Definición del Marco de Seguridad y Privacidad de la Información

Diagnóstico de Seguridad y Privacidad **Busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información.** **Objetivo: La entidad cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos existentes.** **Recursos: Modelo de Seguridad y Privacidad de la Información y NTC-ISO-IEC 27001:2013.**	
Lineamiento	**Aplicabilidad**
LI.ES.01 Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales -cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.	La aplicabilidad de este lineamiento no se observó al no poder identificar el documento Plan Estratégico de las Tecnologías de la Información (PETI).
LI.ES.02 Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.	No se observó si actualmente la Universidad ha implementado acciones propias de la arquitectura empresarial.
LI.GO.01 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.	No se observó si actualmente la Universidad cuenta con un esquema completo de Gobierno de TI. Sin embargo, se observó que existe una política de gestión y un Plan de Desarrollo Institucional en el cual se apoyan algunas decisiones de TI en relación a la seguridad y privacidad.
LI.GO.04 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macroproceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI.	No se observó si actualmente la Universidad ha implementado acciones propias del macroproceso de Gestión de TI con base en los lineamientos del MinTIC.
LI.ST.14 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.	En el macroproceso de gestión de TIC, no se observó si se han implementado acciones propias con respecto al análisis de vulnerabilidades de la infraestructura tecnológica. Se tiene análisis de Firewall a través de la consola de Sonic Wall.

Tabla 1. Diagnóstico de Seguridad y Privacidad

Plan de Seguridad y Privacidad de la Información **Busca generar un plan de seguridad y privacidad alineado con el propósito misional.** **Objetivo: La entidad define las acciones a implementar a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.** **Recursos: Modelo de Seguridad y Privacidad de la Información, Guías del modelo de seguridad y privacidad de la información y NTC-ISO-IEC 27001:2013**	
Lineamiento	**Aplicabilidad**
LI.ES.02 Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución	Se observó que actualmente la entidad no ha implementado acciones propias de la arquitectura empresarial.
LI.ES.06 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI.	Se observó que actualmente la entidad no cuenta con un esquema completo de Gobierno de TI. Sin embargo, se observó que se han desarrollado actividades relacionadas con la seguridad de la información, planes de contingencia y continuidad del negocio, y acceso a la información pública por parte de los diferentes usuarios.
LI.ES.08 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI. Así mismo, debe asegurar la conformidad del proyecto con los lineamientos de la AE definidos para la institución.	No se observó que el macroproceso de gestión de TIC participe activamente en la creación y actualización del proyecto de fortalecimiento de Seguridad de TI determinado en el Plan de Desarrollo Institucional de la Universidad del Quindío a 2020.
LI.GO.01 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.	No se observó si actualmente la entidad cuenta con un esquema completo de Gobierno de TI. Sin embargo, se observó que existe una política de gestión y un Plan de Desarrollo Institucional en el cual se apoyan algunas decisiones de TI en relación a la seguridad y privacidad.
LI.GO.04 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macroproceso de gestión de TI, según los lineamientos del	Se observó que actualmente la entidad no ha implementado acciones propias del macroproceso de Gestión de TI con base en los lineamientos del MinTIC.

Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI.	
LI.GO.09 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas. La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá liderar el trabajo sobre el componente de TI conforme con los lineamientos de la AE institucional.	No se observó que el macroproceso de gestión de TIC participe activamente en la creación y actualización del proyecto de fortalecimiento de Seguridad de TI determinado en el Plan de Desarrollo Institucional de la Universidad del Quindío a 2020.
LI.SIS.22 En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.	Se observó que el macroproceso de gestión de TIC adelanta labores que propenden por la privacidad de la información a través de controles como: control de acceso, gestión de cuentas de usuario, registro de incidentes y la Política de Usuarios y Contraseñas.

Implementación del Plan de Seguridad

Gestión de Riesgos de Seguridad y Privacidad de la Información **Busca proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.** **Objetivo: La entidad implementa el plan de seguridad y privacidad de la información, clasifica y gestiona controles.** **Recursos: Modelo de Seguridad y Privacidad de la Información, Guías del modelo de seguridad y privacidad de la información y NTC-ISO-IEC 27001:2013.**	
Lineamiento	**Aplicabilidad**
LI.INF.15 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los Componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dicho Componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.	Se observó que el macroproceso de gestión de TIC esta implementado un repositorio de datos. Sin embargo, el acceso y uso de esta herramienta no está disponible aún para toda la entidad al momento del Diagnóstico.
LI.SIS.22 En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.	Se observó que actualmente se cuenta con una Política de Seguridad Informática que implementa mecanismos de control de acceso.

Tabla 2. Gestión de Riesgos de Seguridad y Privacidad de la Información

Monitoreo y Mejoramiento Continuo

Evaluación del Desempeño
Busca hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información.

Objetivo 1: La entidad cuenta con actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad con el fin de generar los ajustes o cambios pertinentes y oportunos.

Objetivo 2: La entidad revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la Información.

Recursos: Modelo de Seguridad y Privacidad de la Información, Guías del modelo de seguridad y privacidad de la información y NTC-ISO-IEC 27001:2013.

Lineamiento	Aplicabilidad
LI.ES.13 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un tablero de indicadores sectorial y por institución, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI.	Se observó que el macroproceso de gestión de TIC no cuenta con el monitoreo mencionado.
LI.GO.03 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir y realizar actividades que conduzcan a evaluar, monitorear y direccionar los resultados de las soluciones de TI para apoyar los procesos internos de la institución. Debe además tener un plan específico de atención a aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo de gestión, a fin de cumplir con el compromiso de mejoramiento continuo de la administración pública de la institución.	Se observó que el macroproceso de gestión de TIC no administra indicadores que monitorean, evalúan y direccionan las soluciones de TI implementadas en el área. Adicionalmente, se observó que se han elaborado planes de mejoramiento producto de las auditorías internas de gestión.
LI.GO.12 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macro-proceso de Gestión TI.	Aunque se observó que en el macroproceso de gestión de TIC se aplican indicadores de gestión de TI. Se hacen desde la gestión de Calidad.
LI.GO.13 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar áreas con oportunidad de mejora, de acuerdo con los criterios de calidad establecidos en el Modelo Integrado de Planeación y Gestión de la institución, de modo que pueda focalizar esfuerzos en el mejoramiento de los procesos de TI para contribuir con el cumplimiento de las metas institucionales y del sector.	No se observó que el macroproceso de gestión de TIC anualmente solicite a las diferentes áreas las necesidades en materia de tecnología para elaborar el Plan Anual de Adquisiciones.