

METODOLOGIA PARA REALIZAR EL ANÁLISIS GAP DE ISO 27001:2013

CONTROL DOCUMENTAL

Historia

| Versión | Autor | Tipo de Revisión | Descripción | Aprobado por | Fecha |
|---------|----------|------------------|-------------|--------------|-------|
| 1.0 | SISTESEG | Creación | Proyecto | | |
| | | | | | |
| | | | | | |

Distribución

| Copia | Destinatario | Destino / Dirección |
|----------|--------------|---------------------|
| Original | SISTESEG | |
| Copia | SISTESEG | |

Referencias

| Ref. | Documento o ítem referenciado |
|------|-------------------------------|
| | |
| | |

Control de Acceso

| Sección | Disponibilidad |
|---------|----------------|
| Todo | |
| | |

TABLA DE CONTENIDO

| | | |
|-----|--|----|
| 1 | INTRODUCCION..... | 5 |
| 2 | OBJETIVOS | 5 |
| 2.1 | Objetivo general..... | 5 |
| 2.2 | Objetivo Específicos | 5 |
| 3 | CONCEPTOS FUNDAMENTALES DEL GAP | 5 |
| 4 | METODOLOGIA RECOMENDADA | 7 |
| 4.1 | Elaboración de los cuestionarios | 8 |
| 4.2 | Entrevistas e Inspecciones en Sitio | 9 |
| 4.3 | Consolidación de Resultados | 9 |
| 4.4 | Análisis de Resultados | 9 |
| 4.5 | Elaboración de Informes y Plan de Acción | 9 |
| 4.6 | Presentación de Resultados..... | 10 |
| 5 | GLOSARIO..... | 11 |
| | BIBLIOGRAFÍA | 14 |

LISTADO DE ILUSTRACIONES

| | |
|--|---|
| Ilustración 1. Objetivos de la seguridad de la información..... | 6 |
| Ilustración 2. Metodología Recomendada..... | 8 |

LISTADO DE TABLAS

| | |
|---|---|
| Tabla 1. Dominios de la norma ISO 27001:2013 | 6 |
| Tabla 2. Niveles de Madurez..... | 9 |

1 INTRODUCCION

La seguridad de la información debe ser un componente crítico dentro de la estrategia de seguridad de la información. El análisis de brecha es recomendable realizarlo para iniciar el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI), ya que este análisis permite conocer el nivel de madurez con que se cuenta, para luego, proponer un plan de acción para la futura implementación del modelo de seguridad en una organización.

2 OBJETIVOS

2.1 Objetivo general

Presentar la metodología recomendada con respecto a la norma NTC/ISO 27001:2013 con el fin de comprender el estado de madurez de la seguridad de la información.

2.2 Objetivo Específicos

Detallar la metodología recomendada para se obtengan el:

1. Nivel de madurez por dominios
2. Nivel de madurez por control

3 CONCEPTOS FUNDAMENTALES DEL GAP

El cuidado de la información es importante para el funcionamiento para que las organizaciones logren la consecución de su misión. Contar con una serie de controles para mitigar el riesgo según NTC/ISO 27001:2013 ayuda a gestionar y proteger la información.

El marco teórico propio de este documento está basado con la norma NTC/ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL y la norma ISO 27032:2009. Estas recomendaciones se establecen para contar con una guía para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un (SGSI).

| Dominio ISO 27001:2013 | Objetivo de control |
|--|--------------------------|
| 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 ISO 27001:2013

Los objetivos de la seguridad de la información según la norma ISO 27001:2013 son:

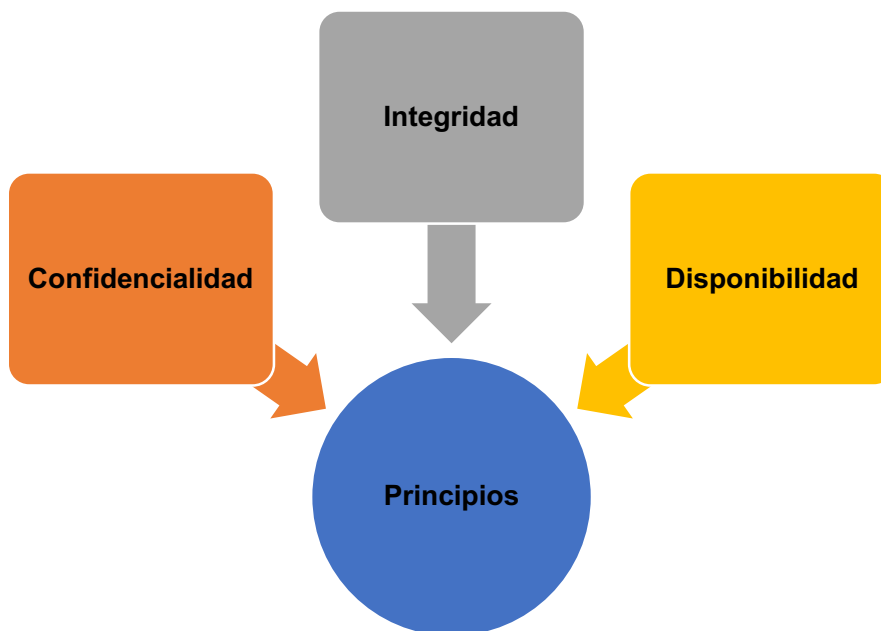


Ilustración 1. Objetivos de la seguridad de la información.

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

4 METODOLOGIA RECOMENDADA

A continuación presentamos la metodología recomendada para realizar el GAP (análisis de brecha) con relación a la NTC/ISO 27001:2013. El GAP considera los diferentes dominios de la NTC/ISO 27001:2013.



Ilustración 2. Metodología Recomendada.

4.1 Elaboración de los cuestionarios

En esta fase se deben realizar las siguientes actividades:

1. Revisión de la NTC/ISO 27001:2013 y del MSPI
2. Elaboración de preguntas
3. Definición de criterios de madurez

A continuación se presenta la tabla utilizada para definir los niveles y criterios de madurez:

| NIVEL | PORCENTAJE | CRITERIOS |
|-------------|------------|---|
| Inexistente | 0% | No se cuenta con la cláusula o control. |
| Incipiente | 1-25% | El control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe. |
| Repetible | 26-50% | El control esta implementado y además es soportado por un documento que contiene una política de alto nivel y otras políticas operativas debidamente aprobadas. |
| Definido | 51-75% | El control esta implementado y soportado por políticas, procedimientos y estándares de configuración publicados y socializados. |
| Gestionado | 76-99% | En este nivel se realizan mediciones sobre la efectividad de los controles. |
| Optimo | 100% | En este nivel se encuentran las organizaciones en las cuales se mide la efectividad de los controles con el fin de mejorarlos y optimizarlos. |

Tabla 2. Niveles de Madurez

4.2 Entrevistas e Inspecciones en Sitio

En esta esta etapa se recomienda realizar las siguientes actividades:

- Entendimiento de la estructura organizacional
- Revisión de los perfiles, cargos y caracterización de los procesos
- Elaboración agenda preliminar
- Ejecución de las entrevistas e inspecciones en sitio

4.3 Consolidación de Resultados

En esta fase se realizaron las siguientes actividades:

- Estimación del nivel de madurez de las cláusulas
- Estimación del nivel de madurez de los dominios
- Revisión de calificaciones

4.4 Análisis de Resultados

En esta se deben realizar las siguientes actividades:

- Elaboración de graficas de madurez y brecha
- Selección de hallazgos más importantes

4.5 Elaboración de Informes y Plan de Acción

En esta fase se deben realizar las siguientes actividades:

- Definición de objetivos, alcance

- Presentación de principales hallazgos
- Elaboración de recomendaciones
- Definición de dominios críticos
- Definición de controles críticos
- Definición de los plazos de implementación

4.6 Presentación de Resultados

En esta fase se realizarán las siguientes actividades:

1. Selección de los puntos más relevantes del informe
2. Elaboración de presentación ejecutiva
3. Revisión por parte de la Entidad, de la presentación ejecutiva
4. Ajustes a la presentación
5. Convocatoria
6. Presentación

5 GLOSARIO

- **Actividades críticas:** Operaciones críticas y/o actividades que soportan los objetivos de la Entidad.
- **Activo:** Cualquier cosa que tenga valor para la organización.
- **Activos de información:** Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte. Se pueden clasificar de la siguiente manera:
 - Personas: Incluyendo sus calificaciones, competencias y experiencia.
 - Intangibles: Ideas, conocimiento, conversaciones.
 - Electrónicos: Bases de datos, archivos, registros de auditoría, aplicaciones, herramientas de desarrollo y utilidades.
 - Físicos: Documentos impresos, manuscritos y hardware.
 - Servicios: Servicios computacionales y de comunicaciones.
- **Análisis de riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo
- **Área IT:** Es el área encargada de soportar, diseñar y mantener los activos electrónicos y el hardware propiedad de la Entidad.
- **BCP:** Por sus siglas en inglés (Business Continuity Planning) el plan de continuidad del negocio es un proceso de desarrollo y documentación de procedimientos que permiten a una organización responder ante eventos que interrumpen las actividades críticas de los procesos críticos, afectando considerablemente la prestación de servicios públicos a una comunidad.
- **BIA:** (Business Impact Analysis) Proceso diseñado para priorizar las actividades críticas del negocio evaluando el impacto potencial principalmente de manera cuantitativa.
- **Confidencialidad:** Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Contratistas:** Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una Entidad.
- **Consultor:** Persona idónea en capacidad de prestar servicios de asesoría, diseño, y creación de propiedad intelectual.

- **Custodio:** Encargado de proteger la información por delegación del propietario. Generalmente este rol es ejecutado por el Área IT.
- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la Entidad.
- **Desastre:** Evento que causa grandes daños o pérdidas. En el ambiente del negocio, es un evento que crea incapacidad en la organización sobre la ejecución de las actividades críticas del negocio por un periodo de tiempo.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.
- **DRP (PRD):** Por sus siglas en inglés (Disaster Recovery Planning). Es un documento en que definen los recursos, acciones, tareas y datos requeridos para gestionar el esfuerzo de recuperación de los sistemas de información y tecnología en general ante un evento catastrófico.
- **Estándares:** Un producto o mecanismo específico el cual es seleccionado desde un punto de vista universal, para su uso a lo largo de toda la organización, con el objetivo fundamental de soportar una política ya aceptada y aprobada por las directivas de la Entidad.
- **Falla:** Daño o afectación de un dispositivo por un periodo determinado
- **Incidente:** Un evento o una serie de eventos no deseados o inesperados que tienen una posibilidad significativa de comprometer las operaciones del servicio y amenazar la continuidad del Sistema.
- **Información:** Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:
 - Una noticia que escuchamos por la radio.
 - Una señal de tráfico que advierte un peligro.

La información se representa mediante conjuntos de símbolos, que pueden ser de diferente naturaleza:

- Textuales o numéricos, como las letras y números que usamos al escribir.
 - Sonoros, como los fonemas, las notas musicales...
 - Cromáticos, como los colores de los semáforos.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **Lista de verificación:** Herramienta para recordar y/o validar que tareas tienen que ser cumplidas y que recursos están disponibles en una etapa de recuperación.
- **Procedimientos:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **Propietario:** Es el responsable y dueño del activo de información. Define también sus niveles de clasificación.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sitio alternativo:** Un sitio alternativo es aquel que en caso de un desastre o incidente de seguridad utilizaremos para realizar los procesos interrumpidos. Este tipo de sitios se puede calificar de acuerdo con:
 - **SGSI:** Sistema de Gestión de la Seguridad de la Información.
 - **Terceros:** Entendemos por terceros a proveedores, contratistas, clientes y visitantes al Sistema.
 - **Usuario:** Es el que utiliza los activos de información para llevar a cabo las funciones de su trabajo.

BIBLIOGRAFÍA

Business Continuity Institute (2013) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

Disaster Recovery Institute International (DRII) (2012) *Professional Practices for Business Continuity Practitioners*, DRII, New York.

ISO 22301 (2012) – Societal security – Business continuity management systems – Requirements

ISO 22301 (2012) – Societal security – Business continuity management systems – Guidance

ISO 22301 (2012) – Societal security – Terminology

ISO 27001:2013 Information security.

www.sans.org