

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.