CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Implementación de un SGSI

Workshop N°2

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Expositor

Carlos Lobos de Medina

Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional de la Universidad de Chile.

Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.

carlos.lobos@usach.cl

https://www.linkedin.com/in/clobos/

Estructura de Procesos del SGSI

Agilidad y eficiencia en los procesos

- Las obligaciones de la norma son muy precisas: Proceso de Gestión de Riesgos
- Podemos articular definiciones de una mejor forma?
- Podemos disminuir significativamente el número de procesos?
- Podemos hacer esto más eficiente?

POR SUPUESTO QUE SI!!!

Cual es el core del SGSI?

Clausula 1:	Objeto y campo de aplicación
Clausula 2:	Referencias normativas
Clausula 3:	Términos y definiciones
Clausula 4:	Contexto de la organización
Clausula 5:	Liderazgo
Clausula 6:	Planificación
Clausula 7:	Soporte
Clausula 8:	Operación
Clausula 9:	Evaluación del desempeño
Clausula 10:	Mejora

- Si queremos avanzar en la implementación de un SGSI una buena prácticas es instalar en principio el Sistema de Gestión.

- Beneficio principal, es fácil de una visión de procesos y te posibilita tener definiciones claves establecidas:
  - Gobernanza
  - Roles y Responsabilidades
  - Analisis del Contexto
  - Alcance y procesos de apoyo
  - Estrategia
  - Formalización de Políticas basales

Otra forma de verlo

Procesos de Gestión

Procesos Core

Procesos de Soporte

Es fácil de implementar si entendemos y articulamos conceptos claves.

Cual es el rol de la dirección?

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;

c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;

d) comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información;

e) asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos;

f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

g) promoviendo la mejora continua; y

h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

Debe demostrar liderazgo y compromiso!!!

Debe asegurar, comunicar, dirigir, apoyar, promover…….!!!

Tiene que implementar? Es responsable especifico de una implementación?

Rol A (Accountability): Tiene que asegurar que las cosas que se hagan!!!

En la vision de procesos es clave la responsabilidad!!!

			Alta Dirección	3ª Linea de Defensa	2ª Linea de Defensa	2ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa
Ambito	Clausula	Actividad	Comité de Seguridad de la Información	Auditoria	Gestión de Riesgos	Oficial de Seguridad	Director de TI	Encargado del SGSI	Gerentes de TI	Responsables de Riesgos	Usuario Final
Contexto de la organización	4.1	Analisis del Contexto	A	I	R	R	C	R	C	C	I
Contexto de la organización	4.2	Analisis Partes Interesadas	A	I	C	C	C	R	C	C	I
Contexto de la organización	4.3	Alcance del SGSI	A/R	I	I	C	C	C	C	C	I
Contexto de la organización	4.4	SGSI	I	I	I	A	R	R	R	I	I
Liderazgo	5.1	Liderazgo y Compromiso	A/R	I	I	I	R	R	R	I	I
Liderazgo	5.2	Politica	A	I	C	C	R	R	C	I	I
Liderazgo	5.3	Roles y Responsabilidades	A	I	I	C	R	R	R	I	I
Planificación	6.1.2	Evaluación de Riesgos	C	I	R	R	C	A/R	C	R	C
Planificación	6.1.3	Tratamiento de Riesgos	R	I	R	R	R	A/R	R	R	R
Planificación	6.2	Objetivos de SGSI	C	I	I	C	A	R	C	I	I
Planificación	6.3	Planificación de Cambios	C	I	I	I	R	A/R	R	R	I
Soporte	7.1	Recursos	A/R	I	I	C	C	R	R	R	I
Soporte	7.2	Competencia	C	C	C	C	R	A/R	R	C	R
Soporte	7.3	Concienciación	C	C	C	C	R	A/R	R	C	R
Soporte	7.4	Comunicación	C	I	C	C	R	A/R	R	I	I
Soporte	7.5	Documentación	R	I	C	R	R	R	R	R	I
Operación	8.1	Planificación y control operacional	C	I	I	C	R	A/R	R	R	I
Operación	8.2	Evaluación de Riesgos	I	I	I	C	R	A/R	R	R	I
Operación	8.3	Tratamiento de Riesgos	I	I	I	C	R	A/R	R	R	I
Evaluación	9.1	Segumiento, medición, analisis y evaluación	C	I	I	C	R	A/R	R	R	I
Evaluación	9.2	Auditoría Interna	A	R	C	C	R	R	R	R	I
Evaluación	9.3	Revisión por la Dirección	A/R	C	C	C	C	R	C	C	I
Mejora	10.1	Mejora Continua	A	C	C	C	R	R	R	R	I
Mejora	10.2	No Conformidades	C	C	C	C	R	A/R	R	R	I

Nota: Este SGSI tiene como alcance en un área de TI

Ejemplo: Revisión de Politicas

¿Necesito un Proceso?

Planificar

- Cuando hacerlo?
- Input claves
- Liderazgo

Hacer

- Realizarlo conforme a lo establecido
- Actualización Periódica
- Comunicar las políticas

Verificar

- Se han actualizado las políticas?
- Se alinean a las necesidades organizacionales?

Actuar

- Vamos por buen camino
- Se han cumplido los compromisos

Cuestionamientos claves

- Tenemos las competencias para abordar estos procesos?
- Lo haremos con consultoría? de que forma?
- Somo capaces de asumir las responsabilidades?
- Cuantos procesos debemos implementar?
- Sabemos que realmente estamos haciendo?

Principio UNO!!!!

Es un importante cambio que debe realizar en la organización, requiere prácticas de gestión ad-hoc

Debe gestionar la implementación como un Proyecto, empleando metodologías ad-hoc

La Implementación de un Sistema de Gestión se basa en el Ciclo PDCA

#01	La implementación del SGSI no sólo involucra a TI, deber ser abordado desde una perspectiva integral y con buenas prácticas de gestión

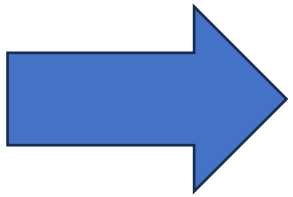
Estructura de Procesos del SGSI (Parte 2)

¿Como avanzar de manera agil?

- Entendiendo lo que se debe hacer en un SGSI
  - Comprensión de las clausulas
  - Comprensión de los entregables relacionados
  - Competencias de personas

- Definiendo roles y responsabilidades
  - A nivel de clausulas
  - A nivel de actividades

- Estableciendo definiciones simples de un proceso
  - Roles que entiendas su responsabilidad
  - Responsabilidades con capacidades asociadas
  - Entregables con responsabilidades claras



OBJETIVO:

Implementar los requisitos de la norma

Ejemplo 1: Analisis del Contexto

Clausula	Requisito	Actividad requerida	Medios de Verificación
4.1	Comprensión de la organización y de su contexto	La organización determina cuestiones externas e internas relevantes para su propósito y que afectan su capacidad para lograr los resultados previstos del sistema de gestión de seguridad de la información (SGSI)	Contexto Externo: - Análisis PESTEL Contexto Interno: - Análisis Estratégico - Análisis FODA - Análisis Arquitectura Empresarial - Análisis de Riesgos (Alto Nivel) - Análisis GAP

Debo describir en mi proceso como realizo las actividades específicas asociados a los entregables (Medios de Verificación)?

Ejemplo 2: Analisis de Partes Interesadas

Clausula	Requisito	Actividad requerida	Medios de Verificación
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	La organización determina las partes interesadas relevantes para el SGSI y sus requisitos relevantes para la seguridad de la información	- Identificación de Partes Interesadas - Clasificación de Partes Interesadas - Mapas de relación Influencia/Interés - Requisito de Seguridad - Requisitos de Negocio - Requisitos de Servicios/Productos - Requisitos de Clientes - Requisitos de Reguladores - Mapeo de Requisitos con el SGSI

Debo describir en mi proceso como realizo las actividades específicas asociados a los entregables (Medios de Verificación)?

Clausula Liderazgo

Clausula	Requisito	Actividad requerida	Medios de Verificación
5.1	Liderazgo y Compromiso	La alta dirección demuestra liderazgo y compromiso con respecto al SGSI.	- Definición de objetivos - Plan de implementación - Presupuesto - Modelo de Gobernanza
5.2	Política	La alta dirección establece una política de seguridad de la información	- Política de Seguridad de la Información - Plan de comunicación y concientización
5.3	Roles, responsabilidades y autoridades organizacionales	La alta dirección asegura que las responsabilidades y autoridades para los roles relevantes para la seguridad de la información se asignen y se comuniquen en toda la organización.	- Organigrama - Modelo Roles y responsabilidades - Perfiles de Cargo Claves

Clausula Planificación

Clausula	Requisito	Actividad requerida	Medios de Verificación
6.1	Acciones para tratar los riesgos y oportunidades	La organización define y aplica un proceso de evaluación y tratamiento de riesgos de seguridad de la información.	- Política de Gestión de Riesgos - Marco de Gestión de Riesgo - Proceso de Gestión de Riesgo - Matriz de Riesgos - Plan de Tratamiento de Riesgos - Declaración de Aplicabilidad de Controles (SoA)
6.2	Objetivos de seguridad de la información y planificación para su consecución	La organización establece objetivos de seguridad de la información y planea alcanzarlos en las funciones y niveles relevantes.	- Objetivos del SGSI - Mapa de KPI - Cuadro de Mando Integral - Plan de implementación - Proceso de Evaluación de Performance
6.3	Planificación de cambios	La organización realiza de manera planificada la implementación de cambios en el SGSI	- Proceso de Mejora Continua

Clausula Soporte

Clausula	Requisito	Actividad requerida	Medios de Verificación
7.1	Recursos	La organización determina y proporciona los recursos para establecer, implementar, mantener y mejorar continuamente el SGSI.	- Plan de implementación - Presupuesto
7.2	Competencia	La organización determina la competencia de las personas necesarias para el desempeño de la seguridad de la información y asegura que las personas sean competentes.	- Perfiles de Cargo Claves - DNC (Detección de necesidades de capacitación) - Plan de capacitación - Plan de concienciación - Desarrollo de actividades de concienciación y capacitación
7.3	Concienciación	La organización informa a las personas sobre la política de seguridad de la información, su contribución a la eficacia del SGSI, los beneficios de mejorar la seguridad de la información y las implicaciones de no cumplir con los requisitos del SGSI.	
7.4	Comunicación	La organización determina las necesidades de comunicaciones internas y externas relacionadas con el SGSI.	- Proceso de Comunicaciones - Plan de Comunicaciones
7.5	Información documentada	La organización incluye información documentada en el SGSI según lo requiere directamente la norma ISO 27001, así como también lo determina la organización como necesaria para la eficacia del SGSI	- Proceso de Gestión Documental - Plantillas de Documentos - Maestro de Documentos

Clausula Soporte y Operación

Clausula	Requisito	Actividad requerida	Medios de Verificación
8.1	Planificación y control operacional	La organización planifica, implementa y controla los procesos, sus requisitos y documentación requerida, de forma interna como externa, para alcanzar sus objetivos y gestionar los riesgos de seguridad de la información.	- Plan de implementación - Plan de Tratamiento de Riesgos
8.2	Evaluación de los riesgos de seguridad de la información	La organización efectúa evaluaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes	- Proceso de Gestión de Riesgo - Matriz de Riesgos - Plan de Tratamiento de Riesgos
8.3	Tratamiento de los riesgos de seguridad de la información	La organización implementa el plan de tratamiento de los riesgos de seguridad de la información.	- Plan de implementación - Plan de Tratamiento de Riesgos

Clausulas Evaluación

Clausula	Requisito	Actividad requerida	Medios de Verificación
9.1	Seguimiento, medición, análisis y evaluación	La organización realiza el seguimiento, medición, análisis y evaluación del SGSI para determinar su desempeño y eficacia.	- Objetivos del SGSI - Mapa de KPI - Cuadro de Mando Integral - Plan de implementación
9.2	Auditoría interna	La organización realiza auditorías internas a intervalos planificados en los procesos y riesgos claves de la seguridad de la información	- Proceso de Auditoría - Plan de auditoría - Programas de auditoría - Informes de auditoría - Informes de seguimiento
9.3	Revisión por la dirección	La dirección realiza revisiones periódicas de los resultados de la gestión de seguridad de la información y tomas las acciones necesarias para la mejora continua.	- Plan de Revisión de Dirección - Plantilla de Presentación - Actas de Revisión

Clausula Mejora

Clausula	Requisito	Actividad requerida	Medios de Verificación
10.1	Mejora continua	La organización establece un proceso para mejora la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.	- Procesos de Mejora Continua - Plan de Implementación
10.2	No conformidad y acciones correctivas	La organización establece un proceso para gestionar de manera oportuna las no conformidad y oportunidades de mejoras, realizando los análisis de causas necesarios para su identificación	- Proceso de Gestión de no conformidades - Análisis de causas - Cierre de no conformidades

En la vision de procesos es clave la responsabilidad!!!

			Alta Dirección	3ª Linea de Defensa	2ª Linea de Defensa	2ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa	1ª Linea de Defensa
Ambito	Clausula	Actividad	Comité de Seguridad de la Información	Auditoria	Gestión de Riesgos	Oficial de Seguridad	Director de TI	Encargado del SGSI	Gerentes de TI	Responsables de Riesgos	Usuario Final
Contexto de la organización	4.1	Analisis del Contexto	A	I	R	R	C	R	C	C	I
Contexto de la organización	4.2	Analisis Partes Interesadas	A	I	C	C	C	R	C	C	I
Contexto de la organización	4.3	Alcance del SGSI	A/R	I	I	C	C	C	C	C	I
Contexto de la organización	4.4	SGSI	I	I	I	A	R	R	R	I	I
Liderazgo	5.1	Liderazgo y Compromiso	A/R	I	I	I	R	R	R	I	I
Liderazgo	5.2	Politica	A	I	C	C	R	R	C	I	I
Liderazgo	5.3	Roles y Responsabilidades	A	I	I	C	R	R	R	I	I
Planificación	6.1.2	Evaluación de Riesgos	C	I	R	R	C	A/R	C	R	C
Planificación	6.1.3	Tratamiento de Riesgos	R	I	R	R	R	A/R	R	R	R
Planificación	6.2	Objetivos de SGSI	C	I	I	C	A	R	C	I	I
Planificación	6.3	Planificación de Cambios	C	I	I	I	R	A/R	R	R	I
Soporte	7.1	Recursos	A/R	I	I	C	C	R	R	R	I
Soporte	7.2	Competencia	C	C	C	C	R	A/R	R	C	R
Soporte	7.3	Concienciación	C	C	C	C	R	A/R	R	C	R
Soporte	7.4	Comunicación	C	I	C	C	R	A/R	R	I	I
Soporte	7.5	Documentación	R	I	C	R	R	R	R	R	I
Operación	8.1	Planificación y control operacional	C	I	I	C	R	A/R	R	R	I
Operación	8.2	Evaluación de Riesgos	I	I	I	C	R	A/R	R	R	I
Operación	8.3	Tratamiento de Riesgos	I	I	I	C	R	A/R	R	R	I
Evaluación	9.1	Segumiento, medición, analisis y evaluación	C	I	I	C	R	A/R	R	R	I
Evaluación	9.2	Auditoría Interna	A	R	C	C	R	R	R	R	I
Evaluación	9.3	Revisión por la Dirección	A/R	C	C	C	C	R	C	C	I
Mejora	10.1	Mejora Continua	A	C	C	C	R	R	R	R	I
Mejora	10.2	No Conformidades	C	C	C	C	R	A/R	R	R	I

Nota: Este SGSI tiene como alcance en un área de TI

En la vision de procesos es clave la responsabilidad!!!

Rol	Actividad	Responsabilidad	
Comité de Seguridad de la Información	Analisis del Contexto	- Garantizar el desarrollo periodico y cuando existan cambios relevantes en el contexto interno o interno de la organización. - Evaluar los resultados del analisis del contexto, comprender las brechas, las oportunidades y consecuencias. - Monitorear las acciones llevadas a cabos para gestionar potenciales riesgos derivados del analisis del contexto.	A
Gestión de Riesgos	Analisis del Contexto	- Proveer información relevantes del contexto de riesgos interno y externo. - Alertar frente a cambios en el contexto interno y externos que puedan afectar los resultados del SGSI. - Monitorear las acciones llevadas a cabos para gestionar potenciales riesgos derivados del analisis del contexto.	R
Oficial de Seguridad	Analisis del Contexto	- Proveer información relevantes del contexto de riesgos interno y externo. - Alertar frente a cambios en el contexto interno y externos que puedan afectar los resultados del SGSI. - Monitorear las acciones llevadas a cabos para gestionar potenciales riesgos derivados del analisis del contexto.	R
Director de TI	Analisis del Contexto	- Proveer información relevantes del contexto de riesgos interno y externo. - Alertar frente a cambios en el contexto interno y externos que puedan afectar los resultados del SGSI. - Monitorear las acciones llevadas a cabos para gestionar potenciales riesgos derivados del analisis del contexto.	C
Encargado del SGSI	Analisis del Contexto	- Desarrollar el analisis del contexto interno y externos con los instrumentos pertinentes. - Validar el analisis del contexto interno y externo con las partes interesadas. - Comunicar a la partes interesadas la formalización del analisis del contexto. - Actualizar el analisis del contexto interno y externo frente a cambios que puedan actualizar los resultados del SGSI. - Monitorear las acciones realizadas para gestionar potenciales riesgos derivados del analisis del contexto.	R
Gerentes de TI	Analisis del Contexto	- Proveer información relevantes del contexto de riesgos interno y externo. - Alertar frente a cambios en el contexto interno y externos que puedan afectar los resultados del SGSI.	C
Responsables de Riesgos	Analisis del Contexto	- Proveer información relevantes del contexto de riesgos interno y externo. - Alertar frente a cambios en el contexto interno y externos que puedan afectar los resultados del SGSI.	C

Definición de Actividades Claves!!!

Definición de Actividades

SubProceso	Clausulas	Actividades
Análisis del Contexto	4.1 Comprensión de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas	1.- El responsable del SGSI establecerá la coordinación de las actividades para el desarrollo del Análisis del Contexto Externo e Interno y el Análisis del Partes Interesadas. 2.- El responsable del SGSI desarrollará los registros formales asociados al Análisis del Contexto Interno, Contexto Externo y Partes Interesadas, desarrollando una presentación ejecutiva para su presentación al Comité de Seguridad de la Información 3.- El responsable del SGSI enviará a los miembros del Comité de Seguridad de la Información los registros asociados y presentación ejecutiva desarrollada, con al menos 15 días de anticipación a la próxima sesión del Comité 4.- El responsable realizará la presentación al Comité de Seguridad de la Información, quienes deberán validar los análisis desarrollados y realizar sus observaciones, las cuales deben estar resueltas para la próxima sesión del Comité.

→ Planificación

→ Ejecución

→ Verificación

→ Actuar

Definición de Actividades

SubProceso	Clausulas	Actividades
Objetivos y Planificación	5.1 Liderazgo y compromiso 6.2 Objetivos de seguridad de la información y planificación	1.- El responsable del SGSI empleando los registros obtenidos del Análisis del Contexto, Planificación Estratégica y lineamientos estratégicos de Tecnologías de Información formulará los Objetivos Generales, Objetivos Específicos y Planificación Estratégica del SGSI. 2.- El responsable del SGSI desarrollará los registros formales asociados los Objetivos Generales, Objetivos Específicos y Planificación Estratégica del SGSI, desarrollando una presentación ejecutiva para su presentación al Comité de Seguridad de la Información 3.- El responsable del SGSI enviará a los miembros del Comité de Seguridad de la Información los registros asociados y presentación ejecutiva desarrollada, con al menos 15 días de anticipación a la próxima sesión del Comité 4.- El responsable realizará la presentación al Comité de Seguridad de la Información, quienes deberán validar los análisis desarrollados y realizar sus observaciones, las cuales deben estar resueltas para la próxima sesión del Comité. 5.- En el caso de cambios relevantes en los Objetivos Generales, Objetivos Específicos y Planificación Estratégica del SGSI , el responsable del SGSI deberá presentar dichos cambios al Comité en la sesión más cercana, siguiendo el ciclo de validación establecido en el paso 3..

→ Planificación

→ Ejecución

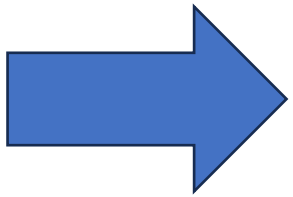
→ Verificación

→ Actuar

→ Mejora Continua

¿Como avanzar de manera agil?

- Planificación
  - Plazos
  - Responsable
- Hacer
  - Foco en instrumentos y resultados
  - Procesos, controles, tecnologías y personas
  - Gestionar riesgos criticos
- Verificar
  - Revisión de Indicadores
  - Revisión de la Dirección
- Mejora
  - Resultados de la Revisión
  - Acciones concretas de desarrollar



OBJETIVO:

Implementar los requisitos de la norma

21 Pasos de Implementación

1.- Creación de la Urgencia

2.- Formar una coalición

3.- Comprender el Estado Actual

4.- Entender el Contexto

5.- Formulación de Objetivos

6.- Plan de Implementación

7.- Formalización de Comité de Seguridad de la Información

8.- Programa de capacitación, entrenamiento y concientización

9.- Definir la Gobernanza y Gestión de la Seguridad de la Información

10.- Establecimiento del Política de Seguridad

11.- Implementación de procedimientos de apoyo del SGSI

12.- Implementación de procedimientos y controles bases del SGSI

13.- Definir Metodología e Implementación de Apreciación de Riesgos

14.- Desarrollar el Plan de Tratamiento de Riesgos

15.- Implementación de Políticas, Procedimientos y Controles

16.- Gestión de Indicadores de Performance

17.- Monitoreo del SGSI

18.- Auditoría al SGSI

19.- Revisión de la Dirección al SGSI

20.- Mejora Continua

21.- Preparación para la Auditoría Certificación

1.- Creación de Urgencia

Prever lo que pasará a futuro, para bien y para mal

PARA MAL

- ¿Cumplimos actualmente con la Ley?
- ¿En el sector hay ciberataques?
- ¿Estamos expuestos actualmente?
- ¿Cuál es el potencial impacto?
  - ¿Si perdemos datos sensibles?
  - ¿Se paralizaría nuestra operación?
  - ¿Podríamos afectar a pacientes?
- ¿Cómo responderíamos a un ciberataque?

PARA BIEN

- ¿Tenemos las capacidades internas?
- ¿Cuál es nuestro estado actual?
- ¿Qué es lo que debemos hacer?
- ¿Cómo mejorar nuestras falencias?
- ¿Qué recursos se necesitan?
- ¿Cómo armamos un plan?
- ¿Quiénes nos pueden ayudar?
- ¿Cuánto demorará la implementación?

#02	Lograr que los directivos y tomadores de decisión se den cuenta que sería un error no realizar cambios necesarios, que lleguen a las mismas conclusiones.

Casos de Negocio

- Algo simple, pero contundente
- Plantee algunos escenarios representativos
- Identifique algunos riesgos claves
- Identifique los potenciales efectos
- El análisis BIA es un buen amigo
- Considere la realidad organizacional
- Plantee algo realista
- Tenga claro a quien va dirigido
  - Ver Lección Aprendida 3

Casos de Negocio

Ciberataques

Fuga de Información

Casos de Negocio

Ingeniería Social

Fraude del CEO

Casos de Negocio

Continuidad del Negocio

Proveedores Criticos

2.- Formar una coalición

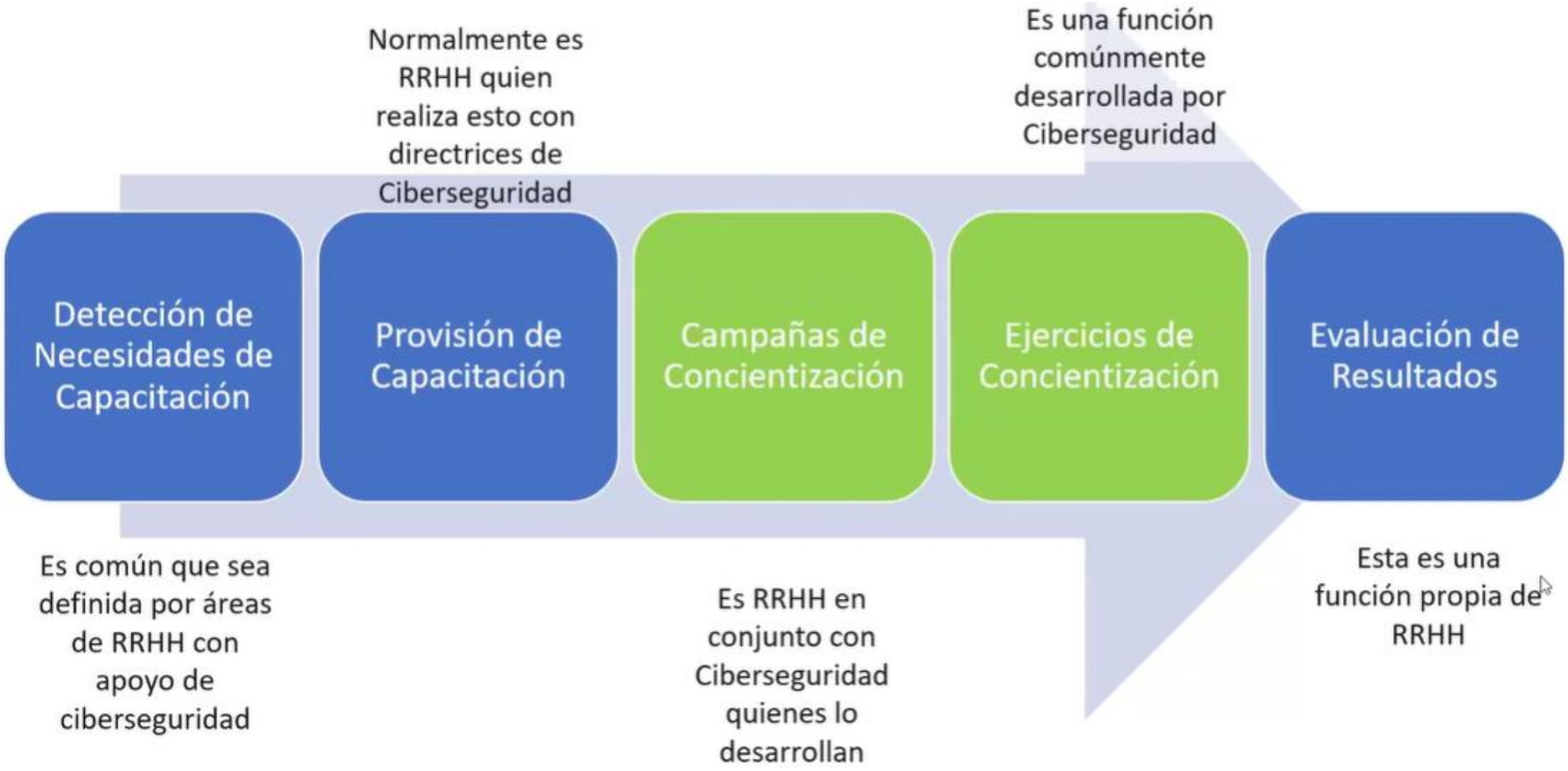
- No es solo una función de TI ni de Ciberseguridad
- El impacto en los procesos claves de negocio es una forma de buscar potenciales aliados
- Quienes manejan información sensible son buenos candidatos
- Áreas administrativas tienen un rol importante: RRHH, Operaciones, Adquisiciones, entre otros.

#03	Articular un equipo de trabajo representativo que comparta la misma visión y hacerles participe del cambio, involucrarlos y trabajar juntos.

Caso 1: Definición de Politicas de Ciberseguridad

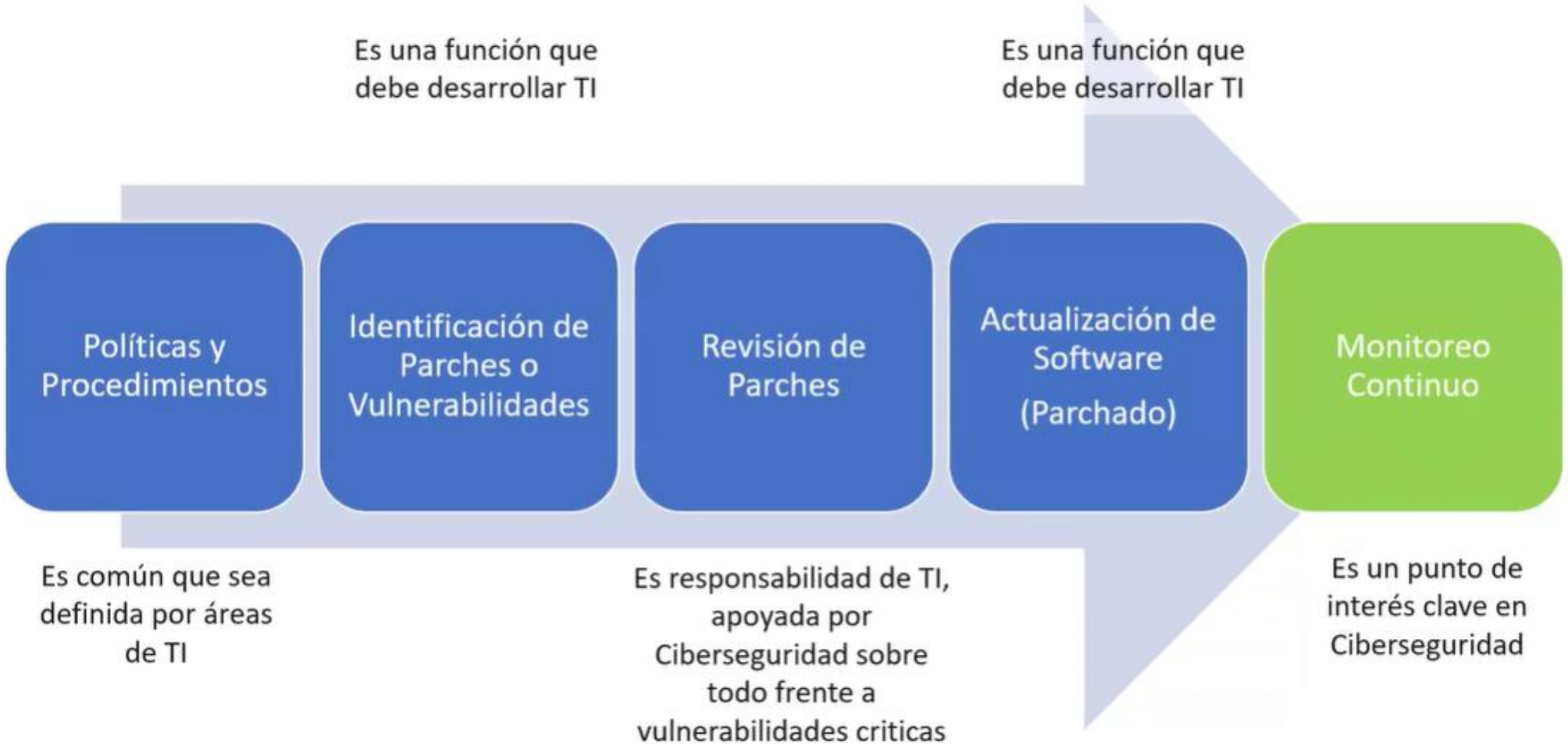
Caso 2: Protección de Malware

Caso 3: Capacitación y Concientización

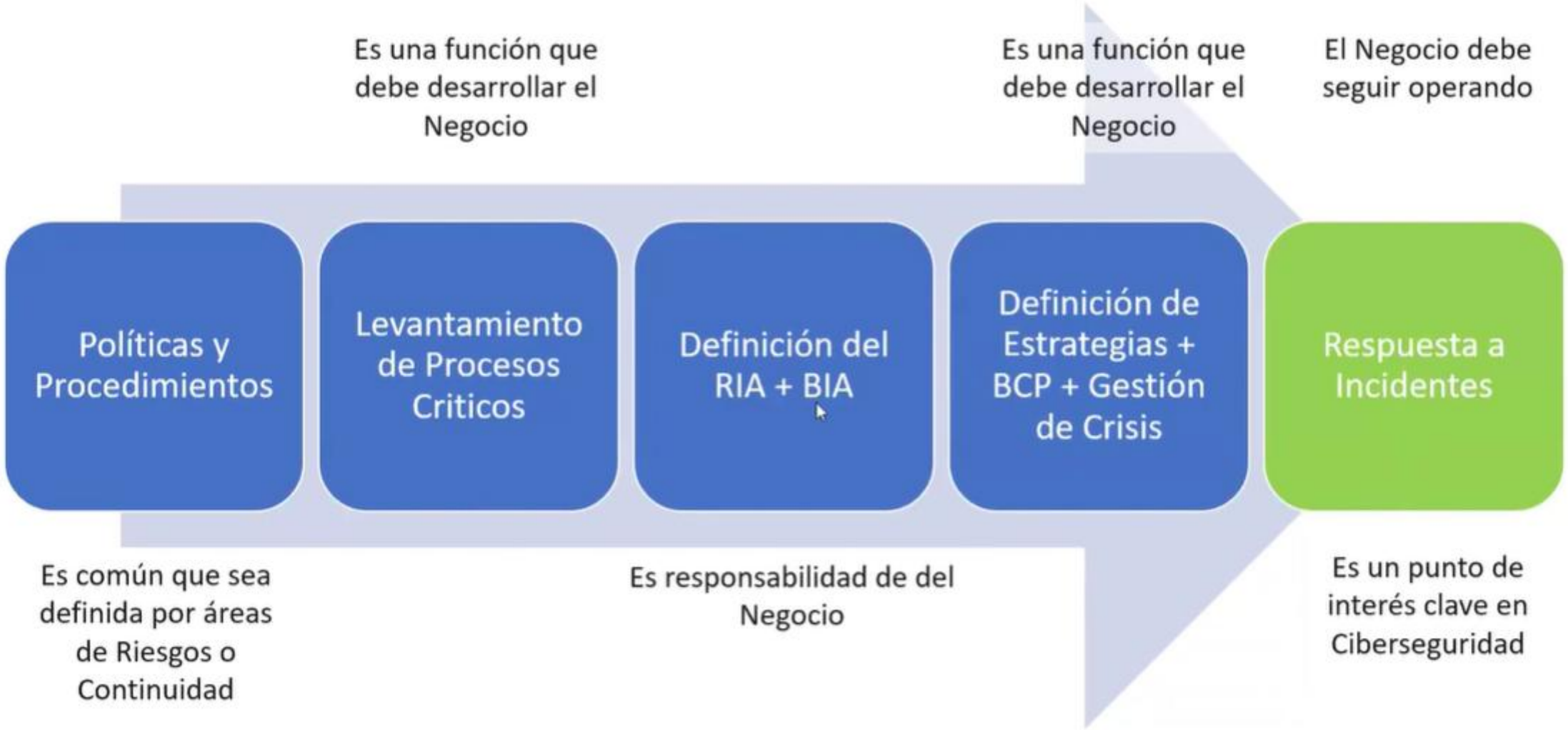


Caso 4: Control de Accesos

Caso 5: Gestión de Vulnerabilidades



Caso 5: Continuidad del Negocio



2.- Formar una coalición

- No es solo una función de TI ni de Ciberseguridad
- El impacto en los procesos claves de negocio es una forma de buscar potenciales aliados
- Quienes manejan información sensible son buenos candidatos
- Áreas administrativas tienen un rol importante: RRHH, Operaciones, Adquisiciones, entre otros.

#03	Articular un equipo de trabajo representativo que comparta la misma visión y hacerles participe del cambio, involucrarlos y trabajar juntos.

3.- Comprender el Estado Actual

Uso de Check List

CMMC Levels, Processes and Practices

Uso de Modelos de Madurez

Estudios Comparativos

#04	Realice evaluaciones realistas de las brechas y capacidades, considerando los aspectos de mejora priorizados que deben ser desarrollados.

4.- Comprender el Contexto Externo

#05	Desarrolle el análisis centrado en la organización y con una visión de negocio, el publico objetivo es la dirección y que comprenda potenciales riesgos.

4.- Comprender el Contexto Interno

#06	Sea objetivos en los análisis, su organización probablemente tenga muchas debilidades, reconocerlas es un paso fundamental.

5.- Formulación de Objetivos

1.- Creación de la Urgencia

2.- Formar una coalición

3.- Comprender el Estado Actual

4.- Entender el Contexto

→ Acciones concretas a desarrollar para subsanar brechas

#07	Sea coherente con las necesidades identificadas y su realidad, la formulación de un alcance y expectativas realista ayudará en el éxito.

Matriz de Analisis FODA

Estrategias FO	Estrategias FA	Estrategias DO	Estrategias DA
También conocidas como estrategias de éxito. Consiste en determinar cómo usar las fortalezas para aprovechar las oportunidades	También conocidas como estrategias de reacción. Consiste en determinar cómo usar las fortalezas para mitigar las amenazas	También conocidas como estrategias de adaptación. Consiste en determinar cómo usar las oportunidades para corregir las debilidades	También conocidas como estrategias de supervivencia. Consiste podemos mantenernos a pesar de las debilidades y las amenazas.

Matriz de Analisis FODA

MATRIZ FODA	FORTALEZAS	DEBILIDADES
OPORTUNIDADES	ESTRATEGIAS FO	ESTRATEGIAS DO
AMENAZAS	ESTRATEGIAS FA	ESTRATEGIAS DA

Sector Servicios

	FORTALEZAS		DEBILIDADES	
1	Flexibilidad laboral	1	Poca experiencia del equipo de trabajo
2	Alta capacidad de resolución de problemas	2	Falta de políticas, procedimientos y controles
3	Alta capacitación en sus colaboradores. Equipo certificado en ISO 27001	3	Definición de autoridad, responsabilidad y actividades poco clara, baja segregación de funciones
4	Compromiso y proactividad del equipo	4	Información no respaldada
5	Gran red de contactos	5	Postergación e improvisación en actividades
6	Buen ambiente laboral	6	Falta de medios de comunicación
7	Experiencia en modelos desarrollados y planes formativos de excelencia	7	Planificación, procesos y metodologías mejorables
8	Bajo costo de los servicios	8	Definición de política de licenciamiento de software
9	El "Know how" que posee la empresa	9	Poca explotación de la parte comercial

OPORTUNIDADES		ESTRATEGIA FO		ESTRATEGIA DO	
1	La globalización, expansión territorial en la entrega de sus servicios.	FO1	F3;F5;F7;F8;F9 y O1;O6;O7 Ampliar cartera de productos y cobertura geográfica	DO1	D2;D3;D5 y O6;O7 Desarrollar un plan estratégico y un modelo de cultura organizacional
2	Alto desempleo como incentivo a capacitarse				
3	Nuevas amenazas cibernéticas amplían la demanda de los servicios	FO2	F3;F4 y O3;O6;O7 Optimizar/capacitar constantemente al Capital Humano	DO2	D9; y O1;O2;O4 Mejorar la estructura financiera y comercial para abarcar un mayor mercado
4	Mayores regulaciones sectoriales y el alza en la globalizacion en temas de ciberseguridad	FO3	F5 y O2;O4 Generar nuevos clientes y crear bases de información sobre estos	DO3	D2;D4;D6;D7;D8 y O3;O5 Implementar planes, políticas y controles de seguridad de la información y continuidad del negocio.
5	Conexión 5G y beneficios para el teletrabajo				
6	Distribución de equipo en el centro-sur del país	FO4	F1;F4 y O5;O6 Reforzar trabajo flexible y por objetivos.	DO4	D1 y O3;O7 Potenciar/capacitar al personal, adoptar mejores procesos y metodologías para expandir la cartera de productos y servicios
7	Aumento de servicios y/o productos en la cartera.				
AMENAZAS		**ESTRATEGIA FA**		**ESTRATEGIA DA**	
1	Alta dependencia de servicios críticos, sin plan de continuidad operativa	FA1	F5;F7;F9 y A2;A5 Implementar la entrega de un servicio único e integrado	DA1	D2;D5;D7;D8 y A3;A4;A7 Implementar planes y políticas para la continuidad del negio y contingecias
2	Alta oferta de servicio/capacitacion online				
3	Exposición a eventos maliciosos que pueden afectar la continuidad del negocio			DA2	D7;D9 y A2;A5 Estructurar la organización para entregar un servicio único, de alto estándar, abarcando mayor mercado y a bajo costo
4	Posibles reclamos por derechos de autor de libros compartidos	FA2	F2;F8 y A1;A3;A4;A7 Implementar planes y políticas de continuidad de negocio y contingencias		
5	La oferta de servicios y/o productos similares			DA3	D1;D7 y A6 Optimizar/capacitar constantemente al Capital Humano
6	Avance constante de las tecnologías	FA3	F1;F4 y A6 Optimizar/capacitar constantemente al Capital Humano	DA4	D3; D5;D6 y A1 Definir roles, responsabilidades y uso de canales de comunicación.
7	Alta dependencia de nuestros partner				

6.- Plan de Implementación

The Objective

How to avoid failure in the implementation of national cybersecurity strategies

Cyber-Insecurity 3:

Absence of a dedicated cybersecurity budget

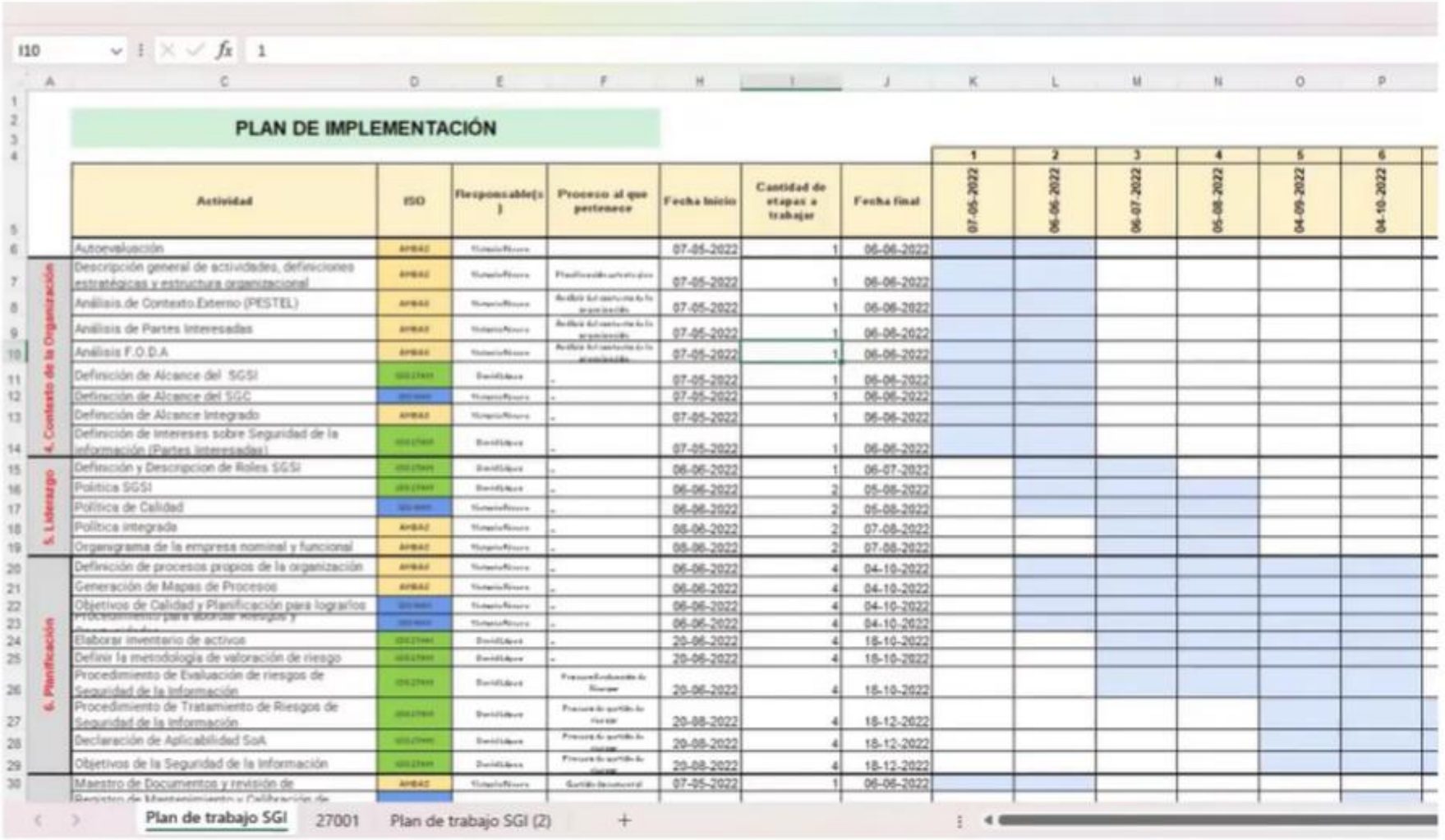
Solutions

- ✓ Create a dedicated budget line for cybersecurity
- ✓ Consider allocation of resources based on risk tolerance
- ✓ Provide contingency for changing technologies and mitigation in the event of the unexpected
- ✓ Consider mechanisms to ensure buy-in and implementation by all players

#08	Un plan de implementación implica establecer metas, pero también responsable y recursos (personas, tecnologías, servicios, recursos).

6.- Plan de Implementación

- Contexto + Planificación (1 mes)
- Definición de roles + política´+ organigrama (1 mes)
- Procesos Internos + inventario + matriz de riesgo + procesos SGSI (4 meses)
- Gestión documental (1 mes)
- Evolución y madurez de procesos + operación 5 meses)
- Evaluación del desempeño (3 meses)
- Mejora continua (1 mes)



PLAN DE IMPLEMENTACIÓN

	Actividad	ISO	Responsable(s)	Proceso al que pertenece	Fecha inicio	Cantidad de etapas a trabajar	Fecha final	1 07-05-2022	2 06-06-2022	3 06-07-2022	4 05-08-2022	5 04-09-2022	6 04-10-2022
4. Contexto de la Organización	Autoevaluación				07-05-2022	1	06-06-2022						
	Descripción general de actividades, definiciones estratégicas y estructura organizacional				07-05-2022	1	06-06-2022						
	Análisis de Contexto Externo (PESTEL)				07-05-2022	1	06-06-2022						
	Análisis de Partes Interesadas				07-05-2022	1	06-06-2022						
	Análisis F.O.D.A				07-05-2022	1	06-06-2022						
	Definición de Alcance del SGSI				07-05-2022	1	06-06-2022						
	Definición de Alcance del SGC				07-05-2022	1	06-06-2022						
	Definición de Alcance Integrado				07-05-2022	1	06-06-2022						
	Definición de Intereses sobre Seguridad de la información (Partes Interesadas)				07-05-2022	1	06-06-2022						
5. Liderazgo	Definición y Descripcion de Roles SGSI				06-06-2022	1	06-07-2022						
	Política SGSI				06-06-2022	2	05-08-2022						
	Política de Calidad				06-06-2022	2	05-08-2022						
	Política integrada				08-06-2022	2	07-08-2022						
	Organigrama de la empresa nominal y funcional				08-06-2022	2	07-08-2022						
6. Planificación	Definición de procesos propios de la organización				06-06-2022	4	04-10-2022						
	Generación de Mapas de Procesos				06-06-2022	4	04-10-2022						
	Objetivos de Calidad y Planificación para lograrlos				06-06-2022	4	04-10-2022						
	Procedimiento para abordar riesgos y				06-06-2022	4	04-10-2022						
	Elaborar inventario de activos				20-06-2022	4	18-10-2022						
	Definir la metodología de valoración de riesgo				20-06-2022	4	18-10-2022						
	Procedimiento de Evaluación de riesgos de Seguridad de la Información				20-06-2022	4	18-10-2022						
	Procedimiento de Tratamiento de Riesgos de Seguridad de la Información				20-08-2022	4	18-12-2022						
	Declaración de Aplicabilidad SoA				20-08-2022	4	18-12-2022						
	Objetivos de la Seguridad de la Información				20-08-2022	4	18-12-2022						
	Maestro de Documentos y revisión de				07-05-2022	1	06-06-2022						

Plan de trabajo SGI | 27001 | Plan de trabajo SGI (2)

8.- Programa de capacitación, entrenamiento y concientización

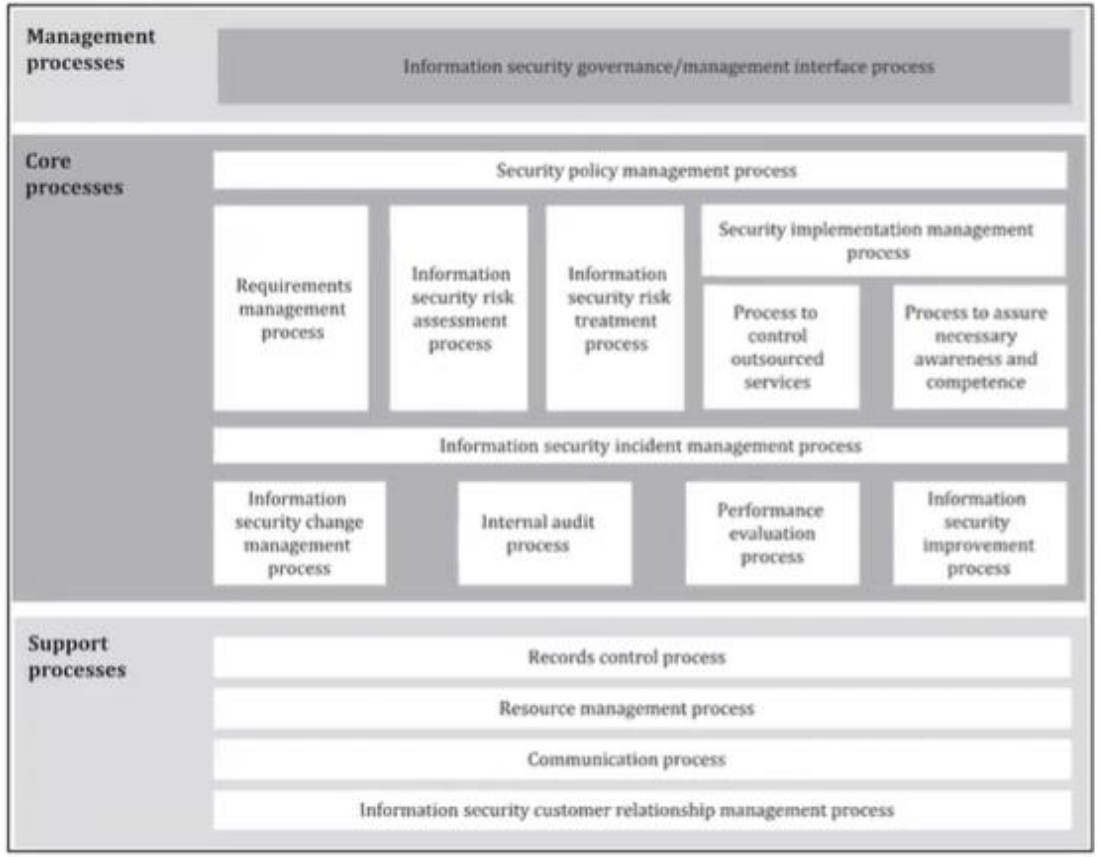
Tres Líneas de Defensa – The IIA

ENISA – Roles de Ciberseguridad

NICE Framework

#10	Considere un programa distintivo y orientado en los roles, tomadores de decisión, gerencial, roles específicos de ciberseguridad y usuarios generales.

11.- Implementación de procedimientos de apoyo del SGSI



- Procesos en general de adopción inicial:
  - Gestión Documental
  - Gestión de Comunicaciones
  - Gestión de Gobernanza
  - Gestión de Políticas de Seguridad
  - Auditoría Interna
  - Gestión de RRHH

- Son independiente de los Riesgos, los deberá implementar, ayudarán a generar rápidos resultados del proyecto.

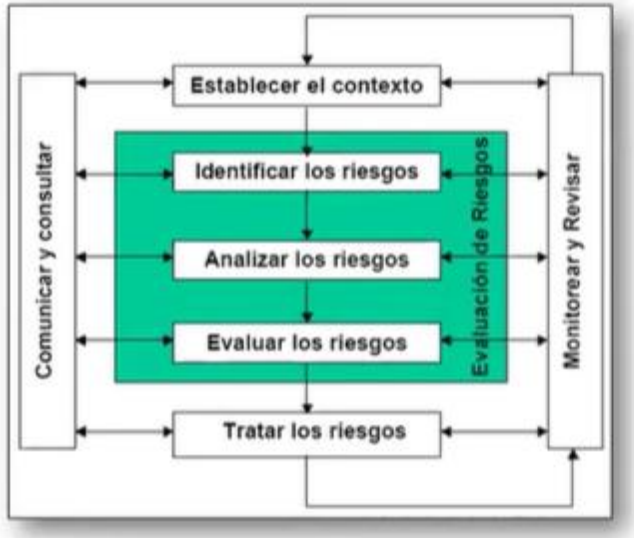
#13	La adopción de plantillas de procesos es una buena práctica, pero deben reflejar el quehacer organizacional, el copiar-pegar no sirve.

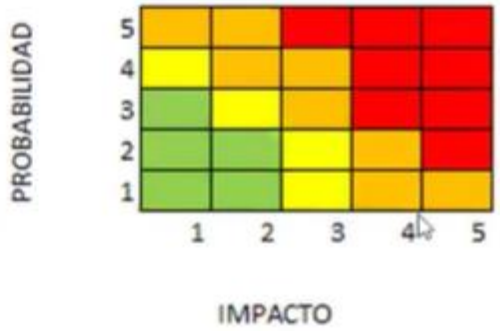
12.- Implementación de procedimientos de apoyo del SGSI

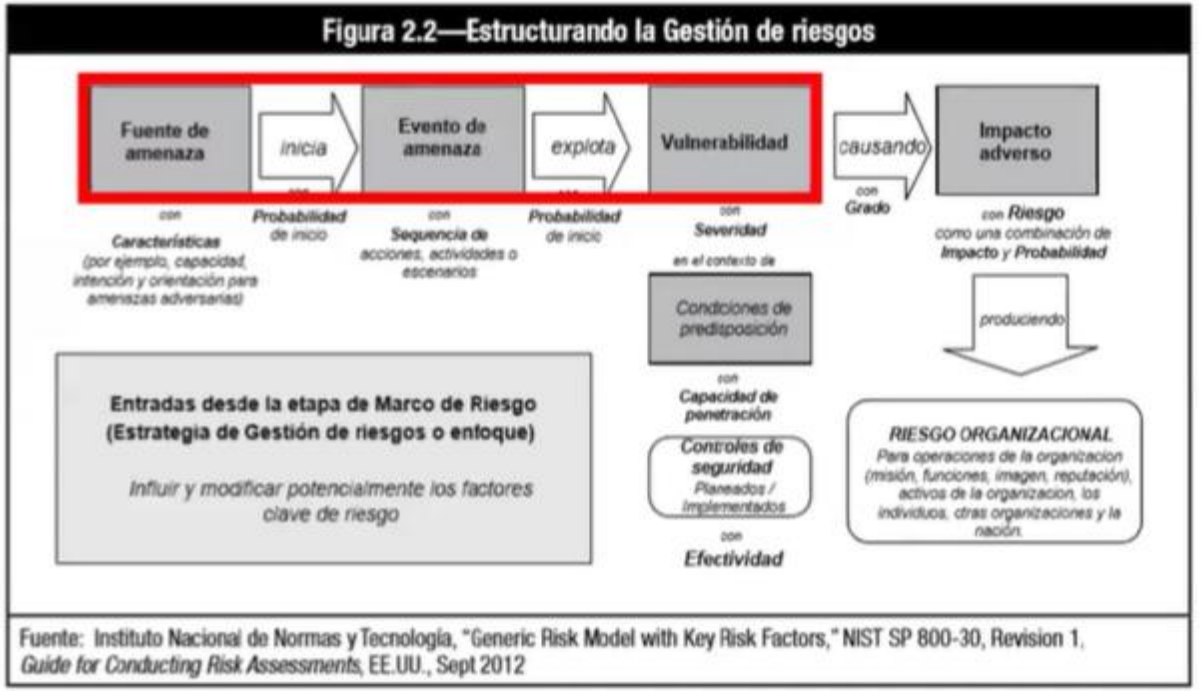
Política del SGSI	Política Teletrabajo	Política Uso de Activos	Política Desarrollo RRHH
Gestión de Incidentes	Continuidad del Negocio	Gestión de Proveedores	Gestión de Operaciones
Control de Acceso	Privacidad y Cumplimiento		

- Temas claves
  - Análisis del Contexto
  - Necesidades de Partes Interesadas
  - Contexto de Riesgos
  - Alcance
- Resultados
  - Procesos del SGSI implementado
  - PT Riesgos implementado
  - Aumento de la Madurez
- Desafíos
  - Revisión de la Dirección
  - Diseño y Monitoreo de Registros

13.- Definir Metodologia de Riesgos

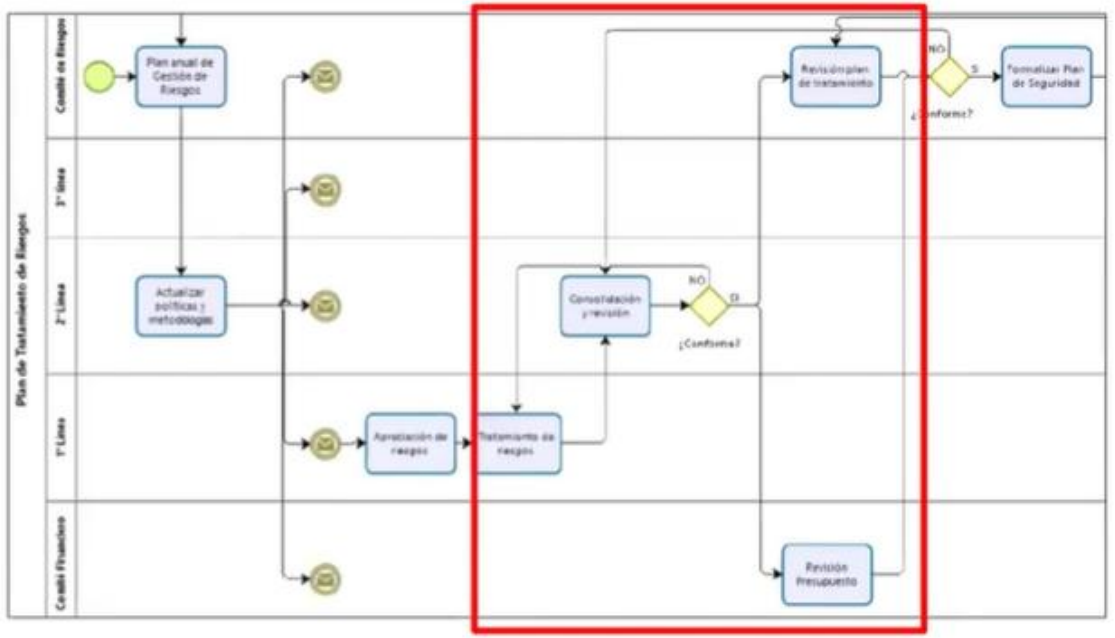






#15	El proceso y los instrumentos para la gestión de riesgos son aspectos de mayor complejidad en el SGSI, emplee modelos funcionales y considere la capacitación especial basada en casos a los responsables

14.- Desarrollar el Plan de Tratamiento de Riesgos



#16	La definición del proceso es simple, pero procure establecer los elementos de revisión y consolidación idóneos entre las partes.
#17	Cada plan de tratamiento de riesgos procure gestionarlo como proyecto, ayudará en su capacidad de gestión y monitoreo

15.- Implementación!!!

Se implementan de diversa forma, con diversos mecanismos y recursos.

#18	Establezca claramente los alcances de la implementación de controles, evalué la pertinencia de la documentación y el uso de recursos (persona, tecnologías, servicios, infraestructura, entre otros).

16.- Gestión de Indicadores - KPI

Deben medir una gestión que sea necesaria de controlar y pueda aportar en la mejora continua

Related ISMS processes and controls (Clause or control number in ISO/IEC 27001:2013)	Measurement construct example names
5.1, 7.1	B.2 Resource allocation
7.5.2, A.5.1.2	B.3 Policy review
5.1, 9.3	B.4 Management commitment
8.2, 8.3	B.5 Risk exposure
9.2, A.18.2.1	B.6 Audit programme
10	B.7 Improvement actions
10	B.8 Security incidents cost
10, A.16.1.6	B.9 Learning form information security incidents
10.1	B.10 Corrective action implementation
A.7.2	B.11 ISMS training or ISMS awareness
A.7.2.2	B.12 Information security training
A.7.2.1, A.7.2.2	B.13 Information security awareness compliance
A.7.2.2	B.14 ISMS awareness campaigns effectiveness
A.7.2.2, A.9.3.1, A.16.1	B.15 Social engineering preparedness
A.9.3.1	B.16 Password quality – manual
A.9.3.1	B.17 Password quality – automated
A.9.2.5	B.18 Review of user access rights
A.11.1.2	B.19 Physical entry controls system evaluation
A.11.1.2	B.20 Physical entry controls effectiveness
A.11.2.4	B.21 Management of periodic maintenance
A.12.1.2	B.22 Change management
A.12.2.1	B.23 Protection against malicious code
A.12.2.1	B.24 Anti-malware
A.12.2.1, A.17.2.1	B.25 Total availability
A.12.2.1, A.13.1.3	B.26 Firewall rules
A.12.4.1	B.27 Log files review
A.12.6.1	B.28 Device configuration
A.12.6.1, A.18.2.3	B.29 Pentest and vulnerability assessment
A.12.6.1	B.30 Vulnerability landscape
A.15.1.2	B.31.1/B.31.2 Security in third party agreements
A.16	B.32 Security incident management effectiveness
A.16.1	B.33 Security incidents trend
A 16.1.3	B.34 Security event reporting
A.18.2.1	B.35 ISMS review process
A.18.2.3	B.36 Vulnerability coverage

ISO 27004 –
Indicadores del SGSI

#19	Defínalos a un alto nivel de actividades (son claves), a nivel de procesos es una buena práctica, cuestiónese la utilidad y su pertinencia de uso, principalmente en la toma de decisiones.

17.- Monitoreo del SGSI

- Temas claves
  - Todo el personal es parte de la mejora continua
  - **Definición de objetivos en los procesos**
  - Responsables de procesos e indicadores
  - Revisión interna y permanente de documentación y registros
  - Fortalecer el desarrollo de auditorías internas
  - Articularlo al proceso de Acciones Correctivas y Preventivas
  - Fortalecer el rol de los Comités

- Desafíos
  - Evaluación de indicadores
  - La auditoría interna
  - Revisión de la dirección

18.- Auditoría al SGSI

Understand the Business	Define IT Universe	Perform Risk Assessment	Formalize Audit Plan
• Identify the organization's strategies & business objectives • Understand the high risk profile for the organization • Identify how the organization structures their business operations • Understand the IT service support model	• Dissect the business fundamentals • Identify significant applications that support the business operations • Identify critical infrastructure for the significant applications • Understand the role of supporting technologies • Identify major projects and initiatives • Determine realistic audit subjects	• Develop processes to identify risks • Assess risk and rank audit subjects using IT risk factors • Assess risk and rank subjects using business risk factors	• Select audit subjects and bundle into distinct audit engagements • Determine audit cycle and frequency • Add appropriate engagements based on management requests or opportunities for consulting • Validate the plan with business management

#21	Las capacidades de los auditores es una importante brecha a subsanar, la actividad es el clave para el aseguramiento y mejora del SGSI, principalmente en la evaluación de controles y actividades criticas.

19.- Revisión de la Dirección

#22	La revisión de la dirección debe ser periódica e integral, recogiendo todos los puntos de atención necesarios que signifiquen una potencial de brecha en los objetivos establecidos o una desviación, tomando decisiones oportunas para su corrección o fortalecimiento de medidas.

21.- Preparación para la Auditoria de Certificación

6 PASOS PARA LA CERTIFICACIÓN ISO/IEC 27001

Definición del alcance y ámbito de aplicación del SGSI.

Auditoría de certificación fase I: Planificación y definición de grado de preparación para certificación mediante auditoría in situ. Planificación Fase II.

Auditoría de certificación fase II
Planificación. Auditoría in situ .Trabajos post auditoría. Emisión certificado.

Auditoría de mantenimiento.

Auditoría de renovación.

#24	La inversión en la certificación es marginal en la implementación de un SGSI, tiende a aportar valor y compromiso a las partes interesadas

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Implementación de un SGSI

Workshop N°2

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD