Normatividad corporativa de seguridad de la información

Desarrollo e implementación de soluciones para la transformación digital

Servicio Nacional de Aprendizaje - SENA

Normatividad corporativa de seguridad de la información

Las empresas y las organizaciones, en lo relativo a la seguridad de la información, están llamadas a atender y cumplir formalmente con requerimientos, normas, estándares, y, como es lógico, han de estar alertas a mitigar o atender los riesgos a los que se ven enfrentadas permanentemente.

Las normas y estándares que han ido surgiendo, con el fin de fortalecer el cumplimiento y la atención a dichas necesidades, se enunciarán y describirán de manera general, a continuación.

1. Cobit 5

Cobit, de sus siglas en inglés Control *Objectives for Information and related Technology* (Objetivos de control para la información y tecnologías relacionadas), contempla un conjunto de herramientas enfocadas en garantizar el control y el seguimiento del gobierno de tecnologías de la información **T.I.**, a partir de las buenas prácticas y mediante un seguimiento y unas auditorías permanentes.

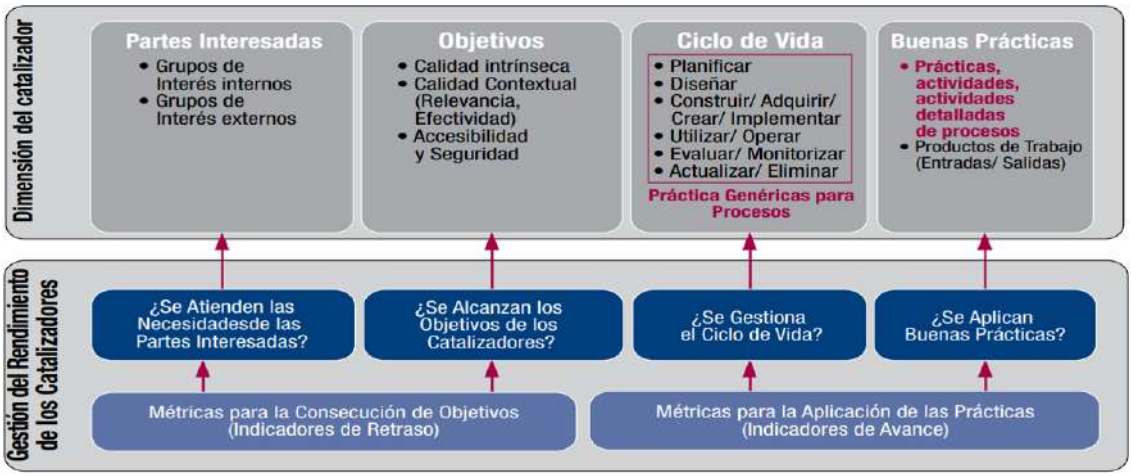
Los Cobit se fundamentan bajo 5 principios, como se puede observar en la Figura 1, los cuales buscan:

Figura 1. Principios de COBIT 5

Nota. Recuperada de COBIT 5: el nuevo marco para la Gobernanza de las TIC - Netmind

Estos principios buscan apalancarse a partir de los 7 catalizadores, como se muestra en la Figura 2, con los cuales se busca que las organizaciones definan y gestionen sus interacciones, facilitando así la integración.

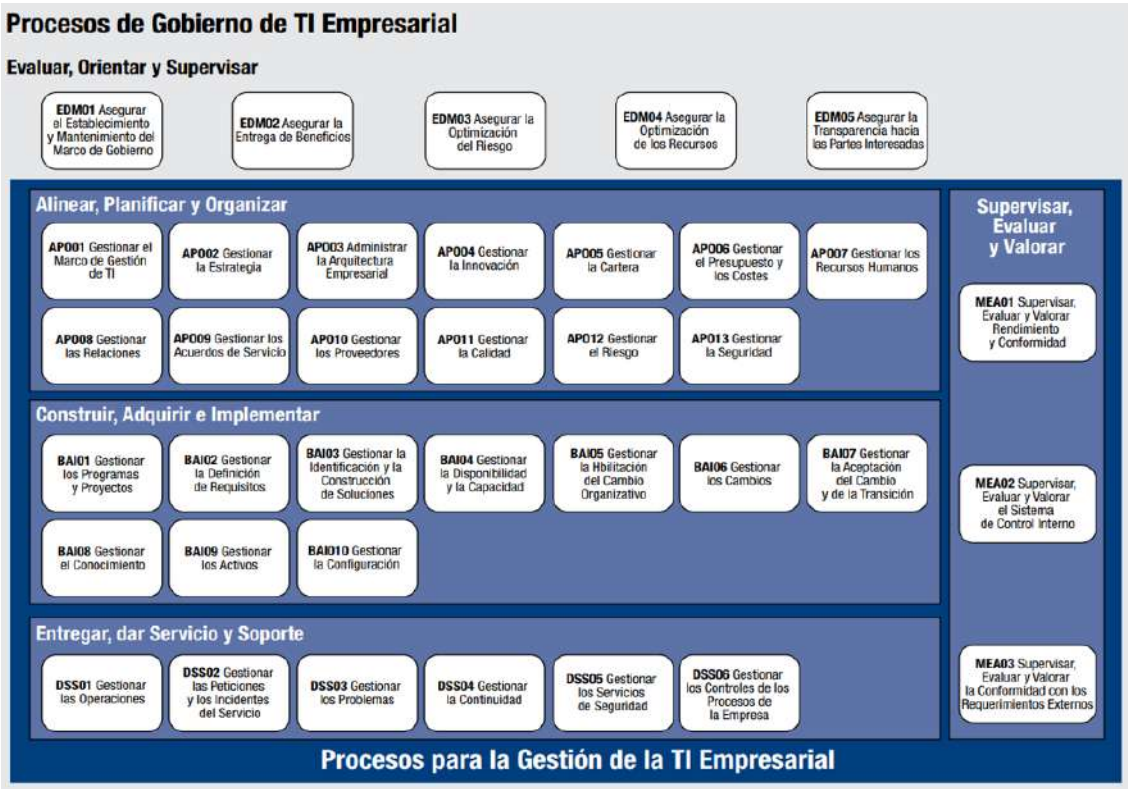
Figura 2. Catalizadores de Cobit 5



Nota. Recuperada de COBIT 5: el nuevo marco para la Gobernanza de las TIC - Netmind

Además, los **Cobit 5** proponen un modelo de objetivos en cascada, con lo cual se busca la integración TI-Negocio, como se muestra en la Figura 3, donde se plantea el modelo de gestión de procesos:

Figura 3. Modelo de procesos de Gobierno de las TI de Cobit 5



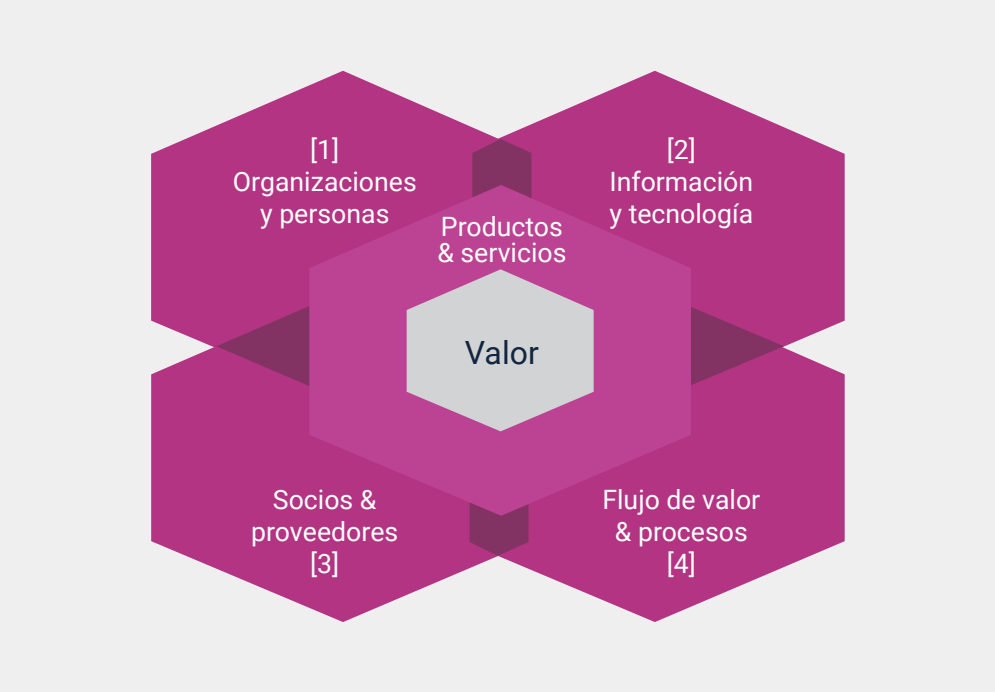
Nota. Recuperada de COBIT 5: el nuevo marco para la Gobernanza de las TIC - Netmind

2. ITIL v4

ITIL, de sus siglas en inglés Information *Technology Infrastructure Library* (Biblioteca de Infraestructura de Tecnologías de la Información), esta biblioteca incorpora un marco de buenas prácticas para la gestión de los servicios y la tecnología, y se enfoca en mejorar los servicios de T.I.

Esta librería está basada en 4 dimensiones, con las cuales se busca respaldar de manera holística la gestión de los servicios, como se puede apreciar en la Figura 4.

Figura 4. Dimensiones de ITIL v4

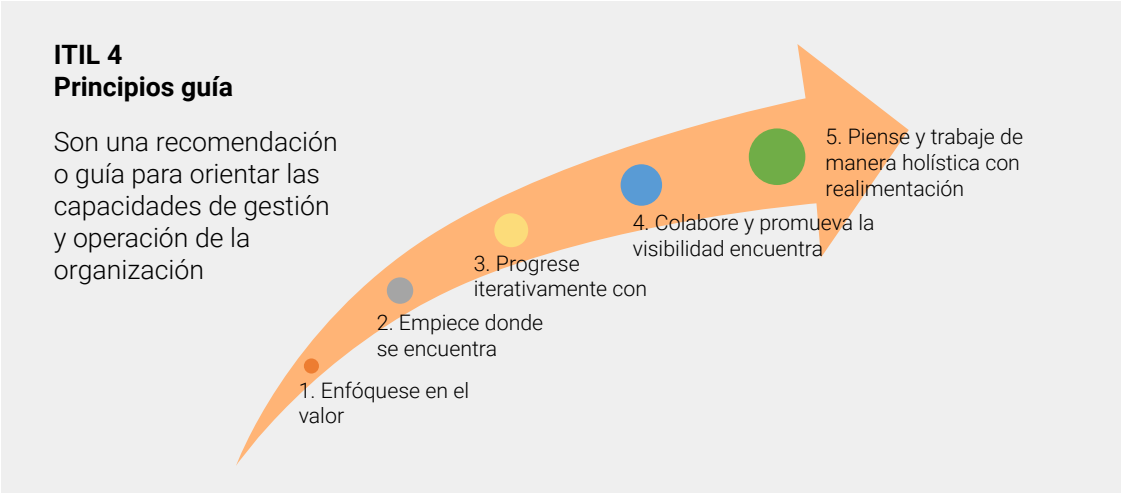


Nota. Recuperada de La Gestión de Servicios e ITIL4 - Opcion Tecnologica

- **1. Organización y personas:** En la cual se orienta sobre la adopción de una cultura saludable, que respalde los objetivos desde las capacidades de talento humano, por lo que sugiere:
  - Adoptar de guías de ITIL v4.
  - Velar porque el talento humano relacionado con el servicio se alinee con la cultura y objetivos de la organización.
- **2. Información y tecnología:** Nos orienta sobre la importancia de gestionar el conocimiento a lo largo del tiempo, para lo cual no direcciona a la gestión de las tecnologías como apoyo.
- **3. Socios & proveedores:** Sugiere que los socios y los proveedores estén alineados con la visión, la cultura y los objetivos de la organización.
- **4. Flujos de valores & procesos:** Define los flujos de valor y los procesos para alcanzar los objetivos.

ITIL v4 se basa en 5 principios con los cuales se busca orientar las capacidades de gestión y operación de la organización, como se puede apreciar en la Figura 5.

Figura 5. Principios de ITIL v4

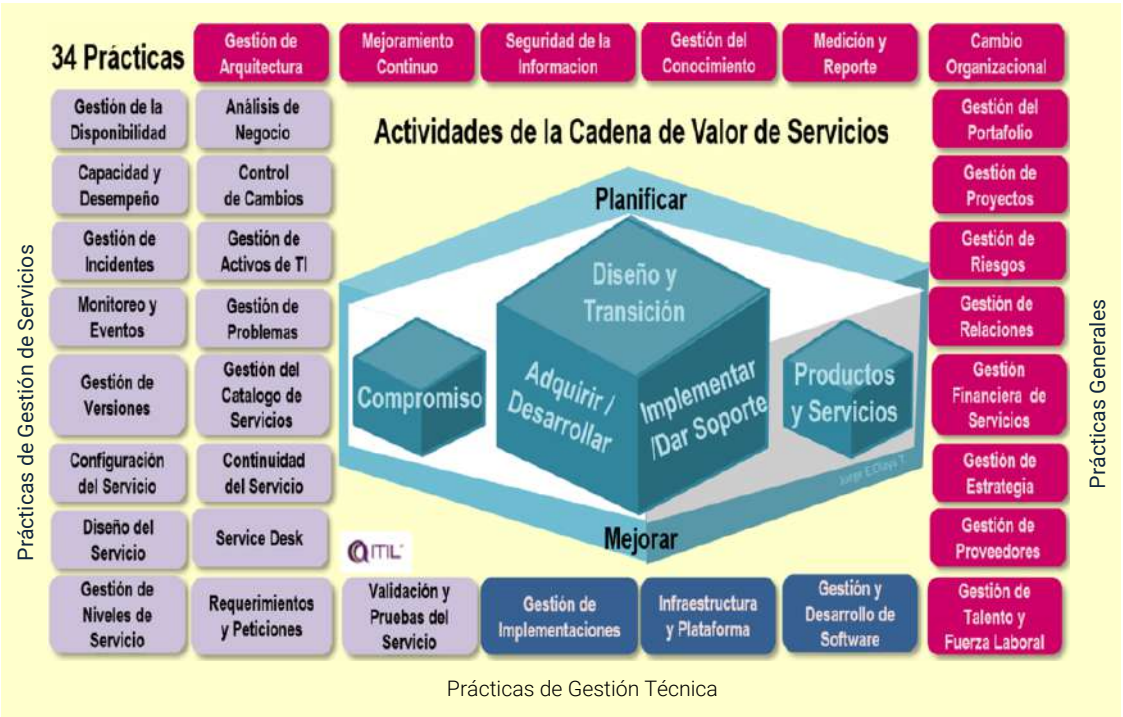


Nota. Recuperada de PRINCIPIOS ITIL4 – BPGurus

Además, cuenta con 34 prácticas, como se puede apreciar en la Figura 6, divididas en los 3 siguientes grupos:

- 14 prácticas generales de gestión.
- 17 prácticas de gestión de servicios.
- 3 prácticas de gestión técnica.

Figura 6. Prácticas de ITIL v4



Nota. Recuperada de La PUCE-SI desarrolló evento virtual "ITIL 4, la siguiente evolución en la gestión de servicios TI" (pucesi.edu.ec)

3. ISO/IEC 20000 - Gestión de Servicios TI

Esta norma establece la implementación y estructura de los servicios de T.I. en una organización de manera fiable, velando porque estos servicios cumplan con las mejores prácticas.

El objetivo principal de esta norma es ofrecer a las empresas una certificación que garantice la implementación y adopción de buenas prácticas en la implementación de sus sistemas de información.

La norma ISO 2000 está compuesta por 8 bloques, pero son más conocidos como parte 1 y parte 2.

Parte 1 - ISO 20000-1:2011
Propone el conjunto de especificaciones para la gestión eficiente del suministro de servicios de tecnologías de la información. Aquí se definen los requerimientos para ofrecer los servicios T.I. con una calidad aceptable, el diseño y transición de los servicios y los siguientes procesos:

- **Procesos de servicios:** Todos aquellos procesos que tienen que ver con la entrega del servicio, como disponibilidad, capacidad, seguridad de la información y otros procesos de gestión de servicios.
- **Procesos de relaciones:** Aquellos procesos relativos a las relaciones y comunicaciones, tanto con el negocio como con los suministradores.
- **Procesos de resolución:** Aquellos procesos de resolución de problemas, incidencias y petición de servicio.
- **Procesos de control:** Todos los procesos relacionados con la configuración, cambios y entrega y despliegue de los servicios.

Figura 7. Organización de un sistema de gestión de servicios TI

Nota. Recuperada de ISO 20000 - Calidad de los servicios TI ISO / IEC 20000 (normas-iso.com)

Parte 2 - ISO 20000-2:2012

Contiene la serie de buenas prácticas que son aceptadas por la industria en cuanto a la gestión de servicios TI. Es fundamental para la aplicación de gestión del servicio y es utilizado para preparar a una empresa para obtener la certificación.

En la Figura siguiente, es posible apreciar la estructura de la norma ISO 20000-2:2012

Figura 8. Estructura de la norma ISO/IEC 20000

Nota. Recuperada de Iso20000-1:2012 - Gestión y Proyectos (gestionyproyectos.co)

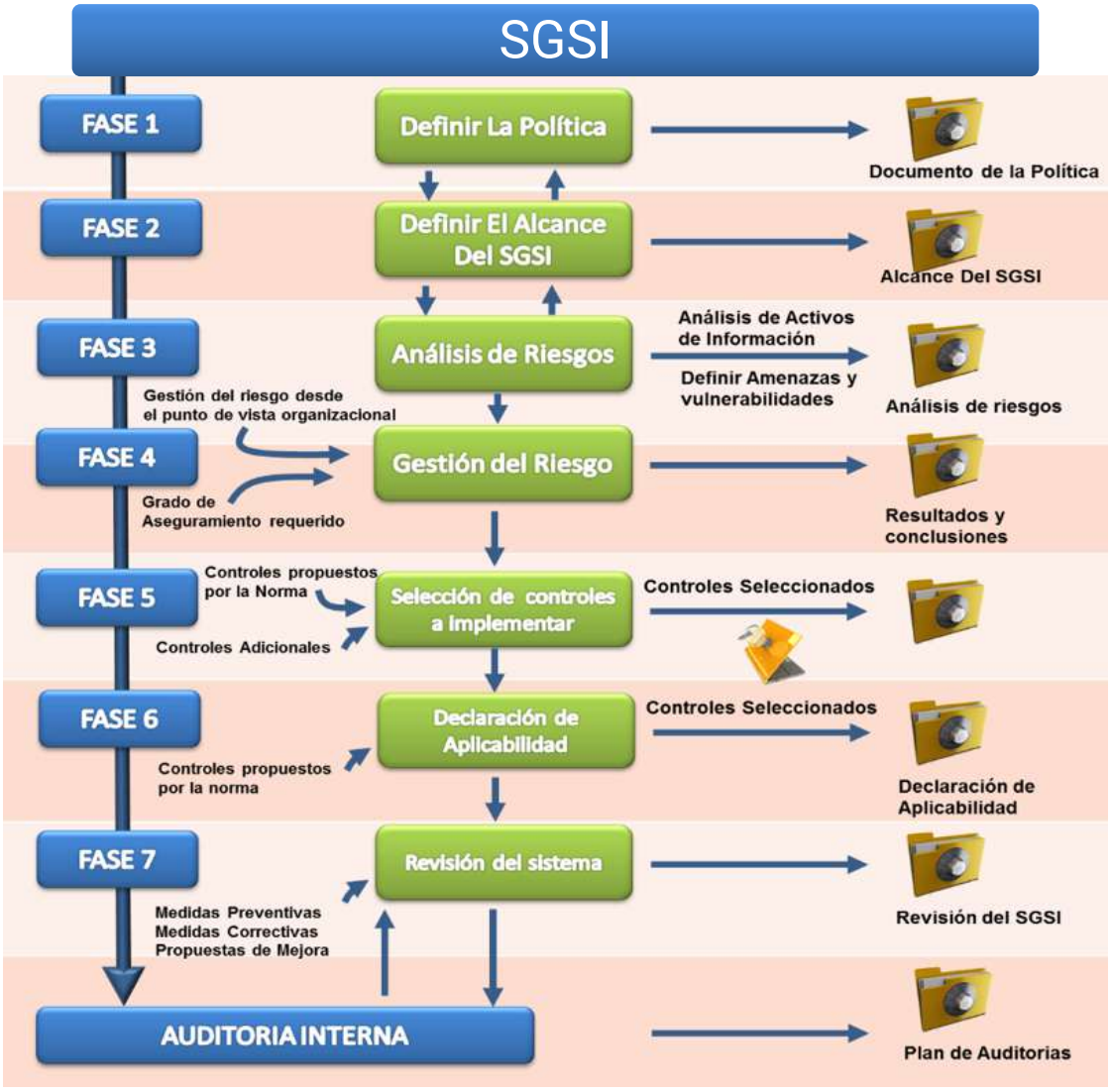
4. ISO/IEC 27001 - Sistemas de gestión de riesgos y seguridad

La norma ISO/IEC 27001:2013 es una norma que establece las pautas para el aseguramiento, la confidencialidad y la integridad de los datos y de la información, así como de los sistemas asociados.

Esta norma permite a las organizaciones implementar la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

En la Figura 9, es posible observar un esquema de los elementos o fases más relevantes en la implementación de un SGSI basado en la norma ISO/IEC 27001:2013

Figura 9. Elementos o fases para la implementación de un SGSI



Nota. Recuperada de ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002 (normas-iso.com)

Esta norma, como todas las normas ISO, adopta la teoría de gestión de la calidad PDCA (también conocida como ciclo de Deming):

- **Planificar ("Plan"):** Primera etapa del diseño del SGSI, en la que se realiza la identificación inicial de los riesgos asociados con la Seguridad de la Información. Esta cuestión se complementa con un análisis cualitativo y cuantitativo (si es necesario) de los riesgos identificados y la planificación de la respuesta y los controles necesarios para la mitigación de estos.
- **Hacer ("Do"):** implantación y operación del Sistema de Gestión de Seguridad de la Información definido y desarrollado.
- **Verificar (*"Check"*):** revisar y evaluar su eficacia y eficiencia. Si el desempeño no es el esperado, analizar las causas y determinar las mejoras.
- **Actuar ("Act"):** mejora continua del SGSI.

5. ISO/IEC 27032 – Marco de Ciberseguridad

Esta norma internacional permite la adopción de entornos de ciberseguridad de colaboración segura y fiables, que garanticen la seguridad de la información.

Esta norma ofrece los lineamientos y buenas prácticas para la adopción de la seguridad de la información en el ciberespacio.

Esta norma fue establecida para abordar los aspectos de ciberseguridad que no se habían tocado en otras normas y facilitar la cooperación entre otros marcos y estándares, como CSF, *CyberSecurity Framework* y el Marco de Ciberseguridad del NITS.

Su enfoque se realiza sobre 4 ejes:

- Seguridad de la información.
- Seguridad de las redes.
- Seguridad en Internet.
- Protección de infraestructuras críticas para la información.

Entre sus principales objetivos se encuentran:

- Ofrecer seguridad a todo el ciberespacio de la empresa.
- Tener un plan de acción en caso de que se llegue a presentar una crisis.
- Planificar la resolución de incidentes.
- Brindar capacitaciones a los miembros de la organización en todo lo relacionado con ciberseguridad y sus riesgos.
- Crear alertas que permitan identificar alguna amenaza que pueda poner en peligro los activos de la empresa.
- Contar con una estrategia para combatir los riesgos que se puedan presentar o que se lleguen a materializar.
- Identificar los riesgos que se puedan presentar en este aspecto.

6. ISO/IEC 27035 - Gestión de incidentes de seguridad

Esta norma propone un estándar con las mejores prácticas destinadas a la gestión de incidentes de seguridad de la información identificados en la norma ISO/IEC 27000.

El objetivo principal de esta norma es aplicar los mejores controles de seguridad en la organización para evitar los incidentes relativos a la seguridad informática.

Se enfoca en:

- Identificar, comunicar y evaluar los incidentes de la seguridad de la información.
- Contestar, gestionar los incidentes de la seguridad de la información.
- Identificar, examinar y gestionar las vulnerabilidades de seguridad de la información.
- Aumentar la mejora de la continuidad de la seguridad de la información y de la gestión de los incidentes, como respuesta a la gestión de incidentes de la seguridad de la información y de las vulnerabilidades.

La norma consolida un proceso con 5 etapas primordiales, que son:

- Prepararse para enfrentarse a los incidentes.
- Reconocer los incidentes de seguridad de la información.
- Examinar los incidentes y tomar las decisiones sobre la forma en que se han llevado a cabo las cosas.
- Dar respuesta a los incidentes, lo que quiere decir, investigarlos y resolverlos.
- Aprender de las lecciones.

Todas estas normas anteriormente descritas permiten su integración en un marco que se adapte a cualquier organización, bien sea pública o privada, y sin importar su tamaño, permitiendo articular estrategias de gobierno corporativo apoyadas desde la tecnología y con un objetivo claro: garantizar la seguridad de la información.