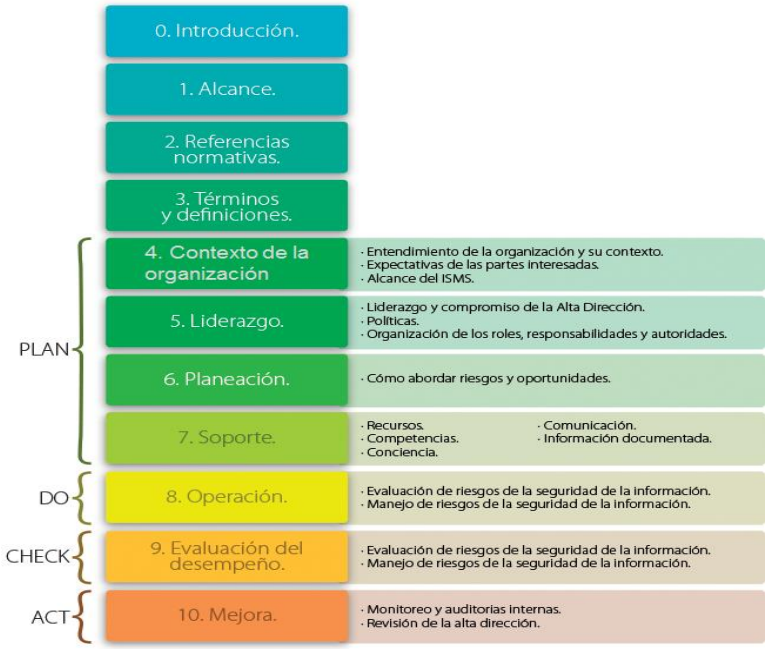
RESUMEN "IMPORTANCIA DEL USO DE BASES DE DATOS Y SEGURIDAD DE LA INFORMACIÓN PARA FORTALECIMIENTO TICS EN EL EJERCICIO DEL CONTROL FISCAL"

El tema técnico "La importancia del uso de base de datos y de la seguridad de la información para el fortalecimiento de las TIC y para el ejercicio eficiente del control" fue desarrollado abordando el tema de seguridad desde la perspectiva de la estructura estándar de la Norma ISO 27001:2013 que ayudó a tener una visión general del estado actual en que se encuentran las EFS, frente al reto de emplear las TIC´s para fortalecer el ejercicio del control fiscal, dado que ésta proporciona un marco para la creación del Sistema de Gestión de la Seguridad de la Información - SGSI[1] que involucra un conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar este Sistema, de tal manera que se cumpla con el objetivo de proporcionar seguridad.

De otra parte, también se abordó la revisión de los Objetivos de Control de seguridad, del mismo estándar que hicieron posible reconocer las principales herramientas con que cuentan las EFS para garantizar la seguridad de la información que procesan y gestionan para su posterior liberación; también para evidenciar las buenas prácticas aplicadas en aspectos de seguridad informática, reconocer los mecanismos de seguridad empleados en el intercambio de información, identificar los riesgos, comprobar la existencia o proceso de conformación de equipos de respuesta a incidentes de seguridad informática, la implementación del SGSI.

Estructura del estándar ISO/IEC 27001:2013



[1] ISMS Information Security Management System o Sistema de Gestión de Seguridad de la Información-SGSI por sus siglas en español

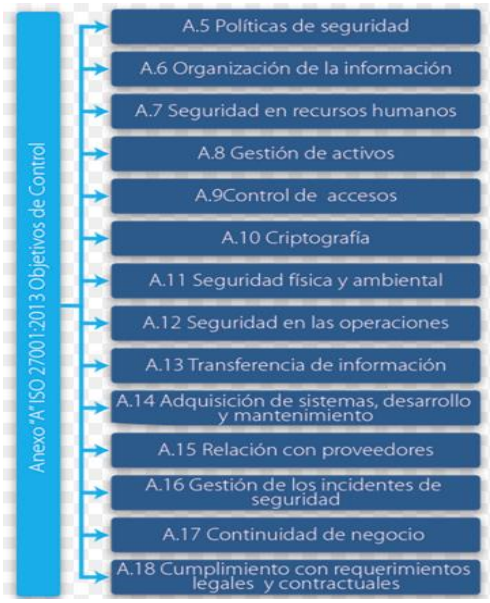


Figura 2. Dominios de ISO 27001:2013

Es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información y prevenir aún más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades humanas; dado que la información se ha reconocido como un activo valioso apoyado por sistemas de información empleados en procesos de misión crítica, misional, de gestión y/o administrativa, por tanto se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Es por ello que con base en el estándar ISO/IEC 27001:2013 se realizó un sondeo del estado en que las EFS se encuentran en relación con los dominios A.8 Gestión de incidentes, A.9 Control de accesos, A.10 Criptografía, A.12 Seguridad de la información, A.13 Transferencia de Información, A.16 Gestión de Incidentes, A.17 Continuidad del negocio; entre otros, en los temas de metodologías para gestión de incidentes, plan de respuesta a incidentes, análisis de vulnerabilidades, procesos para gestión de incidentes, auditoria interna o externa a los procesos de gestión de incidentes y aplicación buenas prácticas

La encuesta también incluyó los temas de Seguridad de la información con terceros, cumplimiento de normas o estándares, organización de la seguridad en las EFS, donde se pretendió evidenciar la existencia de acuerdos de privacidad NDA (Non Disclosure Agreement, por sus siglas en inglés) y de niveles de servicio – SLA (Service Level Agreement) temas incluidos en los Dominios A.7 Seguridad en Recursos Humanos; A.5 Política de Seguridad, A.6 Organización de la Información y A.18 Cumplimiento con requerimientos legales y contractuales. Todo ello dio la posibilidad de visualizar el interés que tienen las EFS por establecer y aplicar mecanismos de seguridad informática y propender por ofrecer niveles de servicio sin correr riegos.