PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN MODELO DE GOBIERNO DE TI UTILIZANDO EL MARCO DE TRABAJO DE COBIT 5 CON ENFOQUE EN SEGURIDAD DE LA INFORMACIÓN. CASO DE ESTUDIO: UNA EMPRESA PRIVADA ADMINISTRADORA DE FONDO DE PENSIONES

ANEXOS

Tesis para optar el Título de **Ingeniero Informático**, que presenta el bachiller:

Henry Jhonatan Beingolea Manavi

ASESOR: Mag. Moisés Antonio Villena Aguilar

Lima, Octubre de 2015

Tabla de contenido

Índice de Tablas

1 Anexo 1: Identificación de objetivos de TI relacionados a los objetivos de negocio.

A continuación por cada uno de las necesidades del negocio, se mostrarán la relación entre los objetivos de negocio y objetivo de TI, indicando si la relación entre ambos es primaria (cuando hay una importante relación) o secundaria (cuando todavía hay una fuerte relación, pero menos importante).

- **Necesidad del negocio:** Mejorar la satisfacción y atención al cliente.

Objetivo de negocio	Cultura de servicio orientada al cliente.	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Alineamiento de TI y las estrategias del negocio.	Primaria
	Realización de beneficios del portafolio de inversiones y servicios de TI.	Secundaria
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Primaria
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Secundaria
Procesos interno	Agilidad de las TI.	Secundaria
	Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	Secundaria
	Entrega de programas que den beneficios en tiempo, presupuesto y satisfaga los requisitos y estándares de calidad.	Secundaria
Aprendizaje y crecimiento	Personal del negocio y de TI competente y motivado.	Secundaria
	Conocimiento, habilidad e iniciativas para la innovación del negocio.	Secundaria

Tabla 1.1 Objetivos de TI identificados para la 1ra necesidad del negocio (Parte a).

- **Necesidad del negocio:** Mejorar la satisfacción y atención al cliente.

Objetivo de negocio	Continuidad y disponibilidad de los servicios del negocio.	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Alineamiento de TI y las estrategias del negocio.	Secundaria
	Gestión de los riesgos del negocio relacionados con TI.	Primaria
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Secundaria
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Secundaria
Proceso interno	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Primaria
	Disponibilidad de información útil y fiable para la toma de decisiones.	Primaria

Tabla 1.2 Objetivos de TI identificados para la 1ra necesidad del negocio (Parte b).

- **Necesidad del negocio:** Reducir la cantidad de observaciones internas y externas.

Objetivo de negocio	Cumplir con leyes y regulaciones externas.	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Cumplimiento y soporte de TI para el cumplimiento de las leyes y regulaciones externas al negocio.	Primaria
	Gestión de los riesgos del negocio relacionados con TI.	Secundaria

Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Secundaria
Proceso interno	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Primaria
	Disponibilidad de información útil y fiable para la toma de decisiones.	Secundaria
	Cumplimiento de las políticas internas de TI.	Secundaria

Tabla 1.3 Objetivos de TI identificados para la 2da necesidad del negocio (Parte a).

- **Necesidad del negocio:** Reducir la cantidad de observaciones internas y externas.

Objetivo de negocio	Cumplir con las políticas internas.	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Cumplimiento y soporte de TI para el cumplimiento de las leyes y regulaciones externas al negocio.	Primaria
	Gestión de los riesgos del negocio relacionados con TI.	Secundaria
Proceso interno	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	Primaria
	Cumplimiento de las políticas internas de TI.	Primaria

Tabla 1.4 Objetivos de TI identificados para la 2da necesidad del negocio (Parte b).

- **Necesidad del negocio:** Ser eficientes al realizar las operaciones del negocio.

Objetivo de negocio	Optimización de los costos del proceso del negocio	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Alineamiento de TI y las estrategias del negocio.	Secundaria

	Realización de beneficios del portafolio de inversiones y servicios de TI.	Primaria
	Transparencia de los costos, beneficios y riesgos de TI.	Primaria
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Secundaria
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Secundaria
Proceso interno	Optimización de los activos, recursos y capacidades de TI.	Primaria
	Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	Secundaria
	Entrega de programas que den beneficios en tiempo, presupuesto y satisfaga los requisitos y estándares de calidad.	Secundaria

Tabla 1.5 Objetivos de TI identificados para la 3ra necesidad del negocio (Parte a).

- **Necesidad del negocio:** Ser eficientes al realizar las operaciones del negocio.

Objetivo de negocio	Productividad operacional y del personal.	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Realización de beneficios del portafolio de inversiones y servicios de TI.	Secundaria
Cliente	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Primaria
Proceso interno	Agilidad de las TI.	Secundaria
	Optimización de los activos, recursos y capacidades de TI.	Secundaria

	Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	Secundaria
Aprendizaje y crecimiento	Personal del negocio y de TI competente y motivado.	Primaria

Tabla 1.6 Objetivos de TI identificados para la 3ra necesidad del negocio (Parte b).

- **Necesidad del negocio:** Realizar innovación tecnológica según las oportunidades y necesidades del negocio.

Objetivo de negocio	Portafolio de productos y servicios competitivos	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Alineamiento de TI y las estrategias del negocio.	Primaria
	Compromiso del directorio ejecutivo para tomar decisiones relacionadas con TI.	Secundaria
	Realización de beneficios del portafolio de inversiones y servicios de TI.	Primaria
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Primaria
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Secundaria
Proceso interno	Agilidad de las TI.	Primaria
	Optimización de los activos, recursos y capacidades de TI.	Secundaria
	Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	Primaria
	Entrega de programas que den beneficios en tiempo, presupuesto y satisfaga los requisitos y estándares de calidad.	Secundaria

	Disponibilidad de información útil y fiable para la toma de decisiones.	Secundaria
Aprendizaje y crecimiento	Personal del negocio y de TI competente y motivado.	Secundaria
	Conocimiento, habilidad e iniciativas para la innovación del negocio.	Primaria

Tabla 1.7 Objetivos de TI identificados para la 4ta necesidad del negocio (Parte a).

- **Necesidad del negocio:** Realizar innovación tecnológica según las oportunidades y necesidades del negocio.

Objetivo de negocio	Cultura de innovación de producto y negocio	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Alineamiento de TI y las estrategias del negocio.	Secundaria
	Compromiso del directorio ejecutivo para tomar decisiones relacionadas con TI.	Secundaria
	Realización de beneficios del portafolio de inversiones y servicios de TI.	Secundaria
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Secundaria
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Secundaria
Proceso interno	Agilidad de las TI.	Primaria
	Optimización de los activos, recursos y capacidades de TI.	Secundaria
	Habilitación y soporte de los procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.	Secundaria
Aprendizaje y crecimiento	Personal del negocio y de TI competente y motivado.	Secundaria

	Conocimiento, habilidad e iniciativas para la innovación del negocio.	Primaria

Tabla 1.8 Objetivos de TI identificados para la 4ta necesidad del negocio (Parte b).

- **Necesidad del negocio:** Mejorar el clima laboral

Objetivo de negocio	Personal cualificado y motivado	
Perspectiva del cuadro de mando integral	**Objetivo relacionado a TI**	**Nivel de relación con el objetivo de negocio**
Financiera	Alineamiento de TI y las estrategias del negocio.	Secundaria
	Compromiso del directorio ejecutivo para tomar decisiones relacionadas con TI.	Secundaria
	Gestión de los riesgos del negocio relacionados con TI.	Secundaria
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Secundaria
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Secundaria
Proceso interno	Agilidad de las TI.	Secundaria
Aprendizaje y crecimiento	Personal del negocio y de TI competente y motivado.	Primaria
	Conocimiento, habilidad e iniciativas para la innovación del negocio.	Secundaria

Tabla 1.9 Objetivos de TI identificados para la 5ta necesidad del negocio.

2 Anexo 2: Identificación de los procesos habilitadores relacionados a los objetivos de TI

A continuación se muestra la relación entre los objetivos de TI seleccionados con los procesos habilitadores que lo soportan, indicando si la relación entre ambos es primaria (cuando hay una importante relación ente el proceso habilitador y objetivo de TI) o secundaria (cuando todavía hay una relación fuerte, pero menos importante).

- **Objetivo de TI:** Alineamiento de TI y las estrategias del negocio.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Primaria
	Asegurar la entrega de beneficios	Primaria
	Asegurar la optimización del riesgo	Secundaria
	Asegurar la optimización de los recursos	Secundaria
	Asegurar la transparencia a los stakeholders	Secundaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Primaria
	Gestionar la estrategia	Primaria
	Gestionar la arquitectura empresarial	Primaria
	Gestionar la innovación	Secundaria
	Gestionar el portafolio	Primaria
	Gestionar el presupuesto y los costos	Secundaria
	Gestionar los recursos humanos	Primaria
	Gestionar las relaciones	Primaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar la calidad	Secundaria
	Gestionar los programas y proyectos	Primaria
	Gestionar la definición de requisitos	Primaria

Construir, adquirir e implementar	Gestionar la identificación y la construcción de soluciones	Secundaria
	Gestionar la habilitación de cambio organizacional	Secundaria
	Gestionar el conocimiento	Secundaria
Entregar, dar servicio y soporte	Gestionar la continuidad	Secundaria
	Gestionar la servicios de seguridad	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria

Tabla 2.1 Procesos habilitadores relacionados al 1er objetivo de TI.

- **Objetivo de TI:** Cumplimiento y soporte de TI para el cumplimiento de las leyes y regulaciones externas al negocio.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la optimización del riesgo	Secundaria
	Asegurar la transparencia a los stakeholders	Secundaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Primaria
	Gestionar los recursos humanos	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar la calidad	Secundaria
	Gestionar el riesgo	Primaria
	Gestionar la seguridad	Primaria
Construir, adquirir e implementar	Gestionar la definición de requisitos	Secundaria
	Gestionar los activos	Secundaria
	Gestionar la configuración	Primaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Secundaria
	Gestionar los problemas	Secundaria
	Gestionar la continuidad	Secundaria

	Gestionar la servicios de seguridad	Primaria
	Gestionar los controles de los procesos de negocio	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria
	Supervisar, evaluar y medir el sistema de control interno	Primaria
	Supervisar, evaluar y medir la conformidad de los requerimientos externos	Primaria

Tabla 2.2 Procesos habilitadores relacionados al 2do objetivo de TI.

- **Objetivo de TI:** Realización de beneficios del portafolio de inversiones y servicios de TI.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la entrega de beneficios	Primaria
	Asegurar la optimización de los recursos	Secundaria
Alinear, planear y organizar	Gestionar la estrategia	Secundaria
	Gestionar la arquitectura empresarial	Secundaria
	Gestionar la innovación	Primaria
	Gestionar el portafolio	Primaria
	Gestionar el presupuesto y los costos	Primaria
	Gestionar las relaciones	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar la calidad	Primaria
Construir, adquirir e implementar	Gestionar los programas y proyectos	Primaria
	Gestionar la definición de requisitos	Secundaria
	Gestionar la identificación y la construcción de soluciones	Secundaria

	Gestionar la disponibilidad y capacidad	Secundaria
	Gestionar la habilitación de cambio organizacional	Secundaria
	Gestionar el cambio	Secundaria
	Gestionar la aceptación del cambio y la transmisión	Secundaria
	Gestionar el conocimiento	Secundaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Secundaria
	Gestionar los problemas	Secundaria
	Gestionar la continuidad	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria
	Supervisar, evaluar y medir la conformidad de los requerimientos externos	Secundaria

Tabla 2.3 Procesos habilitadores relacionados al 3er objetivo de TI.

- **Objetivo de TI:** Entrega de servicios de TI de acuerdo a los requisitos del negocio.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Primaria
	Asegurar la entrega de beneficios	Primaria
	Asegurar la optimización del riesgo	Secundaria
	Asegurar la optimización de los recursos	Secundaria
	Asegurar la transparencia a los stakeholders	Primaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Secundaria
	Gestionar la estrategia	Primaria
	Gestionar la arquitectura empresarial	Secundaria
	Gestionar el portafolio	Secundaria
	Gestionar el presupuesto y los costos	Secundaria
	Gestionar los recursos humanos	Secundaria
	Gestionar las relaciones	Primaria
	Gestionar los acuerdos de servicios	Primaria

	Gestionar los proveedores	Primaria
	Gestionar la calidad	Primaria
	Gestionar el riesgo	Secundaria
	Gestionar la seguridad	Secundaria
Construir, adquirir e implementar	Gestionar los programas y proyectos	Secundaria
	Gestionar la definición de requisitos	Primaria
	Gestionar la identificación y la construcción de soluciones	Primaria
	Gestionar la disponibilidad y capacidad	Primaria
	Gestionar la habilitación de cambio organizacional	Secundaria
	Gestionar el cambio	Primaria
	Gestionar la aceptación del cambio y la transmisión	Secundaria
	Gestionar el conocimiento	Secundaria
	Gestionar los activos	Secundaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Primaria
	Gestionar las respuesta e incidentes del servicio	Primaria
	Gestionar los problemas	Primaria
	Gestionar la continuidad	Primaria
	Gestionar la servicios de seguridad	Secundaria
	Gestionar los controles de los procesos de negocio	Primaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Primaria
	Supervisar, evaluar y medir el sistema de control interno	Secundaria
	Supervisar, evaluar y medir la conformidad de los requerimientos externos	Secundaria

Tabla 2.4 Procesos habilitadores relacionados al 4to objetivo de TI.

- **Objetivo de TI:** Uso adecuado de aplicaciones, información y soluciones tecnológicas.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar la entrega de beneficios	Secundaria
	Asegurar la optimización del riesgo	Secundaria
	Asegurar la optimización de los recursos	Secundaria
Alinear, planear y organizar	Gestionar la estrategia	Secundaria
	Gestionar la arquitectura empresarial	Secundaria
	Gestionar la innovación	Primaria
	Gestionar el portafolio	Secundaria
	Gestionar el presupuesto y los costos	Secundaria
	Gestionar las relaciones	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar la calidad	Secundaria
	Gestionar el riesgo	Secundaria
	Gestionar la seguridad	Secundaria
Construir, adquirir e implementar	Gestionar los programas y proyectos	Secundaria
	Gestionar la definición de requisitos	Secundaria
	Gestionar la identificación y la construcción de soluciones	Secundaria
	Gestionar la disponibilidad y capacidad	Secundaria
	Gestionar la habilitación de cambio organizacional	Primaria
	Gestionar el cambio	Secundaria
	Gestionar la aceptación del cambio y la transmisión	Primaria
	Gestionar el conocimiento	Secundaria
	Gestionar la configuración	Secundaria
	Gestionar las operaciones	Secundaria

Entregar, dar servicio y soporte	Gestionar las respuesta e incidentes del servicio	Secundaria
	Gestionar los problemas	Secundaria
	Gestionar la continuidad	Secundaria
	Gestionar la servicios de seguridad	Secundaria
	Gestionar los controles de los procesos de negocio	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria
	Supervisar, evaluar y medir el sistema de control interno	Secundaria

Tabla 2.5 Procesos habilitadores relacionados al 5to objetivo de TI.

- **Objetivo de TI:** Agilidad de las TI.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la optimización de los recursos	Primaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Primaria
	Gestionar la estrategia	Secundaria
	Gestionar la arquitectura empresarial	Primaria
	Gestionar la innovación	Primaria
	Gestionar el portafolio	Secundaria
	Gestionar los recursos humanos	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Primaria
	Gestionar la calidad	Secundaria
	Gestionar el riesgo	Secundaria
Construir, adquirir e implementar	Gestionar la definición de requisitos	Secundaria
	Gestionar la disponibilidad y capacidad	Secundaria
	Gestionar la habilitación de cambio organizacional	Secundaria

	Gestionar el cambio	Secundaria
	Gestionar la aceptación del cambio y la transmisión	Secundaria
	Gestionar el conocimiento	Primaria
	Gestionar los activos	Secundaria
	Gestionar la configuración	Secundaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Secundaria
	Gestionar los problemas	Secundaria
	Gestionar la continuidad	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria

Tabla 2.6 Procesos habilitadores relacionados al 6to objetivo de TI.

- **Objetivo de TI:** Seguridad de la información, infraestructura de procesamiento y aplicaciones.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la optimización del riesgo	Primaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Secundaria
	Gestionar la arquitectura empresarial	Secundaria
	Gestionar los recursos humanos	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar el riesgo	Primaria
	Gestionar la seguridad	Primaria
Construir, adquirir e implementar	Gestionar la definición de requisitos	Secundaria
	Gestionar el cambio	Primaria
	Gestionar el conocimiento	Secundaria
	Gestionar los activos	Secundaria
	Gestionar la configuración	Secundaria

Entregar, dar servicio y soporte	Gestionar las operaciones	Secundaria
	Gestionar las respuesta e incidentes del servicio	Secundaria
	Gestionar la continuidad	Secundaria
	Gestionar la servicios de seguridad	Primaria
	Gestionar los controles de los procesos de negocio	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria
	Supervisar, evaluar y medir el sistema de control interno	Secundaria
	Supervisar, evaluar y medir la conformidad de los requerimientos externos	Secundaria

Tabla 2.7 Procesos habilitadores relacionados al 7mo objetivo de TI.

- **Objetivo de TI:** Optimización de los activos, recursos y capacidades de TI.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la entrega de beneficios	Secundaria
	Asegurar la optimización de los recursos	Primaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Primaria
	Gestionar la estrategia	Secundaria
	Gestionar la arquitectura empresarial	Primaria
	Gestionar la innovación	Primaria
	Gestionar el portafolio	Secundaria
	Gestionar el presupuesto y los costos	Secundaria
	Gestionar los recursos humanos	Primaria
	Gestionar las relaciones	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar la calidad	Secundaria

Construir, adquirir e implementar	Gestionar los programas y proyectos	Secundaria
	Gestionar la definición de requisitos	Secundaria
	Gestionar la identificación y la construcción de soluciones	Secundaria
	Gestionar la disponibilidad y capacidad	Primaria
	Gestionar la habilitación de cambio organizacional	Secundaria
	Gestionar el cambio	Secundaria
	Gestionar el conocimiento	Secundaria
	Gestionar los activos	Primaria
	Gestionar la configuración	Primaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Primaria
	Gestionar los problemas	Primaria
	Gestionar la continuidad	Secundaria
	Gestionar la servicios de seguridad	Secundaria
	Gestionar los controles de los procesos de negocio	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Primaria

Tabla 2.8 Procesos habilitadores relacionados al 8vo objetivo de TI.

- **Objetivo de TI:** Entrega de programas que den beneficios en tiempo, presupuesto y satisfaga los requisitos y estándares de calidad.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la entrega de beneficios	Secundaria
	Asegurar la optimización del riesgo	Secundaria
	Asegurar la optimización de los recursos	Secundaria
	Asegurar la transparencia a los stakeholders	Secundaria
	Gestionar el marco de gestión de TI	Secundaria

Alinear, planear y organizar	Gestionar la estrategia	Secundaria
	Gestionar el portafolio	Primaria
	Gestionar el presupuesto y los costos	Secundaria
	Gestionar los recursos humanos	Primaria
	Gestionar las relaciones	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar la calidad	Primaria
	Gestionar el riesgo	Primaria
Construir, adquirir e implementar	Gestionar los programas y proyectos	Primaria
	Gestionar la definición de requisitos	Secundaria
	Gestionar la identificación y la construcción de soluciones	Secundaria
	Gestionar la disponibilidad y capacidad	Secundaria
	Gestionar la habilitación de cambio organizacional	Primaria
	Gestionar el cambio	Secundaria
	Gestionar la aceptación del cambio y la transmisión	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria

Tabla 2.9 Procesos habilitadores relacionados al 9no objetivo de TI.

- **Objetivo de TI:** Cumplimiento de las políticas internas de TI.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la optimización del riesgo	Primaria
	Asegurar la transparencia a los stakeholders	Secundaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Primaria
	Gestionar la estrategia	Secundaria

	Gestionar los recursos humanos	Secundaria
	Gestionar las relaciones	Secundaria
	Gestionar los acuerdos de servicios	Secundaria
	Gestionar los proveedores	Secundaria
	Gestionar la calidad	Secundaria
	Gestionar el riesgo	Secundaria
Construir, adquirir e implementar	Gestionar el cambio	Secundaria
	Gestionar la aceptación del cambio y la transmisión	Secundaria
	Gestionar los activos	Secundaria
	Gestionar la configuración	Secundaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Secundaria
	Gestionar las respuesta e incidentes del servicio	Secundaria
	Gestionar los problemas	Secundaria
	Gestionar la continuidad	Secundaria
	Gestionar la servicios de seguridad	Secundaria
	Gestionar los controles de los procesos de negocio	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Primaria
	Supervisar, evaluar y medir el sistema de control interno	Primaria
	Supervisar, evaluar y medir la conformidad de los requerimientos externos	Secundaria

Tabla 2.10 Procesos habilitadores relacionados al 10mo objetivo de TI.

- **Objetivo de TI:** Personal del negocio y de TI competente y motivado.

Dominio	Proceso	Nivel de relación con el objetivo de TI
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Secundaria
	Asegurar la entrega de beneficios	Secundaria

	Asegurar la optimización del riesgo	Secundaria
	Asegurar la optimización de los recursos	Primaria
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Primaria
	Gestionar la estrategia	Secundaria
	Gestionar los recursos humanos	Primaria
	Gestionar las relaciones	Secundaria
	Gestionar la calidad	Secundaria
	Gestionar el riesgo	Secundaria
Construir, adquirir e implementar	Gestionar los programas y proyectos	Secundaria
	Gestionar el conocimiento	Secundaria
Entregar, dar servicio y soporte	Gestionar las operaciones	Secundaria
	Gestionar la continuidad	Secundaria
	Gestionar los controles de los procesos de negocio	Secundaria
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Secundaria

Tabla 2.11 Procesos habilitadores relacionados al 11vo objetivo de TI.

3 Anexo 3: Definición de las actividades, roles y responsabilidades de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.

A continuación se muestra la definición (actividades y matriz RACI) para cada uno de los procesos habilitadores seleccionados para el enfoque de seguridad de la información del gobierno de TI.

Para la matriz RACI (roles y responsabilidades) se utilizará la siguiente nomenclatura para asignar las responsabilidades en las funciones y estructuras organizativas de la empresa.

Abreviatura	Descripción
R	*Responsible* (Responsable de ejecución)
A	Accountable (Responsable de mayor dirección y jerarquía)
C	*Consulted* (Consultado)
I	*Informed* (Informado)

Tabla 3.1 Responsabilidades de la matriz RACI.

- **Proceso habilitador: Asegurar el establecimiento y mantenimiento del marco de gobierno**

Descripción: Este proceso se encarga de analizar y articular los requerimientos de seguridad de la información para el gobierno de TI y establecer estructuras organizativas, procesos y prácticas para alcanzar la misión, metas y objetivos de la empresa.

Práctica clave de gobierno: Evaluar el sistema de gobierno
Analizar e identificar los factores internos y externos del entorno del negocio relacionadas a la seguridad de la información que influenciaran en el diseño del gobierno de TI.
Articular los principios de seguridad de la información que guiarán el diseño del gobierno de TI.

Determina la relevancia de la seguridad de la información y su rol dentro del negocio.
Considerar la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales para determinar cómo serán incorporadas dentro del gobierno de TI.
Práctica clave de gobierno: Orientar el sistema de gobierno
Asignar la responsabilidad y la autoridad de la seguridad de la información dentro del gobierno de TI.
Comunicar los principios de seguridad de la información del gobierno de TI.
Dirigir el establecimiento de un sistema de recompensa para promover el cambio cultural deseable del gobierno de TI con enfoque en seguridad de la información.
Establecer estructuras, procesos y prácticas de gobierno relacionadas a la seguridad de la información.
Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos que tienen la responsabilidad de supervisar y tomar decisiones respecto a la seguridad de la información.
Práctica clave de gobierno: Supervisar el sistema de gobierno
Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.
Evaluar la efectividad y rendimiento del personal a quien se le dio responsabilidad y autoridad para la seguridad de la información dentro del gobierno de TI.
Evaluar periódicamente si las estructuras, procesos y prácticas de gobierno relacionadas a la seguridad de la información están establecidas y operando efectivamente.
Mantener la supervisión para que la empresa satisfaga las obligaciones de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.
Monitorear los mecanismos regulares y rutinarios para asegurar que la empresa cumpla con la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales y políticas internas.

Tabla 3.2 Actividades del 1er proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Asegurar el establecimiento y mantenimiento del marco de gobierno																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Evaluar el sistema de gobierno	A	R	C	C	R		R			C		C	C	C	C	R	C	C	C				
Orientar el sistema de gobierno	A	R	C	C	R	I	R	I	I	C	I	I	I	C	C	R	C	I	I	I	I	I	I
Supervisar el sistema de gobierno	A	R	C	C	R	I	R	I	I	C	I	I	I	C	C	R	C	I	I	I	I	I	I

Tabla 3.3 Matriz RACI del 1er proceso habilitador de TI.

- **Proceso habilitador: Asegurar la entrega de beneficios**

Descripción: Este proceso se encarga de optimizar la contribución de valor al negocio desde las inversiones en los procesos, servicios y activos de TI relacionados a la seguridad de la información.

Práctica clave de gobierno: Evaluar la optimización de valor.
Comprender los requerimientos de los stakeholders, las estrategias de TI y la capacidad actual de las TI relacionada a la seguridad de la información, para cumplir las estrategias del negocio.
Comprender y discutir regularmente las posibles oportunidades que se pueden obtener de las nuevas tendencias de la seguridad de la información y optimizar el valor creado de estas oportunidades.
Evaluar la efectividad de la integración entre las estrategias de la empresa y de TI, para el cumplimiento de los objetivos del negocio.
Práctica clave de gobierno: Orientar la optimización del valor
Dirigir a la gestión a considerar la seguridad de información para permitir que el negocio responda a las nuevas oportunidades del mercado, incremento de la ventaja competitiva o mejore sus procesos.
Dirigir cualquier cambio en la asignación de las responsabilidades para la ejecución de las inversiones en seguridad de la información.
Orienta cualquier cambio realizado en las inversiones de seguridad de la información para realinearlo con los objetivos de la empresa.
Práctica clave de gobierno: Supervisar la optimización de valor
Definir objetivos y métricas para el rendimiento de las inversiones en seguridad de la información.
Después de las revisiones de los informes de seguridad de la información asegurar de que las medidas correctivas son iniciadas y controladas.
Después de las revisiones de los informes de seguridad de la información tomar las medidas de gestión apropiadas para asegurar que el valor esta optimizado.

Tabla 3.4 Actividades del 2do proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Asegurar la entrega de beneficios																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Evaluar la optimización de valor.	A	R	R	C	R		R		C	C		C	C	C	C	R	C	C	C				
Orientar la optimización del valor	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I
Supervisar la optimización de valor	A	R	R	C	R		R		R	C	C	C	C	C	C	R	C	C	C				

Tabla 3.5 Matriz RACI del 2do proceso habilitador de TI.

- **Proceso habilitador: Asegurar la optimización del riesgo**

Descripción: Este proceso se encarga de asegurar que el apetito y tolerancia al riesgo en la empresa son entendidos, incorporados y comunicados. Además de que los riesgos de TI son identificados y gestionados.

Práctica clave de gobierno: Evaluar la gestión de riesgos
Determinar el nivel riesgo (apetito al riesgo) relacionada con TI que la empresa está dispuesta a asumir.
Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.
Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.
Práctica clave de gobierno: Orientar la gestión de riesgos
Dirigir la elaboración de planes de comunicación de los riesgos de seguridad de la información (cubriendo todos los niveles de la empresa), así como los planes de acción de estos riesgos.
Dirigir la implantación de mecanismos apropiados para responder rápidamente a los riesgos y notificar inmediatamente a los niveles adecuados de la gestión.
Dirigir para que el riesgo, las oportunidades, los problemas y preocupaciones de seguridad de la información puedan ser identificados y notificados por cualquier persona en cualquier momento.
Promover una cultura proactiva de identificación de riesgos de seguridad de la información.
Práctica clave de gobierno: Supervisar la gestión de riesgos
Facilitar la revisión a los principales stakeholders el progreso de la empresa hacia los objetivos identificados de seguridad de información.

Informar cualquier problema de gestión de riesgos al directorio.
Monitorear hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales del apetito de riesgo.

Tabla 3.6 Actividades del 3er proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Asegurar la optimización del riesgo																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Evaluar la gestión de riesgos	A	R	C	C	R	C	R		I	R	C	I	C	C	C	R	C						
Orientar la gestión de riesgos	A	R	C	C	R	C	R	I	I	R	I	I	C	C	C	R	C	I	I	I	I	I	I
Supervisar la gestión de riesgos	A	R	C	C	R	C	R	I	I	R	R	I	C	C	C	R	C	I	I	I	I	I	I

Tabla 3.7 Matriz RACI del 3ro proceso habilitador de TI.

- **Proceso habilitador: Gestionar el marco de gestión de TI**

Descripción: Este proceso se encarga de aclarar y mantener la misión y visión del gobierno de TI, así como implementar y mantener mecanismos y autoridades para gestionar la seguridad de la información dentro del gobierno de TI de la empresa.

Práctica clave de gobierno: Definir la estructura organizativa
Alinear la organización de la seguridad de la información dentro de la arquitectura organizacional de la empresa.
Definir el alcance, puestos y roles internos y externos requeridos para la gestión de la seguridad de la información.
Definir los mecanismos de comunicación tanto a nivel horizontal y a nivel vertical dentro de la organización.
Definir los roles y responsabilidades de cada puesto dentro la estructura organizativa de seguridad de la información.
Establecer el involucramiento de los stakeholders para la toma de decisiones respecto a la seguridad de la información.
Establecer un comité directivo de seguridad de la información a nivel de gerencia, para determinar las prioridades de los programas de inversión de seguridad de la información de acuerdo a las estrategias y prioridades del negocio.
Establecer un comité estratégico de seguridad de la información a nivel del directorio, para asegurarse el gobierno de TI se esté contemplando de forma adecuada y pueda brindar una dirección estratégica.
Verificar regularmente la adecuación y la eficacia de la estructura organizativa.
Práctica clave de gobierno: Establecer roles y responsabilidades
Considerar los requisitos de la empresa y de la seguridad de la información al definir los roles.
Establecer y comunicar los roles y responsabilidades de los puestos de seguridad de la información a toda la organización.
Estructurar los roles y responsabilidades para reducir las posibilidades de que un solo rol puede comprometer una actividad critica.
Incluir la descripción de los roles y responsabilidades de seguridad de la información dentro las políticas y procedimientos de gestión.

Supervisar que los roles y responsabilidades se ejecuten adecuadamente y evaluar si tienen la autoridad y recursos suficientes para ejecutar sus roles y responsabilidades.
Práctica clave de gobierno: Mantener los elementos habilitadores del sistema de gestión.
Alinear el entorno de control de TI con las políticas, marcos a nivel nacional o internacional y las regulaciones de la seguridad de la información.
Capacitar a todo el personal involucrado en las políticas de seguridad de la información con la finalidad de integrar las políticas en las operaciones que realicen.
Comprender la visión, dirección y la estrategia de la empresa para poder dirigir la seguridad de la información.
Crear un conjunto de políticas de seguridad de la información para dirigir las expectativas de control de TI en temas de seguridad de la información.
Evaluar y actualizar por los menos una vez al año las políticas de seguridad de la información, según las necesidades del negocio.
Integrar los principios de seguridad de la información con los principios del negocio.
Práctica clave de gobierno: Comunicar los objetivos y la dirección de gestión
Comunicar continuamente los objetivos de seguridad de la información con el apoyo de la alta gerencia.
Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo de los objetivos de seguridad de la información.
Práctica clave de gobierno: Optimizar la ubicación de la función de TI.
Definir la ubicación del área de seguridad de la información dentro de la estructura organizativa y obtener la aprobación.
Entender el contexto y la importancia del área de seguridad de la información.
Definir la propiedad de la información (datos) y del sistema
Contar con un inventario de información (sistemas y datos) con sus respectivos propietarios, custodios y clasificación.

Definir e implementar procedimientos para asegurar la integridad de toda la información que se almacena en formato electrónico como las bases datos y archivos.
Proveer herramientas, técnicas y directrices para brindar seguridad y control sobre la información y los sistemas de información en colaboración su propietario.
Proveer políticas y directrices para asegurar y clasificar la información de la empresa.
Práctica clave de gobierno: Gestionar la mejora continua de los procesos
Considerar que las implementaciones de seguridad de la información no afecten la eficiencia y eficacia de los procesos críticos del negocio.
Identificar los procesos críticos del negocio e identificar puntos de mejora para la seguridad de la información.
Implementar y medir las mejoras acordadas de seguridad de la información en los procesos críticos del negocio.
Práctica clave de gobierno: Mantener el cumplimiento con las políticas y procedimientos.
Analizar los incumplimientos de las políticas y procedimientos de seguridad de la información y tomar acciones apropiadas.
Hacer seguimiento al cumplimiento de las políticas y procedimientos de seguridad de la información.
Integrar el rendimiento y cumplimiento de las políticas y procedimientos de la seguridad de la información dentro los objetivos individuales del personal.

Tabla 3.8 Actividades del 4to proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar el marco de gestión de TI																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Definir la estructura organizativa		C	C	C	C		I		C				R	I	I	A	C	C	C	R	C	C	C
Establecer roles y responsabilidades					I	C			C				C	C	C	A	C	C	C	R	C	C	C
Mantener los elementos habilitadores del sistema de gestión.	C	A	C	R	C	C	I			C	C	C		C	C	R				R			
Comunicar los objetivos y la dirección de gestión		A	R	R	R	I	R	I	I	R	R	I	I	I	I	R	I	I	I	I	I	I	I
Optimizar la ubicación de la función de TI.		C	C	C	C		A		C				C	C	C	R	C	C	C	R	C	C	C

Definir la propiedad de la información (datos) y del sistema		I	I	C	A	R							C	C	C	C	C						C
Gestionar la mejora continua de los procesos				A		R			R				I	C	C	R	R	R	R	R	R	R	R
Mantener el cumplimiento con las políticas y procedimientos.		A				R			R				R	C	I	R	R	R	R	R	R	R	R

Tabla 3.9 Matriz RACI del 4to proceso habilitador de TI.

- **Proceso habilitador: Gestionar los recursos humanos**

Descripción: Este proceso se encarga de proveer los lineamientos de seguridad de la información para que se incorporen en las funciones de los colaboradores de la empresa.

Práctica clave de gobierno: Mantener la dotación de personal suficiente y adecuado.
Asegurar que se entrena a más de una persona en funciones críticas, con la finalidad de reducir la dependencia de una sola persona.
Evaluar el requerimiento del personal de seguridad de la información para cumplir adecuadamente con los objetivos del negocio.
Incluir la revisión de antecedentes en la contratación de personal, contratistas y proveedores que accedan a información crítica del negocio.
Práctica clave de gobierno: Identificar personal clave de TI
Minimizar la dependencia de una sola persona para funciones críticas mediante la documentación y entrenamiento de las funciones críticas.

Probar regularmente los planes de respaldo del personal clave.
Práctica clave de gobierno: Mantener las habilidades y competencias del personal
Definir las habilidades y competencias necesarias del personal de seguridad de la información para asegurar el logro de los objetivos de la empresa.
Proporcionar un plan formal para el desarrollo profesional de las competencias del personal de TI en temas de seguridad de la información.
Revisar periódicamente el desarrollo de las habilidades y competencias del personal de TI en temas de seguridad de la información.
Práctica clave de gobierno: Evaluar el rendimiento del personal
Considerar los objetivos de seguridad de la información para establecer los objetivos individuales.
Desarrollar planes de mejora del desempeño basados en los resultados del proceso de evaluación.
Implementar un proceso de reconocimiento del cumplimiento de los objetivos de seguridad de la información.
Práctica clave de gobierno: Planificar y ubicar el uso de los recursos humanos de TI y del negocio
Entender la demanda actual y futura de los recursos humanos para el logro de los objetivos de seguridad de la información.
Mantener información adecuada sobre el tiempo dedicado a los proyectos de seguridad de la información.
Práctica clave de gobierno: Gestionar los contratos del personal
Comunicar a los contratistas que la empresa se reserva el derecho de supervisar e inspeccionar todo el uso de los recursos de TI (correo, llamadas, programas y archivos).
Establecer acuerdos de confidencialidad y de seguridad de la información dentro de los acuerdos formales con los contratistas.
Implementar políticas y procedimientos para identificar las condiciones para que un trabajo pueda ser externalizado asegurando la seguridad de la información.
Llevar a cabo revisiones periódicas de los derechos y accesos de los contratistas, los cuales tienen que estar alineados con sus funciones.

Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades respecto a la seguridad de la información, adicionales a las de su trabajo.

Tabla 3.10 Actividades del 5to proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar los recursos humanos																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Mantener la dotación de personal suficiente y adecuado.									R	I			R			A	R	R	R	R	R	R	R
Identificar personal clave de TI									R				R			A	R	R	R	R	R	R	R
Mantener las habilidades y competencias del personal									R				R			A	R	R	R	R	R	R	R

Evaluar el rendimiento del personal									R				R			A	R	R	R	R	R	R	R
Planificar y ubicar el uso de los recursos humanos de TI y del negocio					R	C	A	R	R				I			R	R	R	R	R	R	R	R
Gestionar los contratos del personal									R				R			A	R	R	R	R	R	R	R

Tabla 3.11 Matriz RACI del 5to proceso habilitador de TI.

- **Proceso habilitador: Gestionar los proveedores**

Descripción: Este proceso se encarga de que se consideren los lineamientos de seguridad de la información de la empresa al momento de identificar, seleccionar y recibir los servicios o productos que brindan los proveedores que tengan relación con el manejo de la información de la empresa.

Práctica clave de gobierno: Identificar y evaluar las relaciones y contratos con proveedores.
Establecer criterios de seguridad de la información en la evaluación de los proveedores y contratos según el tipo de proveedor, relevancia y criticidad del servicio. En el caso que el proveedor tenga acceso a información de la empresa, deberá de cumplir con la Ley de protección de datos personales.
Establecer criterios para la evaluación del rendimiento del servicio o producto ofrecido por el proveedor según el contrato establecido.
Evaluar y comparar periódicamente el rendimiento de los proveedores actuales con proveedores alternativos para identificar oportunidades de mejoras con los proveedores actuales.
Identificar, registrar y categorizar a los proveedores y contratos según los criterios definidos para mantener un registro de los proveedores que se van a gestionar.

Práctica clave de gobierno: Seleccionar proveedores
Evaluar y mantener evidencia de la evaluación de los RFP según los criterios y proceso establecido.
Revisar que los RFP detallan los requisitos de seguridad de la información claramente definidos.
Seleccionar al proveedor que mejor cumpla el RFP y documentar la decisión tomada, así como el contrato firmado.
Práctica clave de gobierno: Gestionar contratos y relaciones con proveedores
Acordar, gestionar, mantener y renovar los contratos con los proveedores conforme con los estándares legales y regulatorios de la empresa.
Asignar propietarios por cada proveedor que van a ser responsables supervisar el servicio ofrecido.
Definir, comunicar y acordar las formas para implementar los requerimientos de mejora de seguridad de la información.
Especificar un procedimiento formal para comunicarse con los proveedores en caso de falla de los servicios.
Establecer procedimientos para tratar los conflictos contractuales.
Para los proveedores claves, incluir dentro de las cláusulas del contrato revisión de las instalaciones, Prácticas internas y controles de gestión de seguridad de la información de los proveedores.
Práctica clave de gobierno: Gestionar el riesgo del proveedor
Identificar, monitorear y gestionar los riesgos de seguridad de la información en la entrega del servicio.
Práctica clave de gobierno: Supervisar el cumplimiento y el rendimiento del proveedor.
Definir los criterios para supervisar el rendimiento de los proveedores en relación a los niveles de servicios establecidos (SLA).
En caso de proveedores críticos solicitar en caso sea necesario revisiones independientes de las prácticas y controles de seguridad de la información, las cuales deben de estar definidas en el contrato.
Registrar y evaluar los resultados de las revisiones periódicas para identificar las necesidades y oportunidades de mejora con el proveedor.

Supervisar y revisar la entrega de los servicios según los requisitos y condiciones de seguridad de la información establecidos en el contrato.

Tabla 3.12 Actividades del 6to proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar los proveedores																							
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Identificar y evaluar las relaciones y contratos con proveedores.			C			C							C	C	C	A	C	C	C	R	C	C	C
Seleccionar proveedores			C			C							C	C	C	A	C	C	C	R	C	C	C
Gestionar contratos y relaciones con proveedores						I							C	C	C	A	C	R	R	R	C	C	C

Gestionar el riesgo del proveedor						C				R			C	C	C	A	C	R	R		C	C	C
Supervisar el cumplimiento y el rendimiento del proveedor.			I			C				C			C	C	C	A	C	R	R		C	C	C

Tabla 3.13 Matriz RACI del 6to proceso habilitador de TI.

- **Proceso habilitador: Gestionar el riesgo**

Descripción: Este proceso se encarga de identificar, evaluar y reducir los riesgos relacionados con TI, dentro de niveles de tolerancia establecidos por la empresa.

Práctica clave de gobierno: Recopilar datos
Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los riesgos y la forma en la cual estas condiciones afectaban la frecuencia del evento y la magnitud de perdida.
Ejecutar periódicamente el análisis de eventos y factores de riesgos para identificar nuevos riesgos.
Establecer un método para la colección, clasificación y análisis de datos de los riesgos de seguridad de la información, considerando múltiples tipos de eventos, categorías, riesgos y factores de riesgos.
Medir y analizar los datos históricos de riesgos de seguridad de la información ocurridas en la empresa o a empresas del rubro de administración de fondo de pensiones.
Registrar datos de eventos de riesgos que han causado o pueden causar impactos a la entrega de servicios de TI.
Práctica clave de gobierno: Analizar el riesgo
Analizar el costo beneficio de los tipos de tratamiento de riesgos para dar una respuesta optima a los riesgos.

Comparar el riesgo residual con el apetito de riesgo de la empresa e identificar planes de acción para los riesgos que superen el apetito de riesgos.
Construir los escenarios para el análisis de riesgos de seguridad de la información.
Definir el alcance y el nivel de detalle para realizar el análisis de riesgos.
Validar los resultados del análisis de riesgos con los requerimientos de la empresa antes de la toma de decisiones.
Práctica clave de gobierno: Mantener un perfil de riesgo
Capturar información sobre eventos de riesgos de seguridad de la información, para incluirlo en el perfil de riesgo de la empresa.
Contar con un inventario de los procesos de negocio incluyendo al personal, aplicaciones, infraestructura, instalaciones, documentos críticos y proveedores involucrados.
Determinar el perfil de riesgos de la empresa.
Determinar los servicios e infraestructura esenciales de TI para sostener la operación de los procesos de la empresa.
Práctica clave de gobierno: Articular el riesgo
Informar el perfil de riesgo a los stakeholders.
Informar los resultados del análisis de riesgos de seguridad de la información a todos los stakeholders en términos y formatos útiles para la toma de decisiones.
Práctica clave de gobierno: Definir un portafolio de acciones para la gestión de riesgos.
Definir un conjunto de proyectos para reducir los riesgos de mayor impacto, basando en el costo/beneficio.
Determinar si cada área de la empresa supervisa el riesgo y acepta la responsabilidad de operar dentro del nivel de tolerancia del riesgo.
Mantener un inventario de las actividades de control relacionadas a la gestión del riesgo de seguridad de la información.
Práctica clave de gobierno: Responder al riesgo
Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurra un riesgo.

Preparar, mantener y probar los planes que deben de especificar los pasos específicos a seguir en caso se materialice un riesgo de seguridad de la información.

Tabla 3.14 Actividades del 7mo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar el riesgo																							
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Recopilar datos		I				R			R	R	R	I		C	C	A	R	R	R	R	R	R	R
Analizar el riesgo		I				R			C	R	C	I		R	R	A	C	C	C	C	C	C	C
Mantener un perfil de riesgo		I				R			C	A	C	I		R	R	R	C	C	C	C	C	C	C
Articular el riesgo		I				R			C	R	C	I		C	C	A	C	C	C	C	C	C	C

Definir un portafolio de acciones para la gestión de riesgos.		I				R			C	A	C	I		C	C	R	C	C	C	C	C	C
Responder al riesgo		I				R			R	R	R	I		C	C	A	R	R	R	R	R	R

Tabla 3.15 Matriz RACI del 7mo proceso habilitador de TI.

- **Proceso habilitador: Gestionar la seguridad**

Descripción: Este proceso se encarga de definir, operar y supervisar un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa.

Práctica clave de gobierno: Establecer y mantener un SGSI
Comunicar la propuesta del SGSI al directorio.
Definir el alcance y los límites del SGSI según las características de la empresa.
Definir el SGSI acorde a las políticas de la empresa.
Definir y comunicar los roles y responsabilidad del SGSI.
Obtener autorización del directorio para implementar el SGSI.
Realizar una declaración de aplicabilidad que describa el alcance del SGSI.
Práctica clave de gobierno: Definir y gestionar un plan de tratamiento de los riesgos de seguridad de la información
Desarrollar una propuesta para implementar el plan de tratamiento de riesgos de seguridad de la información en un caso de negocio.
Desarrollar y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos.
Mantener un inventario de los componentes que están relacionados con la gestión de la seguridad de la información.
Recomendar programas de formación y concientización en seguridad de la información.
Práctica clave de gobierno: Monitorear y revisar el SGSI
Proporcionar información para el plan mantenimiento de los planes de seguridad de la información.
Realizar auditorías internas del SGSI.

Realizar revisiones periódicas del SGSI por la alta dirección para asegurar que el alcance siga siendo el adecuado.
Realizar revisiones periódicas del SGSI, incluyendo sus políticas, objetivos y prácticas de seguridad.

Tabla 3.16 Actividades del 8vo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar la seguridad																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Establecer y mantener un SGSI		C		C	C	I	C	I	I	C	A	C		C	C	R	I	I	I	R	I	R	C
Definir y gestionar un plan de tratamiento de los riesgos de seguridad de la información		C		C	C	C	C	I	I	C	A	C		C	C	R	C	C	C	R	C	R	C
Monitorear y revisar el SGSI					C	R	C		R		A			C	C	R	R	R	R	R	R	R	R

Tabla 3.17 Matriz RACI del 8vo proceso habilitador de TI.

- **Proceso habilitador: Gestionar los cambios**

Descripción: Este proceso se encarga de que los cambios se realice de manera controlada y asegurando la seguridad de la información.

Práctica clave de gobierno: Evaluar, priorizar y autorizar peticiones de cambio
El dueño del activo debe de aprobar formalmente cada cambio según la evaluación de riesgos realizada.
Evaluar el riesgo de implementar las peticiones de cambio y considerar las implicaciones de seguridad, legales y de cumplimiento normativo.
Las peticiones de cambio deben de ser categorizadas y relacionados con los elementos de configuración que son afectados.
Las peticiones de cambios a los activos de TI deben de cumplir los controles de seguridad y deben de ser aprobados por los dueños de las aplicaciones.
Planificar y programar todos los cambios aprobados.
Práctica clave de gobierno: Gestionar los cambios emergentes
Asegurar que hay un procedimiento para evaluar y autorizar los cambios de emergencia.
Supervisar que todos los cambios de emergencias son revisados después de su implementación.
Verificar que los accesos para los cambios de emergencia están apropiadamente autorizados, documentos y son revocados después de realizar los cambios.
Práctica clave de gobierno: Ubicar y reportar el cambio de estado
Categorizar las peticiones de cambio en el proceso de seguimiento del cambio.
Mantener un sistema de seguimiento y de reporte para todos los cambios solicitados.
Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados dentro de los plazos establecidos y su prioridad, evitando accesos no autorizados.
Práctica clave de gobierno: Cerrar y documentar los cambios
Definir un periodo apropiado para conservar la documentación asociado a la gestión del cambio.

Documentar los cambios como parte integral de la gestión del cambio.

Tabla 3.18Actividades del 9no proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar los cambios																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Evaluar, priorizar y autorizar peticiones de cambio					A	R			C	C				C	C	R	C	R	R	C	R	C	
Gestionar los cambios emergentes					A	I				C				C	C	R	I	R	R		I	C	
Ubicar y reportar el cambio de estado					C	R			C							A		R	R		R		

Cerrar y documentar los cambios					A	R			R	C				C	C	R	C	R	R	I	I		

Tabla 3.19 Matriz RACI del 9no proceso habilitador de TI.

- **Proceso habilitador: Gestionar los activos**

Descripción: Este proceso se encarga de que durante el ciclo de vida del activo se cumplan con los controles de seguridad de la información y asegurar

Práctica clave de gobierno: Identificar y registrar los activos actuales
Determinar regularmente si cada activo de información sigue proporcionando valor para su objetivo.
Identificar los requisitos de seguridad de la información y legales que deben de ser cumplidos en la gestión de los activos.
Registrar todos los activos de información y mantener su alineación con la gestión de cambios y de la configuración.
Verificar que todos los activos de información cuentan con un propietario asignado.
Práctica clave de gobierno: Gestionar los activos críticos
Establecer un plan de mantenimiento preventivo para los activos críticos de información.
Identificar que los activos críticos para proveer los servicios cumplen con los requerimientos de negocios y de seguridad de la información.
Regularmente considerar la necesidad del reemplazo de los activos críticos de información debido al riesgo de falla operativa.
Supervisar el rendimiento de los activos críticos y el cumplimiento de los controles de seguridad de información.
Práctica clave de gobierno: Gestionar el ciclo de vida de los activos
Asignar los activos a los usuarios los cuales firmarán la aceptación de sus responsabilidades.
Desplegar los activos considerando los controles de seguridad de información durante el ciclo de vida de implementación.
Eliminar los activos de forma segura, teniendo en cuenta la eliminación permanente de los datos registrados en dispositivos.
Práctica clave de gobierno: Optimizar el costo de los activos
Evaluar los costes de mantenimiento de los equipos de seguridad, considerar si son razonables e identificar opciones de menor coste.
Revisar la base general de activos de seguridad, teniendo en cuenta si está alineada con los requerimientos del negocio.
Práctica clave de gobierno: Gestionar las licencias
Comparar el número de copias de software instalado con el número de licencias compradas.
Cuando la cantidad de copias usadas sea mayor a la cantidad de copias compradas, considerar primero la posibilidad de desinstalar copias que no se adquirir licencias adicionales para cumplir con los acuerdos de licencia.
Cuando la cantidad de copias usadas sea menor a la cantidad de copias compradas, decidir si existe una necesidad de mantener o cancelar licencias
Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.

Periódicamente llevar a cabo una auditoría para identificar que todas las copias de software instaladas cuenten licencia.

Tabla 3.20 Actividades del 10mo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar los activos																							
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Identificar y registrar los activos actuales			C			C										I	C	C	A	R	C		
Gestionar los activos críticos			C		I	C								C	C		R	R	A	R	C	C	C
Gestionar el ciclo de vida de los activos						C											C	C	A	R	R		
Optimizar el costo de los activos			R		I	C										A	R	R	R	R	R		
Gestionar las licencias.					I	C								C	R	A		R	R	R	C		

Tabla 3.21 Matriz RACI del 10mo proceso habilitador de TI.

- **Proceso habilitador: Gestionar peticiones e incidentes de servicio**

Descripción: Este proceso se encarga de que las respuestas a las peticiones e incidentes de seguridad de la información se den a tiempo y de manera efectiva.

Práctica clave de gobierno: Definir esquemas de clasificación de incidentes y peticiones de servicio.
Definir esquemas de clasificación y priorización para el registro y atención de los incidentes y peticiones de servicios de seguridad de la información.
Definir fuentes de conocimiento para la atención de incidentes y peticiones de servicios de seguridad de la información.
Definir procedimientos y reglas de estalación de los incidentes y peticiones de servicios de seguridad de la información según el nivel de impacto.
Práctica clave de gobierno: Registrar, clasificar y priorizar peticiones e incidentes.
Analizar y clasificar los incidentes y peticiones de servicios de seguridad de la información.
Priorizar la atención de los incidentes y peticiones de servicios de seguridad de la información según los SLA definidos y el impacto en el negocio y la urgencia.
Registrar toda la información relevante de todos los incidentes y peticiones de servicios de seguridad de la información, para atenderlos efectivamente y mantener un registro historio de estos.
Práctica clave de gobierno: Verificar, aprobar y resolver peticiones de servicio
Obtener la aprobación financiera y funcional firmada de las solicitudes.
Verificar los derechos para hacer las peticiones de servicios de seguridad de la información según un proceso definido.
Práctica clave de gobierno: Investigar, diagnosticar y localizar incidentes.
Asignar un especialista para resolver el incidente en caso sea necesario.
Identificar los síntomas relevantes para establecer las causas de los incidentes de seguridad de la información.
Práctica clave de gobierno: Resolver y recuperarse ante incidentes.

Documentar las soluciones de los incidentes de seguridad de la información para usarlas como fuente de conocimiento futuro.
Ejecutar acciones de recuperación si se requieren.
Registrar si se usaron soluciones temporales para resolver los incidentes de seguridad de la información.
Seleccionar y aplicar las soluciones más apropiadas a los incidentes de seguridad de la información.
Práctica clave de gobierno: Cerrar peticiones de servicio e incidentes
Cerrar los incidentes y peticiones de servicios de seguridad de la información.
Verificar con los usuarios afectados si el incidente o petición de servicios de seguridad de la información han sido resueltas satisfactoriamente.
Práctica clave de gobierno: Seguir el estado y emitir de informes
Analizar que las respuestas a los incidentes y peticiones de servicios de seguridad de la información estén dentro de los SLA establecidos, para identificar las brechas o ineficiencias y planificarlo en la mejora continua.
Identificar la información para presentar a los stakeholders sobre la solución de los incidentes de seguridad de la información.
Monitorear y hacer seguimiento del escalamiento de los incidentes que se siguieron para realizar la solución.

Tabla 3.22 Actividades del 11avo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar peticiones e incidentes de servicio																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Definir esquemas de clasificación de incidentes y peticiones de servicio.						C				I	I					A	C	R	R		R	C	C
Registrar, clasificar y priorizar peticiones e incidentes.						I				I	I								A		R		
Verificar, aprobar y resolver peticiones de servicio						R										I		R	R		A		
Investigar, diagnosticar y						R				I	I			I	I	I		C	R		A	C	

localizar incidentes.																							
Resolver y recuperarse ante incidentes.						I				I	I			C	C	I		R	R		A	R	
Cerrar peticiones de servicio e incidentes						I				I	I			I	I	I		I	A		I	R	
Seguir el estado y emitir de informes						I				I	I			I	I	I		I	A		R	I	

Tabla 3.23 Matriz RACI del 11avo proceso habilitador de TI.

- **Proceso habilitador: Gestionar los servicios de seguridad**

Descripción: Este proceso se encarga de proteger la información de la empresa, al nivel aceptable del nivel de riesgo de seguridad de la información.

Práctica clave de gobierno: Proteger contra software malicioso (malware)
Capacitar periódicamente al personal sobre los malware en el uso del correo e internet y recordarles que no deben de instalar software no autorizados.
Comunicar los procedimientos y responsables para la prevención contra software malicioso.
Distribuir el software de protección de forma centralizada.
Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, spyware y phishing).
Instalar y activar herramientas de protección contra software malicioso en los lugares de procesamiento de información crítica.
Revisar y evaluar regularmente la información sobre nuevas amenazas posibles.
Gestionar la seguridad de la red y las conexiones.
Aplicar protocolos de seguridad aprobados para las conexiones de red.

Cifrar la información en tránsito de acuerdo a su clasificación.
Configurar la seguridad en los equipos de red de forma correcta.
Establecer mecanismos de confianza para dar soporte a la transmisión y recepción de la información de manera segura.
Establecer una política de seguridad de las conexiones según los requerimientos del negocio.
Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.
Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa mediante el uso contraseña.
Realizar pruebas de intrusión periódicas para determinar el nivel de protección de la red.
Realizar pruebas de seguridad en los sistemas de manera periódica para determinar el nivel de protección de los sistemas.
Práctica clave de gobierno: Gestionar la seguridad de los puestos de usuario final.
Cifrar la información almacenada de acuerdo a su clasificación.
Configurar la seguridad en los sistemas operativos de forma correcta.
Deshacerse los dispositivos de usuario final de forma segura.
Gestionar el acceso y control remoto.
Gestionar la configuración de seguridad de la red.
Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
Implementar mecanismos de bloqueo en los dispositivos de usuario final.
Proteger la integridad de los sistemas.
Proveer protección física a los dispositivos de usuario final.
Práctica clave de gobierno: Gestionar la identidad del usuario y el acceso lógico

Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto solo en transacciones aprobadas, documentadas y autorizadas por los dueños de los sistemas.
Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI son identificables unívocamente.
Autenticar todos los accesos a los activos de información basándose en la clasificación de seguridad y coordinar con gestión de accesos que los controles de autenticación han sido administrados adecuadamente.
Identificar únicamente todas las actividades del proceso de la información por roles, coordinando con las unidades del negocio y asegurando que todos los roles están definidos consistentemente.
Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de sus funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, la necesidad de tener y la necesidad de conocer.
Mantener registros de auditoría de los accesos a la información clasificada como altamente sensible.
Realizar regularmente revisiones de todas las cuentas y privilegios relacionados.
Segregar y gestionar cuentas de usuario privilegiadas.
Práctica clave de gobierno: Gestionar el acceso físico a los activos de TI
Asegurar que los accesos a las ubicaciones de procesamiento de datos de TI deben darse en funciones de trabajo y responsabilidades.
Escoltar a los visitantes en todo momento mientras esté en las instalaciones de la empresa. Si se encuentra a un individuo que no va acompañado o que no resulta familiar y que no lleva visible la tarjeta de identificación se deberá alertar al personal de seguridad.
Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento.
Instruir a todo el personal para que mantengan visible su tarjeta de identificación en todo momento.
Realizar regularmente concienciación de la seguridad física.
Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar a todos los visitantes incluyendo contratistas y proveedores.

Restringir el acceso a ubicaciones sensibles de TI estableciendo restricciones en el perímetro, como dispositivos de seguridad en las puertas interiores y exteriores y asegurar que los dispositivos registren el ingreso y alerten en caso de un acceso no autorizado. .
Práctica clave de gobierno: Gestionar documentos sensibles y dispositivos de salida.
Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.
Destruir adecuadamente la información sensible (por ejemplo: trituradoras disponibles para destruir documentos confidenciales) y los dispositivos de salida (por ejemplo: desmagnetizando los dispositivos magnéticos, destruyendo físicamente dispositivos de memoria).
Establecer procedimientos para gestionar la recepción, uso, eliminación y destrucción de documentos sensibles y dispositivos de salida dentro y fuera de la empresa.
Establecer un inventario de documentos sensibles y dispositivos de salida para realizar regularmente verificaciones.
Establecer una seguridad física apropiada sobre información sensible y dispositivos sensibles.
Práctica clave de gobierno: Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
Asegurar que los tickets de incidentes de seguridad se crean en el momento oportuno.
Definir y comunicar las características de los potenciales incidentes relacionados con la seguridad de forma que sean fácilmente reconocibles y comprender el impacto para permitir una respuesta adecuada.
Registrar los eventos relacionados con la seguridad reportada por las herramientas de monitorización de seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo.
Revisar regularmente los registros de los eventos para detectar potenciales incidentes de seguridad.

Tabla 3.24 Actividades del 12avo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Gestionar los servicios de seguridad																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio
Proteger contra software malicioso (malware)						R	I			C	A		R	C	C	C	I	R	R		I	R	
Gestionar la seguridad de la red y las conexiones.						I				C	A			C	C	C	I	R	R		I	R	
Gestionar la seguridad de los puestos de usuario final.						I				C	A			C	C	C	I	R	R		I	R	
Gestionar la identidad del						R				C	A		I	C	C	C	I	C	R		I	R	

usuario y el acceso lógico																							
Gestionar el acceso físico a los activos de TI						I				C	A			C	C	C	I	C	R		I	R	I
Gestionar documentos sensibles y dispositivos de salida.										I				C	C	A			R				
Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I		C				I	A			C	C	C	I	C	R		I	R	I

Tabla 3.25 Matriz RACI del 12avo proceso habilitador de TI.

- **Proceso habilitador: Supervisar, evaluar y medir el rendimiento y la conformidad**

Descripción: Este proceso se encarga de supervisar que la seguridad de la información se está realizando acorde al rendimiento acordado y conforme a los objetivos y métricas definidos.

Práctica clave de gobierno: Establecer un enfoque de la supervisión
Acordar los objetivos y métricas de seguridad de la información.
Acordar un proceso de control y de presentación de informes sobre la seguridad de la información.
Identificar las stakeholders que van a monitorear la seguridad de la información.

Identificar periódicamente los nuevos stakeholders, requisitos y recursos para la seguridad de la información.
Involucrar a los stakeholders y comunicar los objetivos y requisitos de seguridad de la información.
Mantener y alinear de forma continua el enfoque de supervisión y evaluación de la seguridad de la información con el enfoque de la compañía.
Solicitar, priorizar y reservar recursos para la supervisión de la seguridad de la información.
Práctica clave de gobierno: Establecer los objetivos de cumplimiento y rendimiento
Comunicar los cambios propuestos para el rendimiento y cumplimiento de las metas de seguridad de la información.
Definir y revisar periódicamente los objetivos y métricas para la seguridad de la información con los stakeholders para identificar cualquier detalle significativo omitido y definir metas razonables.
Evaluar si los objetivos y métricas son adecuados, es decir sean específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).
Práctica clave de gobierno: Recopilar y procesar los datos de cumplimiento y rendimiento.
Consolidar los datos para soportar el cálculo de las métricas acordadas.
Recopilar los datos para la gestión de la seguridad de la información (de forma automatizada cuando sea posible).
Utilizar herramientas y sistemas apropiados para el procesamiento de los datos a analizar.
Práctica clave de gobierno: Analizar e informar sobre el rendimiento
Diseñar informes de rendimiento de los controles de seguridad de la información que sean fáciles de entender y ajustados a las diferentes necesidades de gestión y audiencias para facilitar la toma efectiva y oportuna de decisiones.
Distribuir los informes de seguridad de la información a los stakeholders involucrados.
Recomendar cambios a los objetivos y métricas definidos, cuando sea apropiado.
Práctica clave de gobierno: Asegurar la implantación de medidas correctivas.

Asegurar que se mantiene la asignación de responsabilidades para las acciones correctivas.
Hacer seguimiento de los resultados de las acciones comprometidas.
Informar los resultados a los stakeholders.
Revisar las respuestas, opciones y recomendaciones de la alta dirección con referencia a las medidas de seguridad de la información.

Tabla 3.26 Actividades del 13avo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Supervisar, evaluar y medir el rendimiento y la conformidad																						
Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la	Gestor de Continuidad de Negocio
Establecer un enfoque de la supervisión		A	R	R	R	I	C		I				C	C	C	R	I	C	C	I	C	I	I
Establecer los objetivos de cumplimiento y rendimiento		I	I	I	A	R			I				C			C	C	R	R	I	R	I	I

Recopilar y procesar los datos de cumplimiento y rendimiento.					C	R			I				C			A		R	R	I	R	I	I
Analizar e informar sobre el rendimiento					A	R			C				C	C	C	C	C	R	R	C	R	C	C
Asegurar la implantación de medidas correctivas.	I	I	I	I	C	R			C				C	C	C	A	C	R	R	C	R	C	C

Tabla 3.27 Matriz RACI del 13avo proceso habilitador de TI.

- **Proceso habilitador: Supervisar, evaluar y medir la conformidad con los requerimientos externos**

Descripción: Este proceso se encarga de que se cumpla con los requisitos regulatorios de seguridad de la información en los procesos de TI y del negocio.

Práctica clave de gobierno: Identificar requisitos externos de cumplimiento.
Asignar las responsabilidad de identificar y supervisar los cambios en la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.
Identificar los requerimientos de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales sobre las actividades de TI.
Mantener un inventario de los requisitos legales y regulatorios de la empresa.
Práctica clave de gobierno: Optimizar la respuesta a requisitos externos.

Revisar con regularidad la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales para asegurar el cumplimiento requerido.
Comunicar los requisitos de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales al personal involucrado.
Práctica clave de gobierno: Confirmar el cumplimiento de requisitos externos
Evaluar periódicamente los procesos y actividades de TI y del negocio para asegurar el cumplimiento de circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.
Práctica clave de gobierno: Obtener garantía del cumplimiento de requisitos externos.
Si es necesario, obtener declaraciones de los proveedores de servicio TI externos acerca de su nivel de cumplimiento de la ley de protección de datos personales.
Obtener confirmación regularmente del cumplimiento de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales por parte de los gerentes responsables de su cumplimiento.
Realizar revisiones regulares internas para evaluar los niveles de cumplimiento de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.

Tabla 3.28 Actividades del 14avo proceso habilitador de TI.

Matriz de responsabilidades (matriz RACI)

Supervisar, evaluar y medir la conformidad con los requerimientos externos

Prácticas claves de gobierno	Directorio	Gerente General	Gerente de Finanzas	Gerente de Operaciones	Gerentes	Dueños de Procesos de Negocio	Comité Estratégico de Gerencia	Comité de Proyectos	Jefe de Proyectos	Gerente de Riesgos	Oficial de Seguridad de la Información	Comité de riesgos	Gerente de Gestión Humana	Cumplimiento Normativo	Auditoria	Gerente de TI	Jefe de Arquitectura	Jefe de Desarrollo	Jefe de Operaciones de TI	Jefe de Administración de TI	Gestor de Servicios	Gestor de Seguridad de la	Gestor de Continuidad de Negocio
Identificar requisitos externos de cumplimiento.					A	R								R	R	R							
Optimizar la respuesta a requisitos externos.		R	R	R	A	R	I		R					R	R	R	I	R	R	R	R	R	R
Confirmar el cumplimiento de requisitos externos	I	R	R	R	R	R	I	I	C					A	I	R	C	C	C	C	C	C	C
Obtener garantía del cumplimiento de requisitos externos.	I	I	I	I	C	C	I		C					C	A	R	C	C	C	C	C	C	C

Tabla 3.29 Matriz RACI del 14avo proceso habilitador de TI.

4 Anexo 4: Inventario de activos de información

- **Activos del proceso de atención al cliente**

Proceso	Activo de Información				Ubicación del activo de información		Formato			Valoración			
Actividad	Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo	Física	Lógica	Papel	Electrónico	Otros	Confidencialidad	Integridad	Disponibilidad	Valor
Obtener prospecto y revisar sus datos en la SBS	Datos del prospecto	Datos básicos del nuevo cliente	Primario	Área de operaciones	Archivo del afiliado		x			1	1	1	Bajo
Visitar al cliente y realizar solicitud de traspaso sección 1 y 2	Copia del DNI	Documento nacional de identidad	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto
Verificar los datos y documentos adjuntos	Copia del DNI	Documento nacional de identidad	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto
Verificar la solicitud de traspaso	Copia del DNI	Documento nacional de identidad	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto

Revisar que la solicitud cumpla con los requisitos de la SBS	Copia del DNI	Documento nacional de identidad	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto
Visitar al cliente y realizar solicitud de traspaso sección 1 y 2	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para cambiarse a otra AFP.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto
Llenar sección 3 de la solicitud de traspaso	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para cambiarse a otra AFP.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto

Verificar los datos y documentos adjuntos	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para cambiarse a otra AFP.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto
Verificar la solicitud de traspaso	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para cambiarse a otra AFP.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto
Revisar que la solicitud cumpla con los requisitos de la SBS	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto

		solicitud para cambiarse a otra AFP.											
Adjuntar copia de la boleta de pago del mes anterior	Boleta de pago	Documento que contiene los ingresos mensuales y datos generales de un trabajador.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto
Verificar los datos y documentos adjuntos	Boleta de pago	Documento que contiene los ingresos mensuales y datos generales de un trabajador.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto
Verificar la solicitud de traspaso	Boleta de pago	Documento que contiene los ingresos mensuales y datos generales de un trabajador.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto

Revisar que la solicitud cumpla con los requisitos de la SBS	Boleta de pago	Documento que contiene los ingresos mensuales y datos generales de un trabajador.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto

Tabla 4.1 Activos del proceso de atención al cliente

Activos del proceso de traspasos

Proceso	**Activo de Información**				**Ubicación del activo de información**		**Formato**			**Valoración**			
Actividad	Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo	Física	Lógica	Papel	Electrónico	Otros	Confidencialidad	Integridad	Disponibilidad	Valor
Revisar las solicitudes y aprobarlas	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto

		cambiarse a otra AFP.											
Enviar solicitud de traspaso	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para cambiarse a otra AFP.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto
Crear solicitud de traspasos	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y acceder a los programas asociados al proceso de traspaso	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto
Corregir los traspasos	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto

		acceder a los programas asociados al proceso de traspaso											
Crear solicitud de traspasos	Módulo de digitación	Aplicación que permite digitar todos los datos relacionados a algún formulario definido en la organización	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto
Corregir los traspasos	Módulo de traspasos	Aplicación que permite realizar todas las actividades relacionadas a un traspaso.	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto
Revisar las solicitudes y aprobarlas	Copia del DNI	Documento nacional de identidad	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto
Revisar las solicitudes	Boleta de pago	Documento que	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	1	1	Alto

y aprobarlas		contiene los ingresos mensuales y datos generales de un trabajador.											
Ejecutar proceso de validación	Módulo de traspasos	Aplicación que permite realizar todas las actividades relacionadas a un traspaso.	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto

Tabla 4.2 Activos del proceso de traspasos

- **Activos del proceso de Generar IAT2**

Proceso	Activo de Información				Ubicación del activo de información		Formato			Valoración			
Actividad	Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo	Física	Lógica	Papel	Electrónico	Otros	Confidencialidad	Integridad	Disponibilidad	Valor
Actualizar el estado de las solicitudes	Módulo de traspasos	Aplicación que permite realizar todas las	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto

de traspasos		actividades relacionadas a un traspaso.											
Corregir las solicitudes de traspasos	Módulo de traspasos	Aplicación que permite realizar todas las actividades relacionadas a un traspaso.	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto
Actualizar el estado de las solicitudes de traspasos	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y acceder a los programas asociados al proceso de traspaso	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto
Corregir las solicitudes de traspasos	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y acceder a los	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto

		programas asociados al proceso de traspaso											
Generar carta al cliente explicando el caso de rechazo de la SBS	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y acceder a los programas asociados al proceso de traspaso	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto
Enviar IAT2 a la SBS	IAT2	Documento que contiene las solicitudes de los nuevos traspasos de ingreso	Primario	Área de operaciones	---	Aplicación		x		2	3	2	Alto
Enviar IAT2 a la SBS	Extranet de la SBS	Portal en el cual se realiza los trámites relacionados a los traspasos	Soporte	Área de operaciones	---	Aplicación		x		2	1	3	Alto

Recibir la respuesta de la SBS	IET2	Documento que contiene el detalle de la respuesta de la SBS para cada solicitud de traspaso	Primario	Área de operaciones	---	Aplicación		x		2	3	2	Alto
Recibir la respuesta de la SBS	IOT2	Documento que contiene el resultado de respuesta de la SBS para cada solicitud de traspaso	Primario	Área de operaciones	---	Aplicación		x		2	3	2	Alto
Enviar solicitudes de traspaso a digitalizar	Solicitud de traspaso	Documento en el cual una persona que se encuentra afiliada a una AFP, presenta la solicitud para cambiarse a otra AFP.	Primario	Área de operaciones	Archivo del afiliado	Servidor de digitalización	x	x		3	2	1	Alto
Generar carta al	Carta al cliente	Documento en el cual se	Primario	Área de operaciones	---	Aplicación	x	x		1	1	2	Medio

cliente explicando el caso de rechazo de la SBS		le explica al cliente el resultado final del traspaso											

Tabla 4.3 Activos del proceso de Generar IAT2

- **Activos del proceso de generar IAT5**

Proceso	**Activo de Información**				**Ubicación del activo de información**		**Formato**			**Valoración**			
Actividad	Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo	Física	Lógica	Papel	Electrónico	Otros	Confidencialidad	Integridad	Disponibilidad	Valor
Recibir IAT5	IAT5	Documento que contiene las notificaciones del traspasos	Primario	Área de operaciones	---	Aplicación		x		2	3	2	Alto
Revisar el estado de la solicitud de traspaso	Módulo de traspasos	Aplicación que permite realizar todas las actividades relacionadas a un traspaso.	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto

Generar el archivo de kit de bienvenida	Módulo de traspasos	Aplicación que permite realizar todas las actividades relacionadas a un traspaso.	Soporte	Área de operaciones	---	Aplicación		x		3	3	3	Alto
Revisar el estado de la solicitud de traspaso	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y acceder a los programas asociados al proceso de traspaso	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto
Generar el archivo de kit de bienvenida	Computadora de escritorio	Computadoras que se utilizan para realizar los trámites y acceder a los programas asociados al proceso de traspaso	Soporte	Área de operaciones	Área de operaciones	---		x		2	2	3	Alto

Encriptar y enviar archivo de kit de bienvenida	Archivo de kit de bienvenida	Archivo que contiene los datos necesarios para crear el kit de bienvenida del nuevo afiliado	Primario	Área de operaciones	---	Aplicación		x		2	3	2	Alto
Enviar kit de bienvenida al afiliado	Kit de bienvenida	Documentos de bienvenida que se le dan al nuevo afiliado sobre la información de la empresa y fondo en el que está.	Primario	Área de operaciones	Archivo del afiliado	---	x			2	1	1	Medio
Generar y enviar carta de explicación al afiliado	Carta al cliente	Documento en el cual se le explica al cliente el resultado final del traspaso	Primario	Área de operaciones	---	Aplicación	x	x		1	1	2	Medio

Tabla 4.4 Activos del proceso de generar IAT5

- **Activos transversales de soporte**

Activo de Información				Ubicación del activo de información		Formato			Valoración			
Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo	Física	Lógica	Papel	Electrónico	Otros	Confidencialidad	Integridad	Disponibilidad	Valor
Centro de procesamiento de datos	Lugar en el cual se encuentran almacenado los servidores que dan soporte a las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de tecnología	Centro de computo	---			x	3	3	3	Alto
Servidores de base de datos (ambiente de desarrollo)	Servidor de base de datos en el cual se hacen los desarrollos necesarios para las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto
Servidores de base de datos (ambiente de pruebas)	Servidor de base de datos en el cual se hacen las pruebas de los desarrollos necesarios para las aplicaciones ("Módulo	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto

	de traspasos" y "Módulo de digitación")											
Servidores de base de datos (ambiente de producción)	Servidor de base de datos en el cual se encuentran los datos reales de las transacciones de las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto
Servidores de base de datos (ambiente de contingencia)	Servidor de base de datos en el cual se encuentra una copia de los datos reales de las transacciones de las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto
Servidores de aplicación (ambiente de desarrollo)	Servidor de aplicación en el cual se realizan las nuevas funcionalidades o modificaciones a las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto
Servidores de	Servidor de aplicación en el cual se prueban	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto

aplicación (ambiente de pruebas)	las nuevas funcionalidades o modificaciones a las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")											
Servidores de aplicación (ambiente de producción)	Servidor de aplicación en el cual se encuentran operando las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto
Servidores de aplicación (ambiente de contingencia)	Servidor de aplicación en el cual se encuentra una copia de la funcionalidad de las aplicaciones ("Módulo de traspasos" y "Módulo de digitación")	Soporte	Área de operaciones	Centro de contingencia	---			x	3	3	3	Alto
Servidor de archivos	Servidor que se utiliza para almacenar los archivos que se trabaja en todas las áreas de la empresa	Soporte	Área de operaciones	Centro de computo	---			x	3	3	3	Alto
Backup del servidor de archivos	Servidor que cuenta con una copia del servidor de archivos	Soporte	Área de operaciones	Centro de contingencia	---			x	3	3	3	Alto

Tabla 4.5 Activos transversales de soporte

5 Anexo 5: Matriz de riesgos

Valoración del riesgo

IDENTIFICACION DEL RIESGO						EVALUACIÓN DE RIESGOS		
ID Riesgo	**Fuente de riesgo**	**Tipo evento**	**Factor que origina el riesgo**	**Descripción del riesgo**	**Consecuencia del riesgo**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
Proceso de atención al cliente								
R01	Problemas con la conexión de internet	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible imposibilidad para acceder a los datos del cliente en la aplicación de la SBS por problemas de conectividad.	Posible pérdida de afiliación de un nuevo cliente.	Ocasional	Leve	Bajo
R02	Falta de protección física donde se almacena la información del cliente	Ejecución, entrega y gestión de procesos	Procesos Internos	Posible acceso a la información del cliente por personas no autorizadas	Posible divulgación de la información personal del cliente.	Moderado	Leve	Moderado
R03	Falta de protección física donde se almacena la información del cliente	Ejecución, entrega y gestión de procesos	Procesos Internos	Posible modificación a la solicitud de traspaso del cliente por personas no autorizadas	Posible reclamo por parte del cliente sobre sus datos modificados.	Moderado	Medio	Moderado

R04	Falta de protección física donde se almacena la información del cliente	Ejecución, entrega y gestión de procesos	Personal	Posible pérdida de la información del cliente por dejarla en un lugar desatendido	Posible reclamo del cliente por perder la su información personal.	Ocasional	Medio	Moderado
R05	Falta de protección ambiental en lugar donde se almacena la carpeta del cliente	Ejecución, entrega y gestión de procesos	Procesos Internos	Posible pérdida de la información del cliente porque se incendió el lugar donde se almacena la información del cliente.	Posible información consumida por el fuego.	Ocasional	Leve	Bajo
Proceso de traspasos								
R06	Problemas con el servidor que aloja al módulo de digitación	Daños a activos materiales	Tecnología de Información	Posible indisponibilidad para digitar la solicitud de traslado por una falla en el módulo de digitación	Posible pérdida operativa para poder presentar la solicitud de traslado a la SBS	Ocasional	Muy leve	Bajo
R07	Problemas de conectividad entre la computadora de escritorio y el servidor en el que está alojado la aplicación	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible indisponibilidad para digitar la solicitud de traslado por una falla en la red	Posible pérdida operativa para poder presentar la solicitud de traslado a la SBS	Moderado	Muy leve	Bajo

R08	Problemas en el desarrollo del módulo de digitación	Interrupción de las operaciones y fallos en los sistemas	Procesos Internos	Posible registro erróneo de la solicitud de traslado por una falla interna en el módulo de digitación	Posible reclamo por parte del cliente porque su información se encuentra incorrecta	Moderado	Leve	Moderado
R09	Problemas con el servidor que aloja al módulo traspasos	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible indisponibilidad al ejecutar el proceso de validación de la información de la solicitud de traspaso por una falla del módulo de traspasos	Posible retraso para presentar las solicitudes de traspasos a la SBS	Moderado	Leve	Moderado
R10	Problemas de conectividad entre la computadora de escritorio y el servidor en el que está alojado la aplicación	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible indisponibilidad al ejecutar el proceso de validación de la información de la solicitud de traspaso por una falla de la red	Posible retraso para presentar las solicitudes de traspasos a la SBS	Ocasional	Leve	Bajo
R11	Problemas en el desarrollo del módulo de traspasos	Interrupción de las operaciones y fallos en los sistemas	Procesos Internos	Posible error a ejecutar el proceso de validación de información de la solicitud de traspaso por una falla interna del módulo de traspasos	Posible validación de las solicitud de traspasos con errores	Moderado	Leve	Moderado
Generar IAT02								

R12	Problemas con la conexión del internet	Interrupción de las operaciones y fallos en los sistemas	Eventos Externos	Posible retraso del envió del IAT2 por problemas con la red	Posible pérdida de oportunidad de afiliar clientes	Ocasional	Medio	Moderado
R13	Indisponibilidad de la extranet de la SBS	Interrupción de las operaciones y fallos en los sistemas	Eventos Externos	Posible retraso del envió del IAT2 por fallas en la extranet de la SBS	Posible pérdida de oportunidad de afiliar clientes	Moderado	Medio	Moderado
R14	La computadora donde se genera el IAT2 se encuentre comprometida con algún virus	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible envió de información invalida del IAT2 por modificación no autorizada del archivo	Posible reclamo del cliente por presentar información errada.	Eventual	Medio	Bajo
R15	Problemas con la conexión del internet	Interrupción de las operaciones y fallos en los sistemas	Eventos Externos	Posible problemas para descargar el IET2 y IOT2 por indisponibilidad de la extranet de la SBS	Posible reclamo de los clientes por falta de información sobre el estado de la solicitud de traslado.	Ocasional	Leve	Bajo
R16	Indisponibilidad de la extranet de la SBS	Interrupción de las operaciones y fallos en los sistemas	Eventos Externos	Posible problemas para descargar el IET2 y IOT2 por fallas en la extranet de la SBS	Posible reclamo de los clientes por falta de información sobre el estado de la solicitud de traslado.	Ocasional	Leve	Bajo
R17	Inadecuado proceso de almacenamiento de información	Ejecución, entrega y gestión de procesos	Personal	Posible pérdida de la solicitud de traspaso física por el proveedor de digitalización	Posible reclamo con el cliente.	Ocasional	Medio	Moderado

R18	Equivocación al enviar la información de las solicitudes de traspasos a la empresa	Ejecución, entrega y gestión de procesos	Personal	Posible divulgación de los datos almacenados de los clientes por el proveedor de digitalización.	Posible incumplimiento de la ley de protección de datos personales	Ocasional	Medio	Moderado
Generar IAT5								
R19	Problemas en el desarrollo del módulo de traspasos.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Posible error al generar el archivo de kit de bienvenida por falla en el módulo de traspasos.	Posible demora en la entrega de información al afiliado.	Ocasional	Muy leve	Bajo
R20	Descubrimiento de vulnerabilidad del método de encriptación.	Daños a activos materiales	Eventos Externos	Posible desencriptación del archivo del kit de bienvenida del afiliado por una vulnerabilidad en el método de encriptación	Posible acceso a la información personal no autorizada del afiliado.	Eventual	Medio	Moderado
R21	El servicio de impresión es tercerizado por el proveedor de impresión	Ejecución, entrega y gestión de procesos	Personal	Posible divulgación de la información de los afiliado de la empresa por el proveedor de impresión	Posible denuncia de los cliente por exposición de su información personal.	Ocasional	Medio	Moderado

Tabla 5.1 Valoración del riesgo

- **Tratamiento del riesgo**

ID Riesgo	Opción de tratamiento	Plan de contingencia	Tipo de control	Modalidad de Operación	Cláusula del control ISO/IEC 27002	Control ISO/IEC 27002	Responsable del control
Proceso de atención al cliente							
R01	Mitigar	Contar con un modem adicional con internet móvil.	Preventivo	Manual	13. Seguridad en las telecomunicaciones.	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	Servicios internos
R02	Mitigar	Colocar la información en un espacio designado para los documentos de los afiliados.	Preventivo	Automático	11. Seguridad física y ambiental.	11.1.3 Seguridad de oficinas, despachos y recursos.	Servicios internos
R03	Mitigar	Colocar sellos de seguridad por cada archivo donde se guarda los documentos de los afiliados.	Preventivo	Manual	8. Gestión de activos	8.2.2 Etiquetado y manipulado de la información.	Operaciones
R04	Mitigar	Colocar cámaras de seguridad en el lugar donde se almacena la información.	Correctivo	Automático	11. Seguridad física y ambiental.	11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.5 El trabajo en áreas seguras.	Servicios internos
R05	Mitigar	Colocar detectores de incendio.	Detectivo	Automático	11. Seguridad física y ambiental.	11.1.4 Protección contra las amenazas externas y ambientales.	Servicios internos
Proceso de traspasos							
R06	Mitigar	Informar para que la aplicación funcione en el servidor alterno.	Correctivo	Semi-automático	16. Gestión de incidentes en la seguridad de la información.	16.1.5 Respuesta a los incidentes de seguridad	Tecnología de Información

R07	Mitigar	Acondicionar una computadora alterna para realizar la misma tarea.	Correctivo	Manual	16. Gestión de incidentes en la seguridad de la información.	16.1.5 Respuesta a los incidentes de seguridad	Tecnología de Información
R08	Mitigar	Realizar pruebas de la funcionalidad de la aplicación cada vez que se realiza un cambio.	Detectivo	Automático	14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación	Operaciones
R09	Mitigar	Realizar mantenimientos a los servidores que alojan a la aplicación.	Preventivo	Manual	11. Seguridad física y ambiental.	11.2.4 Mantenimiento de los equipos.	Tecnología de Información
R10	Mitigar	Realizar pruebas de conectividad en la red interna.	Detectivo	Manual	13. Seguridad en las telecomunicaciones.	13.1.1 Controles de red.	Tecnología de Información
R11	Mitigar	Realizar pruebas de funcionalidad en el módulo de traspasos ante cualquier cambio en la funcionalidad.	Detectivo	Manual	14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación	Tecnología de Información / Operaciones
Procesos generar IAT2							
R12	Mitigar	Contar con una conexión de internet móvil.	Detectivo	Manual	13. Seguridad en las telecomunicaciones.	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	Tecnología de Información

R13	Mitigar	Comunicar a la SBS la falla que se está teniendo y preguntar cuál sería el canal a enviar la información.	Correctivo	Manual	15. Relación con proveedores	15.1.2 Tratamiento del riesgo dentro de acuerdos con proveedores.	Operaciones
R14	Mitigar	Comunicar a la SBS que se envió información errada y verificar la actualización y ejecución del antivirus en la computadora.	Correctivo	Semi-automático	12. Seguridad en la operativa.	12.2.1 Controles contra el código malicioso.	Tecnología de Información
R15	Mitigar	Contar con una conexión de internet móvil.	Detectivo	Manual	13. Seguridad en las telecomunicaciones.	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red	Tecnología de Información
R16	Mitigar	Comunicar a la SBS la falla que se está teniendo y preguntar si existe algún mecanismo para que envíen la información.	Correctivo	Manual	15. Relación con proveedores	15.1.2 Tratamiento del riesgo dentro de acuerdos con proveedores.	Operaciones
R17	Mitigar	Capacitar al personal sobre la importancia del cuidado de la información que se maneja de los clientes	Preventivo	Manual	7. Seguridad ligada a los recursos humanos.	7.2.2 Responsabilidades de gestión.	Tecnología de Información / Operaciones

R18	Mitigar	Colocar clausulas en el contrato con el proveedor de digitalización sobre la obligación de acuerdos de confidencialidad y manejo de la información.	Correctivo	Manual	7. Seguridad ligada a los recursos humanos. 13. Seguridad en las telecomunicaciones.	7.2.3 Concienciación, educación y capacitación en seguridad de la información 13.2.4 Acuerdos de confidencialidad y secreto.	Operaciones
Proceso generar IAT5							
R19	Mitigar	Realizar pruebas de la funcionalidad de la aplicación cada vez que se realiza un cambio.	Detectivo	Automático	14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación	Operaciones
R20	Mitigar	Cambiar de método de encriptación por uno de mayor complejidad.	Correctivo	Manual	10. Cifrado	10.1.1 Política de uso de los controles criptográficos.	Tecnología de Información
R21	Mitigar	Colocar clausulas en el contrato con el proveedor de impresión sobre la obligación de acuerdos de confidencialidad y manejo de la información.	Correctivo	Manual	7. Seguridad ligada a los recursos humanos. 13. Seguridad en las telecomunicaciones.	7.2.3 Concienciación, educación y capacitación en seguridad de la información 13.2.4 Acuerdos de confidencialidad y secreto.	Operaciones

Tabla 5.2 Tratamiento del riesgo

6 Anexo 6: Identificación del nivel de madurez de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.

Para poder identificar el nivel de madurez de los procesos habilitadores, primeramente se tendrá que identificar el cumplimiento de cada una de las actividades definidas dentro las actividades y controles que se realizan en la empresa del caso de estudio, para luego poder identificar el nivel de madurez del proceso habilitador según COBIT 5.

Para identificar el nivel de cumplimiento de los procesos se utilizará la siguiente escala:

Escala de puntuación del proceso	Descripción
N (No alcanzado)	Hay poca evidencia o no hay evidencia del logro del proceso analizado. El cumplimiento de las actividades está entre el 0% hasta el 15%.
P (Parcialmente alcanzado)	Existe alguna evidencia de que el proceso tiene un enfoque y algún alcance del atributo definido en el proceso analizado. Algunos aspectos del cumplimiento del atributo pueden ser impredecibles. El cumplimiento de las actividades está entre el 15% hasta el 50%.
L (Ampliamente alcanzando)	Hay evidencia de que el proceso tiene un enfoque sistemático y significativamente a alcanzado el atributo definido en el proceso analizado. Algunas debilidades relacionadas con el atributo pueden existir en el proceso analizado. El cumplimiento de las actividades está entre el 50% hasta el 85%.
F (Completamente alcanzado)	Hay evidencia de un proceso completo o con un enfoque sistemático y completo el alcance del atributo definido para el proceso analizado. No hay debilidades significativas relacionadas con el atributo del proceso analizado. El

	cumplimiento de las actividades está entre el 85% hasta el 100%.

Tabla 6.1 Niveles de cumplimiento de los procesos habilitadores.

Cabe mencionar que la empresa del caso de estudio tiene como objetivo que todos sus procesos habilitadores se encuentren gestionados, es decir en el nivel 2, y sean completamente alcanzados.

- **Proceso habilitador: Asegurar el establecimiento y mantenimiento del marco de gobierno**

Práctica clave de gobierno: Evaluar el sistema de gobierno	
Analizar e identificar los factores internos y externos del entorno del negocio relacionadas a la seguridad de la información que influenciaran en el diseño del gobierno de TI.	Cumple
Articular los principios de seguridad de la información que guiarán el diseño del gobierno de TI.	Cumple
Determina la relevancia de la seguridad de la información y su rol dentro del negocio.	Cumple
Considerar la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales para determinar cómo serán incorporadas dentro del gobierno de TI.	Cumple
Práctica clave de gobierno: Orientar el sistema de gobierno	
Asignar la responsabilidad y la autoridad de la seguridad de la información dentro del gobierno de TI.	Cumple
Comunicar los principios de seguridad de la información del gobierno de TI.	Cumple
Dirigir el establecimiento de un sistema de recompensa para promover el cambio cultural deseable del gobierno de TI con enfoque en seguridad de la información.	No Cumple
Establecer estructuras, procesos y prácticas de gobierno relacionadas a la seguridad de la información.	Cumple

Garantizar que los mecanismos de notificación y de comunicación proporcionan información adecuada a aquellos que tienen la responsabilidad de supervisar y tomar decisiones respecto a la seguridad de la información.	Cumple
Práctica clave de gobierno: Supervisar el sistema de gobierno	
Evaluar la efectividad del diseño del gobierno e identificar las acciones para rectificar cualquier desviación.	Cumple
Evaluar la efectividad y rendimiento del personal a quien se le dio responsabilidad y autoridad para la seguridad de la información dentro del gobierno de TI.	Cumple
Evaluar periódicamente si las estructuras, procesos y prácticas de gobierno relacionadas a la seguridad de la información están establecidas y operando efectivamente.	Cumple
Mantener la supervisión para que la empresa satisfaga las obligaciones de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.	Cumple
Monitorear los mecanismos regulares y rutinarios para asegurar que la empresa cumpla con la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales y políticas internas.	Cumple

Tabla 6.2 Cumplimiento del 1er proceso habilitador de TI.

Resultado: Este proceso se encuentra establecido (nivel 3) y completamente alcanzado, por lo que superó el objetivo definido.

- **Proceso habilitador: Asegurar la entrega de beneficios**

Práctica clave de gobierno: Evaluar la optimización de valor.	
Comprender los requerimientos de los stakeholders, las estrategias de TI y la capacidad actual de las TI relacionada a la seguridad de la información, para cumplir las estrategias del negocio.	Cumple

Comprender y discutir regularmente las posibles oportunidades que se pueden obtener de las nuevas tendencias de la seguridad de la información y optimizar el valor creado de estas oportunidades.	Cumple
Evaluar la efectividad de la integración entre las estrategias de la empresa y de TI, para el cumplimiento de los objetivos del negocio.	Cumple
Práctica clave de gobierno: Orientar la optimización del valor	
Dirigir a la gestión a considerar la seguridad de información para permitir que el negocio responda a las nuevas oportunidades del mercado, incremento de la ventaja competitiva o mejore sus procesos.	Cumple
Dirigir cualquier cambio en la asignación de las responsabilidades para la ejecución de las inversiones en seguridad de la información.	No cumple
Orienta cualquier cambio realizado en las inversiones de seguridad de la información para realinearlo con los objetivos de la empresa.	No cumple
Práctica clave de gobierno: Supervisar la optimización de valor	
Definir objetivos y métricas para el rendimiento de las inversiones en seguridad de la información.	No cumple
Después de las revisiones de los informes de seguridad de la información asegurar de que las medidas correctivas son iniciadas y controladas.	Cumple
Después de las revisiones de los informes de seguridad de la información tomar las medidas de gestión apropiadas para asegurar que el valor esta optimizado.	Cumple

Tabla 6.3 Cumplimiento del 2do proceso habilitador de TI.

Resultado: Este proceso solo se encuentra gestionado (nivel 2) y ampliamente alcanzado, por lo que no cumple el objetivo definido. Se recomienda que se pueda ejecutar por lo menos 2 de las actividades no cumplidas, para cumplir con el objetivo.

- **Proceso habilitador: Asegurar la optimización del riesgo**

Práctica clave de gobierno: Evaluar la gestión de riesgos

Determinar el nivel riesgo (apetito al riesgo) relacionada con TI que la empresa está dispuesta a asumir.	Cumple
Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.	Cumple
Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.	Cumple
Práctica clave de gobierno: Orientar la gestión de riesgos	
Dirigir la elaboración de planes de comunicación de los riesgos de seguridad de la información (cubriendo todos los niveles de la empresa), así como los planes de acción de estos riesgos.	Cumple
Dirigir la implantación de mecanismos apropiados para responder rápidamente a los riesgos y notificar inmediatamente a los niveles adecuados de la gestión.	Cumple
Dirigir para que el riesgo, las oportunidades, los problemas y preocupaciones de seguridad de la información puedan ser identificados y notificados por cualquier persona en cualquier momento.	Cumple
Promover una cultura proactiva de identificación de riesgos de seguridad de la información.	Cumple
Práctica clave de gobierno: Supervisar la gestión de riesgos	
Facilitar la revisión a los principales stakeholders el progreso de la empresa hacia los objetivos identificados de seguridad de información.	Cumple
Informar cualquier problema de gestión de riesgos al directorio.	Cumple
Monitorear hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales del apetito de riesgo.	No cumple

Tabla 6.4 Cumplimiento del 3ro proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y completamente alcanzado, por lo que se cumple el objetivo definido.

- **Proceso habilitador: Gestionar el marco de gestión de TI**

Práctica clave de gobierno: Definir la estructura organizativa	
Alinear la organización de la seguridad de la información dentro de la arquitectura organizacional de la empresa.	Cumple
Definir el alcance, puestos y roles internos y externos requeridos para la gestión de la seguridad de la información.	Cumple
Definir los mecanismos de comunicación tanto a nivel horizontal y a nivel vertical dentro de la organización.	Cumple
Definir los roles y responsabilidades de cada puesto dentro la estructura organizativa de seguridad de la información.	Cumple
Establecer el involucramiento de los stakeholders para la toma de decisiones respecto a la seguridad de la información.	Cumple
Establecer un comité directivo de seguridad de la información a nivel de gerencia, para determinar las prioridades de los programas de inversión de seguridad de la información de acuerdo a las estrategias y prioridades del negocio.	Cumple
Establecer un comité estratégico de seguridad de la información a nivel del directorio, para asegurarse el gobierno de TI se esté contemplando de forma adecuada y pueda brindar una dirección estratégica.	Cumple
Verificar regularmente la adecuación y la eficacia de la estructura organizativa.	Cumple
Práctica clave de gobierno: Establecer roles y responsabilidades	
Considerar los requisitos de la empresa y de la seguridad de la información al definir los roles.	Cumple
Establecer y comunicar los roles y responsabilidades de los puestos de seguridad de la información a toda la organización.	Cumple
Estructurar los roles y responsabilidades para reducir las posibilidades de que un solo rol puede comprometer una actividad critica.	Cumple
Incluir la descripción de los roles y responsabilidades de seguridad de la información dentro las políticas y procedimientos de gestión.	Cumple
Supervisar que los roles y responsabilidades se ejecuten adecuadamente y evaluar si tienen la autoridad y recursos suficientes para ejecutar sus roles y responsabilidades.	Cumple

Práctica clave de gobierno: Mantener los elementos habilitadores del sistema de gestión.	
Alinear el entorno de control de TI con las políticas, marcos a nivel nacional o internacional y las regulaciones de la seguridad de la información.	Cumple
Capacitar a todo el personal involucrado en las políticas de seguridad de la información con la finalidad de integrar las políticas en las operaciones que realicen.	Cumple
Comprender la visión, dirección y la estrategia de la empresa para poder dirigir la seguridad de la información.	Cumple
Crear un conjunto de políticas de seguridad de la información para dirigir las expectativas de control de TI en temas de seguridad de la información.	Cumple
Evaluar y actualizar por los menos una vez al año las políticas de seguridad de la información, según las necesidades del negocio.	Cumple
Integrar los principios de seguridad de la información con los principios del negocio.	Cumple
Práctica clave de gobierno: Comunicar los objetivos y la dirección de gestión	
Comunicar continuamente los objetivos de seguridad de la información con el apoyo de la alta gerencia.	Cumple
Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo de los objetivos de seguridad de la información.	Cumple
Práctica clave de gobierno: Optimizar la ubicación de la función de TI.	
Definir la ubicación del área de seguridad de la información dentro de la estructura organizativa y obtener la aprobación.	Cumple
Entender el contexto y la importancia del área de seguridad de la información.	Cumple
Definir la propiedad de la información (datos) y del sistema	
Contar con un inventario de información (sistemas y datos) con sus respectivos propietarios, custodios y clasificación.	Cumple
Definir e implementar procedimientos para asegurar la integridad de toda la información que se almacena en formato electrónico como las bases datos y archivos.	Cumple

Proveer herramientas, técnicas y directrices para brindar seguridad y control sobre la información y los sistemas de información en colaboración su propietario.	Cumple
Proveer políticas y directrices para asegurar y clasificar la información de la empresa.	Cumple
Práctica clave de gobierno: Gestionar la mejora continua de los procesos	
Considerar que las implementaciones de seguridad de la información no afecten la eficiencia y eficacia de los procesos críticos del negocio.	Cumple
Identificar los procesos críticos del negocio e identificar puntos de mejora para la seguridad de la información.	No cumple
Implementar y medir las mejoras acordadas de seguridad de la información en los procesos críticos del negocio.	No cumple
Práctica clave de gobierno: Mantener el cumplimiento con las políticas y procedimientos.	
Analizar los incumplimientos de las políticas y procedimientos de seguridad de la información y tomar acciones apropiadas.	Cumple
Hacer seguimiento al cumplimiento de las políticas y procedimientos de seguridad de la información.	Cumple
Integrar el rendimiento y cumplimiento de las políticas y procedimientos de la seguridad de la información dentro los objetivos individuales del personal.	Cumple

Tabla 6.5 Cumplimiento del 4to proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y completamente alcanzado, por lo que se cumple el objetivo definido.

- **Proceso habilitador: Gestionar los recursos humanos**

Práctica clave de gobierno: Mantener la dotación de personal suficiente y adecuado.	
Asegurar que se entrena a más de una persona en funciones críticas, con la finalidad de reducir la dependencia de una sola persona.	No cumple
Evaluar el requerimiento del personal de seguridad de la información para cumplir adecuadamente con los objetivos del negocio.	Cumple

Incluir la revisión de antecedentes en la contratación de personal, contratistas y proveedores que accedan a información crítica del negocio.	Cumple
Práctica clave de gobierno: Identificar personal clave de TI	
Minimizar la dependencia de una sola persona para funciones críticas mediante la documentación y entrenamiento de las funciones críticas.	No cumple
Probar regularmente los planes de respaldo del personal clave.	No cumple
Práctica clave de gobierno: Mantener las habilidades y competencias del personal	
Definir las habilidades y competencias necesarias del personal de seguridad de la información para asegurar el logro de los objetivos de la empresa.	Cumple
Proporcionar un plan formal para el desarrollo profesional de las competencias del personal de TI en temas de seguridad de la información.	Cumple
Revisar periódicamente el desarrollo de las habilidades y competencias del personal de TI en temas de seguridad de la información.	Cumple
Práctica clave de gobierno: Evaluar el rendimiento del personal	
Considerar los objetivos de seguridad de la información para establecer los objetivos individuales.	Cumple
Desarrollar planes de mejora del desempeño basados en los resultados del proceso de evaluación.	Cumple
Implementar un proceso de reconocimiento del cumplimiento de los objetivos de seguridad de la información.	Cumple
Práctica clave de gobierno: Planificar y ubicar el uso de los recursos humanos de TI y del negocio	
Entender la demanda actual y futura de los recursos humanos para el logro de los objetivos de seguridad de la información.	Cumple
Mantener información adecuada sobre el tiempo dedicado a los proyectos de seguridad de la información.	No cumple
Práctica clave de gobierno: Gestionar los contratos del personal	

Comunicar a los contratistas que la empresa se reserva el derecho de supervisar e inspeccionar todo el uso de los recursos de TI (correo, llamadas, programas y archivos).	Cumple
Establecer acuerdos de confidencialidad y de seguridad de la información dentro de los acuerdos formales con los contratistas.	Cumple
Implementar políticas y procedimientos para identificar las condiciones para que un trabajo pueda ser externalizado asegurando la seguridad de la información.	Cumple
Llevar a cabo revisiones periódicas de los derechos y accesos de los contratistas, los cuales tienen que estar alineados con sus funciones.	Cumple
Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades respecto a la seguridad de la información, adicionales a las de su trabajo.	No cumple

Tabla 6.6 Cumplimiento del 5to proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y ampliamente alcanzado, por lo que no cumple el objetivo definido. Se recomienda que se pueda ejecutar por lo menos 3 de las actividades no cumplidas, para alcanzar su objetivo.

- **Proceso habilitador: Gestionar los proveedores**

Práctica clave de gobierno: Identificar y evaluar las relaciones y contratos con proveedores.	
Establecer criterios de seguridad de la información en la evaluación de los proveedores y contratos según el tipo de proveedor, relevancia y criticidad del servicio. En el caso que el proveedor tenga acceso a información de la empresa, deberá de cumplir con la Ley de protección de datos personales.	Cumple
Establecer criterios para la evaluación del rendimiento del servicio o producto ofrecido por el proveedor según el contrato establecido.	Cumple
Evaluar y comparar periódicamente el rendimiento de los proveedores actuales con proveedores alternativos para identificar oportunidades de mejoras con los proveedores actuales.	No cumple

Identificar, registrar y categorizar a los proveedores y contratos según los criterios definidos para mantener un registro de los proveedores que se van a gestionar.	Cumple
Práctica clave de gobierno: Seleccionar proveedores	
Evaluar y mantener evidencia de la evaluación de los RFP según los criterios y proceso establecido.	No cumple
Revisar que los RFP detallan los requisitos de seguridad de la información claramente definidos.	No cumple
Seleccionar al proveedor que mejor cumpla el RFP y documentar la decisión tomada, así como el contrato firmado.	No cumple
Práctica clave de gobierno: Gestionar contratos y relaciones con proveedores	
Acordar, gestionar, mantener y renovar los contratos con los proveedores conforme con los estándares legales y regulatorios de la empresa.	Cumple
Asignar propietarios por cada proveedor que van a ser responsables supervisar el servicio ofrecido.	Cumple
Definir, comunicar y acordar las formas para implementar los requerimientos de mejora de seguridad de la información.	Cumple
Especificar un procedimiento formal para comunicarse con los proveedores en caso de falla de los servicios.	Cumple
Establecer procedimientos para tratar los conflictos contractuales.	No cumple
Para los proveedores claves, incluir dentro de las cláusulas del contrato revisión de las instalaciones, Prácticas internas y controles de gestión de seguridad de la información de los proveedores.	Cumple
Práctica clave de gobierno: Gestionar el riesgo del proveedor	
Identificar, monitorear y gestionar los riesgos de seguridad de la información en la entrega del servicio.	Cumple
Práctica clave de gobierno: Supervisar el cumplimiento y el rendimiento del proveedor.	
Definir los criterios para supervisar el rendimiento de los proveedores en relación a los niveles de servicios establecidos (SLA).	Cumple

En caso de proveedores críticos solicitar en caso sea necesario revisiones independientes de las prácticas y controles de seguridad de la información, las cuales deben de estar definidas en el contrato.	Cumple
Registrar y evaluar los resultados de las revisiones periódicas para identificar las necesidades y oportunidades de mejora con el proveedor.	Cumple
Supervisar y revisar la entrega de los servicios según los requisitos y condiciones de seguridad de la información establecidos en el contrato.	Cumple

Tabla 6.7 Cumplimiento del 6to proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y ampliamente alcanzado, por lo que no cumple el objetivo definido. Se recomienda que se pueda ejecutar por lo menos 3 de las actividades no cumplidas, para alcanzar su objetivo.

- **Proceso habilitador: Gestionar el riesgo**

Práctica clave de gobierno: Recopilar datos	
Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los riesgos y la forma en la cual estas condiciones afectaban la frecuencia del evento y la magnitud de perdida.	No cumple
Ejecutar periódicamente el análisis de eventos y factores de riesgos para identificar nuevos riesgos.	No cumple
Establecer un método para la colección, clasificación y análisis de datos de los riesgos de seguridad de la información, considerando múltiples tipos de eventos, categorías, riesgos y factores de riesgos.	Cumple
Medir y analizar los datos históricos de riesgos de seguridad de la información ocurridas en la empresa o a empresas del rubro de administración de fondo de pensiones.	Cumple
Registrar datos de eventos de riesgos que han causado o pueden causar impactos a la entrega de servicios de TI.	Cumple
Práctica clave de gobierno: Analizar el riesgo	

Analizar el costo beneficio de los tipos de tratamiento de riesgos para dar una respuesta optima a los riesgos.	Cumple
Comparar el riesgo residual con el apetito de riesgo de la empresa e identificar planes de acción para los riesgos que superen el apetito de riesgos.	Cumple
Construir los escenarios para el análisis de riesgos de seguridad de la información.	No cumple
Definir el alcance y el nivel de detalle para realizar el análisis de riesgos.	Cumple
Validar los resultados del análisis de riesgos con los requerimientos de la empresa antes de la toma de decisiones.	Cumple
Práctica clave de gobierno: Mantener un perfil de riesgo	
Capturar información sobre eventos de riesgos de seguridad de la información, para incluirlo en el perfil de riesgo de la empresa.	Cumple
Contar con un inventario de los procesos de negocio incluyendo al personal, aplicaciones, infraestructura, instalaciones, documentos críticos y proveedores involucrados.	Cumple
Determinar el perfil de riesgos de la empresa.	Cumple
Determinar los servicios e infraestructura esenciales de TI para sostener la operación de los procesos de la empresa.	Cumple
Práctica clave de gobierno: Articular el riesgo	
Informar el perfil de riesgo a los stakeholders.	Cumple
Informar los resultados del análisis de riesgos de seguridad de la información a todos los stakeholders en términos y formatos útiles para la toma de decisiones.	Cumple
Práctica clave de gobierno: Definir un portafolio de acciones para la gestión de riesgos.	
Definir un conjunto de proyectos para reducir los riesgos de mayor impacto, basando en el costo/beneficio.	Cumple
Determinar si cada área de la empresa supervisa el riesgo y acepta la responsabilidad de operar dentro del nivel de tolerancia del riesgo.	Cumple
Mantener un inventario de las actividades de control relacionadas a la gestión del riesgo de seguridad de la información.	Cumple

Práctica clave de gobierno: Responder al riesgo	
Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurra un riesgo.	Cumple
Preparar, mantener y probar los planes que deben de especificar los pasos específicos a seguir en caso se materialice un riesgo de seguridad de la información.	Cumple

Tabla 6.8 Cumplimiento del 7mo proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y completamente alcanzado, por lo que se cumple el objetivo definido.

- **Proceso habilitador: Gestionar la seguridad**

Práctica clave de gobierno: Establecer y mantener un SGSI	
Comunicar la propuesta del SGSI al directorio.	Cumple
Definir el alcance y los límites del SGSI según las características de la empresa.	Cumple
Definir el SGSI acorde a las políticas de la empresa.	Cumple
Definir y comunicar los roles y responsabilidad del SGSI.	Cumple
Obtener autorización del directorio para implementar el SGSI.	Cumple
Realizar una declaración de aplicabilidad que describa el alcance del SGSI.	No cumple
Práctica clave de gobierno: Definir y gestionar un plan de tratamiento de los riesgos de seguridad de la información	
Desarrollar una propuesta para implementar el plan de tratamiento de riesgos de seguridad de la información en un caso de negocio.	No cumple
Desarrollar y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos.	Cumple
Mantener un inventario de los componentes que están relacionados con la gestión de la seguridad de la información.	Cumple
Recomendar programas de formación y concientización en seguridad de la información.	Cumple
Práctica clave de gobierno: Monitorear y revisar el SGSI	

Proporcionar información para el plan mantenimiento de los planes de seguridad de la información.	Cumple
Realizar auditorías internas del SGSI.	Cumple
Realizar revisiones periódicas del SGSI por la alta dirección para asegurar que el alcance siga siendo el adecuado.	Cumple
Realizar revisiones periódicas del SGSI, incluyendo sus políticas, objetivos y prácticas de seguridad.	Cumple

Tabla 6.9 Cumplimiento del 8vo proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 3) y completamente alcanzado, por lo que superó el objetivo definido.

- **Proceso habilitador: Gestionar los cambios**

Práctica clave de gobierno: Evaluar, priorizar y autorizar peticiones de cambio	
El dueño del activo debe de aprobar formalmente cada cambio según la evaluación de riesgos realizada.	No cumple
Evaluar el riesgo de implementar las peticiones de cambio y considerar las implicaciones de seguridad, legales y de cumplimiento normativo.	No cumple
Las peticiones de cambio deben de ser categorizadas y relacionados con los elementos de configuración que son afectados.	Cumple
Las peticiones de cambios a los activos de TI deben de cumplir los controles de seguridad y deben de ser aprobados por los dueños de las aplicaciones.	Cumple
Planificar y programar todos los cambios aprobados.	Cumple
Práctica clave de gobierno: Gestionar los cambios emergentes	
Asegurar que hay un procedimiento para evaluar y autorizar los cambios de emergencia.	Cumple
Supervisar que todos los cambios de emergencias son revisados después de su implementación.	Cumple

Verificar que los accesos para los cambios de emergencia están apropiadamente autorizados, documentos y son revocados después de realizar los cambios.	No cumple
Práctica clave de gobierno: Ubicar y reportar el cambio de estado	
Categorizar las peticiones de cambio en el proceso de seguimiento del cambio.	Cumple
Mantener un sistema de seguimiento y de reporte para todos los cambios solicitados.	Cumple
Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados dentro de los plazos establecidos y su prioridad, evitando accesos no autorizados.	Cumple
Práctica clave de gobierno: Cerrar y documentar los cambios	
Definir un periodo apropiado para conservar la documentación asociado a la gestión del cambio.	Cumple
Documentar los cambios como parte integral de la gestión del cambio.	Cumple

Tabla 6.10 Cumplimiento del 9no proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y ampliamente alcanzado, por lo que no cumple el objetivo definido. Se recomienda que se ejecutar por lo menos 1 de las actividades no cumplidas, para alcanzar su objetivo.

- **Proceso habilitador: Gestionar los activos**

Práctica clave de gobierno: Identificar y registrar los activos actuales	
Determinar regularmente si cada activo de información sigue proporcionando valor para su objetivo.	Cumple
Identificar los requisitos de seguridad de la información y legales que deben de ser cumplidos en la gestión de los activos.	Cumple
Registrar todos los activos de información y mantener su alineación con la gestión de cambios y de la configuración.	Cumple

Verificar que todos los activos de información cuentan con un propietario asignado.	Cumple
Práctica clave de gobierno: Gestionar los activos críticos	
Establecer un plan de mantenimiento preventivo para los activos críticos de información.	Cumple
Identificar que los activos críticos para proveer los servicios cumplen con los requerimientos de negocios y de seguridad de la información.	Cumple
Regularmente considerar la necesidad del reemplazo de los activos críticos de información debido al riesgo de falla operativa.	No cumple
Supervisar el rendimiento de los activos críticos y el cumplimiento de los controles de seguridad de información.	Cumple
Práctica clave de gobierno: Gestionar el ciclo de vida de los activos	
Asignar los activos a los usuarios los cuales firmarán la aceptación de sus responsabilidades.	Cumple
Desplegar los activos considerando los controles de seguridad de información durante el ciclo de vida de implementación.	Cumple
Eliminar los activos de forma segura, teniendo en cuenta la eliminación permanente de los datos registrados en dispositivos.	Cumple
Práctica clave de gobierno: Optimizar el costo de los activos	
Evaluar los costes de mantenimiento de los equipos de seguridad, considerar si son razonables e identificar opciones de menor coste.	Cumple
Revisar la base general de activos de seguridad, teniendo en cuenta si está alineada con los requerimientos del negocio.	No cumple
Práctica clave de gobierno: Gestionar las licencias	
Comparar el número de copias de software instalado con el número de licencias compradas.	No cumple
Cuando la cantidad de copias usadas sea mayor a la cantidad de copias compradas, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas, y después si es necesario adquirir licencias adicionales para cumplir con los acuerdos de licencia.	No cumple

Cuando la cantidad de copias usadas sea menor a la cantidad de copias compradas, decidir si existe una necesidad de mantener o cancelar licencias adicionales.	No cumple
Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.	Cumple
Periódicamente llevar a cabo una auditoría para identificar que todas las copias de software instaladas cuenten licencia.	Cumple

Tabla 6.11 Cumplimiento del 10mo proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y ampliamente alcanzado, por lo que no cumple el objetivo definido. Se recomienda que se pueda ejecutar por lo menos 3 de las actividades no cumplidas, para alcanzar su objetivo.

- **Proceso habilitador: Gestionar peticiones e incidentes de servicio**

Práctica clave de gobierno: Definir esquemas de clasificación de incidentes y peticiones de servicio.	
Definir esquemas de clasificación y priorización para el registro y atención de los incidentes y peticiones de servicios de seguridad de la información.	Cumple
Definir fuentes de conocimiento para la atención de incidentes y peticiones de servicios de seguridad de la información.	Cumple
Definir procedimientos y reglas de estalación de los incidentes y peticiones de servicios de seguridad de la información según el nivel de impacto.	Cumple
Práctica clave de gobierno: Registrar, clasificar y priorizar peticiones e incidentes.	
Analizar y clasificar los incidentes y peticiones de servicios de seguridad de la información.	Cumple
Priorizar la atención de los incidentes y peticiones de servicios de seguridad de la información según los SLA definidos y el impacto en el negocio y la urgencia.	No cumple
Registrar toda la información relevante de todos los incidentes y peticiones de servicios de seguridad de la información, para atenderlos efectivamente y mantener un registro historio de estos.	Cumple
Práctica clave de gobierno: Verificar, aprobar y resolver peticiones de servicio	
Obtener la aprobación financiera y funcional firmada de las solicitudes.	Cumple
Verificar los derechos para hacer las peticiones de servicios de seguridad de la información según un proceso definido.	No cumple
Práctica clave de gobierno: Investigar, diagnosticar y localizar incidentes.	
Asignar un especialista para resolver el incidente en caso sea necesario.	Cumple
Identificar los síntomas relevantes para establecer las causas de los incidentes de seguridad de la información.	Cumple
Práctica clave de gobierno: Resolver y recuperarse ante incidentes.	

Documentar las soluciones de los incidentes de seguridad de la información para usarlas como fuente de conocimiento futuro.	Cumple
Ejecutar acciones de recuperación si se requieren.	Cumple
Registrar si se usaron soluciones temporales para resolver los incidentes de seguridad de la información.	Cumple
Seleccionar y aplicar las soluciones más apropiadas a los incidentes de seguridad de la información.	Cumple
Práctica clave de gobierno: Cerrar peticiones de servicio e incidentes	
Cerrar los incidentes y peticiones de servicios de seguridad de la información.	Cumple
Verificar con los usuarios afectados si el incidente o petición de servicios de seguridad de la información han sido resueltas satisfactoriamente.	Cumple
Práctica clave de gobierno: Seguir el estado y emitir de informes	
Analizar que las respuestas a los incidentes y peticiones de servicios de seguridad de la información estén dentro de los SLA establecidos, para identificar las brechas o ineficiencias y planificarlo en la mejora continua.	No cumple
Identificar la información para presentar a los stakeholders sobre la solución de los incidentes de seguridad de la información.	Cumple
Monitorear y hacer seguimiento del escalamiento de los incidentes que se siguieron para realizar la solución.	Cumple

Tabla 6.12 Cumplimiento del 11avo proceso habilitador de TI.

Resultado: Este proceso se encuentra establecido (nivel 3) y ampliamente alcanzado, por lo que superó el objetivo definido.

- **Proceso habilitador: Gestionar los servicios de seguridad**

Práctica clave de gobierno: Proteger contra software malicioso (malware)	
Capacitar periódicamente al personal sobre los malware en el uso del correo e internet y recordarles que no deben de instalar software no autorizados.	Cumple

Comunicar los procedimientos y responsables para la prevención contra software malicioso.	Cumple
Distribuir el software de protección de forma centralizada.	Cumple
Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, spyware y phishing).	Cumple
Instalar y activar herramientas de protección contra software malicioso en los lugares de procesamiento de información crítica.	Cumple
Revisar y evaluar regularmente la información sobre nuevas amenazas posibles.	Cumple
Gestionar la seguridad de la red y las conexiones.	
Aplicar protocolos de seguridad aprobados para las conexiones de red.	Cumple
Cifrar la información en tránsito de acuerdo a su clasificación.	Cumple
Configurar la seguridad en los equipos de red de forma correcta.	Cumple
Establecer mecanismos de confianza para dar soporte a la transmisión y recepción de la información de manera segura.	Cumple
Establecer una política de seguridad de las conexiones según los requerimientos del negocio.	Cumple
Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.	Cumple
Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa mediante el uso contraseña.	Cumple
Realizar pruebas de intrusión periódicas para determinar el nivel de protección de la red.	Cumple
Realizar pruebas de seguridad en los sistemas de manera periódica para determinar el nivel de protección de los sistemas.	Cumple
Práctica clave de gobierno: Gestionar la seguridad de los puestos de usuario final.	
Cifrar la información almacenada de acuerdo a su clasificación.	Cumple
Configurar la seguridad en los sistemas operativos de forma correcta.	Cumple
Deshacerse los dispositivos de usuario final de forma segura.	Cumple
Gestionar el acceso y control remoto.	Cumple

Gestionar la configuración de seguridad de la red.	Cumple
Implementar el filtrado del tráfico de la red en dispositivos de usuario final.	Cumple
Implementar mecanismos de bloqueo en los dispositivos de usuario final.	Cumple
Proteger la integridad de los sistemas.	Cumple
Proveer protección física a los dispositivos de usuario final.	Cumple
Práctica clave de gobierno: Gestionar la identidad del usuario y el acceso lógico	
Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto solo en transacciones aprobadas, documentadas y autorizadas por los dueños de los sistemas.	Cumple
Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI son identificables unívocamente.	Cumple
Autenticar todos los accesos a los activos de información basándose en la clasificación de seguridad y coordinar con gestión de accesos que los controles de autenticación han sido administrados adecuadamente.	Cumple
Identificar únicamente todas las actividades del proceso de la información por roles, coordinando con las unidades del negocio y asegurando que todos los roles están definidos consistentemente.	Cumple
Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de sus funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, la necesidad de tener y la necesidad de conocer.	Cumple
Mantener registros de auditoría de los accesos a la información clasificada como altamente sensible.	Cumple
Realizar regularmente revisiones de todas las cuentas y privilegios relacionados.	Cumple
Segregar y gestionar cuentas de usuario privilegiadas.	Cumple
Práctica clave de gobierno: Gestionar el acceso físico a los activos de TI	

Asegurar que los accesos a las ubicaciones de procesamiento de datos de TI deben darse en funciones de trabajo y responsabilidades.	Cumple
Escoltar a los visitantes en todo momento mientras esté en las instalaciones de la empresa. Si se encuentra a un individuo que no va acompañado o que no resulta familiar y que no lleva visible la tarjeta de identificación se deberá alertar al personal de seguridad.	No cumple
Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento.	Cumple
Instruir a todo el personal para que mantengan visible su tarjeta de identificación en todo momento.	Cumple
Realizar regularmente concienciación de la seguridad física.	No cumple
Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar a todos los visitantes incluyendo contratistas y proveedores.	Cumple
Restringir el acceso a ubicaciones sensibles de TI estableciendo restricciones en el perímetro, como dispositivos de seguridad en las puertas interiores y exteriores y asegurar que los dispositivos registren el ingreso y alerten en caso de un acceso no autorizado. .	Cumple
Práctica clave de gobierno: Gestionar documentos sensibles y dispositivos de salida.	
Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	Cumple
Destruir adecuadamente la información sensible (por ejemplo: trituradoras disponibles para destruir documentos confidenciales) y los dispositivos de salida (por ejemplo: desmagnetizando los dispositivos magnéticos, destruyendo físicamente dispositivos de memoria).	Cumple
Establecer procedimientos para gestionar la recepción, uso, eliminación y destrucción de documentos sensibles y dispositivos de salida dentro y fuera de la empresa.	No cumple
Establecer un inventario de documentos sensibles y dispositivos de salida para realizar regularmente verificaciones.	Cumple

Establecer una seguridad física apropiada sobre información sensible y dispositivos sensibles.	Cumple
Práctica clave de gobierno: Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	
Asegurar que los tickets de incidentes de seguridad se crean en el momento oportuno.	Cumple
Definir y comunicar las características de los potenciales incidentes relacionados con la seguridad de forma que sean fácilmente reconocibles y comprender el impacto para permitir una respuesta adecuada.	Cumple
Registrar los eventos relacionados con la seguridad reportada por las herramientas de monitorización de seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo.	Cumple
Revisar regularmente los registros de los eventos para detectar potenciales incidentes de seguridad.	Cumple

Tabla 6.13 Cumplimiento del 12avo proceso habilitador de TI.

Resultado: Este proceso se encuentra establecido (nivel 3) y completamente alcanzado, por lo que superó con el objetivo definido.

- **Proceso habilitador: Supervisar, evaluar y medir el rendimiento y la conformidad**

Práctica clave de gobierno: Establecer un enfoque de la supervisión	
Acordar los objetivos y métricas de seguridad de la información.	Cumple
Acordar un proceso de control y de presentación de informes sobre la seguridad de la información.	Cumple
Identificar las stakeholders que van a monitorear la seguridad de la información.	Cumple
Identificar periódicamente los nuevos stakeholders, requisitos y recursos para la seguridad de la información.	Cumple

Involucrar a los stakeholders y comunicar los objetivos y requisitos de seguridad de la información.	Cumple
Mantener y alinear de forma continua el enfoque de supervisión y evaluación de la seguridad de la información con el enfoque de la compañía.	Cumple
Solicitar, priorizar y reservar recursos para la supervisión de la seguridad de la información.	Cumple
Práctica clave de gobierno: Establecer los objetivos de cumplimiento y rendimiento	
Comunicar los cambios propuestos para el rendimiento y cumplimiento de las metas de seguridad de la información.	Cumple
Definir y revisar periódicamente los objetivos y métricas para la seguridad de la información con los stakeholders para identificar cualquier detalle significativo omitido y definir metas razonables.	Cumple
Evaluar si los objetivos y métricas son adecuados, es decir sean específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).	Cumple
Práctica clave de gobierno: Recopilar y procesar los datos de cumplimiento y rendimiento.	
Consolidar los datos para soportar el cálculo de las métricas acordadas.	Cumple
Recopilar los datos para la gestión de la seguridad de la información (de forma automatizada cuando sea posible).	Cumple
Utilizar herramientas y sistemas apropiados para el procesamiento de los datos a analizar.	No cumple
Práctica clave de gobierno: Analizar e informar sobre el rendimiento	
Diseñar informes de rendimiento de los controles de seguridad de la información que sean fáciles de entender y ajustados a las diferentes necesidades de gestión y audiencias para facilitar la toma efectiva y oportuna de decisiones.	Cumple
Distribuir los informes de seguridad de la información a los stakeholders involucrados.	Cumple
Recomendar cambios a los objetivos y métricas definidos, cuando sea apropiado.	Cumple

Práctica clave de gobierno: Asegurar la implantación de medidas correctivas.	
Asegurar que se mantiene la asignación de responsabilidades para las acciones correctivas.	Cumple
Hacer seguimiento de los resultados de las acciones comprometidas.	Cumple
Informar los resultados a los stakeholders.	Cumple
Revisar las respuestas, opciones y recomendaciones de la alta dirección con referencia a las medidas de seguridad de la información.	Cumple

Tabla 6.14 Cumplimiento del 13avo proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y completamente alcanzado, por lo que alcanzó el objetivo definido.

- **Proceso habilitador: Supervisar, evaluar y medir la conformidad con los requerimientos externos**

Práctica clave de gobierno: Identificar requisitos externos de cumplimiento.	
Asignar las responsabilidad de identificar y supervisar los cambios en la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.	Cumple
Identificar los requerimientos de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales sobre las actividades de TI.	Cumple
Mantener un inventario de los requisitos legales y regulatorios de la empresa.	Cumple
Práctica clave de gobierno: Optimizar la respuesta a requisitos externos.	
Revisar con regularidad la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales para asegurar el cumplimiento requerido.	Cumple
Comunicar los requisitos de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales al personal involucrado.	Cumple

Práctica clave de gobierno: Confirmar el cumplimiento de requisitos externos	
Evaluar periódicamente los procesos y actividades de TI y del negocio para asegurar el cumplimiento de circular N° G-140-2009 - "Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.	Cumple
Práctica clave de gobierno: Obtener garantía del cumplimiento de requisitos externos.	
Si es necesario, obtener declaraciones de los proveedores de servicio TI externos acerca de su nivel de cumplimiento de la ley de protección de datos personales.	Cumple
Obtener confirmación regularmente del cumplimiento de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales por parte de los gerentes responsables de su cumplimiento.	Cumple
Realizar revisiones regulares internas para evaluar los niveles de cumplimiento de la circular N° G-140-2009 -"Gestión de la seguridad de la información" y la ley N° 29733 de protección de datos personales.	Cumple

Tabla 6.15 Cumplimiento del 14avo proceso habilitador de TI.

Resultado: Este proceso se encuentra gestionado (nivel 2) y completamente alcanzado, por lo que alcanzó el objetivo definido.