RECOMENDACIONES PARA LA REALIZACION DEL ANALISIS DE BRECHA SEGÚN LA NORMA ISO 27001:2013.

El cuidado de la información debe tener una importancia fundamental para el funcionamiento e inclusive para que las organizaciones logren en el corto, mediano y largo plazo la consecución de su misión y además garantiza su supervivencia en un entorno cada vez más dinámico y lleno de riesgos. El hecho de disponer de una serie de controles para mitigar el riesgo según NTC/ISO 27001:2013 ayuda a gestionar y proteger los activos de información.

El marco teórico propio de este documento está estrechamente relacionado con la norma NTC/ISO 27001:2013 (Ver Tabla No. 1) y el Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea - GEL. Estos modelos han sido establecidos para ofrecer una guía para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). La adopción de este sistema es una decisión de tipo estratégico. El diseño y la posterior implementación del SGSI ISO 27001, deben estar basados en el tamaño, la estructura, las necesidades, los objetivos y los procesos de la entidad.

Dominio ISO 27001	Objetivo de control ISO 27001
Política de seguridad.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad.	Objetivo de control A.16
Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Tabla 1. Dominios de la norma

Los modelos mencionados poseen tres objetivos fundamentales que son:

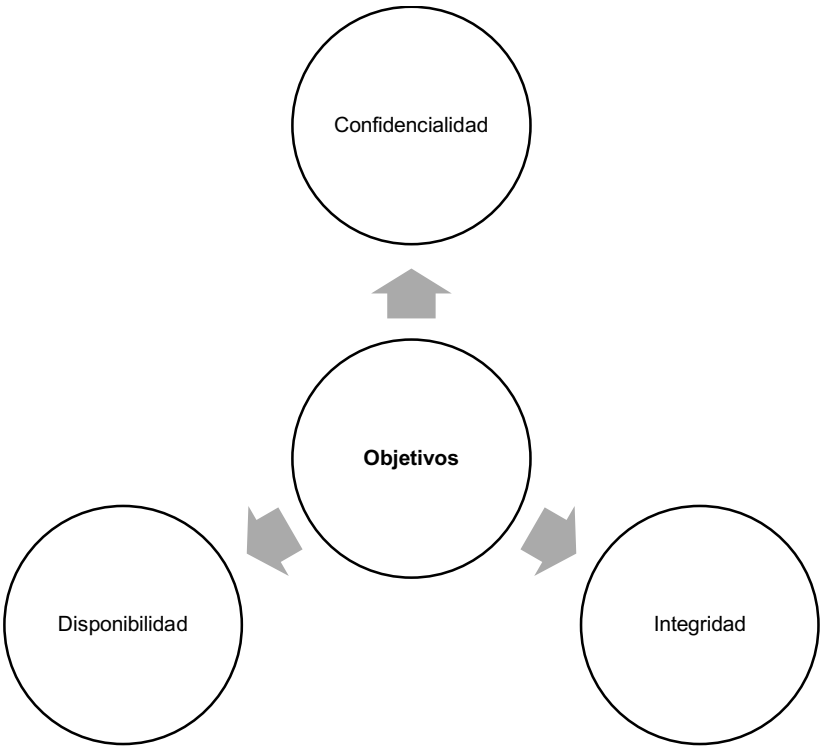

Ilustración 1. Objetivos de la seguridad de la información.

Disponibilidad:

Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Confidencialidad:

Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad:

Propiedad de salvaguardar la exactitud y estado completo de los activos.

Ahora bien, la adecuada seguridad de la información requiere también considerar los siguientes puntos:

- Comprender los requisitos de seguridad de la información de la entidad, y la necesidad de establecer políticas de seguridad de la información ISO 27001

- Implementar y operar controles para disminuir el riesgo de pérdida de la confidencialidad, integridad y disponibilidad de la información según la norma ISO 27001
- Medir el desempeño y la eficacia del SGSI ISO 27001
- Mantener una mejora continua basada en la medición de objetivos.

1 METODOLOGIA RECOMENDADA GAP ISO 27001

A continuación se presenta una descripción de los pasos que se recomiendan realizar para el análisis GAP (análisis de brecha) con relación a la NTC/ISO 27001:2013 y el MSPI. El GAP considera los diferentes dominios de la NTC/ISO 27001:2013 con el fin de evaluar la brecha faltante para cumplir totalmente con estos modelos. Para mayor información contactar info@sisteseg.com.

Ilustración 2. Metodología Recomendada GAP ISO 27001