Ingeniería de Sistemas

Alcance de un SGSI: La Declaración de aplicabilidad (SoA, Statement of applicability)

Seguridad de Sistemas de TI

2022-1

UNIVERSIDAD DE LIMA

Agenda

I. Alcance del SGSI

II. ¿Qué es la Declaración de aplicabilidad?

III. Importancia de la Declaración de aplicabilidad

IV. Necesidad de la Declaración de aplicabilidad

V. Derivaciones y Utilidad de Declaración de aplicabilidad

VI. Conclusiones

UNIVERSIDAD DE LIMA

I. ALCANCE DEL SGSI

Establecer el Alcance

- Realizar un análisis interno y externo de la organización. Se debe revisar el plan estratégico si existiera.
- Definir cual o cuales procesos serán considerados dentro del SGSI
- Especificar activos que participan
  - Listado de contratos y acuerdos
  - Mapas de red
  - Inventario de activos de información.

I. ¿Qué es la Declaración de Aplicabilidad?

¿Qué es la DdA?

- La «**Declaración de aplicabilidad**» (DdA) ó, en inglés, «***Statement of applicability***» (SoA), es uno de los elementos principales de un sistema de gestión de seguridad de la información.
- Consiste en un documento que relaciona los controles que se aplican en el sistema de gestión (mejor dicho, los que son aplicables en concepto de la empresa).

UNIVERSIDAD DE LIMA

¿Qué es la DdA?

- De la relación de 114 controles que la norma ISO/IEC 27001:2013 indica en su anexo "A", una organización debe seleccionar aquellos que ***debe*** implantar y mantener en su sistema.
- El resultado de la elección de los controles forma parte del «**Plan de tratamiento de riesgos**», de modo que éste tiene como salida la "***Declaración de aplicabilidad"***.

UNIVERSIDAD DE LIMA

Ejemplo de DdA

Statement of Applicability for ISO 27001:2013

Isms:	Sample Company ISMS		
Organisation:	Sample Company	Version:	1.0
Published:	18/02/2015 14:53:05	Publisher:	Sample User

A.5.1	Management direction for information security
Objective:	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Control	Title	Description	Applied
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes

Reason(s) for selection

Risk Assessment

Assets

Reputation
Backups

A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes

Reason(s) for selection

Risk Assessment

Assets

Reputation

A.6.1	Internal organization
Objective:	To establish a management framework to initiate and control the implementation and operation of information security within the organization.

UNIVERSIDAD DE LIMA

¿Qué es la DdA?

- Es importante reseñar que si no se aplica(n) alguno(s) de los 114 controles, la organización ***debe demostrar que ha analizado el riesgo de no implantarlo(s)***.

- Por otra parte, es normal que muchos de estos controles ya estén implantados por la empresa, porque de modo natural ya existen numerosas salvaguardas de seguridad desarrolladas en una compañía.

- También es interesante destacar que una empresa puede añadir controles adicionales a éstos 114 porque entiende que pueden faltar controles para cubrir ***sus objetivos*** de seguridad de la información.

UNIVERSIDAD DE LIMA

Otro ejemplo de DdA

Statement of Applicability-

ISO 27001 Compliance Checklist

Reference		Audit area, objective and question		Results	
Checklist	**Standard**	**Section**	**Audit Question**	**Findings**	**Status (%)**
Security Policy					
1.1	**5.1**	**Information Security Policy**			
1.1.1	5.1.1	Information security policy document	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.		
			Whether the policy states management commitment and sets out the organizational approach to managing information security.		
1.1.2	5.1.2	Review of Informational Security Policy	Whether the Information Security Policy is reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.		
			Whether the Information Security policy has an owner, who has approved management responsibility for development, review and evaluation of the security policy.		N/A (ref box value explanation at foot of spreadsheet)
			Whether any defined Information Security Policy review procedures exist and do they include requirements for the management review.		
			Whether the results of the management review are taken into account.		
			Whether management approval is obtained for the revised policy.		
Organization of Information Security					
2.1	**6.1**	**Internal Organization**			
2.11	6.11	Management Commitment to Informaiton Security	Whether management demonstrates active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities.		
2.1.2	6.1.2	Information Security coordination	Whether information security activities are coordinated by representatives from diverse parts of the organization, with pertinent roles and responsibilities		
2.1.3	6.1.3	Allocation of Information Security responsibilities	Whether responsibilities for the protection of individual assets, and for carrying out specific security processes, were clearly identified and defined.		
2.1.4	6.1.4	Authorization process for Information processing facilities	Whether management authorization process is defined and implemented for any new information processing facility within the organization.		
2.1.5	6.1.5	Confidentiality Agreements	Whether the organization's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed.		
			Does this address the requirement to protect the confidential information using legal enforceable terms		

UNIVERSIDAD DE LIMA

II. Importancia de la declaración de aplicabilidad

Relevancia de la DdA

- De hecho, la **Declaración de aplicabilidad** es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información. El objetivo de este documento es definir **cuáles** de los 114 controles (medidas de seguridad) sugeridos en el Anexo "A" de la norma ISO 27001 son los que usted implementará y, para los controles que correspondan, **cómo** se realizará su implementación.

UNIVERSIDAD DE LIMA

III. Necesidad de la Declaración de Aplicabilidad

Necesidad de la DdA (I)

- Ante todo, durante el tratamiento de riesgos se identificaron los controles que debían implementarse porque, primero, se identificaron los riesgos que era necesario disminuir.

- Sin embargo, en la **DdA** *también se debe identificar los controles necesarios por otras razones*; por ejemplo, por motivos legales, por requisitos contractuales, por otros procesos, etc.

UNIVERSIDAD DE LIMA

Necesidad de la DdA (II)

- El Informe sobre la evaluación de riesgos puede resultar bastante largo: algunas organizaciones pueden identificar algunos miles de riesgos (a veces, aún más); por eso, un documento de estas características no resulta realmente útil en el uso operativo diario.
- En cambio, la **Declaración de aplicabilidad** es bastante breve ya que tiene 114 filas (cada una representa un control); esto permite que pueda ser presentada ante la gerencia y que pueda ser actualizada.

Necesidad de la DdA (III)

- La **DdA** debe documentar si cada control aplicable ya está implementado o no.
- Una estrategia efectiva, y que la mayoría de los auditores buscará también, es describir cómo se implementa cada control aplicable; por ejemplo, haciendo referencia a un documento (política, procedimiento, instrucciones de funcionamiento, etc.) o detallando brevemente el procedimiento vigente o el equipo que se utiliza.

IV. Derivaciones y utilidad de la declaración de aplicabilidad

Derivaciones de la DdA

- De hecho, si solicita la certificación ISO 27001, el auditor de certificación solicitará toda la **información documentada** y su **Declaración de aplicabilidad** y recorrerá su empresa verificando si ha implementado los controles de la forma en que lo ha detallado en su **DdA**.
- Es el principal documento que utilizan para realizar la auditoría presencial.

Derivaciones de la DdA

- Muy pocas empresas se dan cuenta de que redactando una buena **Declaración de aplicabilidad** pueden disminuir la cantidad de otros documentos.
- Por ejemplo, si desea documentar un determinado control, pero la descripción del procedimiento para ese control resultase demasiado breve, lo puede incluir en la **DdA**. De esta forma, estaría evitando redactar otro documento.

Utilidad de la DdA

- Por experiencia, se puede afirmar que la mayoría de las empresas que implementan el sistema de gestión de seguridad de la información de acuerdo a la norma ISO 27001 dedican mucho más tiempo en redactar este documento que lo que habían previsto.
- El motivo es que deben pensar cómo implementarán sus controles: ¿Comprarán nuevos equipos? ¿Modificarán el procedimiento? ¿Contratarán un nuevo empleado? Estas son decisiones bastante importantes (y, a veces, costosas), por ello no sorprende que requiera mucho tiempo tomarlas.
- Lo bueno acerca de la **DdA** es que obliga a las organizaciones a hacer las cosas de forma sistemática.

Utilidad de la DdA

- Por lo tanto, no se debería tomar este documento simplemente como uno de esos "documentos innecesarios" que no tienen una utilidad real.
- Piense que es la principal declaración en la que usted define lo que desea hacer con su seguridad de la información.
- Si está redactada correctamente, la **DdA** es un resumen perfecto acerca de lo que se debe hacer en seguridad de la información, por qué se debe hacer y cómo se debe hacer.

UNIVERSIDAD DE LIMA

Conclusiones