Ingeniería de Sistemas

Consideraciones para el Planeamiento e Implementación de un SGSI

Seguridad de Sistemas de TI

2022-01

UNIVERSIDAD DE LIMA

Agenda

Agenda

1. Estructura organizacional para la seguridad
2. Controles requeridos por las normas de seguridad
3. Interpretación de los Controles de seguridad
4. Modelos de madurez de la seguridad
5. Gap analysis – Análisis de Brecha

UNIVERSIDAD DE LIMA

1. Estructura Organizacional para la Seguridad

Aspectos fundamentales para el Diseño de un SGSI

https://www.youtube.com/watch?v=qawa_QcuFfc

UNIVERSIDAD DE LIMA

Estructura Organizacional de Seguridad

- Uno de los factores claves para diseñar e implementar un SGSI es el compromiso y participación y de la Alta Dirección con respecto a la dirección de la Seguridad de la Información.

- Este compromiso se debe materializar en el establecimiento de una ***Política de Seguridad de la Información***, la cual deberá ser el punto de partida para establecer el SGSI.

- Es necesario también establecer los **roles y responsabilidades del personal** en materia de Seguridad de la Información.

- Para ello será necesario conformar un **Comité de Dirección para la Seguridad de la Información**, un **Comité de Gestión**, así como, el **rol del Oficial de Seguridad de la Información o responsable** del modelo.

UNIVERSIDAD DE LIMA

Estructura Organizacional del SGSI

Comité de Dirección (CDSI)

Gerencia General, Gerentes de línea

Comité de Gestión de Seguridad de la Información (CGSI)

- Jefes de Área, Supervisores

Oficial de Seguridad de la Información

Propietarios, Custodios, Usuarios (personal, proveedores, practicantes, otros)

UNIVERSIDAD DE LIMA

Comité de Dirección de Seguridad de la Información (CDSI)

¿Qué implica las funciones y los roles del CDSI?

Revisar y aprobar las Políticas específicas de Seguridad de la Información.
Proveer los recursos necesarios para la Seguridad de la Información.
Asignación de roles específicos y responsabilidades en materia de seguridad dentro de la organización.
Iniciar planes y programas para lograr y mantener la concientización en la seguridad de la información.
Velar por el cumplimiento de programas de seguridad, normas y leyes vigentes.
Realizar evaluaciones periódicas del funcionamiento del SGSI.

UNIVERSIDAD DE LIMA

Comité de Gestión de Seguridad de la Información (CGSI)

¿Qué implica las funciones y los roles del CGSI?

- ☑ Asegurar que las actividades de seguridad sean ejecutadas en cumplimiento con la Política de seguridad de la información.
- ☑ Aprobar las principales iniciativas para incrementar la seguridad de la información.
- ☑ Permitir que el personal exprese sus inquietudes sobre asuntos de seguridad
- ☑ Aprobar metodologías y procesos de seguridad de información
- ☑ Promover la difusión y apoyo a la seguridad de la información dentro de la organización.

UNIVERSIDAD DE LIMA

Oficial de Seguridad de la Información

Es la persona encargada de diseñar, desarrollar, implantar y mantener el Sistema de Gestión de Seguridad de la información en la organización

¿Qué implican las funciones y responsabilidades del Oficial de Seguridad?

- ☑ Proponer metodologías, herramientas, planes, programas y procesos para la seguridad de la información..
- ☑ Asegurar el buen funcionamiento del Sistema de Gestión de Seguridad de la información.
- ☑ Supervisar el cumplimiento de controles de seguridad.
- ☑ Administrar los incidentes y vulnerabilidades de la seguridad de la información a fin de identificar los controles a implementar.
- ☑ Elaborar y actualizar el Planes de Seguridad de la Información.

UNIVERSIDAD DE LIMA

Propietario de los Activos de Información

Es la persona o entidad que tiene la responsabilidad gerencial aprobada sobre los activos de información que se generan y se utilizan en las Unidades u Oficinas administrativas.

¿Qué implican las funciones y responsabilidades del Propietario del Activo?

- ☑ Identificar y Clasificar los activos de su propiedad.
- ☑ Determinar los periodos de retención de los activos de información (electrónica e impresa).
- ☑ Determinar los criterios y niveles de acceso a los activos de su propiedad.
- ☑ Revisar periódicamente la clasificación de la información con la finalidad de verificar el cumplimiento de los requerimientos de seguridad de la organización.
- ☑ Verificar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- ☑ En coordinación con el Oficial de Seguridad de la Información, revisar y evaluar los resultados de la implementación de controles aplicados a los activos de su propiedad.

UNIVERSIDAD DE LIMA

Custodio de los Activos de Información

Es el responsable de la administración y resguardo de los activos de información; asimismo, del monitoreo del cumplimiento de los controles de seguridad en los activos que se encuentren bajo su administración.

¿Qué implican las funciones y responsabilidades del Custodio?

- ☑ Dar acceso a los usuarios de acuerdo con las especificaciones establecidas por los propietarios.
- ☑ Administrar los accesos a los activos
- ☑ Cumplir con los controles implementados para la protección de los activos asignados para su custodia
- ☑ Administrar los procedimientos de backup, recuperación y restauración de información
- ☑ Reportar incidentes y debilidades de seguridad de la información
- ☑ En caso de identificar oportunidades de mejora, debe comunicarlas a los responsables de Seguridad de la Información (Oficial de Seguridad de la Información y propietarios de la información).

UNIVERSIDAD DE LIMA

Usuario de los Activos de Información

Son aquellas personas, llámese personal permanente, personal temporal, consultores y proveedores de bienes y/o servicios, que utilizan los activos de información de la organización como parte de sus actividades diarias.

¿Qué implican las funciones y responsabilidades del Usuario?

- ☑ Cumplimiento a las políticas y directivas de seguridad de la información.
- ☑ Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- ☑ Utilizar la información de su organización sólo para el cumplimiento de sus funciones y/o fines institucionales.
- ☑ Reportar incidentes y debilidades de seguridad de la información.
- ☑ En caso de identificar oportunidades de mejora, debe comunicarlas a los responsables de Seguridad de la Información (Oficial de Seguridad de la Información).

UNIVERSIDAD DE LIMA

2. Controles requeridos por las normas de Seguridad

Estructura de la norma ISO 27001:2013

4 Capítulos Generales

(Capítulos 0 al 3)

7 Capítulos Específicos
(Capítulos 4 al 10 son Obligatorios = 130 requisitos)

Anexo "A"

(14 cláusulas, 35 categorías y 114 controles)

UNIVERSIDAD DE LIMA

Organización de la Norma ISO 27001:2013

La norma ISO 27001 está organizada de la siguiente manera:	
0. Introducción	0.1 Generalidades, 0.2 Compatibilidad con otros sistemas de gestión
1. Alcance	1. Generalidades y aplicación
2. Referencias normativas	2. Otras normas relacionadas
3. Términos y definiciones	3. Terminología principal usada en la norma (ISO 27000)
El SGSI	4. Contexto de la organización 5. Liderazgo 6. Planeamiento 7. Soporte 8. Operación 9. Evaluación de rendimiento 10. Mejoras
Anexos	A.1. Anexo A: Objetivos de Control y Controles (alineados a la cláusula 6.1.3)

UNIVERSIDAD DE LIMA

Introducción a la norma (1 de 3)

General:

- Proporcionar los requisitos para ***establecer, implementar, mantener y mejorar*** de manera continua un SGSI.

- La adopción de un SGSI debería ser una ***decisión estratégica*** para la organización.

- La implementación de un SGSI esta ***influenciada*** por:
  - ✓ **Necesidades y Objetivos de la organización**
  - ✓ **Requisitos de Seguridad**
  - ✓ **Procesos Organizacionales**
  - ✓ **Tamaño y estructura de la organización**

- El SGSI busca conservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de ***Gestión de Riesgos***

UNIVERSIDAD DE LIMA

Introducción a la norma (2 de 3)

General:

- El SGSI sea ***parte y este integrado*** a:
  - ✓ **Los *procesos* de la organización**
  - ✓ **La *estructura de gestión* de la empresa**
  - ✓ **Considerada en el *diseño de los procesos, sistemas de información y controles.***
  - ✓ **La implementación del SGSI sea *escalada* según las necesidades de la organización.**

UNIVERSIDAD DE LIMA

Introducción a la norma (3 de 3)

Compatibilidad con otras normas de Gestión:

- ✓ **Estructura de alto nivel**
- ✓ **Títulos de sub cláusula idénticos**
- ✓ **Texto idéntico**
- ✓ **Estructura de las normas ISO según en Anexo SL (10 puntos)**
- ✓ **Permitirá integrar otras normas de los sistemas de gestión en una sola, de forma mas simple. Ej. SIG.**

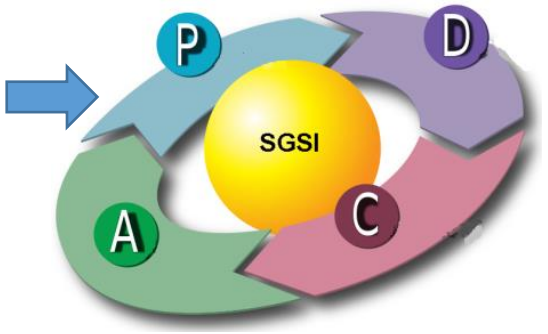
UNIVERSIDAD DE LIMA

EL SGSI

Requisitos Generales:

La organización debe establecer, implementar, mantener y mejorar un SGSI documentado, dentro del contexto de las actividades generales del negocio de la organización y los riesgos a los que se enfrenta.

ESTABLECER EL SGSI:

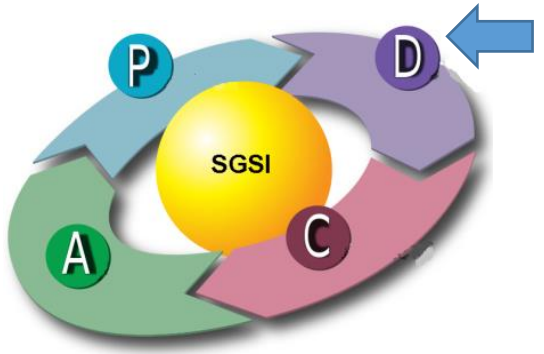


- Definir el alcance y los límites del SGSI
- Definir una política de Seguridad de la Información
- Definir el enfoque para la evaluación de riesgos de la organización
- Identificar los riesgos
- Análizar y evaluar los riesgos
- Identificar y evaluar las opciones para Tratamiento Riesgos
- Seleccionar objetivos de control y controles Tratamiento Riesgos
- Obtener aprobación dirección del riesgo residual propuesto
- Obtener autorización dirección para implementar y operar el SGSI
- Elaborar el SOA (Declaración de Aplicabilidad)

UNIVERSIDAD DE LIMA

EL SGSI

IMPLEMENTAR Y OPERAR EL SGSI:

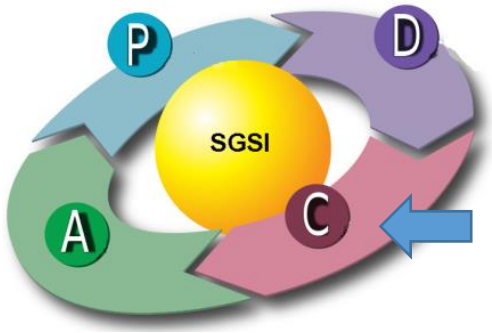


- Formular un Plan de Tratamiento de Riesgos (PTR)
- Implementar un Plan de Tratamiento de Riesgos
- Implementar los controles seleccionados para el TR
- Definir como medir la eficacia de los controles o grupos de controles seleccionados.
- Implementar programas de capacitación y toma de conciencia
- Gestionar la operación del SGSI
- Gestionar los recursos del SGSI
- Implementar procedimientos y otros controles para permitir inmediata detección y respuesta a incidentes de seguridad.

UNIVERSIDAD DE LIMA

EL SGSI

MONITOREAR Y REVISAR EL SGSI:



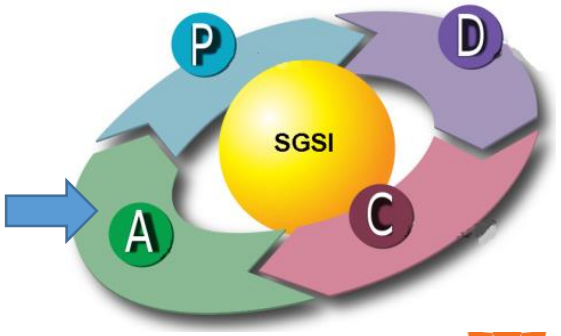
- Ejecutar los Procedimientos de Monitoreo y Revisión
- Realizar revisiones regulares de la eficacia del SGSI
- Medir eficacia de los controles para verificar que se han cumplido con los requisitos de seguridad.
- Revisar las evaluaciones de riesgos a intervalos planificados (revisar riesgos residuales y los niveles de riesgos aceptables)
- Llevar a cabo auditorías internas del SGSI
- Realizar una revisión por la dirección del SGSI
- Registrar acciones y hechos que podrían tener un impacto sobre el desempeño del SGSI.

UNIVERSIDAD DE LIMA

EL SGSI

MANTENER Y MEJORAR EL SGSI:

- Implementar mejoras identificadas en el SGSI
- Ejecutar acciones correctivas y preventivas apropiadas (aplicar las lecciones aprendidas de experiencias de seguridad de la misma organización u otras organizaciones)
- Comunicar acciones y mejoras a todas las partes interesadas.
- Asegurarse que las mejoras logren sus objetivos previstos.



UNIVERSIDAD DE LIMA

Información Documentada

7.5.1 General:
El SGSI debe incluir:

a. ***Información documentada necesaria para esta norma***

b. ***Información documentada definida por la organización*** como necesaria para la efectividad del SGSI

La magnitud de la información documentada para un SGSI puede variar de una organización a otra debido a:

- *El tamaño de la organización, tipo de actividades, procesos, productos, servicios.*
- *Complejidad de los procesos y sus interaccione*
- *Las competencias de las personas*

UNIVERSIDAD DE LIMA

Requisitos de Documentación (1/2)

La documentación del SGSI debe incluir:

4.3 Alcance del SGSI

5.2 Política de Seguridad de la Información

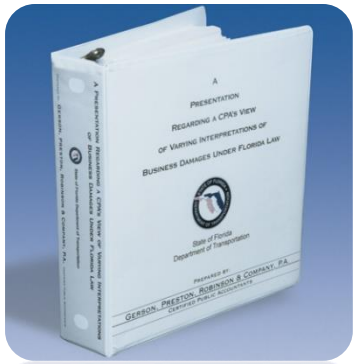
6.1.2 Proceso de Análisis y evaluación de riesgos de seguridad de la información

6.1.3 Proceso de Tratamiento de riesgos de Seguridad de la Información

6.1.3 d) Declaración de Aplicabilidad (SOA)

6.2 Objetivos de Seguridad de la Información

7.2 d) Evidencia de la competencia

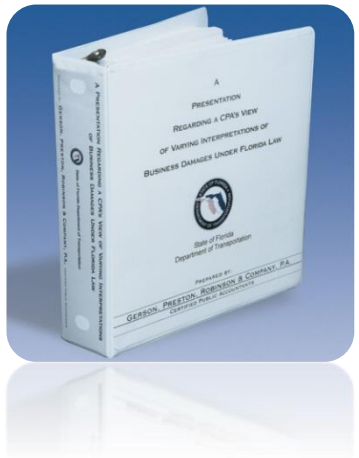


7.5.1 b) Información documentada determinada por la organización como necesaria para la eficacia del SGSI.

<u>Nota</u>: Los documentos y registros pueden estar en cualquier formato o medio.

UNIVERSIDAD DE LIMA

Requisitos de Documentación (2/2)



La documentación del SGSI debe incluir:

8.1 Planificación y control operacional

8.2 Resultados del análisis y evaluación de riesgos de S.I.

8.3 Resultados del tratamiento de riesgos de S.I.

9.1 Evidencia de los resultados de monitoreo y medición

9.2 g) Evidencia del programa de auditoría y los resultados de las auditorías.

9.3 Evidencia de los resultados de las revisiones por la dirección.

10.1.f) Evidencia de la naturaleza de las no conformidades y de cualquier acción tomada posteriormente.

10.1. g) Evidencia de los resultados de cualquier acción correctiva.

Nota: Los documentos y registros pueden estar en cualquier formato o medio.

UNIVERSIDAD DE LIMA

Información Documentada (1/2)

7.5.2 Creación y actualización:

Al crear y actualizar la información documentada, la organización debe asegurar la correspondiente:

a. Identificación y descripción (Ej. Titulo, fecha, autor, número de referencia)

b. Formato (Ej. Idioma, versión de sw, gráficos) y medio (digital, impreso)

c. Revisión y aprobación por conveniencia y suficiencia (*responsable de aprobar información documentada debe ser formalizado*)

UNIVERSIDAD DE LIMA

Información Documentada (2/2)

7.5.3 Control de información documenta:

La información documentada necesaria por el SGSI y por la norma debe ser controlada para asegurar que:

a. Esta disponible y apropiada para su uso, donde y cuando sea necesario

b. Esta debidamente protegida (Ej. Perdidas de confidencialidad, uso inapropiado, perdida de integridad)

Para el control de la información documentada, la organización debe abordar las siguientes actividades:

i. Distribución, acceso, recuperación y uso
ii. Almacenamiento y conservación
iii. Control de cambios
iv. Retención y disposición

UNIVERSIDAD DE LIMA

Ejercicio:

Política de Seguridad de la Información

ULL | Universidad de La Laguna

Política de Seguridad de la Información de la Universidad de La Laguna

3. Interpretación de los controles de Seguridad

Proceso de Análisis de Riesgos

ACTIVOS DE INFORMACIÓN


Personas


Servidores


Data Center


Procesos

1. Inventario

2. Análisis

CONTROLES ACTUALES

Basado en la Norma ISO 27005

3. Evaluación

Amenazas

RIESGO EFECTIVO

Probabilidad

Relevancia

Impacto

Vulnerabilidades

4. Tratamiento

RIESGO RESIDUAL

Mecanismos propuestos

UNIVERSIDAD DE LIMA

Anexo A:
Objetivos de control y controles

Se obtienen de los capítulos 5 al 18 de la ISO/IEC 27001:2013 y se han alineado con estos, el detalle de su implementación y orientación se puede encontrar en la norma indicada.

Los objetivos de control y controles de estas tablas deben seleccionarse como parte del proceso del SGSI especificado en la cláusula 6.1.3 de la norma.

El Anexo A está organizado de la siguiente manera:

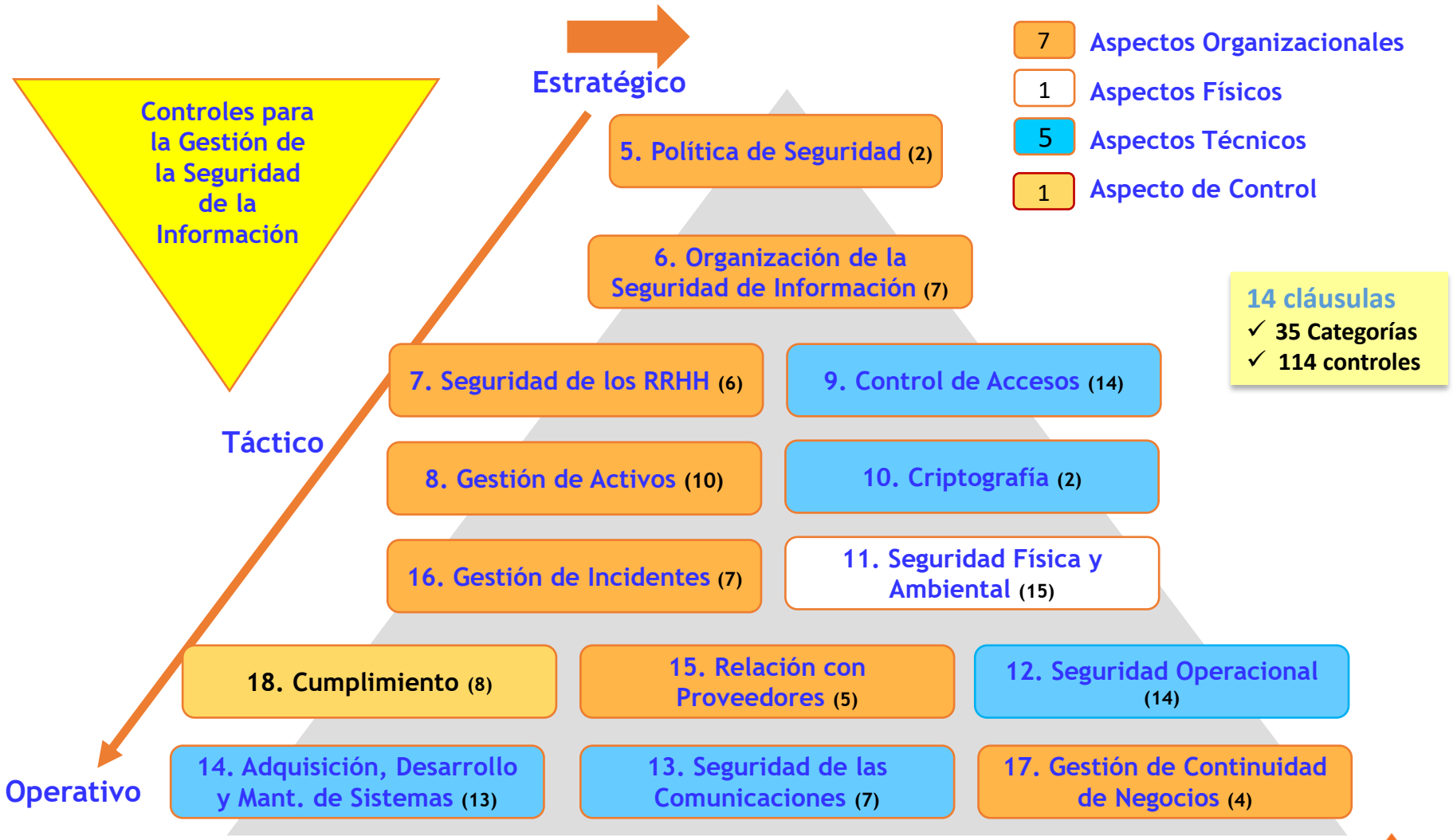
14 cláusulas

35 Categorias y Objetivos de Control

114 Controles

UNIVERSIDAD DE LIMA

Anexo "A" – ISO 27001:2013



UNIVERSIDAD DE LIMA

4. Madurez de los controles de Seguridad

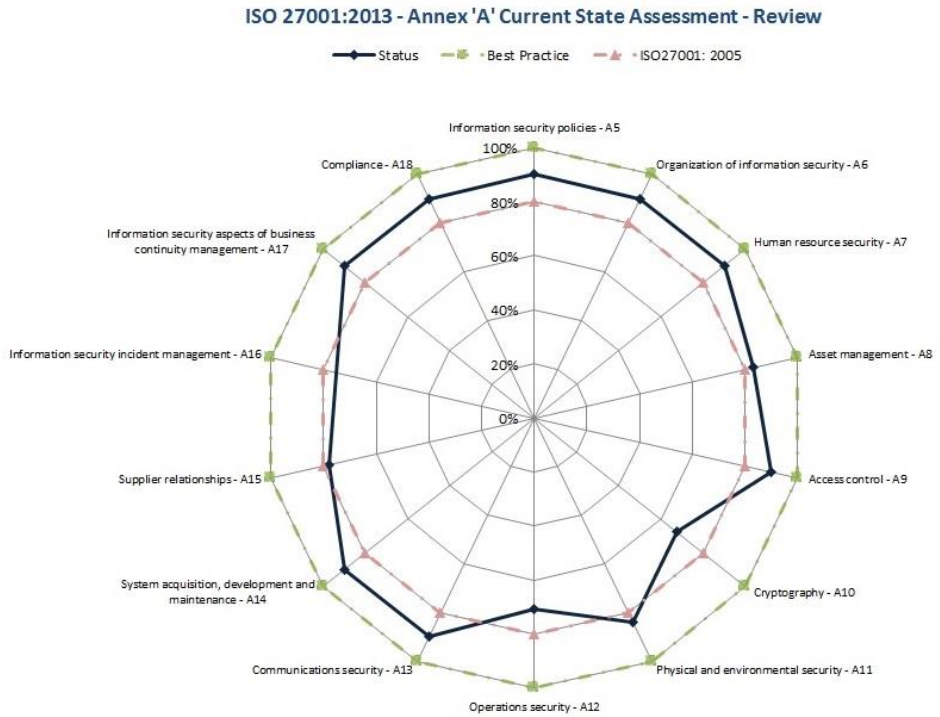
Evaluación de Cumplimiento

Generalidades:

- Tiene como objetivo determinar el nivel de madurez y grado de cumplimiento que posee la organización con respecto a cada uno de los controles y cláusulas de la norma ISO 27001:2013 – Anexo A.
- Determinar que modelo de evaluación del nivel de madurez se utilizara para realizar la evaluación.
- El modelo de evaluación del nivel de madurez puede realizarse utilizando el modelo COBIT, CMMI, ISO 15504, entre otros.
- Es necesario realizar revisiones in situo de cada control para determinar su cumplimiento.
- Revisar información relacionada (politicas, directivas, procedimientos)
- Realizar entrevistas y reuniones de trabajo con cada usuario y personal de las áreas involucradas para cada cláusula del Anexo "A" de la norma.

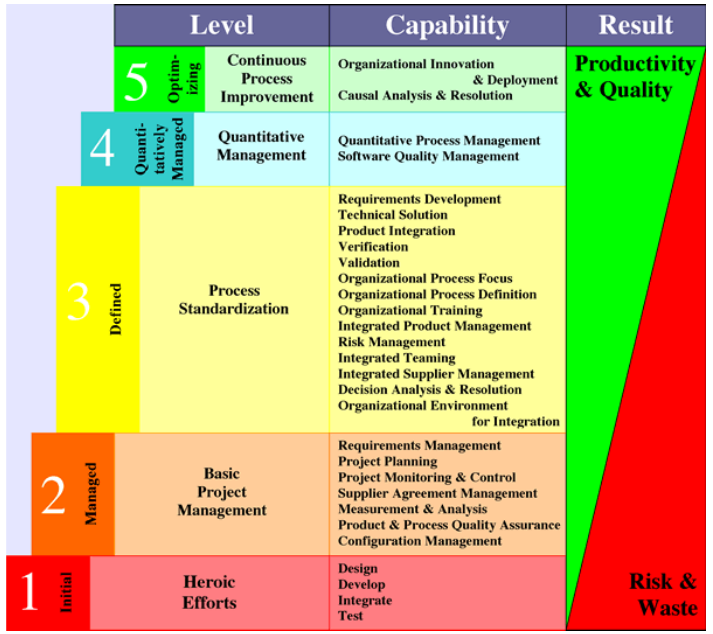
UNIVERSIDAD DE LIMA

Grado de Cumplimiento y Nivel de Madurez



<u>Grado de Cumplimiento</u> de cada Cláusula de la ISO 27001:2013 - Anexo ¨A¨

<u>Nivel de Madurez</u> de cada control de la ISO 27001:2013 – Anexo ¨A¨



Modelo CMMI

Fuente: https://parkinsonhowe.wordpress.com

UNIVERSIDAD DE LIMA

5. Análisis de Brecha o Gap Analysis

Anexo A: controles requeridos por cada cláusula

Nº	14 Cláusulas de la Norma ISO 27001:2013 - Anexo ¨ A ¨	Controles	Aplicables	Implementados
A5	Política de Seguridad de la Información	2	2	2
A6	Organización de Seguridad de la Información	7	7	4
A7	Seguridad de los Recursos Humanos	6	6	3
A8	Gestión de Activos	10	10	5
A9	Control de Acceso	14	13	4
A10	**Criptografía**	**2**	**2**	**0**
A11	Seguridad Física y Ambiental	15	15	10
A12	**Seguridad Operacional**	**14**	**14**	**10**
A13	Seguridad de las Comunicaciones	7	6	2
A14	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	13	13	2
A15	**Relación con Proveedores**	**5**	**5**	**2**
A16	Gestión de Incidentes	7	7	3
A17	Continuidad de Negocios y Recuperación de Desastres	4	4	1
A18	Cumplimiento	8	8	3
	Total Actividades:	114	112	51

UNIVERSIDAD DE LIMA

Nivel de Madurez de los Controles de la Norma

ANÁLISIS DE BRECHA - GAP ANALYSIS

CLAUSULA 7 - Gestión de Activos

ISO	Requerimiento	Aplica (SI/NO)	Situación Actual	Nivel de Madurez	Plazo	Acciones de Control	Documentación SGSI / Registros	Observaciones
7.1	**Responsabilidad sobre los Activos**							
7.1.1	Inventario de activos tecnológicos	SI	Actualmente se tiene una clasificación de activos de información solo en el macro proceso de TI, el cual representa el alcance definido, sin embargo no se ha ampliado para las demás áreas. Se cuenta con inventario de activos institucional donde se encuentran TODOS los activos en general.	3	Corto Plazo	Coordinar con las áreas usuarias para establecer un cronograma de trabajo para el relevamiento de los activos de información y su evaluación de riesgos asociados. Así mismo, establecer quienes son propietarios, custodios, y usuarios de los activos de información.	Dentro del Proceso de Análisis de Riesgos, Informe de Identificación e Inventario de Activos.	-
7.1.2	Responsables de los activos tecnológicos	SI	Se conocen los propietarios de activos a nivel macroproceso de TI. No se tiene un inventario de activos por área. No se conoce por parte de las áreas usuarias las definiciones de Propietario, Custodio y Usuario de la Información.	3	Corto Plazo	Dentro del proceso de Inventario de Activos de Información, se determinará los roles de propietario de activos, usuarios, custodios, entre otros, lo cual permitirá poder tratar y clasificar la información de una forma más segura y organizada y expandir dicha actividad a nivel de toda la organización.	Inventario de Activos de Información	-
7.1.3	Uso aceptable de los activos tecnológicos	SI	Se tiene una política de uso aceptable de sistemas, servicios y recursos, que se basa tambien en la matriz de procesos disciplinarios. También se considera una cláusula de contrato el compromiso del personal con el uso adecuada de los recursos informáticos.	3	Mediano Plazo	Realizar revisiones permanentes de cumplimiento de la política de uso aceptable de los sistemas y servicios.	Política de uso de los sistemas, servicios y recursos de T.I.	-

CALIFICACION	CUMPLIMIENTO
	Con respecto al control, es un control debil, cumple o excede las expectativas
0	No está definido ningún tipo de control
1	No existen controles efectivos – Deficiencias considerables con respecto a lo esperado para el requerimiento
2	Controles Básicos – Deficiencias menores con respecto a lo esperado para el requerimiento
3	El requerimiento se cumple en forma efectiva **(Aprobado)**
4	Controles Gestionados (se controla su aplicación y buen uso)
5	Optimizado – Implementación que mejora el estándar.

UNIVERSIDAD DE LIMA

Plan de Seguridad de la Información

Nº	14 Cláusulas de la Norma ISO 27001:2013 Anexo ¨ A ¨	Corto Plazo	Mediano Plazo	Largo Plazo	Sub Total
A5	Política de Seguridad de la Información	2	-	-	2
A6	Organización de Seguridad de la Información	6	-	-	6
A7	Seguridad de los Recursos Humanos	2	-	-	2
A8	Gestión de Activos	-	1	-	1
A9	Control de Acceso	2	2	3	7
A10	Criptografía	4	6	3	13
A11	Seguridad Física y Ambiental	2	2	2	6
A12	Seguridad Operacional	2	2	2	6
A13	Seguridad de las Comunicaciones	3	1	2	6
A14	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	1	4	2	7
A15	Relación con Proveedores	3	-	1	4
A16	Gestión de Incidentes	1	-	-	1
A17	Continuidad de Negocios y Recuperación de Desastres	-	5	-	5
A18	Cumplimiento	2	1	-	3
	Total Actividades:	29	24	15	68

UNIVERSIDAD DE LIMA

Conclusiones Finales

i. Se constituye como el ***modelo de 4 etapas*** que utiliza para operar el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2013:

ii. Se considera como el ***control principal para iniciar la implementación del SGSI***, el cual permite obtener el compromiso y la responsabilidad de la alta dirección con respecto a la gestión de la seguridad de la información:

iii. La **estructura del Anexo "A"** de la norma ISO 27001:2013 se compone de:

:

UNIVERSIDAD DE LIMA

Ejecución de Ejercicio

Análisis de Brecha:

CLÁUSULA	OBJETIVO	Nº CONTROL	CONTROL	DESCRIPCIÓN DE CONTROL	PREGUNTA	AREA DE CONTACTO	EVIDENCIA / DOCUMENTACION	DESCRIPCIÓN DE EVIDENCIA	NIVEL DE MADUREZ	OBSERVACIONES / NO CONFORMIDADES	RECOMENDACIONES / OPORTUNIDADES DE MEJORA
11			Control de accesos								
11	11.1		Requisitos del negocio para el control de accesos								
11		11.1.1	Política de control de accesos	Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.	¿Se ha establecido y documentado una política de control de accesos y ha sido revisada basándose en los requisitos de seguridad y de negocio?	Dpto de Tecnolodías de Información	SISCOM(Administración) -Entrevistas con el personal del área de TI	A traves de servidor de dominio (se estabelcen perfiles para la red) A traves del sistema se seleccionan los perfiles de acceso para cada usuario		- No se cuenta con una política definida de control de accesos sobre todos los activos de información (logicos y fisicos).	- Definir y documentar los requisitos de negocio para el control de accesos (lógico y físico). - Establecer una política de control de accesos con los derechos de cada usuario (perfiles) o grupo de usuarios. - Establecer niveles de seguridad para cada aplicación del negocio, así como políticas de control de accesos, autorización y manipulación.
11	11.2		Gestión de acceso de usuarios								
11		11.2.1	Registro de usuarios	Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.	¿Existe un procedimiento formal para las altas y bajas y dotar y revocar el acceso a todos los sistemas de información?	Dpto de Tecnolodías de Información	- Formato de Requerimiento - Entrevistas con el personal del área de TI	Cada Jefe de Área cuando ingresa un nuevo usuario manda el Requerimiento especificando las opciones que debería tener en Sistema. En el caso de revocar o dar baja a acesos en algunos casos el Jefe del Área manda correo electrónico indicando cuales son los usuarios		-No existe un procedimiento formal de registro de altas y bajas de usuarios para garantizar la protección de la información, los privilegios de acceso a los sistemas y recursos compartidos.	- Establecer procedimientos adecuados identificando actividades, responsables y registros asociados para dar Accesos y Privilegios a los usuarios de acuerdo al tipo de usuario, al área a la que pertenece o el perfil del sistema solicitado; asimismo, los lineamientos para el registro de altas y bajas de usuarios

Cláusula: 11. Control de Accesos

Controles: 11.1.1 al 11.3.3 (8 controles)

UNIVERSIDAD DE LIMA