo de la instalación de procesamiento de información deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente.

Guía de Implementación:
El nivel de monitoreo requerido para las instalaciones individuales debe ser determinado por una evaluación de riesgos. Una organización debe cumplir con todos los requerimientos legales aplicables a sus actividades de monitoreo. Las áreas que deben ser consideradas incluyen: accesos no autorizados, todas las operaciones privilegiadas, intentos de accesos no autorizados, alertas o fallas del sistema, cambios o intentos de cambio a la configuración y controles de los sistemas de seguridad.
El número de veces que deberían ser revisados las actividades de monitoreo debe depender de los riesgos implicados.

Diagrama de Actividades N°20 - Monitoreando el uso del sistema (10.10.2)

1. El Comité Evaluador solicita que se establezcan procedimientos para monitorear el uso de los sistemas, esta tarea lo asigna al Comité Formulador.
2. El Comité Formulador identifica los sistemas que van a ser monitoreados y realiza la correspondiente evaluación de riesgos. De esta forma identifica el nivel de monitoreo requerido para cada sistema y establece procedimientos para realizar el monitoreo del uso de los sistemas.
3. El Comité Evaluador revisa los procedimientos propuestos, si es que no le parecen adecuados, solicita la corrección de los mismos, por el contrario si es que le parecen que los procedimientos son correctos, solicita al Comité de Seguridad de la Información, la aprobación de los mismos mediante una Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa documentación presentada, luego de ello emite una Resolución para el reconocimiento, difusión y cumplimiento de los procedimientos para monitorear el uso de los sistemas.
5. Una vez que los procedimientos de monitoreo han sido aprobados, el Comité Formulador identifica los factores de riesgo de cada sistema y determina el número de veces a ser revisados las actividades de monitoreo. Terminado ello, procede con realizar el monitoreo planificado a cada sistema según las siguientes áreas consideradas: revisión de accesos autorizados, revisión de las operaciones privilegiadas de los sistemas, revisión de intentos de acceso no autorizados, revisión de alertas o fallas de los sistemas ocurridas en algún momento y revisión de los cambios y/o intentos de cambio a la configuración y controles de los sistemas de seguridad. Acopla todas las revisiones y procede a registrar los monitoreos realizados. Si es que en el transcurso del monitoreo no encontró problemas, lo informa y comunica al Comité Evaluador, pero si es que encontró alguna incidencia, comunica los hallazgos.
6. El Comité Evaluador evalúa hallazgos y toma las medidas correspondientes para disminuir las incidencias, terminado ello, solicita que se revise y estudie el registro realizado para su entendimiento.
7. Una vez que todos los monitoreos se hayan informado, el Comité Formulador evalúa, revisa y estudia cada registro realizado al monitorear los sistemas, ello lo hace para poder informar el estudio y las conclusiones obtenidas sobre el monitoreo de los sistemas.
8. Finalmente, el Comité Evaluador comunica al personal las conclusiones obtenidas para cada sistema.

Diagrama de Procesos N°21 - Monitoreando el uso del sistema (10.10.2)



Formulario N°20 - Monitoreando el uso del sistema (10.10.2)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.10.2 - MONITOREANDO EL USO DEL SISTEMA**	**Código:** [FRM - 10.10.2 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **168** de **1**

1 DEL SISTEMA A SER MONITOREADO: **Fecha:** [dd/mm/aaaa]

Nombre del Sistema: [Indicar el nombre del Sistema de a ser monitoreado]
Descripción del Sistema: [Describir brevemente el Sistema a ser monitoreado]
Riegos encontrados: [Listar los riesgos encontrados en la evaluación respectiva del sistema]

DEL MONITOREO:

Nivel de monitoreo: [Indicar el nivel de monitoreo requerido para el sistema]
Cantidad de veces a revisar: [Indicar la cantidad de veces a revisar las actividades de monitoreo]
Procedimientos de monitoreo: [Listar todos los procedimientos establecidos para monitorear el uso del sistema]
Áreas consideradas para el monitoreo: [Indicar las áreas/actividades del sistema que han sido consideradas a ser monitoreadas]

- ✓ Accesos autorizados/no autorizados al sistema [ ]
- ✓ Operaciones privilegiadas del sistema [ ]
- ✓ Intentos de acceso no autorizados al sistema [ ]
- ✓ Cambio o intentos de cambio a la configuración del sistema [ ]

DE LOS HALLAZGOS:

Hallazgos encontrados: [Listar y detallar los hallazgos encontrados al finalizar el monitoreo]
Incidencias presentadas: [Listar y detallar las incidencias encontradas al finalizar el monitoreo]
Medidas correctivas: [Listar y detallar las medidas correctivas establecidas para disminuir los hallazgos e incidencias negativas encontradas]

**** Número de Resolución de aprobación de los procedimientos para monitorear el uso de los sistemas.***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró los procedimientos para monitorear el uso de los sistemas]	**Nombre:** [Nombre de la persona que revisó los procedimientos para monitorear el uso de los sistemas]	**Nombre:** [Nombre de la persona que emitió la Resolución de Aprobación de los procedimientos para monitorear el uso de los sistemas]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.8.3. Protección de la información de registro.-

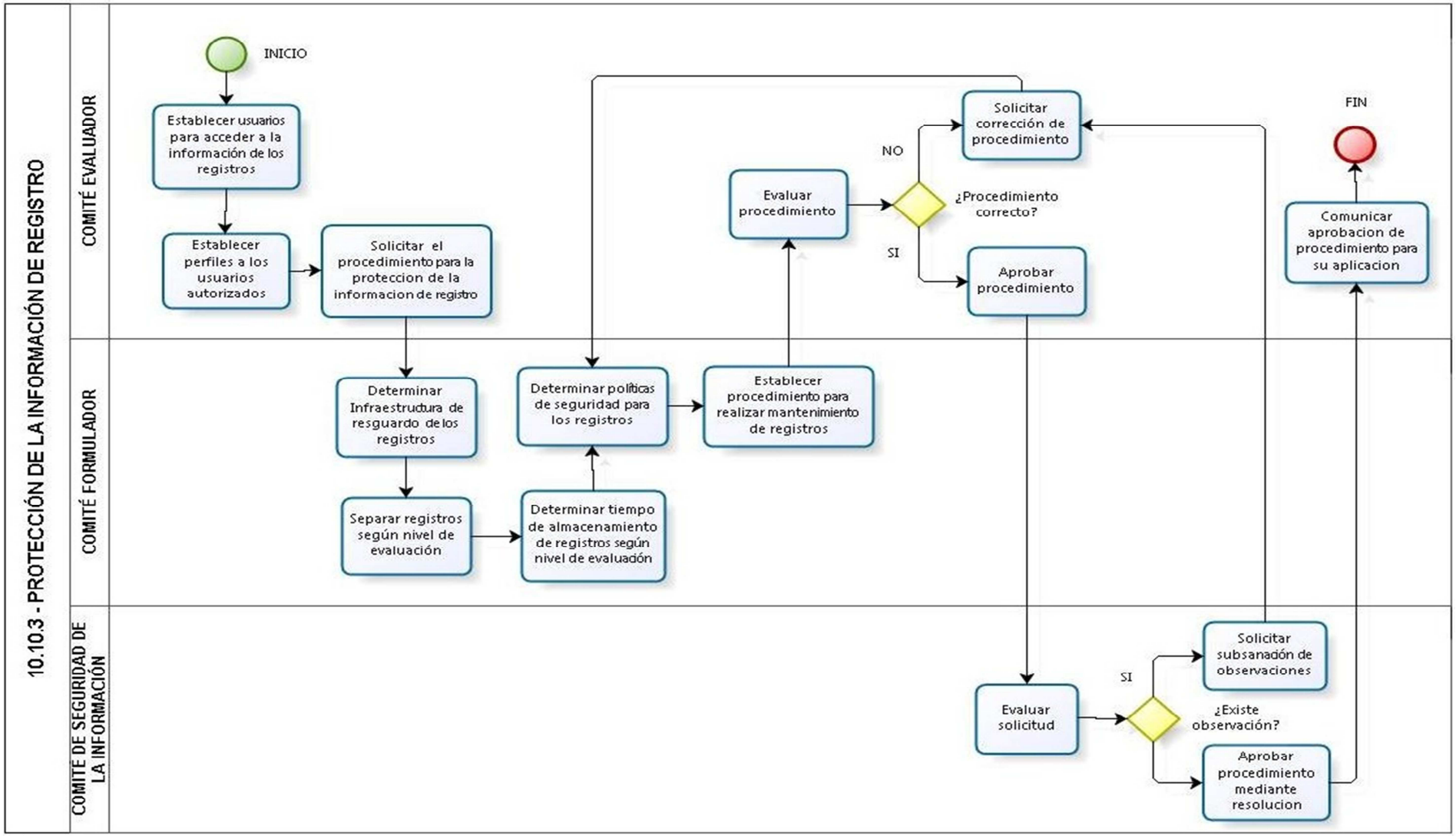
Control:
Las instalaciones de información de registro deben ser protegidas contra acciones forzosas u acceso no autorizado.

Guía de Implementación:
Los controles deben proteger contra cambios no autorizados y problemas operacionales con la instalación de registro incluyendo: alteraciones a los tipos de mensaje que son grabados, archivos de registro editados o eliminados, la capacidad de almacenamiento del medio del archivo de registro que ha sido excedido, resultando en la falla de los eventos almacenados o la sobre escritura de eventos pasados.
Algunos registros de auditoría pueden requerir ser archivados como parte de la política de retención de registros o debido a los requerimientos para recolectar y mantener evidencia.

Diagrama de Actividades N°21 - Protección de la información de registro (10.10.3)

1. El Comité Evaluador determina los usuarios que estarán autorizados para acceder a la información de los registros, establece los perfiles de acceso correspondientes y solicita al Comité Evaluador establecer procedimientos para la protección de la información de registro.
2. El Comité Formulador determina una infraestructura adecuada para mantener a salvo los registros, realiza niveles de evaluación de registros y los separa según el nivel de evaluación, para luego determinar el tiempo de almacenamiento del registro en la infraestructura establecida. A continuación determina políticas de seguridad para todos los registros y establece procedimientos para realizar el mantenimiento respectivo de los mismos, con el fin de mantener un control ordenado del mismo. Terminado ello informa lo determinado al Comité Evaluador.
3. El Comité Evaluador evalúa el procedimiento propuesto, si es que el procedimiento no es correcto, solicita la corrección del mismo, caso contrario, lo aprueba y solicita al Comité de Seguridad de la Información la aprobación respectiva mediante resolución.
4. El Comité de Seguridad de la Información evalúa el procedimiento, si realiza alguna observación, solicita levantar observaciones, caso contrario emite resolución para su aplicación.
5. El Comité Evaluador recibe la resolución de aprobación y comunica al Comité Formulador para su cumplimiento

Diagrama de Procesos N°22 - Protección de la información de registro (10.10.3)



Formulario N°21 - Protección de la información de registro (10.10.3)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.10.3 – PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO**	**Código:** [FRM - 10.10.3 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **172** de **1**

1 DEL PROCESO: **Fecha:** [dd/mm/aaaa]

Nombre : [Nombre de la persona que accede a la información de registro]
Cargo : [Cargo del personal que accede a la información de registro]
Nivel de Acceso: [Descripción del nivel de acceso a la información de registro]
Informe : [Informe con el cual se establece los usuarios y los Perfiles de Acceso a la Información del Registro]
Fecha de Informe: [dd/mm/aaaa]

PERFILES DE ACCESO:

Infraestructura: [Infraestructura donde se almacena el Registro]
Tipo de Registro: [Tipo de Registro]
Tiempo de Almacenamiento: [Tiempo de Almacenamiento de Registro]
Políticas de Seguridad de Registros: [Informe con el cual se presenta las políticas de Seguridad de Registros]

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró plan de protección de la información de registro]	**Nombre:** [Nombre de la persona que revisó el plan de protección de la información de registro]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del plan de protección de la información de registro]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
Firma y Sello	**Firma y Sello**	**Firma y Sello**

4.2.2.8.4. Registro de administradores y operadores.-

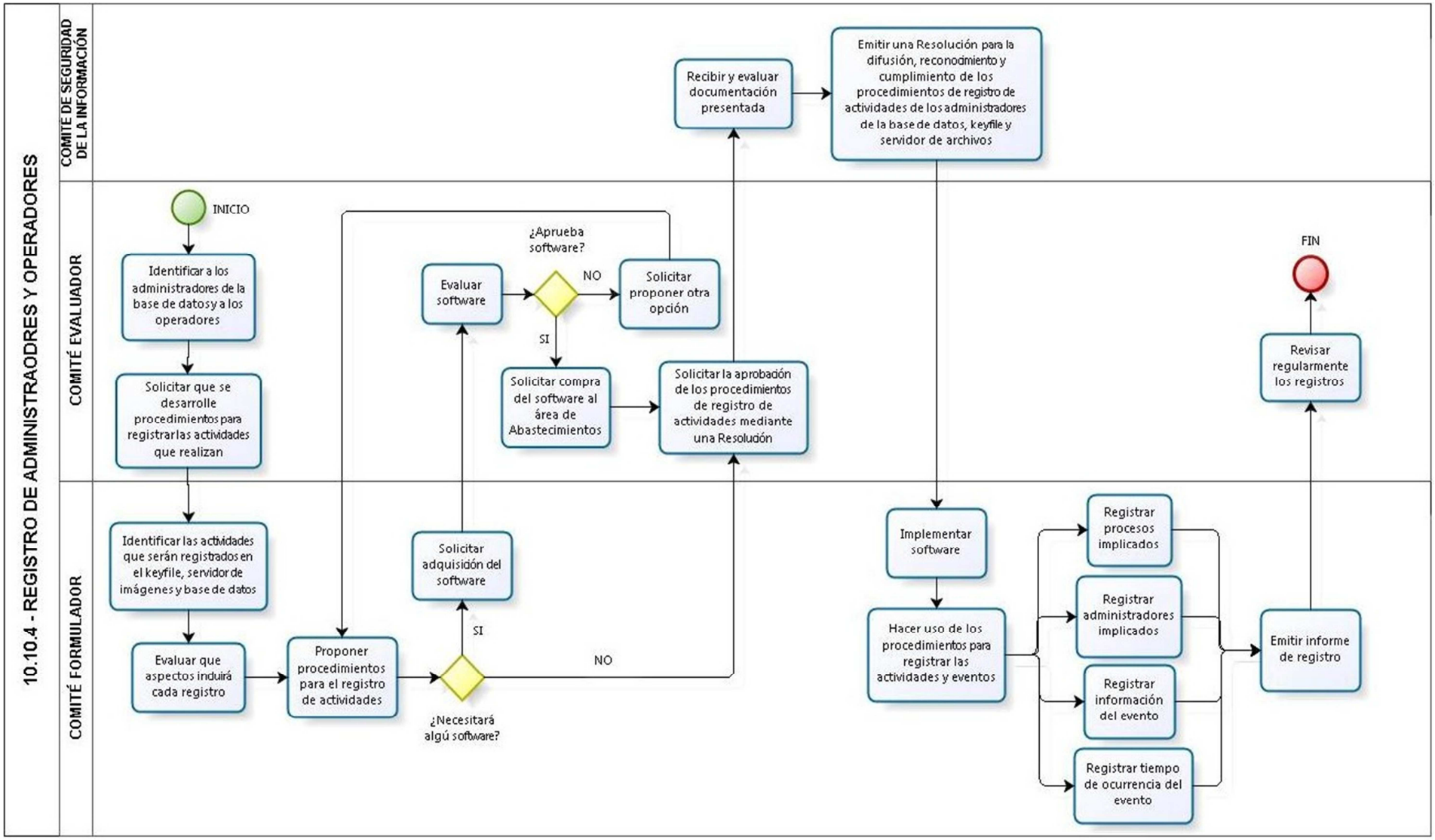
Control:
Las actividades del administrador y de los operadores del sistema deben ser registradas.

Guía de Implementación:
Los registros deben de incluir: el tiempo en el que ocurrió el evento (éxito o fracaso), información acerca del evento o fallas, que cuenta y que administrador u operador fue implicado, que procesos fueron implicados.
Los registros de los administradores y usuarios del sistema deben ser revisados en una base regular.

Diagrama de Actividades N°22 - Registro de administradores y operadores (10.10.4)

1. El Comité Evaluador identifica a los administradores de la base de datos y a los operadores, a los cuales, mediante el Comité Formulador, les solicita que se desarrollen procedimientos para registrar las actividades que realizan cada uno de ellos.
2. El Comité Formulador identifica las actividades principales del servidor de imágenes (keyfile) y del servidor de base de datos que serán registrados. Una vez identificadas las actividades, evalúa qué aspectos incluirá cada registro para luego proponer los procedimientos a realizar para el registro de dichas actividades.
   Si es que alguno de ellos necesitará de algún software para realizar el registro de las actividades, lo comunica y solicita la adquisición al Comité Evaluador
3. El Comité Evaluador evalúa software propuesto, si no lo aprueba, solicita que se proponga otra opción para el registro de las actividades de los administradores y operadores. Si es que lo aprueba, justifica y solicita la compra al área de abastecimientos. Una vez obtenido el software, solicita al Comité de Seguridad de la Información que se emita una Resolución de aprobación de los procedimientos de registro de actividades.
4. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento de los procedimientos de registro de las actividades de los administradores del servidor de base de datos, del servidor Keyfile y del servidor de archivos.
5. El Comité Formulador coordina la implementación del software y su uso en el registro haciendo uso de los procedimientos propuestos inicialmente para realizar dichos registros. En ellos incluyen el registro de los procesos implicados, el registro de otros administradores (personal de apoyo) implicados, el registro de la información de los eventos y el registro de tiempo de ocurrencia del evento. Todo lo mencionado anteriormente lo presentan en un informe, el cual lo dirigen al Comité Evaluador.
6. Finalmente, el Comité Evaluador se encarga de revisar regularmente todos los registros realizados, elaborados cada cierto tiempo.

Diagrama de Procesos N°23 - Registro de administradores y operadores (10.10.4)



Formulario N°22 - Registro de administradores y operadores (10.10.4)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO 10.10.4 - REGISTRO DE ADMINISTRADORES Y OPERADORES**	**Código:** [FRM - 10.10.4 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **176** de **1**

1 DEL SERVIDOR: **Fecha:** [dd/mm/aaaa]

Servidor a evaluar: [Indicar el servidor a ser evaluado]
- ❖ Servidor Keyfile [ ] Servidor de archivos [ ]
- ❖ Servidor Base de Datos [ ] Otro [ ] _____

Actividad/Proceso del servidor: [Describir brevemente la actividad y/o proceso del servidor que será evaluada]

Administrador/Operador: [Nombre completo de la persona encargada de la actividad/proceso del servidor - Cargo que ocupa en la institución]

DEL REGISTRO:

Software a utilizar: [De haberlo, indicar el nombre del software utilizado para realizar el registro de las actividades]

Proceso utilizado: [Indicar y describir el proceso utilizado para registrar las actividades y eventos realizados por el administrador]

Otros administradores: [Listar si lo hubieran, otros administradores implicados]

Evento realizado: [Indicar y describir el evento realizado por el administrador]

Fecha y Hora del evento: [dd/mm/aaaa HH:MM:SS]

Tiempo de ocurrencia [Indicar la duración del evento realizado por el administrador]

Informe del registro: [N°de informe con el que se reporta lo registrado - fecha: dd/mm/aaaa]

**** Número de Resolución de aprobación de los procedimientos de registro de las actividades realizadas por el administrador***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró los procedimientos de registro de las actividades realizadas por el administrador]	**Nombre:** [Nombre de la persona que revisó los procedimientos de registro de las actividades realizadas por el administrador]	**Nombre:** [Nombre de la persona que emitió la Resolución de Aprobación de los procedimientos de registro de las actividades realizadas por el administrador]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**

4.2.2.8.5. Registro de la avería.-

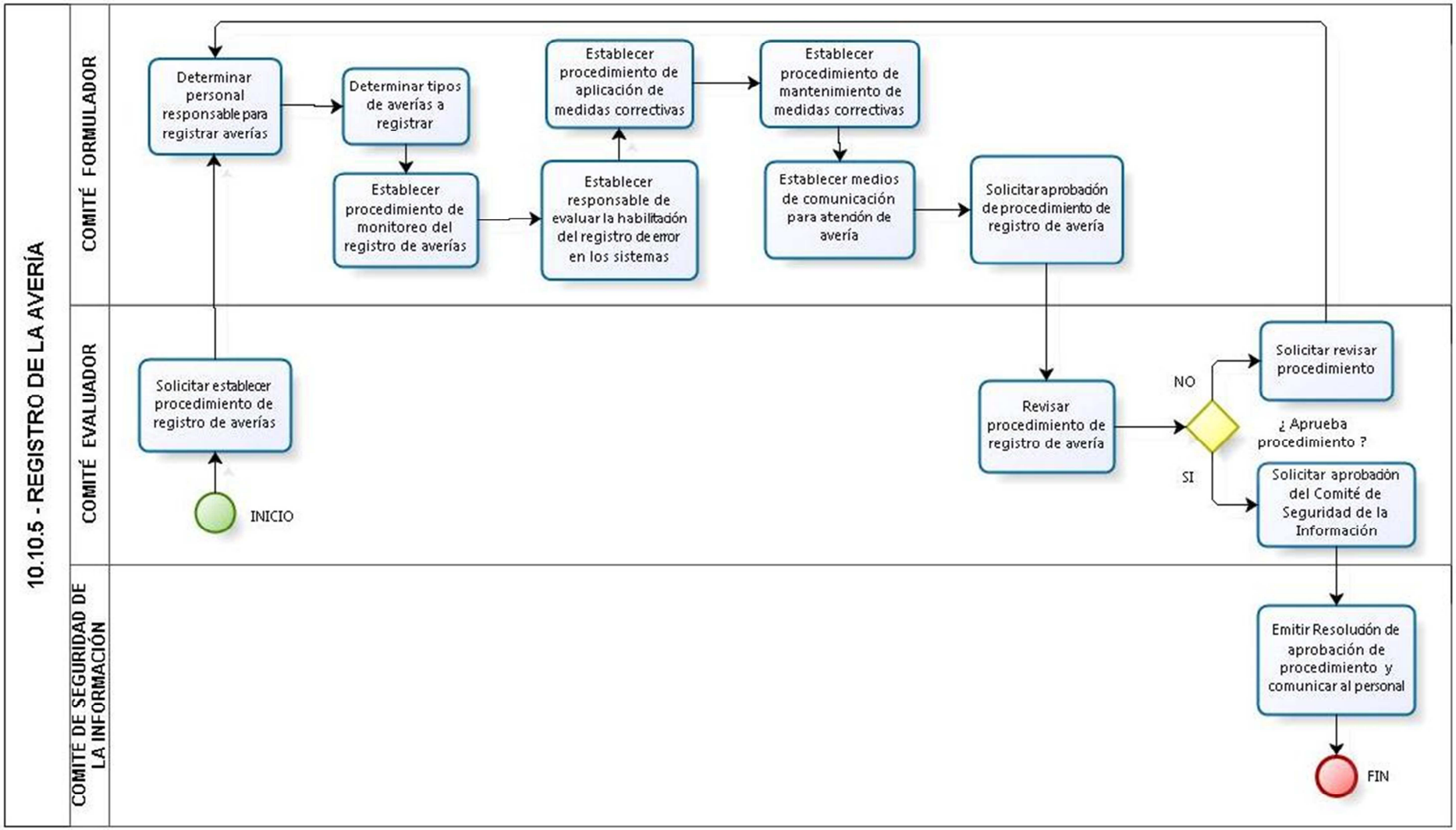
Control:
Las averías deben ser registradas, analizadas y se debe tomar acciones apropiadas.

Guía de Implementación:
Las averías reportadas por usuarios o por programas del sistema relacionados con problemas con el procesamiento o comunicación de la información, deben ser registradas. Deben existir reglas claras para maniobrar las averías reportadas incluyendo: revisión de los registros de averías para asegurar que las fallas han sido resueltas satisfactoriamente, revisión de las medidas correctivas para asegurar que los controles no han sido comprometidos y que la acción realizada es totalmente autorizada.
Se debe asegurar que el registro de error este activado, si es que se encuentra disponible en el sistema.

Diagrama de Actividades N°23 - Registro de la avería (10.10.5)

1. El Comité Evaluador solicita al Comité Formulador establecer un procedimiento a realizar para el registro de averías.
2. El Comité Formulador realiza las siguientes tareas:
   - Determinar el personal responsable del registro de averías
   - Determinar tipos de avería
   - Establecer un procedimiento de seguimiento y/o monitoreo de averías
   - Determinar responsables de evaluar la habilitación de registro de errores en los sistemas
   - Establecer un procedimiento de aplicación de medidas correctivas y un procedimiento de mantenimiento de dichas medidas correctivas
   - Establecer medios de comunicación para atención de avería.
   - Finalmente solicitar al Comité Evaluador la aprobación del procedimiento de registro de avería.
3. El Comité Evaluador evalúa el procedimiento propuesto, si es que el procedimiento no es correcto, solicita la corrección del procedimiento, caso contrario, lo aprueba y solicita al Comité de Seguridad de la Información la aprobación mediante una resolución.
4. El Comité de Seguridad de la Información emite resolución de aprobación y comunica al personal para su aplicación.

Diagrama de Procesos N°24 - Registro de la avería (10.10.5)



Formulario N°23 - Registro de la avería (10.10.5)

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**FORMULARIO** **10.10.5 – REGISTRO DE AVERIA**	**Código:** [FRM - 10.10.5 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **180** de **1**

1 DEL REGISTRO DE AVERÍA.- **Fecha:** [dd/mm/aaaa]

Descripción de avería: [Indicar una descripción de la Avería]
Tipo de avería: [Indicar y describir el Tipo de Avería]
Fecha y Hora de Inicio: [Indicar la Fecha y Hora de Recepción de la Avería en formato: dd/mm/aaaa]
Registrado por: [Nombre completo del personal responsable del registro de avería]

DEL MONITOREO DE AVERIA.-

Medio de Reporte de Avería: [Describir el medio por el cual se reporta la alerta de avería]
- ❖ Correo Electrónico [ ] Presencial [ ] Alertas del Sistema [ ] Otro [ ] _____

Responsable de Errores: [Nombre del responsable de habilitar el registro de error en los sistemas]

DE LAS MEDIDAS CORRECTIVAS.-

Revisión Medidas Correctivas: [Indicar la revisión si existe medidas correctivas de la avería reportada]
Mantenimiento de Medidas correctivas: [Indicar el procedimiento para agregar, actualizar, y/o eliminar las medidas correctivas]
Alojamiento: [Indicar la Infraestructura donde se alojan las medidas correctivas]
Culminación de Avería: [Indicar el medio de comunicación para reportar la atención de avería]

**** Número de Resolución de aprobación de los procedimientos de registro de averías.***

2 DE LA ELABORACIÓN:	3 DE LA REVISIÓN:	4 DE LA APROBACIÓN:
Personal del Comité Formulador	**Personal del Comité Evaluador**	**Personal del Comité de Seguridad de la Información**
Fecha: [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]	**Fecha:** [dd/mm/aaaa]
Nombre: [Nombre de la persona que elaboró registro de avería]	**Nombre:** [Nombre de la persona que revisó el registro de avería]	**Nombre:** [Nombre de la persona que emitió Resolución de aprobación del registro de avería]
Cargo: [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]	**Cargo:** [Indicar el cargo que ocupa en la institución]
_____ **Firma y Sello**	_____ **Firma y Sello**	_____ **Firma y Sello**