PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ESTABLECIMIENTO, IMPLEMENTACIÓN, MANTENIMIENTO Y MEJORA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA ISO/IEC 27001:2013, PARA UNA EMPRESA DE CONSULTORÍA DE SOFTWARE

Anexos

Santos Llanos, Daniel Elías

ASESOR: Luis Silva-Santisteban Sierra

Lima, Agosto del 2016

ANEXOS

Anexo A. Plan de operación y comunicaciones del SGSI

Descripción: Plan que establece las actividades base del periodo para el SGSI, en lo referido a la operación y comunicaciones del sistema.
Aprobado: Versión 1.0 por Representante de la Dirección

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
COM01	Establecer	Comunicación	Comunicar el inicio de ciclo de operación del SGSI	*Ha iniciado el periodo de operación	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Representantes de los procesos, Representante de la dirección	**Documentos:** *Plan de operación y comunicaciones del SGSI (suscrita por la dirección) *Plan de concientización, capacitación y evaluación	1. Coordinar las sesiones para: las actividades del SGSI del periodo	**Resultado esperado:** *Reuniones planificadas	ene-15	ene-15	**Realizado**
OPE01	Establecer	Operación	Entender el contexto	*Ha transcurrido un periodo desde su última revisión *Hay un cambio significativo sobre la organización	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representantes de los procesos	**Documentos:** *Informe de contexto de la organización (anterior, si existe)	1. Evaluar la situación actual (cambios significativos) 2. Preparar o actualizar el documento	**Resultado esperado:** *Informe de contexto de la organización	ene-15	feb-15	**Realizado**
OPE02	Establecer	Operación	Entender los requisitos de las partes interesadas	*Ha transcurrido un periodo desde su última revisión *Hay un cambio significativo sobre la organización	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representantes de los procesos	**Documentos:** *Informe de necesidades y expectativas de las partes interesadas (anterior, si existe)	1. Evaluar las partes interesadas actuales y sus requisitos vigentes 2. Preparar o actualizar el documento	**Resultado esperado:** *Informe de necesidades y expectativas de las partes interesadas	ene-15	feb-15	**Realizado**
OPE03	Establecer	Operación	Establecer un plan para el logro de los requisitos	*Se han aprobado los requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal involucrado	**Documentos:** *Informe de necesidades y expectativas de las partes interesadas	1. Establecer tareas y responsables para el logro de cada requisito 2. Aprobar el plan de trabajo y comprometer a los jefes de los responsables de su ejecución	**Resultado esperado:** *Plan de requisitos de seguridad de información	ene-15	feb-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
COM02	Establecer	Comunicación	Comunicar el plan para el logro de los requisitos	*Se ha aprobado el plan para el logro de los requisitos	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Personal involucrado	**Documentos:** *Plan de requisitos de seguridad de información	1. Comunicar las actividades asignadas a cada responsable	**Resultado esperado:** *Registros de comunicación (correo)	ene-15	feb-15	**Realizado**
OPE4	Establecer	Operación	Ejecutar el plan para el logro de los requisitos	*Se ha aprobado el plan para el logro de los requisitos	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal involucrado	**Documentos:** *Plan de requisitos de seguridad de información	1. Implementar las acciones comprometidas en los planes y reportar avances	**Resultado esperado:** *Implementación de: Plan de requisitos de seguridad de información	feb-15	nov-16	**En proceso**
OPE05	Establecer	Operación	Determinar el alcance del SGSI	*Ha transcurrido un periodo desde su última revisión *Hay un cambio significativo sobre la organización	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representante de la dirección	**Documentos:** *Declaración del alcance del SGSI (anterior, si existe) *Informe de contexto de la organización, Informe de necesidades y expectativas de las partes interesadas	1. Revisar la Declaración del alcance del SGSI 2. Preparar o actualizar el documento	**Resultado esperado:** *Declaración del alcance del SGSI	ene-15	feb-15	**Realizado**
OPE06	Establecer	Operación	Validar la política de seguridad de información	*Ha transcurrido un periodo desde su última revisión *Hay un cambio significativo sobre la organización	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representante de la dirección	**Documentos:** *Política de seguridad de información (anterior, si existe) *Informe de contexto de la organización *Informe de necesidades y expectativas de las partes interesadas *Declaración de objetivos de seguridad de información (anterior, si existe)	1. Revisar la Política de seguridad de información 2. Preparar o actualizar el documento	**Resultado esperado:** *Política de seguridad de información	ene-15	feb-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
COM03	Establecer	Comunicación	Comunicar la política de seguridad de información	*Ha culminado la validación de la Política de seguridad de información	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Todo el personal	**Documentos:** *Política de seguridad de información	1. Enviar comunicados difundiendo o recordando la política a las partes interesadas (internas y externas)	**Resultado esperado:** *Registros de comunicación (correo)	ene-15	feb-15	**Realizado**
COM04	Implementar	Comunicación	Comunicar el inicio de la gestión de riesgos	*Ha transcurrido un periodo desde su última ejecución *Hay un cambio significativo sobre la organización	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Representantes de los procesos *Representante de la dirección	**Documentos:** *Cronograma de gestión de riesgos (propuesto)	1. Coordinar y comunicar el cronograma final para la gestión de riesgos del periodo	**Resultado esperado:** *Registros de comunicación (correo) *Cronograma de gestión de riesgos (aprobado)	mar-15	mar-15	**Realizado**
OPE07	Implementar	Operación	Apreciar los riesgos de los procesos	*Se ha comunicado el inicio de la gestión de riesgos	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representantes de los procesos	**Documentos:** *Metodología de gestión de riesgos *Informe de gestión de riesgos (previo, si existe)	1. Ejecutar la Metodología de gestión de riesgos - apreciación de riesgos 2. Generar el Informe de gestión de riesgos	**Resultado esperado:** *Informe de gestión de riesgos (parcial)	mar-15	may-15	**Realizado**
OPE08	Implementar	Operación	Definir el tratamiento los riesgos identificados	*Se ha culminado la apreciación de riesgos	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representantes de los procesos	**Documentos:** *Metodología de gestión de riesgos *Informe de gestión de riesgos *Declaración de aplicabilidad de controles (previa, si existe)	1. Ejecutar la Metodología de gestión de riesgos - tratamiento de riesgos 2. Completar: Informe de gestión de riesgos 3. Generar: Plan de tratamiento de riesgos y Declaración de aplicabilidad de controles	**Resultado esperado:** *Informe de gestión de riesgos *Plan de tratamiento de riesgos *Declaración de aplicabilidad de controles	may-15	may-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
COM05	Implementar	Comunicación	Comunicar el fin de la gestión de riesgos	*Se ha culminado la gestión de riesgos	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Representantes de los procesos *Representante de la dirección	**Documentos:** *Informe de gestión de riesgos	1. Presentar los resultados de la gestión de riesgos	**Resultado esperado:** *Registros de comunicación (listas de asistencia a la presentación)	may-15	may-15	**Realizado**
OPE09	Implementar	Operación	Ejecutar el tratamiento los riesgos identificados	*Se ha aprobado el Informe de gestión de riesgos	**Responsable:** *Propietarios de los riesgos **Supervisor:** *Coordinador de seguridad de información	**Documentos:** *Plan de tratamiento de riesgos	1. Implementar las acciones comprometidas en los planes y reportar avances 2. Documentar los avances en el Informes de seguimiento de riesgos	**Resultado esperado:** *Informes de seguimiento de riesgos *Implementación de: Plan de tratamiento de riesgos	jun-15	feb-16	**Realizado**
OPE10	Implementar	Operación	Validar los objetivos de seguridad de información	*Se ha culminado la gestión de riesgos *Hay un cambio significativo sobre la organización	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representante de la dirección	**Documentos:** *Declaración de objetivos de seguridad de información (anterior, si existe) *Política de seguridad de información (anterior, si existe) *Informe de necesidades y expectativas de las partes interesadas *Informe de gestión de riesgos *Informe de seguimiento de riesgos	1. Revisar la Declaración de objetivos de seguridad de información 2. Preparar o actualizar el documento	**Resultado esperado:** *Declaración de objetivos de seguridad de información	jun-15	jun-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
OPE11	Implementar	Operación	Establecer un plan para el logro de los objetivos	*Se han aprobado los objetivos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal involucrado	**Documentos:** *Declaración de objetivos de seguridad de información	1. Establecer tareas y responsables para el logro de cada objetivo planteado 2. Aprobar el plan de trabajo y comprometer a los jefes de los responsables de su ejecución	**Resultado esperado:** *Plan de objetivos de seguridad de información	jul-15	jul-15	**Realizado**
COM06	Implementar	Comunicación	Comunicar el plan para el logro de los objetivos	*Se ha aprobado el plan para el logro de los objetivos	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Personal involucrado	**Documentos:** *Plan de objetivos de seguridad de información	1. Comunicar las actividades asignadas a cada responsable	**Resultado esperado:** *Registros de comunicación (correo)	jul-15	jul-15	**Realizado**
OPE12	Implementar	Operación	Ejecutar el plan para el logro de los objetivos	*Se ha aprobado el plan para el logro de los objetivos	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal involucrado	**Documentos:** *Plan de objetivos de seguridad de información	1. Implementar las acciones comprometidas en los planes y reportar avances	**Resultado esperado:** *Implementación de: Plan de objetivos de seguridad de información	jul-15	nov-16	**En proceso**
OPE13	Implementar	Operación	Mantener un plan de concientización, capacitación y evaluación	*Ha transcurrido un periodo desde la última ejecución del plan. *Se identifica que personal con un rol que afecta a la seguridad de información no cuenta con la competencia *Nuevo personal de los procesos ingresa a la organización (inducción y concientización)	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal que participa del SGSI	**Documentos:** *Plan de concientización, capacitación y evaluación (previo, si existe) *Evaluaciones para el personal *Temario de la concientización **Presentación:** *Roles, responsabilidades y actividades del SGSI *Concientización en seguridad de información	1. Establecer las necesidades, fechas y responsables para las charlas y evaluaciones 2. Desarrollar o actualizar los materiales necesarios para estas actividades 3. Aprobar el plan por las jefaturas del personal involucrado	**Resultado esperado:** *Plan de concientización, capacitación y evaluación *Lista de personal para las charlas de concientización *Lista de personal para las capacitaciones	ago-15	ago-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
COM07	Implementar	Comunicación	Comunicar las convocatorias del plan de concientización, capacitación y evaluación	*Se ha aprobado el plan de concientización, capacitación y evaluación	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal que participa del SGSI	**Documentos:** *Plan de concientización, capacitación y evaluación *Evaluaciones para el personal	1. Comunicar las actividades a todos los involucradas	**Resultado esperado:** *Registros de comunicación (correo)	ago-15	ago-15	**Realizado**
OPE14	Implementar	Operación	Ejecutar el plan de concientización, capacitación y evaluación	*Se ha aprobado el plan de concientización, capacitación y evaluación	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de concientización, capacitación y evaluación (previo, si existe) *Evaluaciones para el personal *Temario de la concientización **Presentación:** *Roles, responsabilidades y actividades del SGSI *Concientización en seguridad de información	1. Ejecutar la charla de concientización general 2. Ejecutar capacitaciones al personal que requiere mejorar sus competencias 3. Ejecutar la evaluación del personal capacitado 4. Realizar nuevas capacitaciones evaluadas para los que no superaron la evaluación	**Resultado esperado:** *Listas de asistencia a las presentaciones *Resultados de evaluación de personal	ago-15	ago-15	**Realizado**
OPE15	Mantener	Operación	Definir métricas de Seguridad de Información	*Se han aprobado los objetivos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representantes de los procesos	**Documentos:** *Declaración de objetivos de seguridad de información *Declaración de aplicabilidad de controles *Plan de métricas de seguridad de información (anterior)	1. Revisar el Plan de métricas de seguridad de información (incluye los resultados previos) 2. Preparar o actualizar el documento (respecto a las métricas para los objetivos y los grupos de controles)	**Resultado esperado:** *Plan de métricas de seguridad de información	sep-15	sep-15	**Realizado**
COM08	Mantener	Comunicación	Comunicar los requerimientos para el monitoreo y medición de las métricas	*Se han aprobado el Plan de métricas de seguridad de información	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Representantes de los procesos	**Documentos:** *Plan de métricas de seguridad de información	1. Solicitar información para obtener las métricas de seguridad de información	**Resultado esperado:** *Información para el cálculo de métricas	sep-15	oct-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
OPE16	Mantener	Operación	Analizar y evaluar las métricas	*Se ha obtenido la información requerida en el Plan de métricas de seguridad de información	**Responsable:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información **Registros:** *Información para el cálculo de métricas	1. Procesar la información para la obtención de las métricas del plan	**Resultado esperado:** *Plan de métricas de seguridad de información (con resultados)	oct-15	oct-15	**Realizado**
COM09	Mantener	Comunicación	Comunicar el inicio de la auditoría interna	*Ha transcurrido un periodo desde la última auditoría interna *Ha ocurrido un evento significativo que compromete la seguridad de información	**Emisor:** *Auditor interno del SGSI **Receptor:** *Representante de la dirección *Representantes de los procesos *Coordinador de seguridad de información	**Documentos:** *Plan de auditoría interna del SGSI (propuesto)	1. Comunicar y acordar las fechas de reuniones con los participantes	**Resultado esperado:** *Plan de auditoría interna del SGSI (aprobado)	nov-15	nov-15	**Realizado**
OPE17	Mantener	Operación	Ejecutar la auditoría interna del SGSI	*Se ha aprobado el Plan de auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Personal de la organización	**Documentos:** *Plan de auditoría interna del SGSI (aprobado) *Documentos y registros del SGSI	1. Realizar las reuniones definidas en el plan	**Resultado esperado:** *Informe de resultados de la auditoría interna	nov-15	nov-15	**Realizado**
COM10	Mantener	Comunicación	Comunicar resultados de la auditoría interna	*Se ha elaborado el Informe de resultados de la auditoría interna	**Emisor:** *Auditor interno del SGSI **Receptor:** *Representante de la dirección *Representantes de los procesos *Coordinador de seguridad de información	**Documentos:** *Informe de resultados de la auditoría interna	1. Comunicar los hallazgos a los principales involucrados en la organización para que tomen acciones correctivas (no conformidades) o de mejora (observaciones, oportunidades)	**Resultado esperado:** *Registros de comunicación (listas de asistencia a la presentación del informe) *Informe de resultados de la auditoría interna (aprobado)	nov-15	nov-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
OPE18	Mejorar	Operación	Establecer acciones correctivas y de mejora (auditoría interna)	*Se ha aprobado el Informe de resultados de la auditoría interna	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representante de la dirección *Representantes de los procesos	**Documentos:** *Informe de resultados de la auditoría interna	1. Establecer tareas y responsables para el logro de cada objetivo planteado 2. Aprobar los planes de trabajo y comprometer a los jefes de los responsables de su ejecución	**Resultado esperado:** *Plan de acciones correctivas *Plan de acciones de mejora	nov-15	nov-15	**Realizado**
COM11	Mejorar	Comunicación	Comunicar el plan de acciones correctivas y de mejora (auditoría interna)	*Se han aprobado los planes de acción para atender los hallazgos de la auditoría	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Personal involucrado	**Documentos:** *Plan de acciones correctivas *Plan de acciones de mejora	1. Comunicar las actividades asignadas a cada responsable	**Resultado esperado:** *Registros de comunicación (correo)	dic-15	dic-15	**Realizado**
OPE19	Mejorar	Operación	Ejecutar el plan de acciones correctivas y de mejora (auditoría interna)	*Se han aprobado los planes de acción para atender los hallazgos de la auditoría	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal involucrado	**Documentos:** *Plan de acciones correctivas *Plan de acciones de mejora	1. Implementar las acciones comprometidas en los planes y reportar avances	**Resultado esperado:** *Implementación de: Plan de acciones correctivas y Plan de acciones de mejora	dic-15	nov-16	**En proceso**
COM12	Mantener	Comunicación	Comunicar las convocatorias a la revisión por la dirección	*Ha transcurrido un periodo desde la última revisión por la dirección *Ha ocurrido un evento significativo que compromete la seguridad de información	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Representante de la dirección *Representantes de los procesos	**Presentación:** *Resumen ejecutivo de la operación del SGSI	1. Comunicar y acordar la fecha de reunión con los participantes	**Resultado esperado:** *Registros de comunicación (correo)	dic-15	dic-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
OPE20	Mantener	Operación	Realizar la revisión por la dirección	*Se ha oficializado la convocatoria a la revisión por la dirección	**Responsable:** *Representante de la dirección **Convocado:** *Coordinador de seguridad de información *Representantes de los procesos	**Presentación:** *Resumen ejecutivo de la operación del SGSI **Documentos:** ***Acta de revisión por la dirección (previa, si existe) *Informe de contexto de la organización *Informe de resultados de la auditoría interna *Plan de acciones correctivas *Plan de acciones de mejora *Plan de métricas de seguridad de información *Plan de objetivos de seguridad de información *Plan de tratamiento de riesgos	1. Revisar los resultados de la operación del SGSI 2. Establecer y documentar en un acta las decisiones que la dirección ha decidido en base a los resultados obtenidos.	**Resultado esperado:** *Acta de revisión por la dirección (nueva)	dic-15	dic-15	**Realizado**
OPE21	Mejorar	Operación	Establecer acciones correctivas y de mejora (revisión por la dirección)	*Se ha suscrito el Acta de revisión por la dirección	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Representante de la dirección *Representantes de los procesos	**Documentos:** *Acta de revisión por la dirección	1. Establecer tareas y responsables para atender las disposiciones de la dirección 2. Aprobar los planes de trabajo y comprometer a los jefes de los responsables de su ejecución	**Resultado esperado:** *Plan de acciones correctivas *Plan de acciones de mejora	dic-15	dic-15	**Realizado**
COM13	Mejorar	Comunicación	Comunicar el plan de acciones correctivas y de mejora (revisión por la dirección)	*Se han aprobado los planes de acción para atender las disposiciones de la dirección	**Emisor:** *Coordinador de seguridad de información **Receptor:** *Personal involucrado	**Documentos:** *Plan de acciones de mejora (nuevas acciones)	1. Comunicar las actividades asignadas a cada responsable	**Resultado esperado:** *Registros de comunicación (correo)	dic-15	dic-15	**Realizado**

Plan de operación y comunicaciones del SGSI											
ID	**Etapa**	**Tipo**	**Acción**	**Condiciones**	**Involucrados**	**Recursos**	**Tareas**	**Efectividad**	**Inicio**	**Cierre**	**Resultado**
OPE22	Mejorar	Operación	Ejecutar el plan de acciones correctivas y de mejora (revisión por la dirección)	*Se han aprobado los planes de acción para atender las disposiciones de la dirección	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal involucrado	**Documentos:** *Plan de acciones de mejora (nuevas acciones)	1. Implementar las acciones comprometidas en los planes y reportar avances	**Resultado esperado:** *Implementación de: Plan de acciones correctivas, Plan de acciones de mejora	dic-15	nov-16	**En proceso**

Anexo B. Informe de contexto de la organización

Descripción: Informe que analiza el contexto interno y externo vigente en la organización y establece el marco sobre el cual se realizará la gestión de riesgos.
Aprobado: Versión 1.0 por Representante de la Dirección

Estructura:

- **Contexto externo**
    - Partes interesadas externas
    - Entorno político, legal, reglamentario y contractual
    - Entorno competitivo
    - Entorno social, cultural y natural
    - Entorno económico y financiero
    - Entorno tecnológico
- **Contexto interno**
    - Partes interesadas internas
    - Misión y objetivos estratégicos
    - Procesos de la organización
    - Organización y funciones
    - Recursos disponibles
    - Tecnología vigente
- **Contexto del proceso de gestión del riesgo**
    - Objetivo
    - Estrategia
    - Alcance
    - Parámetros
- **Criterios de riesgo**
- **Procesos críticos respecto a la seguridad de información**

A continuación se desarrollan los aspectos del contexto interno y externo que podrían intervenir en el logro del propósito de la organización y los resultados que se espera obtener del SGSI.

Además, se muestran los elementos relacionados al contexto y criterios de riesgo, a partir de los cuales se realizará la gestión de riesgos de seguridad de información del proceso.

Finalmente, se identifican los procesos que se han determinado como críticos para el negocio, como resultado del entendimiento y evaluación del contexto.

Contexto externo

Aspectos externos	Detalle
AE1. Partes interesadas externas	**Clientes:** Organizaciones que tienen necesidades relacionadas a la implementación y mantenimiento del software, bajo un nivel adecuado de calidad. **Proveedores:** Organizaciones que ofertan insumos, servicios tecnológicos (consultoría, soporte, internet) y servicios generales (limpieza, vigilancia). **Competidores:** Empresas del rubro de desarrollo de software, algunas de las cuales están asociadas a APESOFT. **Reguladores:** Agencias del gobierno que supervisan el cumplimiento de reglamentos y leyes, relacionadas a seguridad de información: ONGEI (PCM), la ANPDP (Ministerio de Justicia).
AE2. Entorno político, legal, reglamentario y contractual	**Político:** En el Perú, no existen restricciones respecto al ámbito de los servicios de consultoría en software, siempre y cuando esto no conlleve al incumplimiento de la ley. **Legal y reglamentario:** Las MYPES cuentan con la ley 28015, aunque esta no cuenta con disposiciones relacionadas a la seguridad de información. El estado peruano dispone de leyes y normas, algunas de las cuales guardan relación con la seguridad de información; entre estas destacan: • Ley de Protección de Datos Personales – 29733. Aplicable a todas las organizaciones • Ley sobre el Derecho de Autor – DL 822. Relevante para el uso de software licenciado. • Ley de Delitos Informáticos – 30096. Aplicable a la confidencialidad e integridad de la información de los sistemas informáticos de clientes. **Contractual:** Para establecer relaciones con el sector público o privado se firman contratos, en base a los cuales se determina el pago, condiciones de entrega y fecha. En caso de incumplir los contratos el proveedor de servicio está sujeto a penalidades, de acuerdo a lo que establezca el acuerdo. En el caso particular del estado como cliente, existen condiciones más restrictivas, las cuales son establecidas en las bases de los proyectos (Ley 30225).
AE3. Entorno competitivo	**Competencia:** El medio de empresas de consultoría en software es altamente competitivo y cuenta con empresas bien posicionadas, algunas de las cuales se encuentran suscritas a APESOFT. Sin embargo, la aparición constante de nuevas tecnologías (lenguajes de programación, plataformas, hardware) permite que una empresa nueva pueda incursionar exitosamente en uno de los nuevos segmentos especializados de este mercado.
AE4. Entorno social, cultural y natural	**Cultural:** El idioma predominante para la elaboración de productos (informes, diagramas de análisis, manuales) es el español. Sin embargo, en la codificación del software muchos proyectos manejan sus estándares en base a una nomenclatura inglesa. **Social:** El entorno social presenta riesgos criminales respecto a las empresas (casos de extorsión, aunque predominan en otros rubros como construcción y comercio). Las marchas o protestas, en el caso de entidades privadas son casi nulas, a diferencia de las del estado. **Natural:** Lima se encuentra en una zona sísmica, son frecuentes los temblores (2 importantes al año) y se tiene previsión de un terremoto en los años próximos. No hay epidemias significativas. El fenómeno del niño suele afectar con un impacto medio a la ciudad debido a precipitaciones fuertes y aumento de la temperatura.
AE5. Entorno económico y financiero	**Económico:** Actualmente, pese a la desaceleración de la economía, las empresas públicas y privadas siguen invirtiendo en proyectos tercerizados para la implementación y mantenimiento de software, e incluso muchas los han programado en sus planes estratégicos (PETI). **Financiero:** La tendencia a la inversión en automatización permanece, por encima de la contratación de personal adicional para realizar funciones operativas.
AE6. Entorno tecnológico	**Tecnología:** En la actualidad, se ha diversificado y abaratado la oferta de servicios tecnológicos remotos: housing, hosting, software como servicio (SAAS), computación en la "nube" o capacitaciones en línea. Por otro lado, la demanda tecnológica se orienta a solicitar software predominantemente web o móvil, que soporte estos nuevos modelos de operación.

Contexto interno

Aspectos internos	Detalle
AI1. Partes interesadas internas	**Dirección:** Socios y gerentes que lideran a la organización. **Gestor de proyecto:** Responsables de administrar los proyectos de desarrollo, incluye al jefe de aseguramiento de calidad. **Operador:** Consultores (analistas / programadores), analistas de calidad, responsables de los servicios de desarrollo de software y del servicio interno de control de calidad. **Operador TIC:** Especialistas encargados de la administración de las plataformas e infraestructura de TI que existe en la organización. **Coordinador de seguridad de información:** Responsable de implementar y operar el SGSI y realizar otras actividades relacionadas a la seguridad de información.
AI2. Misión y objetivos estratégicos	**Propósito** **Misión:** Mejorar la productividad de las empresas peruanas brindando servicios de consultoría en software para que cuenten con soluciones informáticas de calidad, que permitan automatizar sus procesos de manera eficiente y segura. **Resultados esperados** **Visión:** Ser la empresa del rubro con mayor crecimiento de participación en el mercado nacional en el siguiente quinquenio. **Objetivos Estratégicos:** **OE1:** Mejorar la satisfacción de los clientes respecto a los servicios recibidos **OE2:** Fomentar la excelencia del personal que brinda los servicios de consultoría **OE3:** Incrementar la efectividad y productividad de los proyectos de consultoría
AI3. Procesos de la organización	**Procesos estratégicos:** A1. Gestión de la dirección (planificación y recursos) A2. Gestión comercial (ventas y prospectiva de servicios) **Procesos operacionales:** B1. Gestión de proyectos de consultoría B2. Ejecución de servicios de desarrollo y mantenimiento de software B3. Aseguramiento de la calidad del software **Procesos de apoyo:** C1. Gestión de la contabilidad y finanzas C2. Gestión de recursos humanos C3. Gestión de tecnología e infraestructura C4. Gestión de logística y patrimonio
AI4. Organización y funciones	**Gerencia general:** Dirección general de la organización, socio fundador principal. **Gerencia de administración y finanzas:** Maneja la administración de las finanzas, tesorería, activos, proveedores, recursos humanos y el soporte tecnológico. **Gerencia comercial (Gerente de cuentas):** Administra las relaciones y oportunidades comerciales, en las líneas de servicio de la consultora. **Gerencia de operaciones:** Administra los equipos de trabajo para los servicios de consultoría de software, así como también el servicio interno de calidad de software. **Gerencia de servicios TIC:** Administra al servicio interno de soporte tecnológico, así como las plataformas e infraestructura tecnológica de la organización.
AI5. Recursos disponibles	**Personal:** El personal de la organización cuenta con conocimientos relacionados al ciclo de desarrollo de software (lenguajes, metodologías, plataformas); sin embargo, respecto a la seguridad de información, solo el coordinador tiene conocimientos profundos. **Sede:** El local es de material noble, con instalaciones de red y eléctricas relativamente nuevas (2 años), se encuentra ubicado en un distrito de seguridad media, en Lima.
AI6. Tecnología vigente	**Sistemas:** Repositorio general de proyectos (Versionado de Archivos), Sistema de administración y finanzas (ERP). **Software:** Licencias de software de ofimática, desarrollo y gestión de bases de datos. **Equipos:** Se cuenta con equipos de escritorio y laptops, además de servidores de archivos, bases de datos y aplicaciones. **Servicios:** Servicios de almacenamiento remoto, acceso a Internet, además de servicios de soporte tecnológico.

Contexto del proceso de gestión del riesgo

Aspectos	Detalle
Objetivo	Prevenir la materialización de riesgos de seguridad de la información que impacten en la organización, mediante su identificación, evaluación y tratamiento.
Estrategia	Aplicar la **Metodología de Gestión de Riesgos** con los parámetros establecidos en base al contexto de la organización
Alcance	La gestión de riesgos se realiza sobre los procesos delimitados en la **Declaración de alcance del SGSI** vigente.
Parámetros	• **Procesos.** La gestión de riesgos se aplicará sobre todos aquellos procesos definidos en el alcance. • **Recursos.** Sala multiusos de la empresa, horas de trabajo del personal convocado. • **Responsabilidades.** Todos los jefes de los procesos involucrados deben participar o enviar a representantes para que participen en el proceso. Eso no los excluye de su obligación final de revisar y firmar el acta donde se reconocen los resultados de la evaluación y tratamiento de riesgos, así como de la respectiva aprobación del riesgo residual y los riesgos aceptados. • **Autoridades.** El Coordinador de Seguridad, empoderado por el Representante de la Dirección convoca a los Jefes de las áreas participantes (procesos dentro del alcance) y al Jefe de Tecnología y Soporte, como especialista técnico. • **Metodología.** La **Metodología de Gestión de Riesgos**, establece los pasos para identificar y valorar el riesgo, así como evaluar la eficacia de la gestión de riesgos (seguimiento).

Criterios de riesgo

Criterios de riesgo	En la **Metodología de Gestión de Riesgos** se documenta la estrategia para identificar, analizar y atender los riesgos, mediante los siguientes criterios: • **Frecuencia.** Condiciones para efectuar la gestión de riesgos. • **Niveles de consecuencias.** Criterios del impacto producido • **Niveles de probabilidad.** Criterios de la ocurrencia posible • **Cálculo del nivel de riesgo.** Formulación en base a la consecuencia y probabilidad • **Nivel de aceptación del riesgo.** Umbral del nivel de riesgo aceptable • **Criterios de aceptación de riesgos.** Criterio que excluye del tratamiento a un riesgo no aceptable

Procesos críticos respecto a la seguridad de información

Tras identificar el contexto externo e interno, se determina que los procesos donde la información es más crítica para el **propósito** y los **resultados esperados** de la organización, son aquellos enfocados directamente en el negocio, excluyendo los de soporte o administración:

- B1. Gestión de proyectos de consultoría
- B2. Ejecución de servicios de desarrollo y mantenimiento de software
- B3. Aseguramiento de la calidad del software

Anexo C. Informe de necesidades y expectativas de las partes interesadas

Descripción: Informe que lista a las partes interesadas internas y externas, e identifica sus necesidades y expectativas (requisitos) relacionados a la seguridad de información.
Aprobado: Versión 1.0 por Representante de la Dirección

Estructura:

- Generalidades
- Requisitos de partes interesadas

Generalidades

Durante el entendimiento del contexto de la organización se identificaron las partes interesadas internas y externas según las definiciones que se muestran:

Partes interesadas internas:

- **Dirección:** Socios y gerentes que lideran a la organización.
- **Gestor de proyecto:** Responsables de administrar los proyectos de desarrollo, incluye al jefe de aseguramiento de calidad.
- **Operador:** Consultores (analistas / programadores), analistas de calidad, responsables de los servicios de desarrollo de software y del servicio interno de control de calidad.
- **Operador TIC:** Especialistas encargados de la administración de las plataformas e infraestructura de TI que existe en la organización.
- **Coordinador de seguridad de información:** Responsable de implementar y operar el SGSI y realizar otras actividades relacionadas a la seguridad de información.

Partes interesadas externas:

- **Clientes:** Organizaciones que tienen necesidades relacionadas a la implementación y mantenimiento del software, bajo un nivel adecuado de calidad.
- **Proveedores:** Organizaciones que ofertan insumos, servicios tecnológicos (consultoría, soporte, internet) y servicios generales (limpieza, vigilancia).
- **Competidores:** Empresas del rubro de desarrollo de software, algunas de las cuales están asociadas a APESOFT.
- **Reguladores:** Agencias del gobierno que supervisan el cumplimiento de reglamentos y leyes, relacionadas a la seguridad de información: ONGEI (PCM), la ANPDP (Ministerio de Justicia), INDECOPI (PCM).

Para cada uno de los grupos indicados, se ha evaluado si existen requisitos relacionados a la seguridad de información, que corresponden a: necesidades, expectativas, acuerdos contractuales, leyes aplicables, restricciones y, en general, toda relación existente entre la parte interesada y la organización, relacionada a la seguridad de información.

Requisitos de partes interesadas

Se han realizado reuniones para definir con las partes interesadas disponibles los requisitos de la seguridad de información que representan necesidades (obligaciones de carácter legal, contractual, regulatorio interno) o expectativas (metas del negocio en alguno de sus aspectos).

Requisitos de Seguridad de Información	Tipo	Partes interesadas	Sustento
Contratos y acuerdos con clientes (Confidencialidad, Integridad, Disponibilidad): Cumplir con las condiciones de seguridad de información asumidas con el cliente en el contrato y acuerdos relacionados a la seguridad de información.	**N**	**Externas:** Clientes. **Internas:** Dirección (Gerente de operación), Gestor de proyecto	Su incumplimiento puede generar penalidades asociadas a los proyectos.
Contratos y acuerdos con el personal (Confidencialidad, Integridad, Disponibilidad): Asegurar el cumplimiento de las condiciones de seguridad de información asumidas por el personal en el contrato y acuerdos de confidencialidad y reconocimiento de las políticas de seguridad de información.	**N**	**Internas:** Dirección (Gerente de operación, Gerente de administración), Gestor de proyecto, Coordinador de seguridad de información	Su incumplimiento puede generar penalidades asociadas a los proyectos.
Contratos con proveedores de servicios TI (Disponibilidad): Asegurar el cumplimiento de los niveles de servicio respecto a los servicios tecnológicos que sirven de base para la elaboración de los productos.	**N**	**Externas:** Proveedores. **Internas:** Dirección (Gerente de operación), Gestor de proyecto, Operadores (Consultores)	Los servicios de TI externos intervienen en los procesos centrales del negocio.
Ley de Protección de Datos Personales (Confidencialidad): Cumplir con la Ley y su Reglamento, aplicable solo a la información tratada de los trabajadores de la consultora (no existen proyectos con clientes que involucren información personal).	**N**	**Externas:** Reguladores (ANPDP). **Internas:** Dirección, Coordinador de seguridad de información	Su incumplimiento puede generar sanciones económicas a la organización.
Ley sobre el Derecho de Autor (Integridad): Cumplir con la Ley, aplicable sobre la autenticidad del software usado en los procesos de consultoría de la organización.	**N**	**Externas:** Reguladores (INDECOPI). **Internas:** Dirección, Coordinador de seguridad de información	Su incumplimiento puede generar sanciones económicas y legales a la organización.
Ley de Delitos Informáticos (Confidencialidad, Integridad): Cumplir con la Ley, aplicable sobre los productos (sistemas y aplicaciones) que se entregan a los clientes.	**N**	**Externas:** Reguladores (MINJUS). **Internas:** Dirección, Coordinador de seguridad de información	Su incumplimiento puede generar sanciones legales a la organización.
Entrega de productos a clientes (Integridad): Prevenir fallos en las entregas del producto (incompletas o mal versionadas).	**E**	**Externas:** Clientes. **Internas:** Dirección (Gerente de Operación), Gestor de proyecto	Es la principal prioridad del negocio, su incumplimiento se asocia a penalidades.

Anexo D. Declaración de alcance del SGSI

Descripción: Alcance definido para el sistema, especificando los límites de aplicación respecto a procesos, áreas, personal, roles, activos, servicios, ubicación y requisitos.
Aprobado: Versión 1.0 por Representante de la Dirección
Estructura:

- Generalidades
- Procesos y áreas involucradas
- Información de los procesos
- Personal y organización
- Activos y servicios
- Ubicación
- Requisitos de seguridad de información gestionados por el sistema

Generalidades

Para elaborar el **Alcance del SGSI**, se han tomado en cuenta los siguientes informes:

- **Informe de contexto de la organización.** Que contiene una sección de **Procesos críticos respecto a la seguridad de información**.
- **Informe de necesidades y expectativas de las partes interesadas.** Que contiene una sección de **Requisitos de partes interesadas**.

En base a la información recopilada, la dirección ha identificado los procesos en los que la información es más relevante o crítica para la organización, además de aquellos requisitos cuyo cumplimiento es relevante. Por lo que, ha determinado:

- Incorporar dentro del alcance del SGSI aquellos procesos de negocio identificados en el informe de contexto, para el presente periodo.
- Excluir del alcance los demás procesos de la organización.
- Para el caso de los requisitos de seguridad de información identificados, se ha dispuesto su inclusión e implementación en el sistema mediante un **Plan de Requisitos de Seguridad de Información**.

Procesos y áreas involucradas

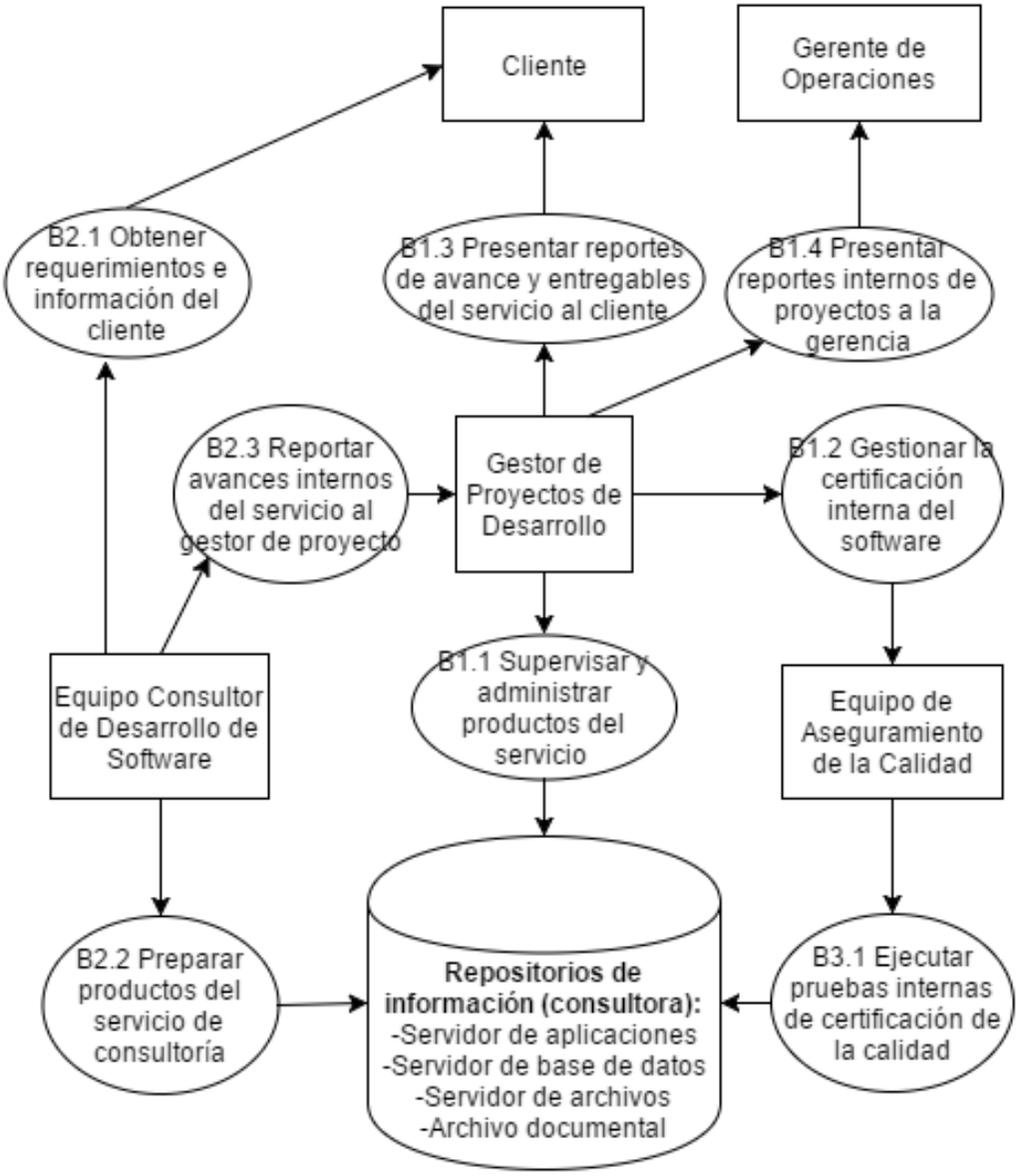
Los procesos considerados para el alcance del SGSI son los siguientes:

- B1. Gestión de proyectos de consultoría
- B2. Ejecución de servicios de desarrollo y mantenimiento de software
- B3. Aseguramiento de la calidad del software

Para la administración de estos procesos, el área encargada es la **Gerencia de operaciones**. Cabe resaltar que a esta gerencia la apoya la **Gerencia de servicios TIC** respecto a la administración del soporte tecnológico. Si bien las demás gerencias se relacionan al proceso, no todas tienen una relación directa con el foco del negocio. Por ello, solo algunos directivos de las mismas están involucrados en el SGSI, como parte del **Comité de Seguridad de Información**.

Información de los procesos

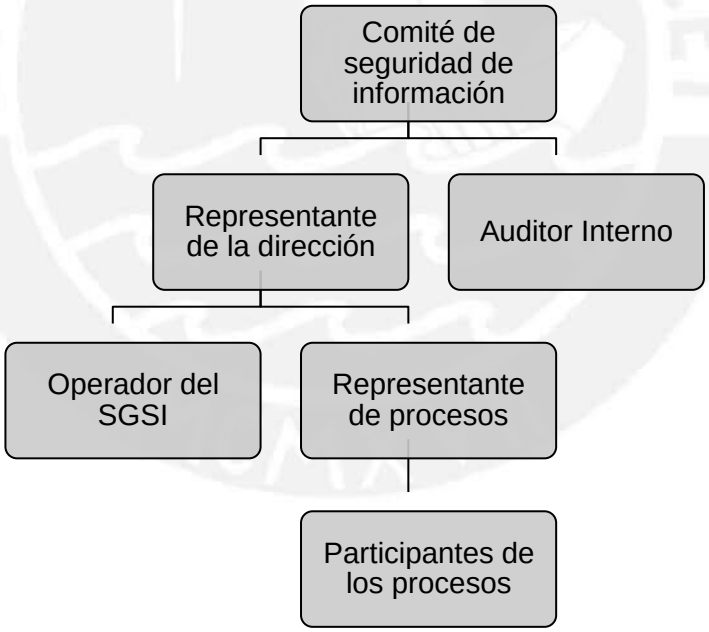
Los tres procesos seleccionados se encuentran directamente relacionados entre sí: **B1. Gestión de proyectos de consultoría, B2. Ejecución de servicios de desarrollo y mantenimiento de software, B3. Aseguramiento de la calidad del software**. Por ello, para un mayor entendimiento de las actividades y las relaciones que tienen entre ellos, se esquematizan sus componentes y relaciones en un diagrama único, como un **Diagrama de Flujo de Datos**:



Personal y organización

La organización alrededor del SGSI cuenta con el siguiente personal, organizado en las jerarquías indicadas:

- **Comité de seguridad de información:**
  - Gerente general (presidente)
  - Gerente de administración y finanzas (miembro)
  - Gerente de operaciones (miembro)
  - Gerente de servicios TIC (miembro)
  - Coordinador de seguridad de información (secretario)
- **Representante de la dirección:** Gerente general, principal socio fundador de la organización, responsable de la orientación estratégica.
- **Representante de procesos - Principal:** Gerente de operaciones, dueño de los procesos involucrados en el alcance del SGSI.
- **Representante de procesos - Soporte:** Gerente de servicios TIC, administra al servicio interno de soporte tecnológico, así como las plataformas e infraestructura tecnológica de la organización.
- **Participantes del proceso:** Jefes de proyecto y operadores (consultores de desarrollo y analistas de calidad) más antiguos, principales conocedores de los ciclos en los que operan los procesos (servicios de desarrollo, mantenimiento y calidad)
- **Operador del SGSI:** Coordinador de seguridad de información, responsable de gestionar y ejecutar las actividades para la operación del sistema
- **Auditor interno:** Auditor en ISO27001 independiente de los procesos



Los roles y responsabilidades de la organización mostrada se encuentran documentados en la **Política específica de seguridad de información** en la sección de **Roles y Responsabilidades de Seguridad de Información**.

Activos y servicios

Para los procesos que forman parte del alcance del SGSI se manejan los siguientes activos y servicios relacionados a la información:

Activos:

- Equipos portátiles (laptops)
- Equipos de escritorio (computadoras)
- Dispositivos de información móviles (USB, discos duros externos, DVD)
- Sistema de gestión de proyectos
- Sistema de versionado de archivos
- Software de desarrollo
- Software de documentación del análisis

Servicios:

- Servicio de red interna
- Servicio de internet
- Servicio de impresión
- Servicio de almacenamiento de archivos local
- Servicio de soporte tecnológico
- Servicio de energía eléctrica

Cabe indicar que si bien los elementos listados comprenden servidores, switches, routers, cableado de red, red eléctrica, tablero eléctrico, y otros elementos particulares, de cara a los procesos que forman parte del alcance del SGSI, estos solo los consideran en conjunto, como parte de los servicios y tecnología que han sido listados.

Ubicación

Los procesos dentro del alcance se desarrollan en la sede principal de la empresa, ubicada en el distrito de **San Borja**, en la ciudad de Lima, en un edificio de 3 plantas con instalaciones de red y eléctricas con una antigüedad de 5 años, que cuenta con un perímetro de seguridad y control de acceso por un servicio de vigilancia externo.

Cabe destacar que los equipos de operadores de servicio (consultores) eventualmente son destacados a los clientes para realizar tareas de relevamiento de información, principalmente, en los siguientes distritos:

- Cercado de Lima
- Miraflores
- San Borja
- San Isidro
- San Miguel

Requisitos de seguridad de información gestionados por el sistema

Los requisitos relevantes para la organización, que son asumidos por el SGSI, son los siguientes:

- **Contratos y acuerdos con clientes (Confidencialidad, Integridad, Disponibilidad):** Cumplir con las condiciones de seguridad de información asumidas con el cliente en el contrato y acuerdos relacionados a la seguridad de información.
- **Contratos y acuerdos con el personal (Confidencialidad, Integridad, Disponibilidad):** Asegurar el cumplimiento de las condiciones de seguridad de información asumidas por el personal en el contrato y acuerdos de confidencialidad y reconocimiento de las políticas de seguridad de información.
- **Contratos con proveedores de servicios TI (Disponibilidad):** Asegurar el cumplimiento de los niveles de servicio respecto a los servicios tecnológicos que sirven de base para la elaboración de los productos.
- **Ley de Protección de Datos Personales (Confidencialidad):** Cumplir con la Ley y su Reglamento, aplicable solo a la información tratada de los trabajadores de la consultora (no existen proyectos con clientes que involucren información personal).
- **Ley sobre el Derecho de Autor (Integridad):** Cumplir con la Ley, aplicable sobre la autenticidad del software usado en los procesos de consultoría de la organización.
- **Ley de Delitos Informáticos (Confidencialidad, Integridad):** Cumplir con la Ley, aplicable sobre los productos (sistemas y aplicaciones) que se entregan a los clientes.
- **Entrega de productos a clientes (Integridad):** Prevenir fallos en las entregas del producto (incompletas o mal versionadas).

Anexo E. Política de seguridad de información

Descripción: Documento que da la orientación y disposiciones generales para la gestión de la seguridad de información dentro de la organización, dada por la dirección.
Aprobado: Versión 1.0 por Representante de la Dirección

La empresa consultora es consciente de la importancia que tiene la información que produce para brindar sus servicios de consultoría de software, así como también aquella que recibe, con el mismo fin, desde sus clientes. Además, reconoce que en la actualidad, en el contexto donde opera, existen muchos riesgos sobre la información que pueden comprometer su **confidencialidad, integridad y disponibilidad**, razón por la cual se compromete a realizar esfuerzos para salvaguardarla en estos tres aspectos.

Por este motivo se dispone establecer una **Declaración de objetivos de seguridad de información**, alineados a los objetivos estratégicos de la consultora, de manera que estos se planifiquen, ejecuten y concreten a un nivel razonable en la organización, mediante el **Plan de Objetivos de Seguridad de Información**.

Además, la organización ha identificado las necesidades y expectativas en seguridad de información, los cuales busca cumplir a través de la ejecución del **Plan de Requisitos de Seguridad de Información**.

Para conseguirlo, ha implementado un **Sistema de Gestión de Seguridad de Información (SGSI)**, que opera permanentemente y se orienta a la mejora continua del mismo y los procesos que forman parte de su alcance.

Se dispone la publicación de la presente política a todo el personal y la comunicación de la misma a todos aquellos interesados o afectados, por su relación con la organización.

Gerencia general

Anexo F. Políticas específicas de seguridad de información

Descripción: Disposiciones específicas para la definición y aplicación de los controles de seguridad de información.
Aprobado: Versión 1.0 por Representante de la Dirección

1. Roles, responsabilidades y autoridades

1.1. Se cuenta con los siguientes roles y responsabilidades relacionados a la seguridad de información y a la operación del SGSI:

a. Comité de seguridad de información. Rol asumido por un presidente (Gerente general) y diversos miembros que representan a las principales áreas involucradas en el SGSI (Gerente de administración y finanzas, Gerente de operaciones, Gerente de servicios TIC y el Coordinador de seguridad de información, como secretario). Este grupo participa de las siguientes actividades:

i Aprobar el diseño de las actividades para la operación y comunicaciones del SGSI.
ii Validar y aprobar la documentación del SGSI: Políticas y alcance.
iii Participar de la auditoría interna del SGSI, en caso alguno de sus miembros sea convocado por el auditor.
iv Participar y tomar decisiones a partir de la revisión por la dirección que se realiza en cada periodo de operación del SGSI.

b. Representante de la dirección. Rol asumido por el Gerente general; participa de las siguientes actividades:

i Aprobar el diseño de las actividades para la operación y comunicaciones del SGSI.
ii Validar y aprobar la documentación del SGSI: Políticas (general y específica de seguridad de información), declaraciones (alcance, objetivos), planes, informes y procedimientos.
iii Promover la asistencia a las charlas y capacitaciones en seguridad de información, así como la difusión de la Política de Seguridad de Información.
iv Aprobar la designación de recursos (personal, insumos, servicios) consignados en los planes del SGSI.
v Participar de las auditorías internas, según lo planificado.
vi Liderar las sesiones de revisión por la dirección, así como también tomar decisiones a partir de los resultados reportados.

c. Representante de procesos / Propietario del riesgo. Rol asumido por el Gerente de operaciones (Procesos Principales) y el Gerente de servicios TIC (Procesos de Soporte). Son propietarios del riesgo cuando están asociados directamente a riesgos identificados durante la gestión de riesgos. Participan de las siguientes actividades:

i Participar de la elaboración de la documentación requerida para las actividades del SGSI (procedimientos, planes, informes, declaraciones)
ii Identificar, evaluar, tratar y gestionar riesgos de seguridad de información, asociadas a sus procesos

iii Participar de las charlas y capacitaciones en seguridad de información.
iv Participar de las auditorías internas, según lo planificado.
v Colaborar con la definición y ejecución de las acciones correctivas y de mejora del sistema.
vi **Propietario del Riesgo.** Aceptar formalmente el nivel de los riesgos residuales; aprobar el plan de tratamiento de los riesgos; participar de la implementación o mejora de los controles involucrados en el tratamiento del riesgo.

d. Participantes del proceso. Rol asumido por el personal que pertenece a los procesos dentro del alcance (Jefes de proyecto y de calidad, analistas, consultores, operadores); son convocados a discreción de los representantes de los procesos para participar de las siguientes actividades:

i Participar de las actividades en que sean convocados por los representantes de los procesos.
ii Participar de la gestión de riesgos de seguridad de información.
iii Participar de las charlas y capacitaciones en seguridad de información.
iv Participar de las auditorías internas, según lo planificado.
v Colaborar con la definición y ejecución de las acciones correctivas y de mejora del sistema.

e. Operador del SGSI. Rol asumido por el Coordinador de Seguridad de Información; participa de las siguientes actividades:

i Diseñar las actividades para la operación del SGSI y gestionar su ejecución una vez aprobadas.
ii Diseñar el esquema de comunicaciones del SGSI y gestionar su ejecución una vez aprobado.
iii Participar de la elaboración de la documentación requerida para las actividades del SGSI (procedimientos, planes).
iv Participar de la elaboración de la documentación requerida para las actividades del SGSI (procedimientos, planes, informes, declaraciones).
v Liderar y brindar orientación a los participantes de la gestión de riesgos de seguridad de información.
vi Realizar o gestionar la realización de las charlas y capacitaciones en seguridad de información.
vii Participar de las auditorías internas, según lo planificado.
viii Gestionar la definición y ejecución de las acciones correctivas y de mejora del sistema.

f. Auditor interno. Rol asumido por el Auditor designado por la organización: externo (tercero) o interno (pero independiente del alcance del SGSI); participa de las siguientes actividades:

i Propone el Plan de Auditoría Interna.
ii Ejecuta las sesiones, inspecciones, pruebas y revisión de evidencias relacionadas a la auditoría interna del SGSI
iii Elabora y presenta el Informe de resultados de la auditoría interna.

2. Requisitos legales

2.1. El responsable de identificar toda aquella legislación aplicable a la organización que pueda afectar a la seguridad de información es el Gerente de Administración, el cual contará con la asesoría del Coordinador de Seguridad de Información para tal fin.
2.2. Se reconocen, para la organización, todas las leyes que el estado peruano disponga como aplicables. Para el caso particular de la seguridad de información se reconoce a las siguientes: Ley de Protección de Datos Personales, Ley sobre el Derecho de Autor, Ley de Delitos Informáticos.
2.3. No se incluye el teletrabajo dentro del marco normativo aplicable, debido a que la organización no maneja esta modalidad laboral.

3. Charlas y capacitación

3.1. Se deben realizar periódicamente actividades de sensibilización y comunicación de eventos relevantes, relacionados a la seguridad de información.
3.2. En los casos en que el personal asuma roles, como participante activo del sistema de gestión, este será evaluado para asegurar su competencia.
3.3. Todo personal que ingrese a trabajar a la organización, sea interno o externo, deberá recibir una inducción para informarse respecto a los lineamientos vigentes en la organización, respecto a la seguridad de información.

4. Riesgos, incidentes y especialistas

4.1. Se denominará gestión de riesgos a la labor de identificar, analizar, evaluar y tratar a los riesgos negativos y positivos (oportunidades) relacionados a la seguridad de información.
4.2. Las condiciones para realizar una nueva gestión de riesgos, los parámetros específicos para su desarrollo y la forma en que se harán están definidos en la **Metodología de Gestión de Riesgos**.
4.3. Todo personal que trabaje en la organización está obligado a reportar eventos (ocurrencias relacionadas a la seguridad de información), incidentes (ocurrencias que generen un impacto negativo) y debilidades (fallos de control que generen potenciales ocurrencias), incluso si no está seguro de que lo sean.
4.4. En el caso de los incidentes, eventos y debilidades se aplicará para su identificación, reporte y atención el **Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información**.
4.5. Es responsabilidad del Coordinador de seguridad de información y del personal de la Gerencia de servicios TIC mantener el contacto con los especialistas externos, ante la necesidad de atender incidentes complejos o de mayor especialización.

5. Continuidad de negocio

5.1. La operación de la organización en escenarios de desastres o interrupciones significativas serán planificadas, implementadas y probadas en base al **Plan operativo de continuidad**.
5.2. Solo podrán omitirse temporalmente aquellos controles de seguridad de información respecto a los cuales el plan lo indique expresamente. La omisión de otros no indicados, se considerará un incumplimiento.

6. Gestión de documentos

6.1. Todo documento producido para el SGSI o sobre controles de seguridad de información debe contener los siguientes atributos de:
   a. Identificación: título y descripción.
   b. Aprobación: versión y aprobador.

6.2. Todos estos documentos serán emitidos en idioma español, en medio digital (formato de la familia Office: Word, Excel, y los que correspondan). Sin embargo, si para efectos de firma o algún registro manuscrito, se produce documentación en físico o impresa, esta deberá ser digitalizada (en formato PDF).

6.3. Todos los documentos aprobados y producidos por la operación del SGSI serán almacenados en la carpeta de red **Seguridad de Información**, que es el repositorio oficial de las últimas versiones de la documentación del sistema.

6.4. Todos los documentos del SGSI contarán con las siguientes restricciones de uso en aspectos de:
   a. Confidencialidad: control de acceso, distribución y disposición (por desuso).
   b. Integridad: cambios controlados (versiones), almacenamiento y preservación.
   c. Disponibilidad: accesibilidad y legibilidad.

6.5. Todos los documentos de origen externo, que sean requeridos para la operación del SGSI, serán incorporados en el repositorio y se le antepondrán las siglas EXT al nombre del archivo.

7. Prácticas Generales de Seguridad

7.1. La organización reconoce un conjunto de buenas prácticas de seguridad de información las cuales deben ser acatadas de forma obligatoria a nivel personal y de áreas, según se indica a continuación:
   a. Personales:
      i Toda persona que se retira de su lugar de trabajo de manera temporal o al finalizar su turno debe bloquear la pantalla de su equipo.
      ii Asimismo, es responsable de no dejar en su escritorio expuesta información sensible, ya sea documental o en dispositivos que puedan ser sustraídos o copiados (USB, agendas, entre otros).
      iii Bajo ninguna circunstancia se permite el uso compartido de contraseñas, ni la publicación de las mismas mediante etiquetas u otros medios expuestos.
      iv No se permite la instalación de software personal en los equipos de cómputo, solo la Gerencia de servicios TIC está autorizada a instalar o cambiar las configuraciones y el software de los equipos de trabajo.
      v Los dispositivos celulares personales no deben ser conectados a los equipos de cómputo de la organización, ni siquiera si esto se realiza solo para la carga eléctrica del dispositivo.
      vi Solo pueden ser usados los dispositivos USB y discos externos autorizados por la organización, y para el personal autorizado por la organización.

b. Organizacionales
   i El traslado de cualquier activo que contenga información de la organización o sus clientes fuera de la sede debe estar autorizado por la jefatura propietaria del mismo.
   ii Todo cambio a nivel de infraestructura, personas, procesos o algún elemento importante de la misma debe ser controlado por la jefatura de la misma.
   iii Toda jefatura es responsable de asignar responsabilidades para su personal que no generen conflictos funcionales, riesgos o acaparamiento de poder.
   iv Todo proyecto está bajo la responsabilidad de la jefatura involucrada, la cual debe prever cualquier riesgo de seguridad de información que pueda existir a partir de su ejecución

8. Desarrollo de software

8.1. Se aplicarán buenas prácticas de seguridad de información antes, durante y después del desarrollo del software creado por la consultora:

a. Antes del desarrollo
   i Todo proyecto de desarrollo debe considerar la inclusión de requisitos no funcionalidades asociados a: criptografía, mecanismos de autenticación, pistas de auditoría, entre otros.
   ii Los proyectos de consultoría se centran en el desarrollo y mantenimiento de sistemas basados en código fuente, no se aplican actividades de decompilación o similares respecto a paquetes de software por considerarse riesgoso.
   iii Los responsables de la administración de accesos para el repositorio de código fuente son el gestor de proyectos y el gerente de operaciones.
   iv Los proyectos serán desarrollados dentro de los repositorios seguros y controlados, administrados por la organización.
   v Los espacios que contienen los productos de consultoría (código fuente y documentación) estarán sujetos permanentemente a un mecanismo de control de cambios.

b. Durante el desarrollo
   i Todo desarrollo para los servicios de consultoría se debe realizar en base al **Protocolo de desarrollo de software y productos del servicio**, que contiene prácticas seguras y estandarizadas para el ciclo de desarrollo.
   ii Se limita la inclusión de personal de empresas competidoras en el desarrollo de los proyectos, por considerarse un riesgo para el negocio.

c. Después del desarrollo
   i Se realizarán pruebas de calidad y seguridad sobre los productos, según el **Protocolo de pruebas sobre los sistemas y aplicaciones**.
   ii El desarrollo de pruebas debe considerarse obligatorio para los siguientes casos: pruebas planificadas, cambios de emergencia, e incluso cambios sobre la infraestructura que soporta a la aplicación o sistema.
   iii Los datos para pruebas sobre el software, sea que provengan o no de alguna fuente real del cliente, no pueden ser copiados sin autorización y su uso está restringido al personal asignado a realizar las pruebas.

9. Control del acceso lógico

9.1. Se consideran obligatorios los siguientes lineamientos, los cuales serán aplicados a través del **Procedimiento de gestión de accesos a servicios tecnológicos**:

a. El operador de servicios TIC es el responsable de asignar equipos de trabajo con acceso a la red interna de la organización, así como las sesiones para usarlo, y los respectivos niveles de privilegios de acceso a los servicios solicitados.
b. Para cualquier asignación de cuentas o permisos se requerirá la autorización del gerente del área del personal solicitante, esto no excluye al personal que administra las plataformas tecnológicas.
c. Se mantendrán pistas de auditoría tanto sobre el personal usuario de los servicios tecnológicos, como también sobre aquellos designados para su administración.
d. Las plataformas de administración del dominio mantendrán configuraciones que obliguen a los usuarios a mantener cuentas con contraseñas seguras, así como también otros parámetros de seguridad respecto a sus sesiones (bloqueo por inactividad, cambio de contraseña, entre otros)
e. Todos los servicios tecnológicos que contengan información de la organización, cuyo carácter no sea público, deberán estar sujetos a mecanismos de autenticación.
f. La Gerencia a la que pertenece el personal es la responsable de comunicar un cese o cambio de área para que se ejecuten de manera oportuna el retiro de accesos o actualización del usuario respectivo.
g. El operador de servicios TIC y el coordinador de seguridad de información realizarán revisiones periódicas de los accesos asignados al personal sobre todas las plataformas.
h. Solo el personal autorizado podrá usar programas de administración de plataformas. Mientras que el uso de otro tipo de programas utilitarios (eliminación de registros, vulneración de controles de seguridad) quedan prohibidos.

10. Seguridad informática

10.1. La gerencia de servicios TIC es la responsable de distribuir y aplicar controles criptográficos, bajo solicitud formal de una gerencia.

10.2. La organización aplica criptografía, para los siguientes casos:

a. Encriptamiento de dispositivos que cuentan con información sensible.
b. Aplicación de cifrado en comunicaciones seguras, para servicios TIC que usan llaves privadas/públicas o mecanismos similares.
c. Uso de dispositivos complementarios de autenticación del tipo token.

10.3. El personal de la gerencia de servicios TIC es responsable de mantener operativos los siguientes controles de seguridad de manera permanente:

a. Mecanismos antivirus y de detección de amenazas informáticas.
b. Registro de bitácoras de auditoría, sobre usuarios y administradores, autogeneradas por las plataformas, asegurando su no alternación o eliminación, sin autorización.
c. Ejecución periódica de análisis de vulnerabilidades sobre las plataformas informáticas, ya sea por el coordinador de seguridad de información o por algún proveedor externo especializado.

11. Equipos informáticos

11.1. El personal de la gerencia de servicios TIC es responsable de administrar los equipos informáticos de la organización, mediante las siguientes actividades:

a. Instalar o gestionar la instalación de los equipos informáticos adquiridos por la organización, adoptando las recomendaciones del fabricante y las mejores prácticas de seguridad.
b. Implementar mecanismos de contingencia eléctrica, y de prevención de daño eléctrico, para aquellos equipos que cuentan con necesidades altas de disponibilidad o que alojan información crítica para el negocio.
c. Ejecutar el mantenimiento preventivo en base al **Plan de mantenimiento y seguimiento de equipos**, así como el correctivo incidental.
d. Mantener el control de los equipos que son transferidos o dados de baja, en cuyo caso corresponderá la aplicación de controles de formateo o eliminación de los componentes que contienen información, según corresponda.

12. Gestión de plataformas

12.1. El personal de la gerencia de servicios TIC es responsable de administrar las plataformas informáticas de la organización, mediante las siguientes actividades:

a. Administrar la capacidad de procesamiento y almacenamiento del hardware y máquinas virtuales que contienen información, previendo riesgos de saturación u otros que comprometan su disponibilidad.
b. Mantener separados los ambientes de desarrollo y pruebas, donde los equipos de consultoría y de calidad trabajan, respectivamente.
c. Normalizar los registros de las plataformas a partir de una medida referencial única, para garantizar la integridad y coherencia de los registros producidos, así como para prevenir fallos de operación de servicios asociados al tiempo.
d. Administrar y probar, previamente, la instalación de software en las plataformas que alojan a los servidores.
e. Implementar mecanismos eléctricos, físicos y de contingencia suficientes para garantizar un nivel de disponibilidad acorde a las necesidades del negocio.

13. Gestión de redes

13.1. El personal de la gerencia de servicios TIC es responsable de administrar la infraestructura y servicios de comunicaciones de la organización, mediante las siguientes actividades:

a. Administrar los controles integrados a la red como son: el firewall, la DMZ, el IDS, IPS, la herramienta para administración del acceso a portales externos, entre otros.
b. Mantener una arquitectura segura de red: red interna independizada en segmentos (administración, calidad, consultoría) además aislada de la red externa (internet).
c. Mantener el servicio de correo electrónico bajo arquitectura y protocolos seguros. Si bien la organización no publica aplicaciones, reconoce que el correo electrónico es un medio expuesto a la red externa que requiere ser asegurado.

14. Gestión de activos

14.1. La gerencia de administración debe mantener el inventario general de los activos de la organización, la cual debe ser complementado por la gerencia de servicios TIC, respecto a los activos tecnológicos, con inventarios específicos, en los cuales se defina al propietario como el principal interesado en la información que aloja o transmite ese activo.

14.2. Toda persona que deja la organización deberá obtener la suscripción de la **Hoja de salida**, en la cual se valida, en uno de los ítems, la devolución de todos los activos entregados por la organización.

14.3. Se ha dado una valoración general a los activos involucrados en el proceso de consultoría como confidenciales (todos los identificados en la matriz de evaluación de riesgos). Los activos fuera de esta lista son considerados regulares.

14.4. Se considera que toda información impresa que salga del repositorio de consultoría debe ser sellada con la etiqueta de “confidencial”, antes de su distribución autorizada, la responsabilidad de esta acción corresponde a la persona que emite dicha impresión.

14.5. Las disposiciones mínimas para el cuidado de los activos están documentadas en el **Decálogo de la seguridad de información**, y deben ser acatadas como parte integral de las políticas.

14.6. Los equipos y repositorios de información que por motivos de mantenimiento, traslado, baja, donación o traslado a cliente, sean llevados fuera de las instalaciones de la organización, deben contar con el permiso respectivo por parte del gerente de administración, que valide el destino del activo, como del gerente de servicios TIC, que valide su condición adecuada y la aplicación de controles necesarios y suficientes respecto a la información que contienen.

15. Seguridad física y ambiental

15.1. La gerencia de administración es responsable de velar por el mantenimiento y operación adecuado de los controles físicos y ambientales que la organización ha implementado:

a. Supervisar el cumplimiento de las funciones del servicio de vigilancia y los registros que este produce.
b. Mantener el servicio de videograbación de la seguridad en operación dentro y fuera del horario de trabajo.
c. Mantener el funcionamiento adecuado de cerraduras en los ambientes de trabajo de la organización.
d. Mantener los mecanismos de detección y reacción ante amenazas ambientales (fuego, aniego, corto circuito, humedad).
e. Velar por la adecuada instalación de los espacios de trabajo, en prevención de accidentes laborales.
f. Controlar el ingreso de productos, equipos y suministros desde la entrada hacia el almacén de la organización.
g. Mantener los mecanismos de contingencia eléctrica en condiciones adecuadas y con un margen de cobertura adecuado para la organización.

16. Gestión de personal

16.1. La gerencia de administración debe aplicar las siguientes restricciones y obligaciones para el personal que ingresa, trabaja y se retira de la organización:

a. Seleccionar al personal considerando sus antecedentes laborales, referencias así como también antecedentes penales o policiales.
b. Comunicar las obligaciones respecto a la seguridad de información, al nuevo personal, incluyéndolas además en el contrato firmado con este.
c. Comunicar la existencia de las políticas de seguridad de información como marco complementario aplicable y sancionable.
d. Aplicar sanciones relacionadas a incumplimientos de las políticas, tomando como referente la **Directiva de administración de personal**.
e. Complementar la relación laboral contractual con la firma de un **Acuerdo de confidencialidad y de reconocimiento de las políticas de seguridad de información**, por parte del empleado.

17. Gestión de terceros

17.1. La gerencia de administración debe mantener las siguientes condiciones relacionadas a la relación con otras organizaciones:

a. Administrar y mantener actualizado el directorio de contactos y emergencias (policía, bomberos, municipalidad, proveedores críticos)
b. Incorporar en los contratos con clientes las disposiciones aplicables de seguridad de información y condiciones relacionadas a la consultoría que dispongan la gerencia general y la gerencia de operaciones.
c. Incorporar en los contratos con proveedores las disposiciones aplicables de seguridad de información y las condiciones relacionadas a niveles de servicio, penalidades y plazos de servicio, según lo dispongan las gerencias interesadas.
d. Supervisar el cumplimiento de las condiciones establecidas en los contratos y centralizar cualquier reclamo comunicado por las gerencias al respecto.
e. Gestionar la aplicación de adendas y la sustitución de proveedores para los casos de incumplimiento.

18. Auditoría de Seguridad de Información

18.1. Las auditorías internas del SGSI se realizarán de la siguiente forma:

a. El auditor elabora un **Programa de Auditoría Interna del SGSI** considerando los procesos involucrados y los resultados de auditorías previas.
b. La dirección valida y aprueba el programa para el periodo.
c. Para cada ciclo de auditoría incluido en el programa, el auditor diseña un **Plan de Auditoría Interna del SGSI**.
d. Se valida el plan respecto a la disponibilidad de los involucrados y se ejecuta el plan actualizado.
e. Los resultados obtenidos son validados con el personal entrevistado, para obtener descargos o corroborar los hallazgos.
f. Finalmente los resultados son documentados en el **Informe de resultados de la auditoría interna**.
g. Este informe es comunicado al representante de la dirección y a todos los participantes de la auditoría.

18.2. Los hallazgos de auditoría serán clasificados en base a los siguientes criterios:
   a. No conformidades. Incumplimientos de los requisitos de la norma o lineamientos internos de la organización.
   b. Observaciones. Hechos que podrían conllevar a una futura no conformidad.
   c. Oportunidades de Mejora. Recomendaciones que, sin estar asociadas a incumplimientos, pueden aportar mejoras al sistema.

18.3. La auditoría interna debe ser realizada por un responsable independiente del proceso, además de competente respecto al conocimiento del estándar ISO 27001 y de la práctica de auditoría.

18.4. El alcance de la auditoría es el comprendido en el **Programa de Auditoría Interna del SGSI**, el cual, debe comprender mínimamente al cumplimiento de las políticas internas y del estándar ISO 27001.

18.5. Se complementará la revisión del sistema con las evaluaciones periódicas de carácter técnico sobre las plataformas tecnológicas (análisis de vulnerabilidades).

18.6. Pese a su carácter confidencial, los registros de auditoría (bitácoras de incidentes, registros de accesos, registros de acciones) podrán ser puestos a disposición de los auditores si estos los solicitan, para revisión y bajo condiciones controladas.

Anexo G. Metodología de Gestión de Riesgos

Descripción: Metodología usada, como parte del SGSI, para apreciar y tratar los riesgos y oportunidades identificadas en los procesos que forman parte del alcance del sistema.
Aprobado: Versión 1.0 por Representante de la Dirección

Estructura:

- Generalidades
- Involucrados
- Parámetros
    - Frecuencia
    - Niveles de consecuencias
    - Niveles de probabilidad
    - Cálculo del nivel de riesgo
    - Nivel de aceptación del riesgo
    - Criterios de aceptación de riesgos
    - Matriz para la identificación de riesgos

- Desarrollo
    - Establecimiento del Contexto
    - Identificación del Riesgo
    - Análisis del Riesgo
    - Evaluación del Riesgo
    - Tratamiento del Riesgo

- Anexos de la metodología
    - Formato de Matriz de Riesgos
    - Formato de Plan de Tratamiento de Riesgos
    - Formato de Declaración de Aplicabilidad de Controles

Generalidades

La Metodología de Gestión de Riesgos detalla las acciones de apreciación y tratamiento de riesgos y oportunidades (riesgos positivos) de seguridad de información, para los procesos que están comprendidos dentro del alcance del SGSI. En adelante nos referiremos a esta actividad simplemente como Gestión de Riesgos.

Involucrados

El siguiente personal participa de la gestión de riesgos:

- **RP-P.** Representante del proceso – principal: Gerente de operaciones
- **RP-S.** Representante del proceso – soporte: Gerente de servicios TIC
- **PP.** Participantes del proceso: Jefe Líder de proyectos de desarrollo, Jefe de Aseguramiento de la Calidad, Operadores.
- **OSG.** Operador del SGSI:

Parámetros

Frecuencia. La gestión de riesgos se ejecutará al iniciar un ciclo de operación del sistema o, eventualmente, cada vez que ocurra algún cambio significativo en los procesos dentro del alcance del SGSI, que pueda implicar algún riesgo.

Niveles de consecuencias. Se definen estos niveles como los niveles de impacto positivo o negativo que podría producir un riesgo determinado en la organización:

- **Desastroso.** Afecta negativamente a toda la organización: imagen, finanzas, fidelización de clientes.
- **Malo.** Afecta negativamente a un área crítica, proceso crítico o proyecto significativo (mayor a 6 meses)
- **Nulo.** No genera una afectación significativa
- **Bueno.** Afecta positivamente a un área crítica, proceso crítico o proyecto significativo (mayor a 6 meses)
- **Excelente.** Afecta positivamente a toda la organización: imagen, finanzas, fidelización de clientes.

Niveles de probabilidad. Se definen los niveles estimados de ocurrencia de los riesgos identificados. Están:

- **Alto.** Es casi seguro que ocurrirá en la organización, bajo su situación actual.
- **Medio.** Puede ocurrir en la organización bajo circunstancias particulares, que podrían presentarse.
- **Bajo.** Es casi imposible que ocurra en la organización.

Cálculo del nivel de riesgo. En base a las aristas de valorización de consecuencia y probabilidad de riesgos, se determina la siguiente formulación para determinar el nivel de riesgo.

Criterio de para apreciación del riesgo		Impacto				
		Desastroso -10	Malo -5	Nulo 0	Bueno +5	Excelente +10
Probabilidad	Alto 10	-100	-50	0	50	100
	Medio 5	-50	-25	0	25	50
	Bajo 1	-10	-5	0	5	10

Nivel de aceptación del riesgo. Se aceptarán aquellos riesgos u oportunidades cuyo valor corresponda al rango indicado en las casillas blancas (Aceptable), en el cálculo del nivel de riesgo, mientras que las grises no (Inaceptable).

Criterios de aceptación de riesgos. Un riesgo no aceptable por si nivel de riesgo / oportunidad, podrá ser aceptado si cumple alguna de las siguientes condiciones:

- Su mitigación / promoción conlleva el incumplimiento de una Ley, la misión u objetivos estratégicos de la organización.
- El costo implementar medidas de mitigación / promoción es superior al daño / beneficio.
- La organización no cuenta con recursos disponibles para implementar las medidas de mitigación / promoción, dentro del periodo.

Marco para la identificación de riesgos

Tipo de Activo	C	I	D	Amenazas que originan riesgos
Documento físico: manuscritos es impresos	X		X	Pérdida / robo
	X	X	X	Uso inadecuado
	X	X	X	Acceso no autorizado
	X			Copia no autorizada
		X	X	Daño ambiental / térmico
		X	X	Desgaste por uso
Documento digital: archivos, bases de datos	X	X	X	Acceso no autorizado
	X			Copia no autorizada
		X		Modificación no autorizada
			X	Eliminación no autorizada
	X	X	X	Infiltración del malware
		X	X	Incompatibilidad
Dispositivos electrónicos: portátiles, de escritorio, móviles, memorias	X		X	Pérdida / robo
	X	X	X	Uso inadecuado
	X	X	X	Acceso no autorizado
		X	X	Daño por contusión
		X	X	Daño ambiental / magnético / térmico
		X	X	Desgaste por uso
		X	X	Obsolescencia
Software: aplicaciones y sistemas		X	X	Cambio inadecuados
	X	X	X	Ataque informático humano
	X	X	X	Infiltración de malware
		X	X	Incompatibilidad
Servicio TI: comunicaciones, almacenamiento, procesamiento	X	X	X	Ataque informático humano
	X	X	X	Infiltración de malware
		X	X	Daño ambiental / magnético / térmico
	X	X	X	Uso inadecuado
			X	Corte de suministro
			X	Saturación de recursos
Personal			X	Impedimento de acceso al puesto
			X	Indisposición del personal
	X	X	X	Suplantación de identidad
	X			Espionaje

Desarrollo

Etapa	N°	Actividad	Responsable
Establecimiento del Contexto	1	Revisan la última versión de: **Informe de contexto de la organización** y el **Informe de necesidades y expectativas de las partes interesadas** y la **Declaración del Alcance del SGSI**.	OSG, RP-P, RP-S
	2	Se revisan los parámetros de riesgos documentados en la **Metodología de Gestión de Riesgos**: Niveles de consecuencias, Niveles de probabilidad, Cálculo del nivel de riesgo, Nivel de aceptación del riesgo, Criterios de aceptación de riesgos.	OSG, RP-P
	3	Se actualizan los cambios necesarios sobre estos documentos (cambios en los procesos, cambio de parámetros de riesgos) y se gestiona su aprobación, si corresponde.	OSG
	4	Se elabora un **Informe de gestión de riesgos**, donde se documentarán todas las actividades y resultados de esta y las siguientes fases del proceso de gestión de riesgos.	OSG
Identificación del Riesgo	5	Se elabora una **Matriz de Riesgos**, dentro del **Informe de gestión de riesgos**, para registrar todo el proceso de apreciación de riesgos.	OSG
	6	Tomando como referencia el diagrama de flujo de datos documentado en la **Declaración del Alcance del SGSI**, se realiza un recorrido de cada una de las **actividades** por las que fluye la información en los procesos.	OSG, RP-P, RP-S
	7	Se identifican a los **activos** que se involucran en el desarrollo de cada actividad.	OSG, RP-P, RP-S
	8	Se identifican riesgos / oportunidades sobre la actividad en base a los activos involucrados, aplicando referencialmente el **Marco para la identificación de riesgos** que presenta la metodología.	OSG, RP-P, RP-S
	9	Se identifica a la persona con responsabilidad y autoridad para atender el riesgo / oportunidad o **propietario del riesgo**.	OSG, RP-P, RP-S
	10	Se documentan los riesgos y propietarios identificados en la **Matriz de Riesgos**.	OSG
Análisis del Riesgo	11	Se identifican los **controles existentes** alrededor del riesgo / oportunidad identificado.	OSG, RP-P, RP-S
	12	En base a la información de controles, para cada riesgo identificado, se asigna un **nivel de consecuencias**.	OSG, RP-P, RP-S
	13	En base a la información de controles, para cada riesgo identificado, se asigna un **nivel de probabilidad**.	OSG, RP-P, RP-S
	14	En base a las consecuencias y probabilidad se calcula el **nivel de riesgo**.	OSG
	15	Se documenta el análisis realizado en la **Matriz de Riesgos**.	OSG

Etapa	N°	Actividad	Responsable
Evaluación del Riesgo	16	Se contrasta el nivel de riesgo contra los criterios de riesgo, para determinar qué riesgos son aceptables.	OSG, RP-P, RP-S
	17	Se asigna un número de prioridad, en base al nivel de riesgo, para aquellos riesgos que no son aceptables.	OSG, RP-P, RP-S
	18	Se documenta la evaluación realizada en la **Matriz de Riesgos**.	OSG
Tratamiento del Riesgo	19	En base a la lista de riesgos priorizados, se completa la sección de tratamiento en la **Matriz de Riesgos**, en el **Informe de gestión de riesgos**.	OSG, RP-P, RP-S
	20	En la **Matriz de Riesgos**, para cada riesgo, se selecciona la opción de tratamiento: **aceptar**, **reducir** o **aumentar**, y se detallan los controles que acompañarán a esa opción, si corresponde.[1]	OSG, RP-P, RP-S
	21	Se documentan los controles necesarios a implementar o mejorar para aplicar la opción de tratamiento seleccionada en la **Matriz de Riesgos**, revisando el **Anexo A de la ISO/IEC 27001:2013**, también se estima el nivel de riesgo residual que se espera lograr.	OSG, RP-P, RP-S
	22	Se elabora la **Declaración de Aplicabilidad de Controles**, que especifica cada control, si está implementado, y justifica su inclusión o exclusión.	OSG
	23	Se prepara el **Plan de Tratamiento de riesgos**, con aquellos controles asociados a riesgos por reducir.	OSG
	23	Se prepara el **Plan de Acciones de mejora**, con aquellos controles asociados a oportunidades por aumentar.	OSG
	24	Se planifican las sesiones de seguimiento al **Plan de Tratamiento de Riesgos**.	OSG, RP-P, RP-S
	25	Se actualiza el **Informe de gestión de riesgos** en base a las versiones finales de la **Matriz de Riesgos** y el **Plan de Tratamiento de Riesgos**.	OSG
	26	Gestionar la firma de: **Informe de gestión de riesgos**, **Plan de Tratamiento de Riesgos** y **Declaración de Aplicabilidad de Controles.**	OSG
	27	Se emite periódicamente un **Informe de Seguimiento de Riesgos**, donde se verifican los avances respecto a la implementación de controles.	OSG

[1] Para aceptar (o mantener) un riesgo deberá ser en base a los criterios de aceptación definidos en la metodología. Reducir el riesgo comprende: evitar o eliminar (reducir la probabilidad a 0), mitigar (reducir parcialmente la probabilidad o el impacto), compartir (reducir solo el impacto: contratos, seguros). Aumentar el riesgo solo es aplicable para los casos de oportunidades.

Anexos de la metodología

Formato de Matriz de Riesgos

Contexto		Identificación					Análisis					Evaluación		Tratamiento			
Fuente	Activos	Riesgo	ID	C	I	D	Controles	Detalle	Propietario del riesgo	Probabilidad	Consecuencia	Nivel de Riesgo Actual	Prioridad	Opción (Criterio) / Acción (Control)	Probabilidad	Consecuencia	Nivel de Riesgo Residual
(1)	(2)	(3)					(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)

1. **Fuente.** Actividad a partir de la cual se identifican los activos por los que fluye la información de los procesos.
2. **Activos.** Asociados a las actividades, en conjunto con estas se usan para determinan los riesgos de seguridad de información.
3. **Riesgo.** Riesgo identificado dentro de las actividades de los procesos, su identificador y la relación con la seguridad de información.
4. **Controles.** Controles existentes que mitigan la ocurrencia o impacto del riesgo.
5. **Detalle.** Especificación de los controles listados.
6. **Propietario del riesgo.** Personal con la autoridad y recursos para afrontar el riesgo identificado y decidir sobre su tratamiento.
7. **Probabilidad.** Nivel de ocurrencia potencial del riesgo identificado.
8. **Consecuencia.** Nivel de impacto potencial del riesgo identificado.
9. **Nivel de riesgo actual.** Nivel calculado a partir de la probabilidad y consecuencia: aceptable o inaceptable.
10. **Prioridad.** Valor referencial para la priorización de la atención del riesgo: corto-1, mediano-2 y largo-3 plazo.
11. **Opción (Criterio) / Acción (Control).** Decisión respecto al riesgo identificado y mecanismo de control a implementar (Anexo A - 27001).
12. **Probabilidad.** Nivel de ocurrencia potencial del riesgo identificado, al aplicar el control propuesto.
13. **Consecuencia.** Nivel de impacto potencial del riesgo identificado, al aplicar el control propuesto.
14. **Nivel de riesgo actual.** Nivel calculado a partir de la probabilidad y consecuencia: aceptable o inaceptable, al aplicar el control propuesto.

Formato de Plan de Tratamiento de Riesgos

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)

1. **ID.** El identificador de la acción.
2. **Etapa.** Para todos los casos la fase de operación es “Implementar”.
3. **Tipo.** Para todos los casos la denominación es “Tratamiento de Riesgos”.
4. **Acción.** Nombre específico de la acción a realizar.
5. **Condiciones.** Situación que ha generado la realización de la acción.
6. **Involucrados.** Personal involucrado en la gestión y realización de las actividades.
7. **Recursos.** Recursos involucrados, que pueden comprender: documentos, tecnología, personas, ubicaciones, entre otros.
8. **Tareas.** Conjunto de actividades que componen a la acción.
9. **Efectividad.** Resultado esperado respecto al cual se verifica si la acción ha sido exitosa o no.
10. **Inicio.** Fecha de inicio del conjunto de actividades que componen la acción.
11. **Cierre.** Fecha de terminación del conjunto de actividades que componen la acción.
12. **Resultado.** Estado de la realización de las acciones: Planeado, En proceso, Realizado.

Formato de Declaración de Aplicabilidad de Controles

Dominio.	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
(1)	(2)	(3)	(4)	(5)	(6)

1. **Dominio.** Grupo organizado de los controles, bajo el enfoque de la organización.
2. **27001-A.** Identificador referencial para vincular los controles con el numeral específico del Anexo A - ISO 27001.
3. **Control ISO.** Descriptor referencial para vincular los controles con el numeral específico del Anexo A - ISO 27001.
4. **Aplica.** Indicador sobre la aplicabilidad o no del control en la organización.
5. **Justificación.** Sustento respecto a la aplicabilidad o no del control a la organización (Decisión de la dirección, Requisito del SGSI, Requisito de seguridad de información o Asociado a riesgos).
6. **Controles: Implementado (IM) / Parcialmente Implementado (PI).** Descripción específica de los controles que existen en la organización.

Anexo H. Informe de gestión de riesgos

Descripción: Informe de resultados obtenidos tras aplicar la metodología de gestión de riesgos: la apreciación y la propuesta de tratamiento de riesgos.
Aprobado: Versión 1.0 por Propietarios de Riesgos

La organización ha realizado la gestión de riesgos del SGSI para su periodo 2015-2016, para lo cual ha realizado las siguientes actividades:

- Establecimiento del Contexto
- Identificación del Riesgo
- Análisis del Riesgo
- Evaluación del Riesgo
- Tratamiento del Riesgo

Establecimiento del Contexto

Se ha revisado el **Informe de contexto de la organización**, el **Informe de necesidades y expectativas de las partes interesadas** y la **Declaración del Alcance del SGSI**. A partir de lo cual se ha determinado que los siguientes procesos serán considerados para la gestión de riesgos: **Gestión de proyectos de consultoría / Ejecución de servicios de desarrollo y mantenimiento de software / Aseguramiento de la calidad del software**. Asimismo, se ha revisado y tomado los parámetros vigentes para aplicar la **Metodología de Gestión de Riesgos**, los cuales son:

Niveles de consecuencias: Desastroso. Afecta negativamente a toda la organización: imagen, finanzas, fidelización de clientes. **Malo.** Afecta negativamente a un área crítica, proceso crítico o proyecto significativo (mayor a 6 meses). **Nulo.** No genera una afectación significativa. **Bueno.** Afecta positivamente a un área crítica, proceso crítico o proyecto significativo (mayor a 6 meses). **Excelente.** Afecta positivamente a toda la organización: imagen, finanzas, fidelización de clientes.

Niveles de probabilidad: Alto. Es casi seguro que ocurrirá en la organización, bajo su situación actual. **Medio.** Puede ocurrir en la organización bajo circunstancias particulares, que podrían presentarse. **Bajo.** Es casi imposible que ocurra en la organización.

Cálculo del nivel de riesgo. En base a las aristas de valorización de consecuencia y probabilidad de riesgos, se determina la siguiente formulación para determinar el nivel de riesgo.

Criterio de para apreciación del riesgo		Impacto				
		Desastroso -10	Malo -5	Nulo 0	Bueno +5	Excelente +10
Probabilidad	Alto 10	-100	-50	0	50	100
	Medio 5	-50	-25	0	25	50
	Bajo 1	-10	-5	0	5	10

Nivel de aceptación del riesgo. Se aceptarán aquellos riesgos u oportunidades cuyo valor corresponda al rango indicado en las casillas blancas, en el cálculo del nivel de riesgo.

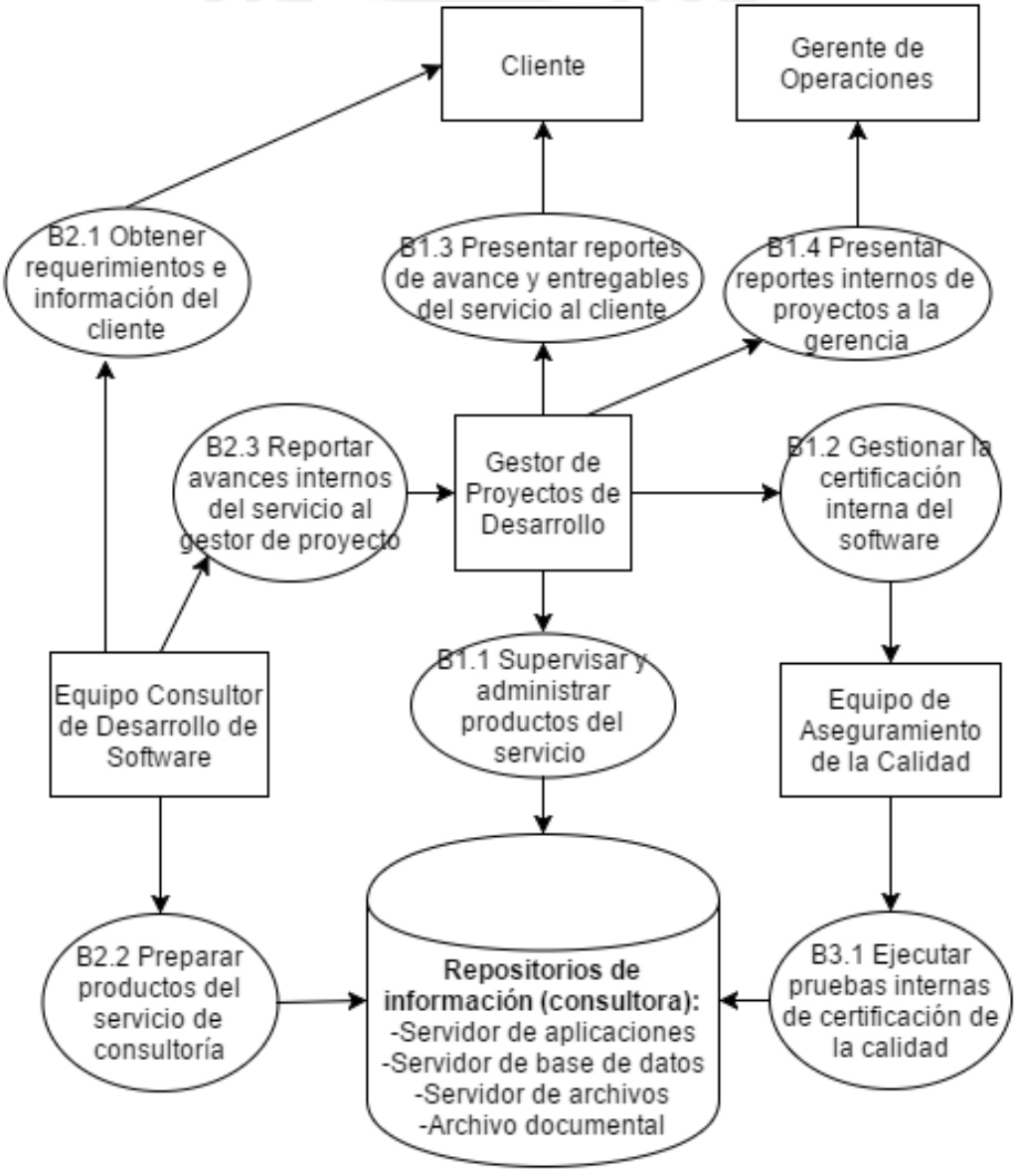
Identificación del Riesgo

Para identificar riesgos se ha tomado el diagrama de flujo de datos de los procesos y sus actividades. Para cada uno de estos nodos se han realizado entrevistas:

- **B1. Gestión de proyectos de consultoría**
  - B1.1 Supervisar y administrar productos del servicio
  - B1.2 Gestionar la certificación interna del software
  - B1.3 Presentar reportes de avance y entregables del servicio al cliente
  - B1.4 Presentar reportes internos de proyectos a la gerencia

- **B2. Ejecución de servicios de desarrollo y mantenimiento de software**
  - B2.1 Obtener requerimientos e información del cliente
  - B2.2 Preparar productos del servicio de consultoría
  - B2.3 Reportar avances internos del servicio al gestor de proyecto

- **B3. Aseguramiento de la calidad del software**
  - B3.1 Ejecutar pruebas internas de certificación de la calidad



A partir de este ejercicio, se han identificado los siguientes riesgos y oportunidades de seguridad de información, con sus respectivos propietarios de riesgos:

Fuente	Activos	Riesgo	ID	Propietario del riesgo
Obtener requerimientos e información del cliente	Laptop de consultoría, gestor de proyecto, consultores, cuadernos de notas, acta de acuerdos de requerimientos	Robo de laptop de consultoría que contiene información del cliente durante la visita o en tránsito desde el cliente	GR15-R01	Gerente de operaciones
		Copia no autorizada de información mediante dispositivo USB desde la laptop de consultoría	GR15-R02	Gerente de servicios TIC
		Infiltración de malware en la laptop de consultoría que contiene información del cliente, generando la eliminación o alteración de archivos	GR15-R03	Gerente de servicios TIC
		Indisponibilidad del gestor de proyecto o consultores críticos para el proyecto por enfermedad o renuncia intempestiva, durante el relevamiento	GR15-R04	Gerente de administración
		Pérdida del acta de acuerdos sobre requerimientos, al retornar desde el cliente	GR15-R05	Gerente de operaciones
		Extravío del cuaderno de notas de los consultores, en tránsito desde el cliente	GR15-R06	Gerente de operaciones
		Conocimiento limitado del personal del cliente respecto a las condiciones contractuales de seguridad de información	GR15-O01	Gerente de operaciones
Preparar productos del servicio de consultoría	Equipos de escritorio de consultoría, servicio de red interna, servidor de archivos, consultores	Copia no autorizada de registros por los consultores, desde el servidor de archivos con información del proyecto	GR15-R07	Gerente de servicios TIC
		Copia no autorizada de registros por el administrador de plataformas, desde el servidor de archivos con información del proyecto	GR15-R08	Gerente de servicios TIC
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la preparación de productos	GR15-R09	Gerente de servicios TIC
		Indisponibilidad de consultores críticos del proyecto, durante la elaboración de productos	GR15-R10	Gerente de administración
		Eliminación o modificación intencional para sabotear productos, por personal descontento	GR15-R11	Gerente de operaciones
		Eliminación o modificación de archivos de productos versionados por infección de malware durante su preparación	GR15-R12	Gerente de servicios TIC
		Conflictos de versionado en los productos del servicio, por uso inadecuado del mecanismo versionador	GR15-R13	Gerente de operaciones
Reportar avances internos del servicio al gestor de proyecto	Equipos de escritorio de consultoría, servicio de red interna, servidor de archivos, consultores, servicio de correo electrónico	Indisponibilidad del gestor de proyecto o consultores críticos para el proyecto por enfermedad o renuncia intempestiva, durante el reporte de avances al gestor	GR15-R14	Gerente de administración
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante el reporte de avances al gestor de proyecto	GR15-R15	Gerente de servicios TIC
		Eliminación o modificación de archivos de productos versionados por infección de malware durante su revisión	GR15-R16	Gerente de servicios TIC
		Copia no autorizada de información enviada por correo al gestor de proyecto, por el administrador de plataformas	GR15-R17	Gerente de servicios TIC
Supervisar y administrar productos del servicio	Equipos de escritorio de consultoría, servicio de red interna, servidor de archivos,	Eliminación o modificación accidental de registros del servidor de versionado desde la cuenta del gestor de proyecto	GR15-R18	Gerente de operaciones
		Fuga de información desde el servidor de archivos con información del proyecto, mediante el correo del Gestor de Proyecto	GR15-R19	Gerente de servicios TIC

Fuente	Activos	Riesgo	ID	Propietario del riesgo
	gestor de proyecto	Fuga de información desde el servidor de archivos con información del proyecto, mediante la grabadora de CD del Gestor de Proyecto	GR15-R20	Gerente de servicios TIC
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la supervisión de los productos del servicio	GR15-R21	Gerente de servicios TIC
Gestionar la certificación interna del software	Equipos de escritorio de calidad, servicio de red interna, servidor de archivos, gestor de proyecto	Indisponibilidad del gestor de proyecto o analistas de calidad para el proyecto por enfermedad o renuncia intempestiva, durante el requerimiento para pruebas	GR15-R22	Gerente de administración
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la solicitud de certificación del software	GR15-R23	Gerente de servicios TIC
		Copia no autorizada de registros por los analistas de calidad, desde el servidor de archivos con información del proyecto	GR15-R24	Gerente de servicios TIC
Ejecutar pruebas internas de certificación de la calidad	Equipos de escritorio de calidad, servicio de red interna, servidor de archivos, analistas de calidad	Indisponibilidad de analistas de calidad para el proyecto por enfermedad o renuncia intempestiva, durante la ejecución de pruebas de calidad	GR15-R25	Gerente de administración
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante las pruebas de calidad	GR15-R26	Gerente de servicios TIC
		Eliminación o modificación accidental de registros del servidor de versionado desde la cuenta del analista de calidad	GR15-R27	Gerente de operaciones
Presentar reportes internos de proyectos a la gerencia	Equipos de escritorio de consultoría, servicio de red interna, servidor de archivos, gestor de proyecto, gerente de operación	Indisponibilidad del gestor de proyecto por enfermedad o renuncia intempestiva, durante el reporte a la gerencia	GR15-R28	Gerente de administración
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante el reporte de avances al gerente	GR15-R29	Gerente de servicios TIC
		Eliminación o modificación accidental de registros del servidor de versionado desde la cuenta del gerente	GR15-R30	Gerente de operaciones
Presentar reportes de avance y entregables del servicio al cliente	Laptop de consultoría, gestor de proyecto, consultores, CD entregable, servicio de red interna, servidor de archivos, acta de entrega e instalación	Indisponibilidad del gestor de proyecto por enfermedad o renuncia intempestiva, durante la presentación de los entregables para el cliente	GR15-R31	Gerente de administración
		Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la preparación del entregable a presentar	GR15-R32	Gerente de servicios TIC
		Fallo en el equipo de grabación de CD, usado para la generación del entregable	GR15-R33	Gerente de servicios TIC
		Pérdida del CD que contiene los componentes presentados en el entregable, en tránsito al cliente	GR15-R34	Gerente de operaciones
		Pérdida del acta de entrega, en tránsito desde el cliente	GR15-R35	Gerente de operaciones
		Fallo durante el apoyo en la instalación de los componentes presentados en el entregable	GR15-R36	Gerente de operaciones

En cada caso, se ha establecido un propietario del riesgo, aquel encargado con autoridad y recursos para gestionarlo.

Análisis del Riesgo

Para los riesgos (36) y la oportunidad (1) identificados, se han definido los niveles de probabilidad y consecuencia respectivos.

Riesgo	ID	Probabilidad	Consecuencia
Robo de laptop de consultoría que contiene información del cliente durante la visita o en tránsito desde el cliente	GR15-R01	**Medio**	**Desastroso**
Copia no autorizada de información mediante dispositivo USB desde la laptop de consultoría	GR15-R02	**Alto**	**Malo**
Infiltración de malware en la laptop de consultoría que contiene información del cliente, generando la eliminación o alteración de archivos	GR15-R03	**Medio**	**Malo**
Indisponibilidad del gestor de proyecto o consultores críticos para el proyecto por enfermedad o renuncia intempestiva, durante el relevamiento	GR15-R04	**Medio**	**Malo**
Pérdida del acta de acuerdos sobre requerimientos, al retornar desde el cliente	GR15-R05	**Bajo**	**Malo**
Extravío del cuaderno de notas de los consultores, en tránsito desde el cliente	GR15-R06	**Medio**	**Nulo**
Copia no autorizada de registros por los consultores, desde el servidor de archivos con información del proyecto	GR15-R07	**Alto**	**Malo**
Copia no autorizada de registros por el administrador de plataformas, desde el servidor de archivos con información del proyecto	GR15-R08	**Medio**	**Desastroso**
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la preparación de productos	GR15-R09	**Medio**	**Malo**
Indisponibilidad de consultores críticos del proyecto, durante la elaboración de productos	GR15-R10	**Medio**	**Malo**
Eliminación o modificación intencional para sabotear productos, por personal descontento	GR15-R11	**Medio**	**Desastroso**
Eliminación o modificación de archivos de productos versionados por infección de malware durante su preparación	GR15-R12	**Medio**	**Malo**
Conflictos de versionado en los productos del servicio, por uso inadecuado del mecanismo versionador	GR15-R13	**Alto**	**Malo**
Indisponibilidad del gestor de proyecto o consultores críticos para el proyecto por enfermedad o renuncia intempestiva, durante el reporte de avances al gestor	GR15-R14	**Medio**	**Malo**
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante el reporte de avances al gestor de proyecto	GR15-R15	**Medio**	**Malo**
Eliminación o modificación de archivos de productos versionados por infección de malware durante su revisión	GR15-R16	**Medio**	**Malo**
Copia no autorizada de información enviada por correo al gestor de proyecto, por el administrador de plataformas	GR15-R17	**Medio**	**Malo**
Eliminación o modificación accidental de registros del servidor de versionado desde la cuenta del gestor de proyecto	GR15-R18	**Bajo**	**Desastroso**
Fuga de información desde el servidor de archivos con información del proyecto, mediante el correo del Gestor de Proyecto	GR15-R19	**Medio**	**Malo**
Fuga de información desde el servidor de archivos con información del proyecto, mediante la grabadora de CD del Gestor de Proyecto	GR15-R20	**Medio**	**Malo**

Riesgo	ID	Probabilidad	Consecuencia
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la supervisión de los productos del servicio	GR15-R21	**Medio**	**Malo**
Indisponibilidad del gestor de proyecto o analistas de calidad para el proyecto por enfermedad o renuncia intempestiva, durante el requerimiento para pruebas	GR15-R22	**Medio**	**Malo**
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la solicitud de certificación del software	GR15-R23	**Medio**	**Malo**
Copia no autorizada de registros por los analistas de calidad, desde el servidor de archivos con información del proyecto	GR15-R24	**Alto**	**Malo**
Indisponibilidad de analistas de calidad para el proyecto por enfermedad o renuncia intempestiva, durante la ejecución de pruebas de calidad	GR15-R25	**Medio**	**Malo**
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante las pruebas de calidad	GR15-R26	**Medio**	**Malo**
Eliminación o modificación accidental de registros del servidor de versionado desde la cuenta del analista de calidad	GR15-R27	**Bajo**	**Desastroso**
Indisponibilidad del gestor de proyecto por enfermedad o renuncia intempestiva, durante el reporte a la gerencia	GR15-R28	**Medio**	**Malo**
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante el reporte de avances al gerente	GR15-R29	**Medio**	**Malo**
Eliminación o modificación accidental de registros del servidor de versionado desde la cuenta del gerente	GR15-R30	**Bajo**	**Desastroso**
Indisponibilidad del gestor de proyecto por enfermedad o renuncia intempestiva, durante la presentación de los entregables para el cliente	GR15-R31	**Medio**	**Malo**
Pérdida de acceso a productos versionados por falla física en el servidor o en la red interna, durante la preparación del entregable a presentar	GR15-R32	**Medio**	**Malo**
Fallo en el equipo de grabación de CD, usado para la generación del entregable	GR15-R33	**Medio**	**Malo**
Pérdida del CD que contiene los componentes presentados en el entregable, en tránsito al cliente	GR15-R34	**Medio**	**Desastroso**
Pérdida del acta de entrega, en tránsito desde el cliente	GR15-R35	**Bajo**	**Malo**
Fallo durante el apoyo en la instalación de los componentes presentados en el entregable	GR15-R36	**Medio**	**Malo**
Conocimiento limitado del personal del cliente respecto a las condiciones contractuales de seguridad de información	GR15-O01	**Alto**	**Bueno**

Evaluación del Riesgo

En base a los niveles de probabilidad y consecuencia se determina si el nivel de riesgo es aceptable o inaceptable, para este último caso, se han definido prioridades para definir si estos controles serán realizados en el corto (1), mediano (2) o largo (3) plazo:

ID	Probabilidad	Consecuencia	Nivel de Riesgo Actual	Prioridad
GR15-R01	**Medio**	**Desastroso**	Inaceptable	1
GR15-R02	**Alto**	**Malo**	Inaceptable	1
GR15-R03	**Medio**	**Malo**	Aceptable	-
GR15-R04	**Medio**	**Malo**	Aceptable	-
GR15-R05	**Bajo**	**Malo**	Aceptable	-
GR15-R06	**Medio**	**Nulo**	Aceptable	-
GR15-R07	**Alto**	**Malo**	Inaceptable	1
GR15-R08	**Medio**	**Desastroso**	Inaceptable	1
GR15-R09	**Medio**	**Malo**	Aceptable	-
GR15-R10	**Medio**	**Malo**	Aceptable	-
GR15-R11	**Medio**	**Desastroso**	Inaceptable	2
GR15-R12	**Medio**	**Malo**	Aceptable	-
GR15-R13	**Alto**	**Malo**	Inaceptable	2
GR15-R14	**Medio**	**Malo**	Aceptable	-
GR15-R15	**Medio**	**Malo**	Aceptable	-
GR15-R16	**Medio**	**Malo**	Aceptable	-
GR15-R17	**Medio**	**Malo**	Aceptable	-
GR15-R18	**Bajo**	**Desastroso**	Aceptable	-
GR15-R19	**Medio**	**Malo**	Aceptable	-
GR15-R20	**Medio**	**Malo**	Aceptable	-
GR15-R21	**Medio**	**Malo**	Aceptable	-
GR15-R22	**Medio**	**Malo**	Aceptable	-
GR15-R23	**Medio**	**Malo**	Aceptable	-
GR15-R24	**Alto**	**Malo**	Inaceptable	1
GR15-R25	**Medio**	**Malo**	Aceptable	-
GR15-R26	**Medio**	**Malo**	Aceptable	-
GR15-R27	**Bajo**	**Desastroso**	Aceptable	-
GR15-R28	**Medio**	**Malo**	Aceptable	-
GR15-R29	**Medio**	**Malo**	Aceptable	-
GR15-R30	**Bajo**	**Desastroso**	Aceptable	-
GR15-R31	**Medio**	**Malo**	Aceptable	-
GR15-R32	**Medio**	**Malo**	Aceptable	-
GR15-R33	**Medio**	**Malo**	Aceptable	-
GR15-R34	**Medio**	**Desastroso**	Inaceptable	1
GR15-R35	**Bajo**	**Malo**	Aceptable	-
GR15-R36	**Medio**	**Malo**	Aceptable	-
GR15-O01	**Alto**	**Bueno**	Inaceptable	2

Tratamiento del Riesgo

Para los riesgos y oportunidades inaceptables se han validado alternativas de tratamiento con los propietarios del riesgo, para llegar a un nivel aceptable:

Riesgo	ID	Nivel de Riesgo Actual	Opción (Criterio) / Acción (Control)	Probabilidad	Consecuencia	Nivel de Riesgo Residual
Robo de laptop de consultoría que contiene información del cliente durante la visita o en tránsito desde el cliente	GR15-R01	Inaceptable	**Reducir** **8.3.3 Encriptamiento de unidades de disco duro destinadas fuera de la empresa** Implementar el encriptamiento a nivel de BIOS para el disco duro de las laptops de consultoría.	**Medio**	**Malo**	Aceptable
Copia no autorizada de información mediante dispositivo USB desde la laptop de consultoría	GR15-R02	Inaceptable	**Reducir** **11.2.8 Bloqueo automático de equipos por inactividad** Reducir a 3 minutos el tiempo de bloqueo por inactividad en el equipo de consultoría	**Alto**	**Nulo**	Aceptable
Copia no autorizada de registros por los consultores, desde el servidor de archivos con información del proyecto	GR15-R07	Inaceptable	**Reducir** **8.3.1 Bloqueo de puertos USB en los equipos - consultores** Implementar el bloqueo de puertos USB en los equipos de los consultores	**Bajo**	**Malo**	Aceptable
Copia no autorizada de registros por el administrador de plataformas, desde el servidor de archivos con información del proyecto	GR15-R08	Inaceptable	**Reducir** **7.2.2 Charla de sensibilización - administrador de plataformas** Realizar charlas sobre seguridad de información específicas para el administrador de plataformas y sus funciones	**Alto**	**Nulo**	Aceptable
Eliminación o modificación intencional para sabotear productos, por personal descontento	GR15-R11	Inaceptable	**Reducir** **7.2.3 Penalización por sabotajes o daños intencionales** Incluir en el contrato el reconocimiento de que en caso se reciban penalidades a la empresa, originadas en un intento de daño intencional por el empleado, este asumirá la totalidad del monto de pérdida.	**Bajo**	**Malo**	Aceptable
Conflictos de versionado en los productos del servicio, por uso inadecuado del mecanismo versionador	GR15-R13	Inaceptable	**Reducir** **12.1.1 Protocolo de desarrollo de software y productos del servicio** Actualizar el protocolo de desarrollo de software, de manera que especifique en un anexo los lineamientos técnicos para manejar un conflicto de versiones o duplicidad de componentes.	**Alto**	**Nulo**	Aceptable
Copia no autorizada de registros por los analistas de calidad, desde el servidor de archivos con información del proyecto	GR15-R24	Inaceptable	**Reducir** **8.3.1 Bloqueo de puertos USB en los equipos - analistas de calidad** Implementar el bloqueo de puertos USB en los equipos de los analistas de calidad	**Bajo**	**Malo**	Aceptable
Pérdida del CD que contiene los componentes presentados en el entregable, en tránsito al cliente	GR15-R34	Inaceptable	**Reducir** **9.4.1 Protección por contraseña del acceso a discos compactos (CD/DVD)** Establecer la obligación para el consultor de realizar todas las grabaciones de discos para clientes usando una capa de autenticación	**Medio**	**Malo**	Aceptable
Conocimiento limitado del personal del cliente respecto a las condiciones contractuales de seguridad de información	GR15-O01	Inaceptable	**Aumentar** **7.2.2 Charlas explicativas de las condiciones de seguridad de información para los clientes** Establecer la presentación detallada de los límites y responsabilidades establecidas en el contrato con los clientes para evitar reclamos sin sustento y propiciar la retroalimentación de mejoras	**Medio**	**Malo**	Aceptable

Anexo I. Plan de tratamiento de riesgos

Descripción: Plan de los controles definidos para atender los riesgos y oportunidades de seguridad de información obtenidos a partir de la gestión de riesgos.
Aprobado: Versión 1.0 por Representante de la Dirección, Propietarios de Riesgos: Gerente de administración, Gerente de operaciones, Gerente de servicios TIC

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
PTR01	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R01: Robo de laptop de consultoría que contiene información del cliente durante la visita o en tránsito desde el cliente	*Se ha planificado la implementación del control: 8.3.3 Encriptamiento de unidades de disco duro destinadas fuera de la empresa	**Gestor:** *Coordinador de seguridad de información **Ejecutor:** *Especialista de soporte TI	**Documentos:** *Inventario de laptops **Tecnología:** *Software de administración de BIOS	1. Implementar el encriptamiento a nivel de BIOS para el disco duro de las laptops de consultoría.	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	ago-15	**Realizado**
PTR02	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R02: Copia no autorizada de información mediante dispositivo USB desde la laptop de consultoría	*Se ha planificado la implementación del control: 11.2.8 Bloqueo automático de equipos por inactividad	**Gestor:** *Coordinador de seguridad de información **Ejecutor:** *Especialista de soporte TI	**Tecnología:** *Consola de administración del dominio	1. Reducir a 3 minutos el tiempo de bloqueo por inactividad en el equipo de consultoría	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	ago-15	**Realizado**
PTR03	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R07: Copia no autorizada de registros por los consultores, desde el servidor de archivos con información del proyecto	*Se ha planificado la implementación del control: 8.3.1 Bloqueo de puertos USB en los equipos - consultores	**Gestor:** *Coordinador de seguridad de información **Ejecutor:** *Especialista de soporte TI	**Tecnología:** *Software de administración de equipos	1. Implementar el bloqueo de puertos USB en los equipos de los consultores	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	ago-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
PTR04	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R08: Copia no autorizada de registros por el administrador de plataformas, desde el servidor de archivos con información del proyecto	*Se ha planificado la implementación del control: 7.2.2 Charla de sensibilización - administrador de plataformas	**Gestor:** *Coordinador de seguridad de información **Ejecutor:** *Coordinador de seguridad de información	**Presentación:** *Concientización en seguridad de información **Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop y proyector	1. Realizar charlas sobre seguridad de información específicas para el administrador de plataformas y sus funciones	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	ago-15	**Realizado**
PTR05	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R11: Eliminación o modificación intencional para sabotear productos, por personal descontento	*Se ha planificado la implementación del control: 7.2.3 Penalización por sabotajes o daños intencionales	**Gestor:** *Gerente de administración **Ejecutor:** *Asistente de administración	**Documentos:** *Procedimiento de gestión de personal *Contratos *Adendas de contratos **Servicios:** Asesoría legal	1. Incluir en el contrato el reconocimiento de que en caso se reciban penalidades a la empresa, originadas en un intento de daño intencional por el empleado, este asumirá la totalidad del monto de pérdida.	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	nov-15	**Realizado**
PTR06	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R13: Conflictos de versionado en los productos del servicio, por uso inadecuado del mecanismo versionador	*Se ha planificado la implementación del control: 12.1.1 Protocolo de desarrollo de software y productos del servicio	**Gestor:** *Gerente de operaciones **Ejecutor:** *Gestor de proyectos	**Documentos:** *Protocolo de desarrollo de software y productos del servicio	1. Actualizar el protocolo de desarrollo de software, de manera que especifique en un anexo los lineamientos técnicos para manejar un conflicto de versiones o duplicidad de componentes.	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	nov-15	**Realizado**
PTR07	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R24: Copia no autorizada de registros por los analistas de calidad, desde el servidor de archivos con información del proyecto	*Se ha planificado la implementación del control: 8.3.1 Bloqueo de puertos USB en los equipos - analistas de calidad	**Gestor:** *Coordinador de seguridad de información **Ejecutor:** *Especialista de soporte TI	**Tecnología:** *Software de administración de equipos	1. Implementar el bloqueo de puertos USB en los equipos de los analistas de calidad	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	ago-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
PTR08	Implementar	Tratamiento de Riesgos	Atender el riesgo GR15-R34: Pérdida del CD que contiene los componentes presentados en el entregable, en tránsito al cliente	*Se ha planificado la implementación del control: 9.4.1 Protección por contraseña del acceso a discos compactos (CD/DVD)	**Gestor:** *Gerente de operaciones **Ejecutor:** *Gestor de proyectos	**Documentos:** *Protocolo de desarrollo de software y productos del servicio	1. Establecer la obligación para el consultor de realizar todas las grabaciones de discos para clientes usando una capa de autenticación	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	ago-15	**Realizado**
PTR09	Implementar	Tratamiento de Riesgos	Atender la oportunidad GR15-O01: Conocimiento limitado del personal del cliente respecto a las condiciones contractuales de seguridad de información	*Se ha planificado la implementación del control: 7.2.2 Charlas explicativas de las condiciones de seguridad de información para los clientes	**Gestor:** *Gerente de operaciones **Ejecutor:** *Gestor de proyectos	**Presentación:** *Compromisos de seguridad de información asociados al contrato del servicio	1. Establecer la presentación detallada de los límites y responsabilidades establecidas en el contrato con los clientes para evitar reclamos sin sustento y propiciar la retroalimentación de mejoras	**Resultado esperado:** *Seguimientos con avances según lo planificado *Riesgo mitigado a un nivel aceptable **Cálculo de efectividad:** *El control es implementado dentro de los plazos establecidos	jun-15	nov-15	**Realizado**

Anexo J. Informe de seguimiento de riesgos

Descripción: Informe que contiene el estado vigente de los riesgos de seguridad de información identificados, así como también la situación de los controles que están siendo implementados para subsanarlos.
Aprobado: Versión 1.0 por Representante de la Dirección

En base al Plan de Tratamiento de Riesgos vigente, se ha realizado el seguimiento de los controles planificados, donde cada uno de estos se encuentra en el estado que se indica a continuación:

Fecha de revisión: 29/09/2015

ID	Riesgo	Control	Tareas	Inicio	Cierre	Estado	Detalle
PTR01	GR15-R01: Robo de laptop de consultoría que contiene información del cliente durante la visita o en tránsito desde el cliente	8.3.3 Encriptamiento de unidades de disco duro destinadas fuera de la empresa	1. Implementar el encriptamiento a nivel de BIOS para el disco duro de las laptops de consultoría.	jun-15	ago-15	**Realizado**	Se han encriptado bajo contraseña los discos de las 2 laptops usadas para consultoría en el exterior (la asignada al Gestor de Proyecto y al Gerente de Operaciones). Ambas encriptaciones han sido verificadas.
PTR02	GR15-R02: Copia no autorizada de información mediante dispositivo USB desde la laptop de consultoría	11.2.8 Bloqueo automático de equipos por inactividad	1. Reducir a 3 minutos el tiempo de bloqueo por inactividad en el equipo de consultoría	jun-15	ago-15	**Realizado**	Se ha realizado manualmente la configuración de seguridad a la laptop del Gestor de Proyecto, mediante la cuenta de administrador del equipo. En el caso del Gerente de Operaciones este control no es aplicable, pues no es usada en el trabajo de campo de las reuniones con clientes.
PTR03	GR15-R07: Copia no autorizada de registros por los consultores, desde el servidor de archivos con información del proyecto	8.3.1 Bloqueo de puertos USB en los equipos - consultores	1. Implementar el bloqueo de puertos USB en los equipos de los consultores	jun-15	ago-15	**Realizado**	Se ha realizado el bloqueo de puertos, debido a que no se ha podido realizar el bloqueo mediante la herramienta de administración, se ha tenido que realizar manualmente para todos los equipos de escritorio de los consultores.
PTR04	GR15-R08: Copia no autorizada de registros por el administrador de plataformas, desde el servidor de archivos con información del proyecto	7.2.2 Charla de sensibilización - administrador de plataformas	1. Realizar charlas sobre seguridad de información específicas para el administrador de plataformas y sus funciones	jun-15	ago-15	**Realizado**	Se ha realizado la charla informando al administrador de plataformas sobre sus responsabilidades y los controles relacionados a su función. Se ha tomado una evaluación con resultados exitosos.

ID	Riesgo	Control	Tareas	Inicio	Cierre	Estado	Detalle
PTR05	GR15-R11: Eliminación o modificación intencional para sabotear productos, por personal descontento	7.2.3 Penalización por sabotajes o daños intencionales	1. Incluir en el contrato el reconocimiento de que en caso se reciban penalidades a la empresa, originadas en un intento de daño intencional por el empleado, este asumirá la totalidad del monto de pérdida.	jun-15	nov-15	**En proceso**	Se ha revisado con la asesoría legal externa la narrativa que se especificará en la adenda, por cumplimiento del marco legal la penalización solo será aplicable cuando sea objetivamente demostrado que ha habido intencionalidad (dolo). Se espera iniciar con la suscripción de las adendas para el mes de octubre.
PTR06	GR15-R13: Conflictos de versionado en los productos del servicio, por uso inadecuado del mecanismo versionador	12.1.1 Protocolo de desarrollo de software y productos del servicio	1. Actualizar el protocolo de desarrollo de software, de manera que especifique en un anexo los lineamientos técnicos para manejar un conflicto de versiones o duplicidad de componentes.	jun-15	nov-15	**En proceso**	Se tiene el documento completo en versión borrador, pero queda pendiente la validación con el gerente de operaciones para su aprobación. Se estima que la nueva versión esté vigente desde mediados de octubre.
PTR07	GR15-R24: Copia no autorizada de registros por los analistas de calidad, desde el servidor de archivos con información del proyecto	8.3.1 Bloqueo de puertos USB en los equipos - analistas de calidad	1. Implementar el bloqueo de puertos USB en los equipos de los analistas de calidad	jun-15	ago-15	**Realizado**	Se ha realizado el bloqueo de puertos, debido a que no se ha podido realizar el bloqueo mediante la herramienta de administración, se ha tenido que realizar manualmente para todos los equipos de escritorio de los analistas de calidad.
PTR08	GR15-R34: Pérdida del CD que contiene los componentes presentados en el entregable, en tránsito al cliente	9.4.1 Protección por contraseña del acceso a discos compactos (CD/DVD)	1. Establecer la obligación para el consultor de realizar todas las grabaciones de discos para clientes usando una capa de autenticación	jun-15	ago-15	**Realizado**	Se implementó inmediatamente para los entregables a la fecha. Además, se ha realizado una actualización del protocolo para que incluya esta práctica como una obligación permanente. Queda pendiente aprobar esta actualización por el Gerente de Operaciones.
PTR09	Atender la oportunidad GR15-O01: Conocimiento limitado del personal del cliente respecto a las condiciones contractuales de seguridad de información	7.2.2 Charlas explicativas de las condiciones de seguridad de información para los clientes	1. Establecer la presentación detallada de los límites y responsabilidades establecidas en el contrato con los clientes para evitar reclamos sin sustento y propiciar la retroalimentación de mejoras	jun-15	nov-15	**En proceso**	Se implementó inmediatamente para el proyecto más reciente que se ha desarrollado. Además, se ha realizado una actualización del protocolo para que incluya esta práctica como una obligación permanente. Queda pendiente aprobar esta actualización por el Gerente de Operaciones y aplicar las charlas en aquellos proyectos antiguos.

Anexo K. Declaración de aplicabilidad de controles

Descripción: Lista de controles requeridos por la organización, la razón de su necesidad, así como también el estado que cada uno de estos presenta en la actualidad. En cada caso se muestra la relación que existe con el Anexo A del estándar ISO/IEC 27001:2013.
Aprobado: Versión 1.0 por Representante de la Dirección

A continuación se declaran todos los controles implementados (IM) y en proceso de implementación (PI) los cuales son identificados como necesarios para la organización:

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Dirección - Política general	5.1.1	Política para seguridad de información	**SI**	Decisión de la dirección La dirección aprobó una política como marco general para regular la gestión de la seguridad de información, y un paquete de políticas específicas para regulas aspectos puntuales. Estas deben ser adecuadas para la organización, por lo que son revisadas periódicamente por los líderes de la organización para posibles actualizaciones futuras. Requisito del SGSI La creación y revisión de la política de seguridad de información son requisitos de la ISO 27001:2013.	(IM) Política de Seguridad de Información (IM) Políticas Específicas de Seguridad de Información (PESI)
	5.1.2	Revisión de las políticas de seguridad de información	**SI**		(IM) Política de Seguridad de Información (IM) Plan de operación y comunicaciones del SGSI (IM) Acta de revisión por la dirección
Dirección - Roles, responsabilidades y autoridades	6.1.1	Roles y responsabilidades de seguridad de información	**SI**	Decisión de la dirección La dirección requiere que los miembros de la organización cumplan con roles y responsabilidades específicos, por lo que han adoptado un marco dentro del cual ellos también tienen una participación. Entre sus roles destaca el de la gerencia, que revisa el SGSI periódicamente y aprueba los principales documentos para su operación. Requisito del SGSI La definición de roles y responsabilidades, y la evidencia del liderazgo sobre el sistema son requisitos de la ISO 27001:2013.	(IM) PESI - 1. Roles, responsabilidades y autoridades (IM) Plan de operación y comunicaciones del SGSI (IM) Acta de designación de roles del SGSI
	7.2.1	Responsabilidades de la gerencia	**SI**		(IM) PESI - 1. Roles, responsabilidades y autoridades (IM) Acta de designación de roles del SGSI

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Dirección - Requisitos legales	18.1.1	Identificación de legislación aplicable y requisitos contractuales	**SI**	Decisión de la dirección La dirección requiere contar con un responsable de identificar toda legislación aplicable a la seguridad de información, para evitar sanciones originadas en incumplimientos legales. Requisito de seguridad de información Se han identificado las siguientes leyes, frente a las cuales la organización ha especificado su cumplimiento respecto a los aspectos de seguridad de información que comprenden: Ley de Protección de Datos Personales, Ley sobre el Derecho de Autor, Ley de Delitos Informáticos. Requisito del SGSI La identificación y cumplimiento de los requisitos de seguridad de información (legales y contractuales) son requisitos de la ISO 27001:2013. **Exclusiones (6.2.2)** **Debido a que el negocio no desarrolla actividades de Teletrabajo la ley relacionada a este tipo de actividad no es considerada como un requisito aplicable.**	(IM) PESI - 2. Requisitos legales (IM) Informe de contexto de la organización (IM) Informe de necesidades y expectativas de las partes interesadas
	18.1.2	Derechos de propiedad intelectual	**SI**		(IM) PESI - 2. Requisitos legales (IM) Inventario de software por equipo (PI) Plan de requisitos de seguridad de información
	18.1.4	Privacidad y protección de información de identificación personal	**SI**		(IM) PESI - 2. Requisitos legales (IM) Inscripción del banco de datos de personal de la organización. (PI) Plan de requisitos de seguridad de información
	6.2.2	Teletrabajo	**NO**		-
Coordinador de Seguridad - Charlas y capacitación	7.2.2	Concientización, educación y entrenamiento en seguridad de información	**SI**	Decisión de la dirección La dirección ha dispuesto que su personal esté capacitado y concientizado en temas de seguridad de información, en particular los que asumen un rol dentro del SGSI. Requisito del SGSI La capacitación y concientización del personal son requisitos de la ISO 27001:2013. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (AI15-001, RD15-001, GR15-O01).	(IM) PESI - 3. Charlas y capacitación (IM) Plan de concientización, capacitación y evaluación (IM) Charlas sobre seguridad de información al personal de consultoría (GR15) (PI) Mentorías de seguridad de información (AI15-001) (PI) Portal e-learning (RD15-001) (PI) Charlas de sensibilización - administrador de plataformas (GR15-R04) (PI) Charlas explicativas de las condiciones de seguridad de información para los clientes (GR15-O01)

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Coordinador de Seguridad - Riesgos, incidentes y especialistas	6.1.4	Contacto con grupos de interés especiales	SI	Decisión de la dirección La dirección requiere que se atiendan los eventos, debilidades e incidentes relacionados a seguridad de información, para lo cual se requiere contar con especialistas internos (mesa de ayuda, coordinador de seguridad de información) y externos (especialistas de seguridad de los proveedores) para casos más severos. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (AI15-003)	(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información (IM) Lista de contactos externos de proveedores y especialistas en seguridad
	16.1.1	Responsabilidades y procedimientos (incidentes)	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información (IM) Operador TIC designado como responsable de la función de mesa de ayuda, deriva requerimientos a los especialistas (IM) Decálogo de la seguridad de información
	16.1.2	Reporte de eventos de seguridad de información	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información
	16.1.3	Reporte de debilidades de seguridad de información	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información (PI) Buzón de retroalimentación de partes interesadas (AI15-003)
	16.1.4	Evaluación y decisión sobre eventos de seguridad de información	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información
	16.1.5	Respuesta a incidentes de seguridad de información	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información
	16.1.6	Aprender de incidentes de seguridad de información	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información
	16.1.7	Recolección de evidencia (incidentes)	SI		(IM) PESI - 4. Riesgos, incidentes y especialistas (IM) Procedimiento de gestión de eventos, incidentes y debilidades de seguridad de información

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Coordinador de Seguridad - Continuidad de negocio	17.1.1	Planificación de la continuidad de la seguridad de información	**SI**	<u>Decisión de la dirección</u> La dirección requiere que se asegure la continuidad de la operación de la organización para los casos en que incidentes o riesgos significativos lleguen a impactarla, sin que esto comprometa la omisión de los controles de seguridad de información necesarios para su custodia. <u>Asociado a riesgos</u> Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 5. Continuidad de negocio (IM) Plan operativo de continuidad
	17.1.2	Implementación de la continuidad de la seguridad de información	**SI**		(IM) PESI - 5. Continuidad de negocio (IM) Los roles asociados a servicios cuentan con colaboradores alternos que pueden cubrirlos (GR15) (IM) Designación de responsables del plan operativo de continuidad
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de información	**SI**		(IM) PESI - 5. Continuidad de negocio (IM) Registros de pruebas del plan operativo de continuidad
Operación - Gestión de documentos	12.1.1	Procedimientos operativos documentados	**SI**	<u>Decisión de la dirección</u> La dirección dispone que se mantenga vigente la documentación de las actividades centrales del negocio: servicio de consultoría, actividades de control de calidad y gestión de proyectos. <u>Asociado a riesgos</u> Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (GR15-R06). <u>Requisito del SGSI</u> La gestión adecuada de la documentación generada por el SGSI y sus controles es un requisito de la ISO 27001:2013.	(IM) PESI - 6. Gestión de documentos (IM) Protocolo de gestión de proyectos (GR15) (IM) Protocolo de atención de clientes de consultoría (GR15) (IM) Protocolo de desarrollo de software y productos del servicio (GR15) (PI) Protocolo de desarrollo de software y productos del servicio (GR15-R06) - mejora (IM) Protocolo de pruebas sobre los sistemas y aplicaciones (IM) Protocolo de asesoría en la implantación de los sistemas (GR15)
Operación - Prácticas Generales de Seguridad - Personales	11.2.8	Equipo de usuario desatendido	**SI**	<u>Decisión de la dirección</u> La dirección dispone que se acaten un conjunto de buenas prácticas personales respecto al trabajo desarrollado dentro de la organización por su personal, estas son las preexistentes y documentadas en el decálogo de la seguridad de información. <u>Asociado a riesgos</u>	(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Decálogo de la seguridad de información (PI) Bloqueo automático de equipos por inactividad (GR15-R02)
	11.2.9	Política de escritorio y pantalla limpios	**SI**		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Decálogo de la seguridad de información
	8.1.3	Uso aceptable de activos	**SI**		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Decálogo de la seguridad de información

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
	9.3.1	Uso de la información de autenticación secreta	SI	Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (RD15-002, GR15-R02, GR15-R07, GR15-R03)	(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Decálogo de la seguridad de información
	12.6.2	Restricción en la instalación de software	SI		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Decálogo de la seguridad de información (PI) Revisión periódica para verificar el software instalado (RD15-002)
	6.2.1	Política de dispositivos móviles	SI		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Decálogo de la seguridad de información (IM) PESI - Prácticas Generales de Seguridad. Política de dispositivos móviles (GR15)
	8.3.1	Gestión de medios removibles	SI		(IM) PESI - 7. Prácticas Generales de Seguridad. Gestión de medios removibles (GR15) (IM) Decálogo de la seguridad de información (PI) Bloqueo de puertos USB en los equipos - analistas de calidad (GR15-R07) (PI) Bloqueo de puertos USB en los equipos - consultores (GR15-R03)
Operación - Prácticas Generales de Seguridad - Organizacionales	13.2.1	Políticas y procedimientos de transferencia de información	SI		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Directiva de seguridad de información (IM) Acceso restringido a internet mediante una lista blanca de portales (GR15)
	12.1.2	Gestión del cambio	SI	<u>Decisión de la dirección</u> La dirección dispone que se acaten un conjunto de buenas prácticas personales respecto al trabajo desarrollado dentro de la organización por sus áreas funcionales (gerencias o jefaturas), estas son las preexistentes y documentadas en la directiva de la seguridad de información. <u>Asociado a riesgos</u> Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Directiva de seguridad de información (IM) Responsables designados para la administración de la instalación de productos (GR15) (IM) Responsables designados para la administración del cambio en los repositorios (GR15) (IM) Protocolo de gestión de proyectos (GR15)
	6.1.2	Segregación de deberes	SI		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Directiva de seguridad de información
	6.1.5	Seguridad de información en la gestión de proyectos	SI		(IM) PESI - 7. Prácticas Generales de Seguridad (IM) Directiva de seguridad de información (IM) Designación de responsabilidades sobre la seguridad en las partes involucradas (GR15) (IM) Protocolo de gestión de proyectos (GR15)

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Operación - Desarrollo de software - antes	14.1.1	Análisis y especificación de requisitos de seguridad de información	SI	Decisión de la dirección La dirección, respecto al alcance y forma de ejecución del servicio de consultoría ha aprobado protocolos que restringen y orientan la práctica de las actividades que deben hacerse y cómo deben hacerse, así como también aquellas actividades no permitidas: antes del desarrollo. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de gestión de proyectos (GR15) (IM) Protocolo de atención de clientes de consultoría (GR15)
	14.2.4	Restricción en cambios a paquetes de software	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de gestión de proyectos (GR15) (IM) Protocolo de atención de clientes de consultoría (GR15)
	9.4.5	Control de acceso a código fuente de programas	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de gestión de proyectos (GR15) (IM) Protocolo de atención de clientes de consultoría (GR15)
	14.2.2	Procedimientos de control de cambios en sistemas	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de gestión de proyectos (GR15) (IM) Protocolo de atención de clientes de consultoría (GR15)
	14.2.6	Entorno de desarrollo seguro	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de gestión de proyectos (GR15) (IM) Protocolo de atención de clientes de consultoría (GR15)
Operación - Desarrollo de software - durante	14.2.1	Política de desarrollo seguro	SI	Decisión de la dirección La dirección, respecto al alcance y forma de ejecución del servicio de consultoría ha aprobado protocolos que restringen y orientan la práctica de las actividades que deben hacerse y cómo deben hacerse, así como también aquellas actividades no permitidas: durante el desarrollo. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de desarrollo de software y productos del servicio (GR15)
	14.2.5	Principios de ingeniería para sistemas seguros	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de desarrollo de software y productos del servicio (GR15)
	14.2.7	Desarrollo externalizado	NO	**Exclusiones (14.2.7)** **Entre las actividades limitadas está la decisión de no involucrar a empresas competidoras en el desarrollo de los proyectos, la integración de nuevo personal al proyecto solo se podrá hacer mediante la contratación del mismo.**	-

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Operación - Desarrollo de software - después	14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma operativa	SI	Decisión de la dirección La dirección, respecto al alcance y forma de ejecución del servicio de consultoría ha aprobado protocolos que restringen y orientan la práctica de las actividades que deben hacerse y cómo deben hacerse, así como también aquellas actividades no permitidas: después del desarrollo.	(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de pruebas sobre los sistemas y aplicaciones
	14.2.9	Pruebas de aceptación del sistema	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de pruebas sobre los sistemas y aplicaciones
	14.2.8	Pruebas de seguridad del sistema	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de pruebas sobre los sistemas y aplicaciones
	14.3.1	Protección de datos de prueba	SI		(IM) PESI - 8. Desarrollo de Software (IM) Protocolo de pruebas sobre los sistemas y aplicaciones
Soporte de TI - Control del acceso lógico	9.1.1	Política de control de accesos	SI	Decisión de la dirección La dirección necesita que se controle adecuadamente el acceso a la información y los recursos que la almacenan o procesan, por lo que ha aprobado un esquema de administración que regula esta actividad (política), además de un procedimiento que regula las actividades y responsables de su aplicación. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (AI15-002, GR15-R08)	(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.1.2	Acceso a redes y servicios de red	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.2.1	Registro y anulación de usuario	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.2.2	Provisión de acceso a usuario	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.2.3	Gestión de derechos de acceso privilegiados	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos (IM) Pistas de auditoría para el personal administrador de plataformas
	9.2.4	Gestión de la información de autenticación secreta de los usuarios	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.2.5	Revisión de los derechos de acceso de los usuarios	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos (PI) Revisión periódica de accesos para verificar permisos (AI15-002)
	9.2.6	Retiro o ajuste de los derechos de acceso	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.4.1	Restricción de acceso a la información	SI		(IM) PESI - 9. Control del acceso lógico (IM) Equipos de cómputo protegidos con contraseña (GR15) (PI) Protección por contraseña del acceso a discos compactos (CD/DVD) (GR15-R08)
	9.4.2	Procedimiento de autenticación segura	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.4.3	Sistema de gestión de contraseñas	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos
	9.4.4	Uso de programas utilitarios privilegiados	SI		(IM) PESI - 9. Control del acceso lógico (IM) Procedimiento de gestión de accesos a servicios tecnológicos

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Soporte de TI - Seguridad informática - Criptografía	10.1.1	Política de uso de controles criptográficos	SI	Decisión de la dirección La dirección dispone que se apliquen controles criptográficos para algunos casos asociados a un nivel mayor de confidencialidad en la transmisión y almacenamiento de datos, por su carácter sensible.	(IM) PESI - 10. Seguridad informática (IM) Uso de protocolos seguros para comunicaciones
	10.1.2	Gestión de claves (criptográficas)	SI		(IM) PESI - 10. Seguridad informática
	18.1.5	Regulación de controles criptográficos	SI		(IM) PESI - 10. Seguridad informática
Soporte de TI - Seguridad informática - Controles	12.2.1	Controles contra el software malicioso	SI	Decisión de la dirección La dirección ha gestionado la implementación de mecanismos de control de seguridad informática a lo largo de la existencia de la organización, por considerarlos necesarios y ha dispuesto su mantenimiento en el tiempo en las políticas aprobadas. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (AI15-002, GR15-R08)	(IM) PESI - 10. Seguridad informática (IM) Solución antimalware para equipos de la consultora (GR15)
	12.4.1	Registro de eventos	SI		(IM) PESI - 10. Seguridad informática (IM) Registros de actividad de los servidores, servicios y plataformas (GR15)
	12.4.2	Protección de información de registros	SI		(IM) PESI - 10. Seguridad informática (IM) Registros de auditoría incluidos dentro de los respaldos de información
	12.4.3	Registros de administrador y operador	SI		(IM) PESI - 10. Seguridad informática (IM) Pistas activas cubren los registros de operación de cuentas administradoras
	18.1.3	Protección de registros	SI		(IM) PESI - 10. Seguridad informática (IM) Registros de auditoría incluidos dentro de los respaldos de información
	12.6.1	Gestión de vulnerabilidades técnicas	SI		(IM) PESI - 10. Seguridad informática (IM) Análisis de vulnerabilidades periódicos y planificados anualmente
Soporte de TI - Equipos informáticos	11.2.1	Ubicación y protección de equipos	SI	Decisión de la dirección La dirección reconoce que la principal instancia donde se aloja la información del negocio y donde se desarrolla la labor de consultoría son los equipos informáticos, por lo que ha dispuesto que se manejen controles relacionados a su adquisición, instalación, uso, mantenimiento y baja controlada: equipos de escritorio. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 11. Equipos informáticos (IM) Cadenas con candado de seguridad para equipos de cómputo (GR15) (IM) Equipos instalados en ubicaciones seguras física y ambientalmente (GR15)
	11.2.3	Seguridad del cableado	SI		(IM) PESI - 11. Equipos informáticos (IM) Mecanismos de aseguramiento y provisión de comunicaciones y energía (GR15)
	11.2.4	Mantenimiento de equipos	SI		(IM) PESI - 11. Equipos informáticos (IM) Mantenimiento regular de equipos y servidores (GR15) (IM) Plan de mantenimiento y seguimiento de equipos
	11.2.5	Retiro de activos	SI		(IM) PESI - 11. Equipos informáticos (IM) Hoja de ingreso / salida de bienes
	8.3.2	Disposición de medios	SI		(IM) PESI - 11. Equipos informáticos (IM) Inventario de equipos y hardware (IM) Hoja de baja / transferencia de equipos
	11.2.7	Eliminación segura o reutilización de equipos	SI		(IM) PESI - 11. Equipos informáticos (IM) Hoja de baja / transferencia de equipos

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Soporte de TI - Gestión de plataformas	12.1.3	Gestión de la capacidad	SI	Decisión de la dirección La dirección reconoce que la principal instancia donde se aloja la información del negocio y donde se desarrolla la labor de consultoría son los equipos informáticos, por lo que ha dispuesto que se manejen controles relacionados a su adquisición, instalación, uso, mantenimiento y baja controlada: servidores y equipos de comunicaciones. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 12. Gestión de plataformas (IM) Planificación en la capacidad de los servidores (espacio, procesamiento)
	12.1.4	Separación de ambientes de desarrollo, prueba y operación	SI		(IM) PESI - 12. Gestión de plataformas (IM) Ambientes de desarrollo y calidad mantenidos en servidores separados
	12.3.1	Respaldo de información	SI		(IM) PESI - 12. Gestión de plataformas (IM) Mecanismo de control de versiones en línea (GR15) (IM) Respaldos de la información de los servidores (GR15) (IM) Servicio de alojamiento sincronizado de archivos en línea (copias de respaldo versionadas) (GR15)
	12.4.4	Sincronización del reloj	SI		(IM) PESI - 12. Gestión de plataformas (IM) Servicio de tiempo, en base al cual se sincronizan los demás servidores
	12.5.1	Instalación de software en sistemas operacionales	SI		(IM) PESI - 12. Gestión de plataformas (IM) Se realizan pruebas previas a la instalación o actualización de software en los servidores
	17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI		(IM) PESI - 12. Gestión de plataformas (IM) Mecanismos alternos disponibles para el servicio de consultoría (GR15)
Soporte de TI - Gestión de redes	13.1.1	Controles de red	SI	Decisión de la dirección La dirección reconoce que las redes interna y externa a la organización son el principal medio donde se trasmite la información del negocio, a partir de la labor de consultoría, por lo que ha dispuesto que se manejen controles relacionados a su administración, control y protección. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 13. Gestión de redes (IM) Mecanismos de protección de la red interna: el firewall, la DMZ, el IDS, IPS, la herramienta para administración del acceso a portales externos
	13.1.2	Seguridad de servicios de red	SI		(IM) PESI - 13. Gestión de redes (IM) Mecanismos de protección de la red interna: el firewall, la DMZ, el IDS, IPS, la herramienta para administración del acceso a portales externos
	13.1.3	Segregación en redes	SI		(IM) PESI - 13. Gestión de redes (IM) Red interna independizada en segmentos (administración, calidad, consultoría) además aislada de la red externa (internet)
	13.2.3	Mensajería electrónica	SI		(IM) PESI - 13. Gestión de redes. Uso del servicio de correo electrónico (GR15) (IM) Servicio de correo electrónico bajo arquitectura y protocolos seguros (GR15)
	14.1.2	Asegurar aplicaciones de servicio en redes públicas	SI		(IM) PESI - 13. Gestión de redes. Uso del servicio de correo electrónico (GR15) (IM) Servicio de correo electrónico bajo arquitectura y protocolos seguros (GR15)
	14.1.3	Proteger transacciones de servicios de aplicación	SI		(IM) PESI - 13. Gestión de redes. Uso del servicio de correo electrónico (GR15) (IM) Servicio de correo electrónico bajo arquitectura y protocolos seguros (GR15)

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Administrador - Gestión de activos	8.1.1	Inventario de activos	SI	Decisión de la dirección La dirección reconoce que los activos que maneja tienen un valor en función a la información que alojan, razón por la cual ha dispuesto que la gerencia de administración complemente a la de servicios TIC para la adecuada custodia de estos. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (GR15-R01).	(IM) PESI - 14. Gestión de activos (IM) Inventario de hardware y dispositivos (IM) Inventario de software y aplicaciones (IM) Inventario general de
	8.1.2	Propiedad de activos	SI		(IM) PESI - 14. Gestión de activos (IM) Inventario de hardware y dispositivos (IM) Inventario de software y aplicaciones
	8.1.4	Retorno de activos	SI		(IM) PESI - 14. Gestión de activos (IM) Inventario de hardware y dispositivos (IM) Inventario de software y aplicaciones (IM) Hoja de salida - trabajadores
	8.2.1	Clasificación de información	SI		(IM) PESI - 14. Gestión de activos (IM) Inventario de hardware y dispositivos (IM) Inventario de software y aplicaciones
	8.2.2	Etiquetado de información	SI		(IM) PESI - 14. Gestión de activos
	8.2.3	Manejo de activos	SI		(IM) PESI - 14. Gestión de activos (IM) Decálogo de la seguridad de información
	11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI		(IM) PESI - 11. Equipos informáticos (IM) Uso de transporte controlado y seguro (GR15)
	8.3.3	Transferencia física de medios	SI		(IM) PESI - 14. Gestión de activos (PI) Encriptamiento de unidades de disco duro destinadas fuera de la empresa (GR15-R01)

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Administrador - Seguridad física y ambiental	11.1.1	Perímetro de seguridad física	SI	Decisión de la dirección La dirección reconoce que existen riesgos relacionados a amenazas externas e internas, físicas y ambientales, motivo por el cual ha autorizado la implementación progresiva y mantenimiento en el tiempo de los controles de este tipo que a la fecha operan en la organización. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 15. Seguridad física y ambiental (IM) Servicio permanente de vigilancia (IM) Cámaras de seguridad en el acceso a la organización
	11.1.2	Controles físicos de entrada	SI		(IM) PESI - 15. Seguridad física y ambiental (IM) Ambientes sensibles protegidos con mecanismos de control de acceso (GR15) (IM) Servicio permanente de vigilancia
	11.1.3	Aseguramiento de oficinas, salas e instalaciones	SI		(IM) PESI - 15. Seguridad física y ambiental (IM) Puertas con cerradura en todos los ambientes internos de trabajo
	11.1.4	Protección frente a amenazas externas y ambientales	SI		(IM) PESI - 15. Seguridad física y ambiental (IM) Detectores de humo y aniego instalados en ubicaciones estratégicas (IM) Mecanismos de extinción del fuego
	11.1.5	Trabajar en áreas seguras	SI		(IM) PESI - 15. Seguridad física y ambiental (IM) Distribución planificada de espacios de trabajo (IM) Inspecciones municipales de defensa civil respecto a la idoneidad de las instalaciones
	11.1.6	Áreas de despacho y carga	SI		(IM) PESI - 15. Seguridad física y ambiental (IM) Protocolo de recepción de proveedores y productos (IM) Zona de carga y zona de almacén definidas
	11.2.2	Utilidades de soporte	SI		(IM) PESI - 15. Seguridad física y ambiental (IM) Equipo de contingencia eléctrica UPS (IM) Generador eléctrico a base de combustible
Administrador - Gestión de personal	7.1.1	Filtración	SI	Decisión de la dirección La dirección reconoce que su personal es el actor principal respecto a la administración y uso de la información, motivo por el cual, mantiene controles relacionados a los lineamientos aplicables antes, durante y después de la relación contractual con sus empleados. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados (GR15-R05).	(IM) PESI - 16. Gestión de personal (IM) Directiva de selección de personal (IM) Procedimientos de administración - personal
	7.1.2	Términos y condiciones de empleo	SI		(IM) PESI - 16. Gestión de personal. Términos y condiciones de empleo (GR15) (IM) Contratos con disposiciones específicas sobre la seguridad de información (GR15) (IM) Procedimientos de administración - personal
	7.2.3	Proceso disciplinario	SI		(IM) PESI - 16. Gestión de personal (IM) Directiva de administración de personal (PI) Penalización por sabotajes o daños intencionales (GR15-R05) (IM) Procedimientos de administración - personal
	7.3.1	Responsabilidades de terminación o cambio de puesto	SI		(IM) PESI - 16. Gestión de personal (IM) Directiva de administración de personal (IM) Procedimientos de administración - personal
	13.2.4	Acuerdos de confidencialidad o no divulgación	SI		(IM) PESI - 16. Gestión de personal (IM) Acuerdo de confidencialidad y de reconocimiento de las políticas de seguridad de información (IM) Procedimientos de administración - personal

Dominio	27001-A	Control ISO	Aplica	Justificación	Controles: Implementados (IM) / Por Implementar (PI)
Administrador - Gestión de terceros	6.1.3	Contacto con autoridades	SI	Decisión de la dirección La dirección reconoce que existe una interacción significativa con terceros que implica intercambio de información, por lo que ha establecido condiciones relacionadas a la forma en que mantendrá estas relaciones con otras organizaciones y su personal. Asociado a riesgos Se ha identificado que es necesario mantener este control para la prevención de riesgos o fallos del sistema identificados.	(IM) PESI - 17. Gestión de terceros (IM) Directorio de contactos y emergencias
	13.2.2	Acuerdos de transferencia de información	SI		(IM) PESI - 17. Gestión de terceros (IM) Contratos delimitan las responsabilidades del cliente y la consultora respecto a las condiciones de instalación (GR15) (IM) Contratos delimitan las responsabilidades del cliente y la consultora respecto a las condiciones del proyecto (GR15) (IM) La consultora y sus clientes cuentan con copias de todo documento firmado (GR15)
	15.1.1	Política de seguridad de información para la relación con proveedores	SI		(IM) PESI - 17. Gestión de terceros (IM) Contratos con proveedores incluyen condiciones de seguridad de información y otras asociadas a la disponibilidad y nivel de servicio (IM) Procedimientos de administración - proveedores
	15.1.2	Dirigiendo la seguridad en los acuerdos de provisión	SI		(IM) PESI - 17. Gestión de terceros (IM) Contratos con proveedores incluyen condiciones de seguridad de información y otras asociadas a la disponibilidad y nivel de servicio, y las respectivas penalizaciones por incumplimiento (IM) Procedimientos de administración - proveedores
	15.1.3	Cadena de suministro de tecnologías de información y comunicación	SI		(IM) PESI - 17. Gestión de terceros (IM) Contratos con proveedores incluyen condiciones de seguridad de información y otras asociadas a la disponibilidad y nivel de servicio, y las respectivas penalizaciones por incumplimiento (IM) Procedimientos de administración - proveedores
	15.2.1	Monitoreo y revisión del proveedor de servicios	SI		(IM) PESI - 17. Gestión de terceros (IM) Procedimientos de administración - proveedores
	15.2.2	Gestionar cambios a proveedores de servicio	SI		(IM) PESI - 17. Gestión de terceros (IM) Procedimientos de administración - proveedores
Auditor Interno - Auditoría de seguridad de información	18.2.1	Revisión independiente de la seguridad de información	SI	Decisión de la dirección La dirección reconoce la necesidad de revisar el estado de la seguridad de información por observadores independientes, por ese motivo, incorpora la función de auditoría interna al marco organizacional, la cual puede ser asumida por un tercero (proveedor de auditoría). Requisito del SGSI La revisión periódica del SGSI y los controles de seguridad de información son requisitos de la ISO 27001:2013.	(IM) PESI - 18. Auditoría de seguridad de información (IM) Programa de auditoría interna del SGSI (IM) Plan de auditoría interna del SGSI (IM) Informe de resultados de la auditoría interna
	18.2.2	Cumplimiento de políticas de seguridad y estándares	SI		(IM) PESI - 18. Auditoría de seguridad de información (IM) Programa de auditoría interna del SGSI (IM) Plan de auditoría interna del SGSI (IM) Informe de resultados de la auditoría interna
	18.2.3	Revisión del cumplimiento técnico	SI		(IM) PESI - 18. Auditoría de seguridad de información (IM) Revisiones periódicas de Ethical Hacking
	12.7.1	Controles de auditoría en sistemas de información	SI		(IM) PESI - 18. Auditoría de seguridad de información

Anexo L. Declaración de objetivos de seguridad de información

Descripción: Objetivos vigentes en la organización respecto a la situación de la seguridad de información que se desea lograr.
Aprobado: Versión 1.0 por Representante de la Dirección
Estructura:

- Generalidades
- Objetivos estratégicos de la organización
- Objetivos de seguridad de información

Generalidades:

La organización ha definido una serie de objetivos estratégicos, los cuales han sido identificados en el **Informe de contexto y requisitos de seguridad de información, Contexto interno – AI2. Misión y objetivos estratégicos**. En base a ellos y en cumplimiento con el compromiso establecido en la **Política de Seguridad de Información**, respecto al aseguramiento de la confidencialidad, integridad y disponibilidad de la información se han establecido los objetivos de seguridad de información, bajo la correspondencia mostrada:

Objetivos estratégicos de la organización

OE1: Fomentar la excelencia del personal que brinda los servicios de consultoría
OE2: Mejorar la satisfacción de los clientes respecto a los servicios recibidos
OE3: Incrementar la efectividad y productividad de los proyectos de consultoría

Objetivos de seguridad de información

OSI1: Fomentar la difusión del cumplimiento de la confidencialidad en el manejo de la información de los proyectos
OSI2: Mejorar la integridad de los productos de consultoría en cuanto a versiones exactas y completitud
OSI3: Incrementar la disponibilidad de la información y servicios requeridos para realizar las actividades de consultoría

Anexo M. Plan de objetivos de seguridad de información

Descripción: Plan de las actividades requeridas para implementar la declaración de objetivos de seguridad de la información:
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
OBJ01	Implementar	Objetivos	Propiciar el logro del objetivo 1	*Se ha aprobado el objetivo 1: "Fomentar la difusión del cumplimiento de la confidencialidad en el manejo de la información de los proyectos"	**Responsable:** *Gerente de Operaciones **Convocado:** *Coordinador de seguridad de información	**Documentos:** *Evaluaciones para el personal **Presentación:** *Roles, responsabilidades y actividades del SGSI **Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop y proyector	1. Ejecutar los planes de capacitación incorporando en el sílabus temas específicos de cuidados respecto al manejo de información confidencialidad 2. Acompañar las charlas con evaluaciones para evaluar el nivel de éxito obtenido de estas	**Resultado esperado:** *Incremento del nivel de concientización del personal de consultoría **Cálculo de efectividad:** *La efectividad del control es medida en una de las métricas del sistema	jul-15	jun-16	**Realizado**
OBJ02	Implementar	Objetivos	Propiciar el logro del objetivo 2	*Se ha aprobado el objetivo 2: "Mejorar la integridad de los productos de consultoría en cuanto a versiones exactas y completitud"	**Responsable:** *Gerente de Operaciones **Convocado:** *Representantes de los procesos (Gerente de Operaciones, Gestor de Proyectos, Jefe de Calidad)	**Documentos:** *Lista de verificación de entregables finales **Personal:** *Analista de calidad **Tecnología:** *Carpeta de control de calidad final en el versionador	1. Establecer dentro del ciclo de desarrollo una última prueba de calidad antes de la entrega. 2. Ejecutar las pruebas dejando constancia en listas de verificación	**Resultado esperado:** *Incremento del nivel de los productos elaborados y presentados **Cálculo de efectividad:** *La efectividad del control es medida en una de las métricas del sistema	jul-15	jun-16	**Realizado**
OBJ03	Implementar	Objetivos	Propiciar el logro del objetivo 3	*Se ha aprobado el objetivo 3: "Incrementar la disponibilidad de la información y servicios requeridos para realizar las actividades de consultoría"	**Responsable:** *Gerente de servicios TIC **Convocado:** *Responsable de tecnología y soporte (operador TIC)	**Documentos:** *Plan de monitoreo de servicios TIC *Reportes de servicio de los proveedores **Personal:** *Operador TIC	1. Realizar el seguimiento a los servicios TIC de terceros en base al plan de monitoreo 2. Contrastar la información contra los reportes recibidos de los proveedores 3. Escalar las diferencias significativas al gerente de servicios TIC para que gestione reclamos, de ser necesarios.	**Resultado esperado:** *Incremento de la disponibilidad de los servicios TIC **Cálculo de efectividad:** *La efectividad del control es medida en una de las métricas del sistema	jul-15	jun-16	**Realizado**

Anexo N. Plan de requisitos de seguridad de información

Descripción: Plan para la atención de los requisitos de seguridad de información que han sido reconocidos dentro del alcance del sistema.
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
REQ01	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Contratos y acuerdos con clientes	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información *Contratos y acuerdos con clientes	1. Incluir disposiciones que regulen el cumplimiento de las condiciones de los contratos con clientes en las Políticas Específicas 2. Establecer una verificación periódica de estos cumplimientos por parte del Coordinador de Seguridad de Información	**Resultado esperado:** *Registros de incidentes de incumplimientos con clientes relacionados a la seguridad de información	ago-15	nov-16	**En proceso**
REQ02	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Contratos y acuerdos con el personal	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información *Contratos y acuerdos con personal	1. Incluir disposiciones que regulen el cumplimiento de las condiciones de los contratos con trabajadores en las Políticas Específicas 2. Establecer una verificación periódica de estos cumplimientos por parte del Coordinador de Seguridad de Información	**Resultado esperado:** *Registros de incidentes de incumplimientos de personal relacionados a la seguridad de información	ago-15	nov-16	**En proceso**
REQ03	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Contratos con proveedores de servicios TI	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información *Contratos y acuerdos con proveedores de servicios TI	1. Designar al operador de TI, para que reporte al Coordinador de Seguridad de Información cualquier incidente relacionado a interrupciones de servicio. 2. Mantener una estadística permanente de este tipo de servicios	**Resultado esperado:** *Estadística de la disponibilidad de los servicios	jul-15	nov-16	**En proceso**
REQ04	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Ley de Protección de Datos Personales	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información *Ley y reglamento de Protección de Datos Personales	1. Analizar la ley y el reglamento para delimitar el alcance de su aplicación. 2. Inscribir en la APDP los bancos de datos definidos. 3. Implementar los demás artículos relacionados a la seguridad de información en la ley: mejoras de controles	**Resultado esperado:** *Implementación de un esquema para cumplir con la Ley de Protección de Datos Personales	jul-15	nov-16	**En proceso**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
REQ05	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Ley sobre el Derecho de Autor	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información *Ley sobre el Derecho de Autor	1. Analizar la ley para delimitar el alcance de su aplicación, respecto al uso de software no licenciado. 2. Designar un responsable de la verificación (para que sea periódica). 3. Implementar un plan de verificación y subsanación de los hallazgos obtenidos	**Resultado esperado:** *Implementación de un esquema para cumplir con la Ley sobre Derecho de Autor	jul-15	nov-16	**En proceso**
REQ06	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Ley de Delitos Informáticos	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información *Ley de Delitos Informáticos	1. Analizar la ley para delimitar el alcance de su aplicación. 2. Establecer las disposiciones en las políticas necesarias para cumplir con los artículos aplicables de la Ley. 3. Difundir las nuevas disposiciones entre el personal responsable de cumplirlas.	**Resultado esperado:** *Implementación de un esquema para cumplir con la Ley de Delitos Informáticos	jul-15	nov-16	**En proceso**
REQ07	Implementar	Requisitos	Propiciar el cumplimiento del requisito de: Entrega de productos a clientes	*Se ha aprobado el plan de requisitos de seguridad de información	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de requisitos de seguridad de información	1. Establecer una última etapa de revisión (personal de calidad) sobre el producto creado (CD) para identificar si contiene errores. 2. Reportar los resultados a la gerencia de operaciones, antes de la entrega del producto (CD).	**Resultado esperado:** *Reportes de verificación final del entregable	jul-15	nov-16	**En proceso**

Anexo O. Plan de concientización, capacitación y evaluación

Descripción: Plan de las acciones a desarrollar para capacitar y concientizar al personal de la organización, así como también para evaluar si se ha logrado realizar con efectividad.
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
CON01	Implementar	Capacitación	Evaluar la competencia del personal	*Se ha aprobado el plan de concientización, capacitación y evaluación	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal que participa del SGSI	**Documentos:** *Plan de concientización, capacitación y evaluación *Evaluaciones para el personal	1. Diseñar pruebas para evaluar al personal designado para cumplir roles en el sistema 2. Ejecutar la evaluación del personal	**Resultado esperado:** *Resultados de evaluación de personal	jul-15	ago-15	**Realizado**
CON02	Implementar	Capacitación	Charlas de Concientización	*Se ha aprobado el plan de concientización, capacitación y evaluación	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal de la organización	**Documentos:** *Plan de concientización, capacitación y evaluación *Temario de la concientización **Presentación:** *Concientización en seguridad de información **Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop y proyector	1. Ejecutar la charla de concientización general - Grupo 1 2. Ejecutar la charla de concientización general - Grupo 2 2. Ejecutar la charla de concientización general (rezagados)	**Resultado esperado:** *Listas de asistencia a la presentación *Personal concientizado	ago-15	ago-15	**Realizado**
CON03	Implementar	Capacitación	Capacitaciones para roles específicos	*Se ha aprobado el plan de concientización, capacitación y evaluación *Se ha completado la primera evaluación de la competencia del personal	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Personal que participa del SGSI	**Documentos:** *Plan de concientización, capacitación y evaluación *Evaluaciones para el personal **Presentación:** *Roles, responsabilidades y actividades del SGSI **Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop y proyector	1. Identificar personal que requiere mejorar o adquirir ciertas competencias, en base a los resultados de las evaluaciones previas 2. Ejecutar capacitaciones al personal identificado 3. Ejecutar la re-evaluación del personal capacitado	**Resultado esperado:** *Listas de asistencia a la presentación *Personal del sistema competente	ago-15	ago-15	**Realizado**

Anexo P. Plan de métricas de seguridad de información

Descripción: Plan que define las métricas del SGSI, los controles de seguridad de información y los objetivos de seguridad de la información, que administra el SGSI.
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
MET01	Mantener	Métricas	Ejecutar métrica: Operación del SGSI 1 - Implementación de Controles	*Se ha aprobado la métrica: Avance en la implementación de controles del Plan de Tratamiento de Riesgos	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Plan de tratamiento de riesgos	1. Indagar con cada uno de los responsables de implementar los controles del Plan de Tratamiento de Riesgos el estado de los mismos 2. Analizar si el avance es acorde a lo planeado, si hay adelanto o retraso. 3. Determinar el porcentaje de avance actual.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET02	Mantener	Métricas	Ejecutar métrica: Operación del SGSI 2 - Concientización del Personal	*Se ha aprobado la métrica: Cobertura respecto a la adecuada concientización del personal	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Plan de concientización, capacitación y evaluación	1. Obtener las listas de asistencia a las charlas. 2. Analizar si el porcentaje de asistentes es significativo. 3. Determinar el porcentaje de cobertura actual.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET03	Mantener	Métricas	Ejecutar métrica: Operación del SGSI 3 - Cumplimiento de Requisitos	*Se ha aprobado la métrica: Avance en el cumplimiento del plan de requisitos	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Plan de Requisitos de Seguridad de Información	1. Indagar con cada uno de los responsables de implementar el Plan de Requisitos de Seguridad de Información sobre su estado 2. Analizar si el avance es acorde a lo planeado, si hay adelanto o retraso. 3. Determinar el porcentaje de avance actual.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
MET04	Mantener	Métricas	Ejecutar métrica: Operación del SGSI 4 - Implementación de acciones correctivas	*Se ha aprobado la métrica: Avance en la implementación de acciones correctivas	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Plan de Acciones Correctivas	1. Indagar con cada uno de los responsables de implementar el Plan de Acciones Correctivas sobre su estado 2. Analizar si el avance es acorde a lo planeado, si hay adelanto o retraso. 3. Determinar el porcentaje de avance actual.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET05	Mantener	Métricas	Ejecutar métrica: Operación del SGSI 5 - Implementación de acciones de mejora	*Se ha aprobado la métrica: Avance en la implementación de acciones de mejora	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Plan de Acciones de Mejora	1. Indagar con cada uno de los responsables de implementar el Plan de Acciones de Mejora sobre su estado 2. Analizar si el avance es acorde a lo planeado, si hay adelanto o retraso. 3. Determinar el porcentaje de avance actual.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET06	Mantener	Métricas	Ejecutar métrica: Grupos de Controles 1 - Control de accesos a plataformas de trabajo donde se aloja información	*Se ha aprobado la métrica: Porcentaje de cuentas activas en los servidores de archivos, desarrollo y base de datos, justificadas y autorizadas	**Monitor-Medidor:** *Operador TIC **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Formatos de altas y bajas de sistemas y servicios *Registros de usuarios en los sistemas y servicios	1. Obtener los registros vigentes de cuentas activas sobre los sistemas y servicios TI. 2. Analizar estos registros contra los formatos de autorización. 3. Determinar qué porcentaje de las cuentas tienen una asignación con privilegios adecuados.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET07	Mantener	Métricas	Ejecutar métrica: Grupos de Controles 2 - Acuerdos de Confidencialidad en personal interno	*Se ha aprobado la métrica: Porcentaje de personal que ha firmado los acuerdos de confidencialidad	**Monitor-Medidor:** *Gerente de administración **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Registros de personal activo en la organización *Registros de acuerdos de confidencialidad suscritos	1. Obtener los acuerdos de confidencialidad suscritos a la fecha. 2. Analizar contra la lista de personal vigente si existe alguno que no haya suscrito el acuerdo. 3. Determinar qué porcentaje del personal cuenta con cobertura del acuerdo.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
MET08	Mantener	Métricas	Ejecutar métrica: Grupos de Controles 3 - Adecuada cobertura antimalware en equipos de usuarios	*Se ha aprobado la métrica: Porcentaje de equipos de usuario que cuentan con el antivirus activo y actualizado	**Monitor-Medidor:** *Operador TIC **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Registros de la consola antivirus	1. Revisar los estados de la consola antivirus para todos los nodos. 2. Analizar si existen justificaciones para aquellos puestos que no tienen la cobertura actualizada. 3. Determinar el porcentaje de cobertura en todos los nodos respecto a mecanismos antimalware.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET09	Mantener	Métricas	Ejecutar métrica: Grupos de Controles 4 - Personal que cumple con las prácticas de escritorio limpio y bloqueo de pantallas	*Se ha aprobado la métrica: Porcentaje de personal que cumple con la práctica de escritorio limpio y el bloqueo de pantalla en ausencia	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información **Ubicación:** *Áreas de trabajo de los procesos	1. Revisar las ubicaciones de trabajo del personal que participa de los procesos en el alcance. 2. Analizar el estado en que se encontró cada lugar de trabajo y equipo. 3. Determinar el porcentaje de personal que cumple con la política de escritorio limpio y el bloqueo de pantalla en ausencia	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET10	Mantener	Métricas	Ejecutar métrica: Grupos de Controles 5 - Equipos de usuarios con software autorizado instalado	*Se ha aprobado la métrica: Porcentaje de equipos de usuario que cuentan solo con software autorizado y licenciado	**Monitor-Medidor:** *Operador TIC **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Registros del control de licencias	1. Revisar los estados de la consola de monitoreo de software instalado. 2. Analizar si existen diferencias respecto al registro de control de licencias. 3. Determinar el porcentaje de personal que cuenta con software autorizado en sus equipos.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
MET11	Mantener	Métricas	Ejecutar métrica: Objetivos de Seguridad de Información 1 - Fomentar la difusión del cumplimiento de la confidencialidad en el manejo de la información de los proyectos	*Se ha aprobado la métrica: Porcentaje de personal de los equipos de consultoría, concientizado en la seguridad y confidencialidad de la información usada en los proyectos	**Monitor-Medidor:** *Coordinador de seguridad de información **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Plan de concientización, capacitación y evaluación	1. Obtener las evaluaciones del personal de consultoría, respecto a las charlas. 2. Analizar los resultados obtenidos para validar cuáles tienen puntaje satisfactorio. 3. Determinar el porcentaje de personal con puntaje satisfactorio.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET12	Mantener	Métricas	Ejecutar métrica: Objetivos de Seguridad de Información 2 - Mejorar la integridad de los productos de consultoría en cuanto a versiones exactas y completitud	*Se ha aprobado la métrica: Porcentaje de operaciones de actualización regulares respecto a su integridad, en los repositorios de versionado	**Monitor-Medidor:** *Operador TIC **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Registros de actualización del software de versionado.	1. Obtener los registros del software de versionado. 2. Analizar los registros, clasificándolos como regulares si no estuvieron asociados a conflictos de versiones o saltos a una versión anterior. 3. Determinar el porcentaje de registros de tipo regular respecto al total.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**
MET13	Mantener	Métricas	Ejecutar métrica: Objetivos de Seguridad de Información 3 - Incrementar la disponibilidad de la información y servicios requeridos para realizar las actividades de consultoría	*Se ha aprobado la métrica: Porcentaje de disponibilidad de servicios tecnológicos y equipos usados para los proyectos, respecto al horario laboral	**Monitor-Medidor:** *Operador TIC **Analizador-Evaluador:** *Coordinador de seguridad de información	**Documentos:** *Plan de métricas de seguridad de información *Registros de operación de la red y los servidores.	1. Obtener los registros de operación de la red y los servidores. 2. Analizar las interrupciones dentro del horario regular de operación (8am-8pm). 3. Determinar el porcentaje de tiempo en que estos servicios han estado operando adecuadamente.	**Resultado esperado:** *Registros y resultados de métrica definidos	sep-15	oct-15	**Realizado**

Anexo Q. Informe de Métricas de Seguridad de Información

Descripción: Informe de los resultados de las métricas de seguridad de información que se han establecido para el SGSI.
Aprobado: Versión 1.0 por Representante de la Dirección

Fecha de corte: 29/10/2015

ID	Métrica	Resultado	Detalle
MET01	Operación del SGSI 1 - Implementación de Controles	85%	El nivel de avance de la implementación delos 9 controles del PTR es de 85%, debido a que algunos de ellos todavía están pendientes para terminar en el mes de noviembre.
MET02	Operación del SGSI 2 - Concientización del Personal	100%	La totalidad del personal de la organización, incluyendo personal administrativo o el gerente general han participado de al menos una de las charlas.
MET03	Operación del SGSI 3 - Cumplimiento de Requisitos	32%	Se ha obtenido un avance global de 32 % de los planes de implementación de requisitos.
MET04	Operación del SGSI 4 - Implementación de acciones correctivas	-	No existen acciones correctivas a la fecha, por lo que esta métrica no ha podido ser medida.
MET05	Operación del SGSI 5 - Implementación de acciones de mejora	-	No existen acciones de mejora a la fecha, por lo que esta métrica no ha podido ser medida.
MET06	Grupos de Controles 1 - Control de accesos a plataformas de trabajo donde se aloja información	81%	De los 16 usuarios evaluados, se ha detectado que 3 de ellos no cuentan con los formatos requeridos para las asignaciones dadas.
MET07	Grupos de Controles 2 - Acuerdos de Confidencialidad en personal interno	68%	Se ha logrado que todo el personal de servicios de consultoría (11) firme los acuerdos de confidencialidad. Quedan pendientes los que pertenecen a la parte administrativa (5).
MET08	Grupos de Controles 3 - Adecuada cobertura antimalware en equipos de usuarios	100%	Todos los equipos cuentan con cobertura antimalware, con las actualizaciones vigentes.
MET09	Grupos de Controles 4 - Personal que cumple con las prácticas de escritorio limpio y bloqueo de pantallas	62%	En base a la inspección de los 8 puestos de trabajo evaluados se identificó que solo 5 de ellos aplicaban la política de bloqueo de equipos en ausencia.
MET10	Grupos de Controles 5 - Equipos de usuarios con software autorizado instalado	19%	Solo 3 de la totalidad de personal evaluado tienen coincidencias entre el software evaluado y la que se maneja en el registro de licencias (inventario).
MET11	Objetivos de Seguridad de Información 1 - Fomentar la difusión del cumplimiento de la confidencialidad en el manejo de la información de los proyectos	87%	Del total de personal evaluado (16) se ha identificado que 14 han pasado la prueba con puntaje satisfactorio.
MET12	Objetivos de Seguridad de Información 2 - Mejorar la integridad de los productos de consultoría en cuanto a versiones exactas y completitud	89%	De los 2972 registros de actualización se identificó que 2661 tienen carácter regular.
MET13	Objetivos de Seguridad de Información 3 - Incrementar la disponibilidad de la información y servicios requeridos para realizar las actividades de consultoría	98%	En base a los reportes de disponibilidad del software de monitoreo de red y servidores, se ha obtenido el valor de 98% de disponibilidad, para el horario laboral regular (08:00-20:00) de lunes a viernes

Anexo R. Programa de auditoría interna del SGSI

Descripción: Programa que establece los parámetros para las auditorías sobre el sistema.
Aprobado: Versión 1.0 por Representante de la Dirección

Alcance

El alcance de las auditorías internas del SGSI será realizado en base a lo que establezca, para el momento de la ejecución de la auditoría, el documento **Declaración de alcance del SGSI**.

Objetivos

- Identificar no conformidades respecto al cumplimiento del estándar ISO 27001:2013
- Identificar incumplimientos de la reglamentación interna de la organización: Política de seguridad de información, Políticas específicas de seguridad de información y el resto del marco normativo interno.
- Identificar el incumplimiento de los requisitos de seguridad de información aplicables a la organización.
- Identificar mejoras sobre el SGSI y los controles de seguridad de información.

Métodos de auditoría

Las auditorías se realizarán a discreción del equipo auditor, bajo los siguientes métodos:

- Entrevistas de auditoría
- Inspección de ambientes dentro del alcance de la auditoría
- Pruebas de controles de seguridad de información (muestras, simulaciones)

Responsabilidades de auditoría

- Convocante: Dirección de la alta dirección – Gerente general.
- Ejecutor: Equipo auditor – Auditor líder y especialistas que puedan ser convocados por este.
- Participantes: Todo el personal y terceros que puedan ser convocados a discreción del auditor, como parte de su investigación.

Criterios de auditoría

Los criterios respecto a los cuáles se evaluará el sistema son:

- Los requisitos establecidos por la norma ISO 27001:2013
- Las disposiciones en seguridad de información asumidas por la organización.

Frecuencia (Cronograma)

Meses de ejecución	Frecuencia
Noviembre	Anual

Anexo S. Plan de auditoría interna del SGSI

Descripción: Plan que detalla las sesiones que comprenden la auditoría interna del periodo.
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
AUD01	Mantener	Auditoría	Reunión de inicio de auditoría	*Se ha aprobado el Plan de auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Representante de la dirección (Gerente general) *Representantes de los procesos (Gerente de Operaciones, Gestor de Proyectos, Jefe de Calidad) *Coordinador de seguridad de información	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Presentar el Plan de Auditoría (final) 2. Ejecutar la reunión de auditoría	**Resultado esperado:** *Compromiso de asistencia de los involucrados y su personal a las reuniones de auditoría	nov-15	nov-15	**Realizado**
AUD02	Mantener	Auditoría	Auditoría al Representante de la Dirección	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Representante de la dirección	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD03	Mantener	Auditoría	Auditoría al Responsable de la Seguridad de Información	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Coordinador de seguridad de información	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD04	Mantener	Auditoría	Auditoría a los representantes de los procesos	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Representante del Proceso (Gerente de Operaciones, Gestor de Proyectos, Jefe de Calidad)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
AUD05	Mantener	Auditoría	Auditoría a participantes de los procesos	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Participantes de los procesos (Gestor de Proyecto, Jefe de Calidad, consultores, analistas de calidad)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD06	Mantener	Auditoría	Auditoría al responsable de seguridad física	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Responsable de seguridad física (Gerente de Administración)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD07	Mantener	Auditoría	Auditoría al responsable de recursos humanos	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Responsable de recursos humanos (Gerente de Administración)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD08	Mantener	Auditoría	Auditoría al responsable de logística y patrimonio	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Responsable de logística y patrimonio (Gerente de Administración)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD09	Mantener	Auditoría	Auditoría al responsable de tecnología y soporte	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Responsable de tecnología y soporte (Gerente de servicios TIC)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
AUD10	Mantener	Auditoría	Inspección a ambientes de trabajo de los procesos	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Participantes de los procesos (Gestor de Proyecto, Jefe de Calidad, consultores, analistas de calidad)	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD11	Mantener	Auditoría	Inspección al centro de datos	*Se ha iniciado la auditoría interna del SGSI	**Responsable:** *Auditor interno del SGSI **Convocado:** *Responsable de tecnología y soporte (Gerente de servicios TIC, operador TIC)	**Ubicación:** *Centro de procesamiento de datos	1. Ejecutar la reunión de auditoría 2. Solicitar evidencia complementaria, si corresponde	**Resultado esperado:** *Asistencia de los convocados *Evidencias solicitadas durante la reunión	nov-15	nov-15	**Realizado**
AUD12	Mantener	Auditoría	Reunión de fin de auditoría	*Se han concluido las reuniones e inspecciones de auditoría interna	**Responsable:** *Auditor interno del SGSI **Convocado:** *Representante de la dirección (Gerente general) *Representantes de los procesos (Gerente de Operaciones, Gestor de Proyectos, Jefe de Calidad) *Coordinador de seguridad de información	**Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop con acceso controlado (auditor) a registros de operación del SGSI	1. Presentar los resultados de auditoría 2. Suscribir el acta de cierre de la auditoría	**Resultado esperado:** *Asistencia de los convocados *Acta de cierre de auditoría	nov-15	nov-15	**Realizado**

Anexo T. Informe de resultados de la auditoría interna

Descripción: Informe de resultados obtenidos de la auditoría interna del periodo.
Aprobado: Versión 1.0 por Representante de la Dirección

Equipo auditor:

- Auditor Líder
- Auditor

Alcance

Procesos evaluados:

- Gestión de proyectos de consultoría
- Ejecución de servicios de desarrollo y mantenimiento de software
- Aseguramiento de la calidad del software

Se ha considerado al personal, activos, servicios y ubicaciones asociados a los procesos listados, además de los requisitos de seguridad establecidos para el SGSI.

Resultados

Se han obtenido los siguientes hallazgos (no conformidades, observaciones) y recomendaciones (oportunidades de mejora)

Hallazgo / Referencia	Evidencia	Categoría
7.2 Competencia **AI15-001:** Si bien existen registros de las capacitaciones dadas al personal, y el personal conoce cuáles son sus funciones en el sistema, algunos de ellos conocen parcialmente la metodología de gestión de riesgos, pese a ser parte del equipo responsable de realizarla.	Entrevista al personal, registros de la evaluación de riesgos	No conformidad
A.9.2.5 Revisión de acceso a los usuarios **AI15-002:** Si bien se tiene el control de altas y bajas del personal en repositorio de consultoría, en algunos casos, el formato no cuenta con las firmas requeridas, por lo que se evidencia falta de revisiones de control.	Registros de altas y bajas en servicios TI	Observación
Recomendaciones	**Evidencia**	**Categoría**
9.3.d Retroalimentación de partes interesadas **AI15-003:** Implementar y difundir un buzón de recomendaciones de seguridad de información, a fin de que las partes interesadas internas y externas puedan comunicar sugerencias para retroalimentar el sistema	Entrevista al personal	Oportunidad de Mejora

Anexo U. Acta de revisión por la dirección

Descripción: Acta con los resultados y acuerdos de la última revisión por la dirección del SGSI.
Aprobado: Versión 1.0 por Representante de la Dirección

Sesión: SGSI -2015

Fecha: martes 29/12/2015

Participantes:

- Gerente general (presidente)
- Gerente de administración y finanzas
- Gerente de operaciones
- Gerente de servicios TIC
- Coordinador de seguridad de información (secretario)

Agenda:

El coordinador de seguridad de información presenta los registros de los siguientes documentos:

- Política de seguridad de información (vigencia)
- Acta de revisión por la dirección anterior (no aplica)
- Informe de contexto de la organización (1 registro)
- Plan de objetivos de seguridad de información (3 registros)
- Informe de métricas de seguridad de información (13 registros)
- Informe de resultados de la auditoría interna (3 registros)
- Plan de tratamiento de riesgos (9 registros)
- Informe de seguimiento de riesgos (9 registros)
- Plan de acciones correctivas (2 registros)
- Plan de acciones de mejora (1 registro)

Acuerdos:

- **RD15-001: Mejoras en la capacitación**
  - **Detalle:** Se dispone la preparación de un curso e-learning consistente en un video y cuestionario en línea, como material de inducción obligatorio para todo personal y proveedores nuevos.
  - **Responsable:** Coordinador de seguridad de información

- **RD15-002: Superación de la métrica de software autorizado**
  - **Detalle:** Se dispone la revisión y depuración de software no autorizado en los equipos de la organización, así como la nueva medición de la métrica asociada para verificar que esta alcance un nivel razonable.
  - **Responsable:** Gerente de Servicios TIC

Anexo V. Plan de acciones correctivas

Descripción: Plan con las actividades para el desarrollo de las acciones correctivas sobre el sistema y sus controles.
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
ACO01	Mejorar	Correctiva	Aplicar la acción correctiva al hallazgo AI15-001 (no conformidad)	*Se ha identificado una no conformidad durante la auditoría interna: "AI15-001: Si bien existen registros de las capacitaciones dadas al personal, y el personal conoce cuáles son sus funciones en el sistema, algunos de ellos conocen parcialmente la metodología de gestión de riesgos, pese a ser parte del equipo responsable de realizarla"	**Responsable:** *Representante de la dirección (Gerente general) **Convocado:** *Coordinador de seguridad de información	**Documentos:** *Informe de resultados de la auditoría interna *Plan de concientización, capacitación y evaluación *Evaluaciones para el personal **Presentación:** *Roles, responsabilidades y actividades del SGSI **Ubicación:** *Sala de reuniones de la consultora **Tecnología:** *Laptop y proyector	**Corrección:** 1. Convocar a la lista de personal que ha sido observado por el auditor, respecto al conocimiento de sus roles dentro del sistema 2. Brindar una capacitación reiterativa de las actividades y responsabilidades asociadas a sus roles **Causas:** 1. Las capacitaciones dadas para los roles de mayor complejidad no han sido suficientes, ya que son justamente estos los que presentan mayores deficiencias **Eliminación:** 1. Complementar la capacitación con mentorías bimestrales para revisar los registros generados a partir de las actividades de estos roles y si estos han sido adecuadamente realizados.	**Resultado esperado:** *Personal con roles en el SGSI con un nivel adecuado de competencia	dic-15	nov-16	**En proceso**
ACO02	Mejorar	Correctiva	Aplicar la acción correctiva al hallazgo AI15-002 (observación)	*Se ha identificado un hallazgo durante la auditoría interna: "AI15-002: Si bien se tiene el control de altas y bajas del personal en repositorio de consultoría, en algunos casos, el formato no cuenta con las firmas requeridas, por lo que se evidencia falta de revisiones de control"	**Responsable:** *Responsable de tecnología y soporte (Gerente de servicios TIC) **Convocado:** *Operador TIC *Coordinador de seguridad de información	**Documentos:** *Plan de concientización, capacitación y evaluación *Informe de resultados de la auditoría interna	**Corrección:** 1. Identificar a las cuentas que cuentan con privilegios que no corresponden o que existen cuando deberían ser eliminadas. 2. Ejecutar los cambios requeridos a partir del análisis realizado. **Causas:** 1. La administración de cuentas no contempla una actividad de seguimiento o revisión periódica de las mismas, para identificar asignaciones omitidas, incorrectas, o cambios de emergencia que deben ser revertidos. **Eliminación:** 1. Establecer revisiones mensuales con el Coordinador de Seguridad de Información para revisar los registros de accesos a recursos TI.	**Resultado esperado:** *Registros de accesos a recursos TI coherentes con los permisos establecidos en los formatos de autorización y perfiles del personal.	dic-15	nov-16	**En proceso**

Anexo W. Plan de acciones de mejora

Descripción: Plan con las actividades para el desarrollo de las acciones de mejora sobre el sistema y sus controles.
Aprobado: Versión 1.0 por Representante de la Dirección

ID	Etapa	Tipo	Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Cierre	Resultado
AME01	Mejorar	Mejora	Aplicar la acción de mejora al hallazgo AI15-003	*Se ha identificado una oportunidad de mejora durante la auditoría interna: "AI15-003: Implementar y difundir un buzón de recomendaciones de seguridad de información, a fin de que las partes interesadas internas y externas puedan comunicar sugerencias para retroalimentar el sistema "	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Gerente de Operaciones *Gerente de servicios TIC	**Documentos:** *Informe de resultados de la auditoría interna **Tecnología:** *Servicio de correo electrónico	**Mejora:** 1. Crear la cuenta de correo para el buzón de sugerencias relacionadas a la seguridad de información. 2. Difundir la existencia del buzón entre los directivos y el personal de la organización, así como también entre clientes y proveedores.	**Resultado esperado:** *Información de retroalimentación de las partes interesadas	dic-15	nov-16	**En proceso**
AME02	Mejorar	Mejora	Aplicar la acción de mejora para atender el acuerdo RD15-001	*Se ha identificado una mejora durante la revisión por la dirección: "RD15-001: Se dispone la preparación de un curso e-learning consistente en un video y cuestionario en línea, como material de inducción obligatorio para todo personal y proveedores nuevos"	**Responsable:** *Coordinador de seguridad de información **Convocado:** *Gerente de Operaciones *Gerente de servicios TIC *Gerente de administración	**Documentos:** *Diseño de cuestionario de seguridad de información **Presentación:** *Material de capacitaciones de seguridad de información **Tecnología:** *Portal interno de la organización	**Mejora:** 1. Adaptar el material de las capacitaciones para elaborar el video instructivo 2. Implementar la sección de e-learning en el portal 3. Establecer la obligatoriedad para que todo nuevo ingreso o proveedor con el que la organización entable una relación, reciba la inducción por este medio.	**Resultado esperado:** *Personal nuevo instruido en los fundamentos de la seguridad de información en la consultora	dic-15	nov-16	**En proceso**
AME03	Mejorar	Mejora	Aplicar la acción de mejora para atender el acuerdo RD15-002	*Se ha identificado una mejora durante la revisión por la dirección: "RD15-002: Se dispone la revisión y depuración de software no autorizado en los equipos de la organización, así como la nueva medición de la métrica asociada para verificar que esta alcance un nivel razonable"	**Responsable:** *Gerente de servicios TIC **Convocado:** *Operador TIC	**Documentos:** *Registros de inventario de software *Registros de software instalado en los equipos	**Mejora:** 1. Identificar al personal que cuenta con software no autorizado en sus equipos 2. Realizar el proceso de depuración para los casos en que el software no cuente con una justificación 3. Validar con gerencia general la necesidad de adquisición del software no autorizado pero necesario.	**Resultado esperado:** *Mejora en la métrica asociada a la instalación de software autorizado en los equipos.	dic-15	nov-16	**En proceso**