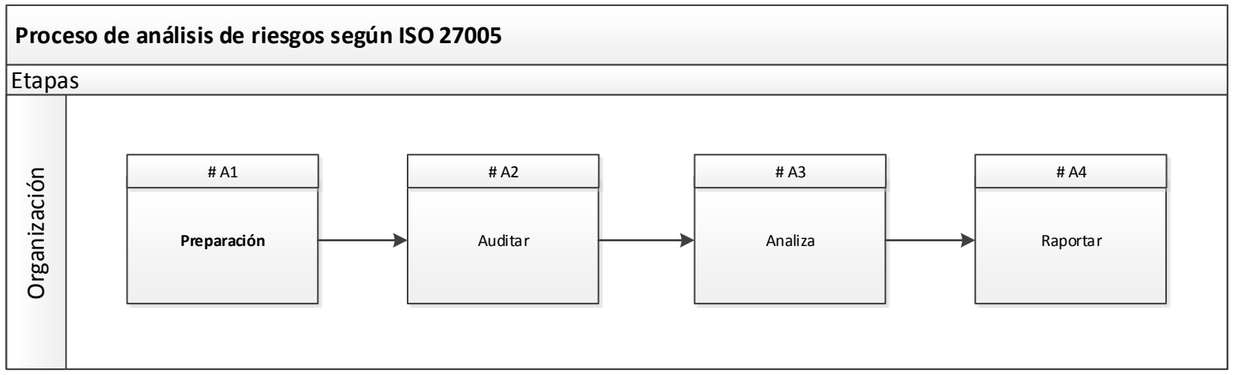
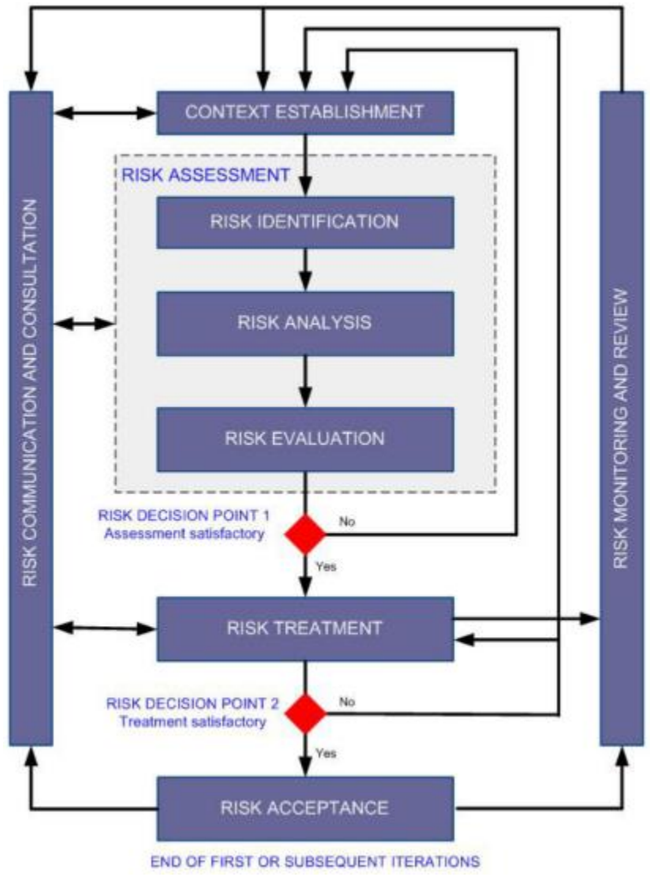


Versión mai 2017, Autor: Christophe Jolivet – PR4GM4 inc. 418-261-6320

(Rojo: etapas ISO 27005)

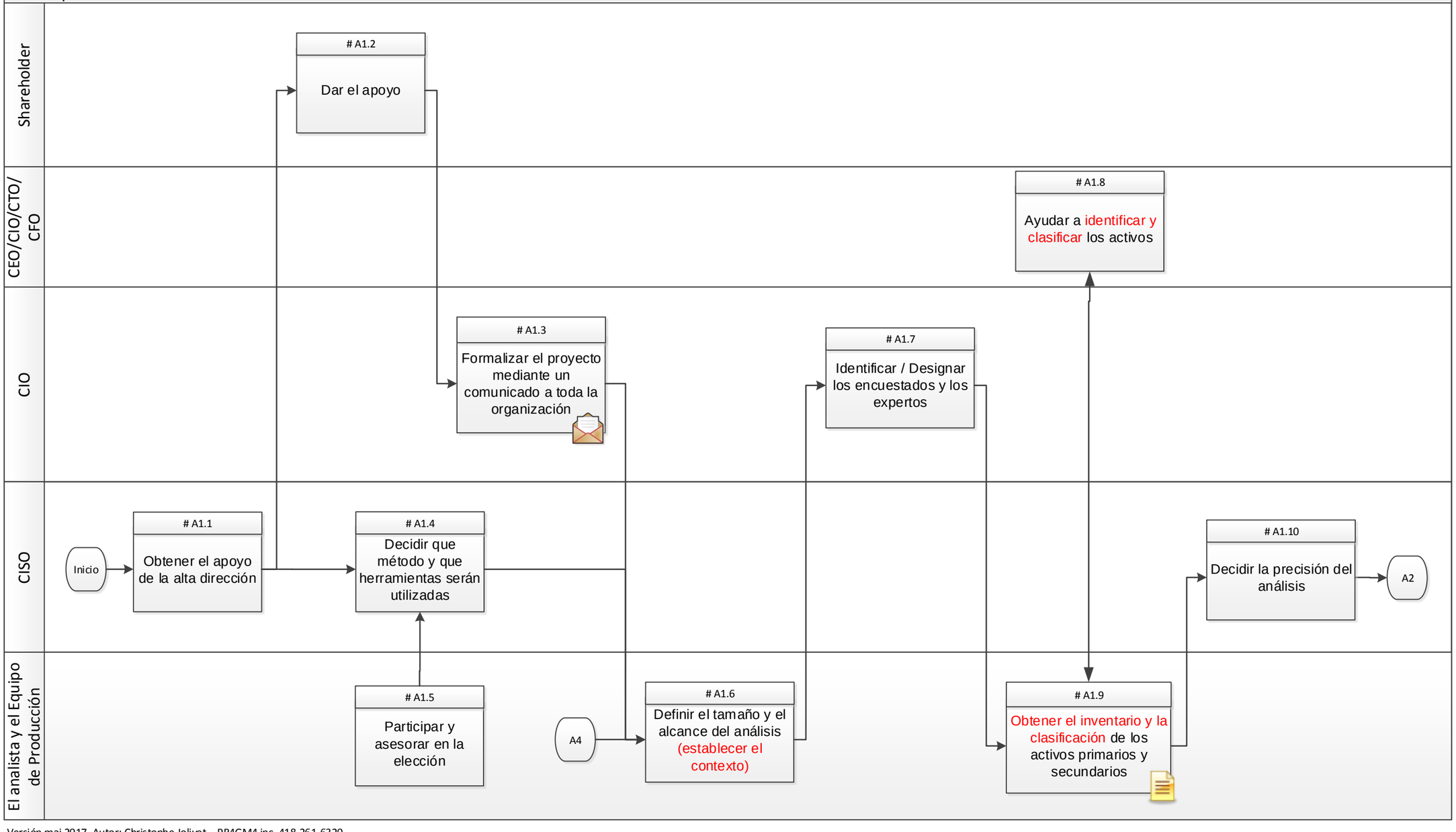
ALTAVOCES:
CSAI: Comisión de Seguridad de los activos de información
Shareholder: Accionistas
CTO: chief technology officer
CIO: Chief information officer
CISO: Chief information security officer y ***el análisis del equipo de realización de trabajo para él / ella***

ISO 27005



Proceso de análisis de riesgos según ISO 27005

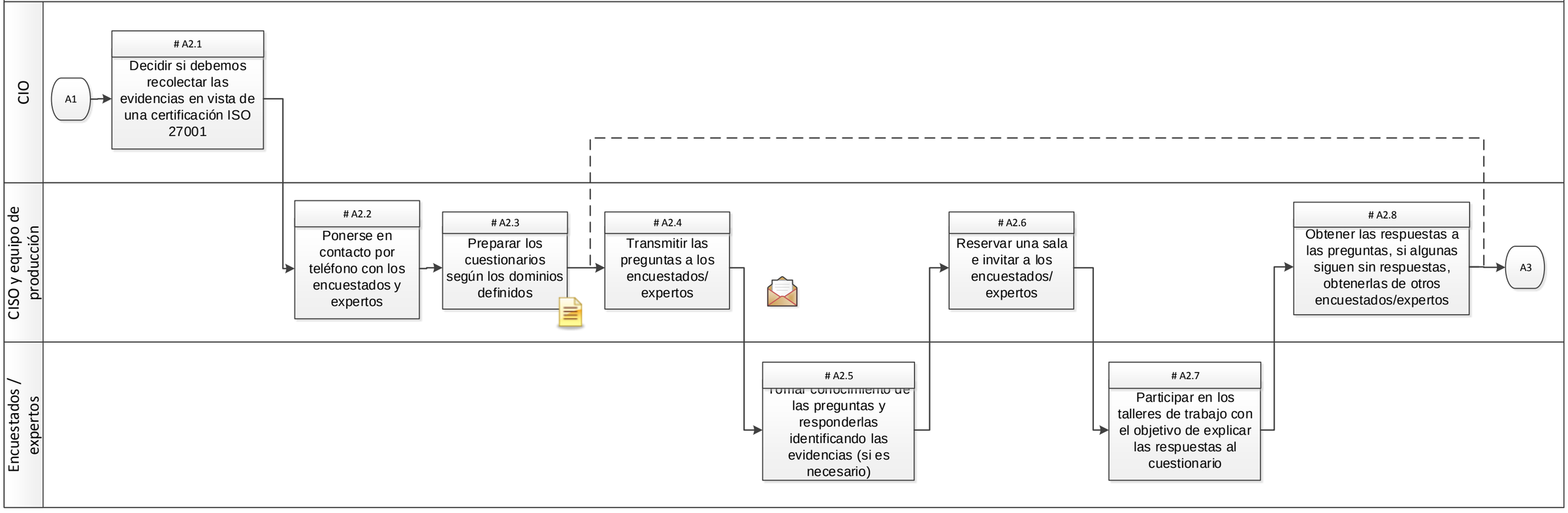
A1 - Preparación



N°	Actividad	Descripción	Entregable
Etapa: Preparación			
A1.1	Obtener el apoyo de la alta dirección	Para facilitar la colaboración de las partes interesadas, lo mejor es el CISO obtenga el apoyo de la alta dirección.	
A1.2	Dar el apoyo	La alta dirección brinda el apoyo	
A1.3	Formalizar el proyecto mediante un comunicado a toda la organización	La obtención del apoyo de la alta dirección se debe formalizar con un comunicado del CIO enviado a todas las personas involucradas de la organización	Comunicado oficial
A1.4	Decidir que método y que herramientas serán utilizadas	El CISO debe decidir que método y herramienta será utilizado. En efecto, diversos métodos y herramientas son disponibles en el mercado.	
A1.5	Participar y asesorar en la elección	El analista y el equipo de trabajo participa y asesora mediante el análisis preliminar, las demostraciones y haciendo la elección a largo plazo.	
A1.6	Definir el tamaño y el alcance del análisis (establecer el contexto)	El equipo de trabajo define el tamaño y el alcance del análisis. ¿El análisis se realiza como parte de un proyecto? ¿Está relacionado a un servicio, una dirección o a toda la organización?	
A1.7	Identificar / Designar los encuestados y los expertos	El CIO identifica y designa a los encuestados y expertos por sectores de actividad, áreas, direcciones y campos de experiencia.	
A1.8	Ayudar a identificar y clasificar los activos	Partiendo de los procesos de negocios y con la ayuda de los titulares se identifican los activos	
A1.9	Obtener el inventario y la clasificación de los activos primarios y secundarios	Obtener el inventario y la clasificación de los activos primarios y secundarios de sus titulare (si no fue realizado) quienes son frecuentemente los CEO/CIO/CTO/CFO, etc.	Clasificación de los activos
A1.10	Decidir la precisión del análisis	Decidir la precisión del análisis. ¿Deseamos obtener las respuestas Si/No o deseamos evaluar la presencia de medidas de seguridad en una escala de madurez como ISO 15504?	

Proceso de análisis de riesgos según ISO 27005

A2 - Auditar

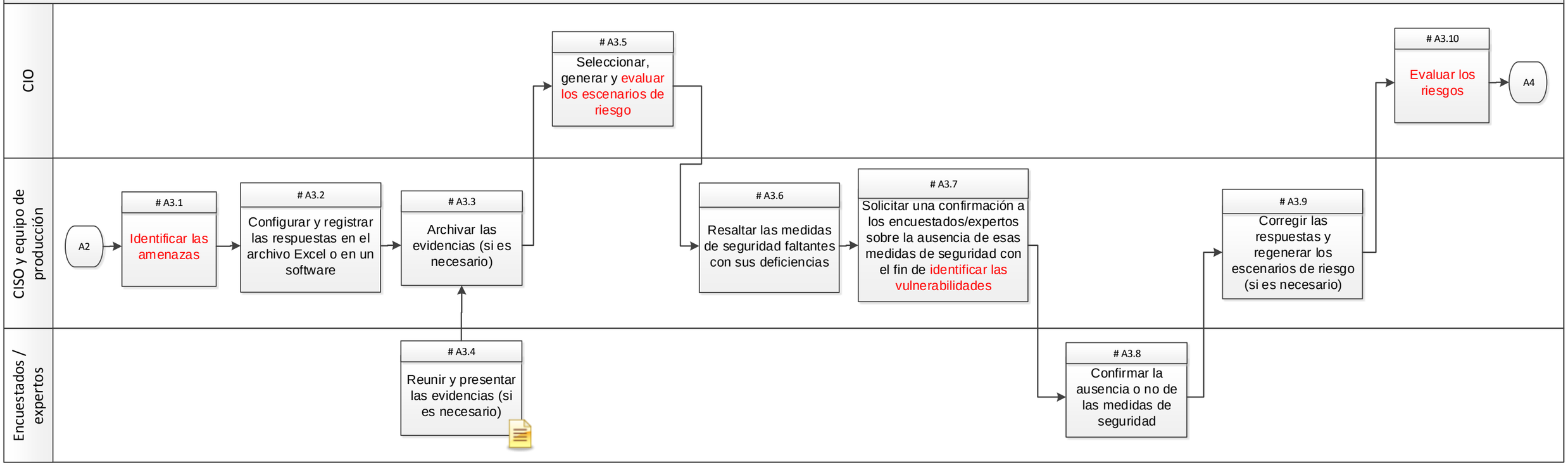


Versión mai 2017, Autor: Christophe Jolivet – PR4GM4 inc. 418-261-6320

Etapa: Auditar			
A2.1	Decidir si debemos recolectar las evidencias en vista de una certificación ISO 27001.	Decidir si debemos recolectar las evidencias en vista de una certificación ISO 27001. En efecto, el auditor externo exigirá ver las evidencias en la forma de procesos, directivas, copias de pantallas, etc.	
A2.2	Ponerse en contacto por teléfono con los encuestados y expertos	Ponerse en contacto por teléfono con los encuestados/expertos, esto facilita los siguientes intercambios y permite asegurarse que los encuestados/expertos designados puedan responder a las preguntas.	
A2.3	Preparar los cuestionarios según los dominios definidos	Preparar los cuestionarios según los dominios definidos y los encuestados/expertos identificados anteriormente según el organigrama de la organización.	
A2.4	Transmitir las preguntas a los encuestados/expertos	Transmitir las preguntas a los encuestados/expertos para que ellos puedan tomar conocimiento previo al taller de trabajo.	
A2.5	Tomar conocimiento de las preguntas y responderlas identificando las evidencias (si es necesario)	Los encuestados/expertos toman conocimiento de las preguntas y las responden identificando las evidencias (si es necesario).	
A2.6	Reservar una sala e invitar a los encuestados/expertos	Reservar una sala e invitar a los encuestados/ expertos a los talleres de trabajo de un máximo de dos horas. Organizar la cantidad necesaria de talleres.	
A2.7	Participar en los talleres de trabajo	Participar en los talleres de trabajo con el objetivo de explicar las respuestas al cuestionario.	
A2.8	Obtener las respuestas	Obtener las respuestas a las preguntas, si algunas siguen sin respuestas, obtenerlas de otros encuestados/expertos. En efecto, puede que después de los talleres, algunas preguntas deben ser realizadas a otras personas.	

Proceso de análisis de riesgos según ISO 27005

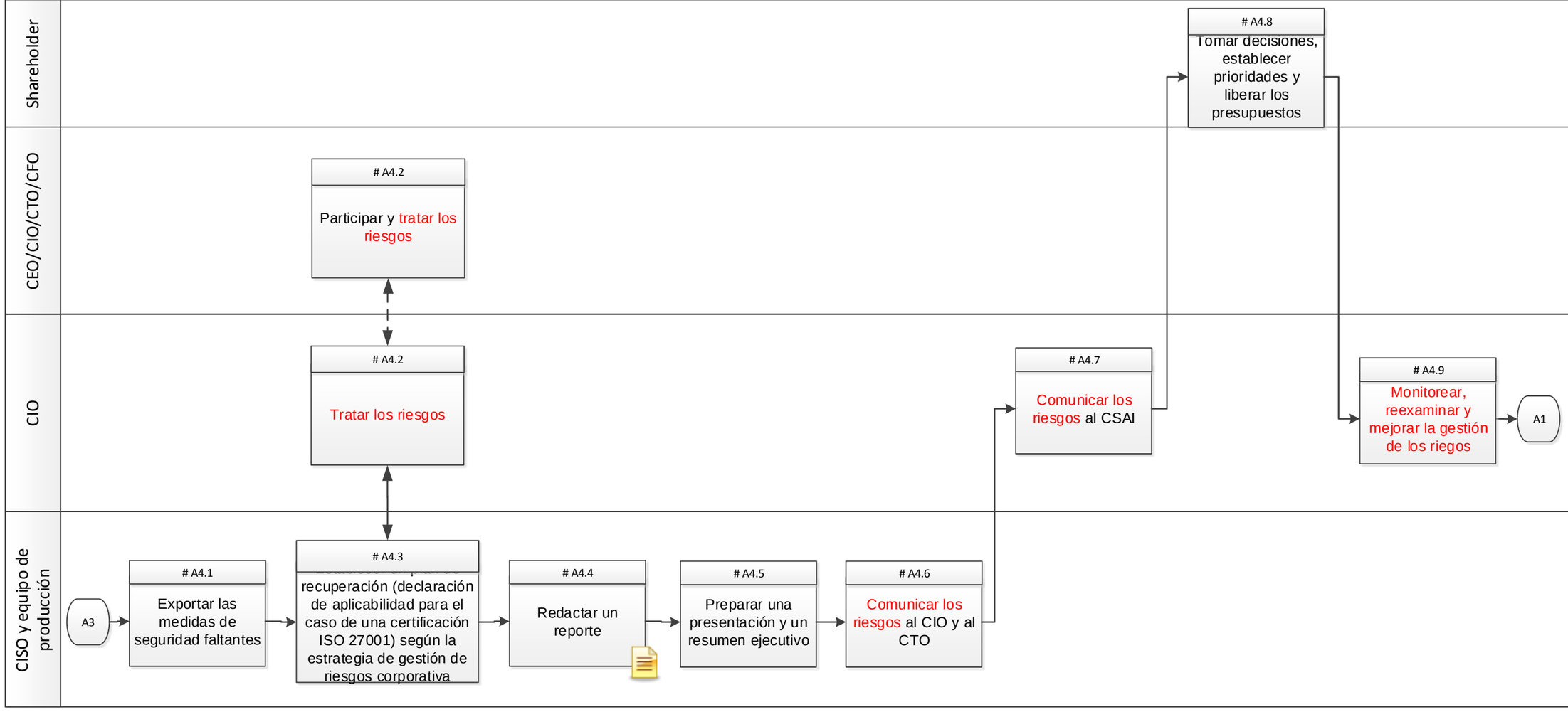
A3 - Analizar



Etapa: Analizar			
A3.1	Identificar las amenazas	En la norma ISO 27005, se exige identificar las amenazas.	
A3.2	Configurar y registrar las respuestas	Configurar y registrar las respuestas en el archivo Excel o en un software	
A3.3	Archivar las evidencias (si es necesario)	Archivar las evidencias (si es necesario)	Evidencias 
A3.4	Reunir y presentar las evidencias (si es necesario).	Reunir y presentar las evidencias (si es necesario).	
A3.5	Seleccionar, generar y evaluar los escenarios de riesgo	Seleccionar, generar y evaluar los escenarios de riesgo según la envergadura del proyecto a partir de las líneas de negocios.	
A3.6	Resaltar las medidas de seguridad faltantes con sus deficiencias	Resaltar las medidas de seguridad faltantes con sus deficiencias	
A3.7	Solicitar una confirmación a los encuestados/expertos sobre la ausencia de esas medidas de seguridad con el fin de identificar las vulnerabilidades	Solicitar una confirmación a los encuestados/expertos sobre la ausencia de esas medidas de seguridad con el fin de identificar las vulnerabilidades. En efecto, no es raro que los encuestados/expertos reconsideren sus respuestas con el fin de contextualizar las ausencias. Esto evita que s presenten riesgos que podrían ser "alarmantes".	
A3.8	Confirmar la ausencia o no de las medidas de seguridad	Confirmar la ausencia o no de las medidas de seguridad	
A3.9	Corregir las respuestas y regenerar los escenarios de riesgo (si es necesario)	Corregir las respuestas y regenerar los escenarios de riesgo (si es necesario)	
A3.10	Evaluar los riesgos	Evaluar los riesgos. Esto se puede hacer automáticamente mediante un archivo Excel o un software.	

Proceso de análisis de riesgos según ISO 27005

A4 - Raportar



Etapa: Reportar			
A4.1	Exportar las medidas de seguridad faltantes	Exportar las medidas de seguridad faltantes del archivo Excel o del software con el fin de utilizar esta información para tratar los riesgos.	
A4.2	Tratar los riesgos	Tratar los riesgos seleccionando y priorizando las medidas que atenúen la mayor cantidad de riesgos.	
A4.3	Establecer un plan de recuperación según la estrategia de gestión de riesgos	Establecer un plan de recuperación (declaración de aplicabilidad para el caso de una certificación ISO 27001) según la estrategia de gestión de riesgos corporativa.	Plan de recuperación 
A4.4	Redactar un reporte	Redactar un reporte en un formato esperado y de acuerdo a las practicas organizacionales.	Reporte 
A4.5	Preparar una presentación y un resumen ejecutivo	Preparar una presentación y un resumen ejecutivo dirigido a la alta dirección.	Presentación y resumen ejecutivo
A4.6	Comunicar los riesgos al CIO y al CTO	Comunicar los riesgos al CIO y al CTO	
A4.7	Comunicar los riesgos al CSAI	Comunicar los riesgos al CSAI y a los accionistas.	
A4.8	Tomar decisiones, establecer prioridades y liberar los presupuestos	Tomar decisiones, establecer prioridades y liberar los presupuestos	Minuta del comité 
A4.9	Monitorear, reexaminar y mejorar la gestión de los riegos	Con el fin de seguir la norma ISO 27005, es recomendable de monitorear, reexaminar y mejorar la gestión de los riegos.	