



# UNINPAHU

# UNIVERSIDAD INPAHU

**PROGRAMA: ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA**

**FESTO INDUSTRIAS 4.0**

William Rene Alvarado Ordoñez

INGENIERO DE SISTEMAS, ESPECIALISTA EN SEGURIDAD  
INFORMATICA

CPTE, CDFE, ISO 27001AL, COBIT



# AGENDA

- Introducción
- Que es la norma ISO
- Tipos de Normas ISO Aplicadas a la seguridad de la Información y seguridad Informática.
- Que es la seguridad de la Información, Seguridad Informática y Ciberseguridad.
- Norma ISO 27001
- Preguntas e Inquietudes



# REGLAS DE JUEGO

- Asistencia 10%
- Trabajo 40%
- Laboratorios y Ejercicios 40%
- Laboratorios Virtuales 10

Dia 6H/5H			
	Desde		Hasta
1H	7:00:00 a. m.		7:45:00 a. m.
2H	7:45:00 a. m.		8:30:00 a. m.
3H	8:30:00 a. m.		9:15:00 a. m.
breake	9:15:00 a. m.		9:30:00 a. m.
4H	9:30:00 a. m.		10:15:00 a. m.
5H	10:15:00 a. m.		11:00:00 a. m.
6H	11:00:00 a. m.		11:45:00 a. m.
Alm	11:45:00 a. m.		12:30:00 p. m.
7H	12:30:00 p. m.		1:15:00 p. m.
8H	1:15:00 p. m.		2:00:00 p. m.
breake	2:00:00 p. m.		2:15:00 a. m.
9H	2:15:00 a. m.		3:00:00 a. m.
10H	3:00:00 a. m.		3:45:00 a. m.
11H	3:45:00 a. m.		4:30:00 a. m.



# QUE ES LA SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA

## SEGURIDAD DE LA INFORMACIÓN

- Medidas y actividades orientadas a proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.

## SEGURIDAD INFORMÁTICA

- Conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen.
- Dentro de esta categoría, se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos de una empresa por ejemplo.

## CIBERSEGURIDAD

- Conjunto de medidas de “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.



# PILARES DE SEGURIDAD DE LA INFORMACION



Preservar las restricciones autorizadas de acceso y divulgación,

La protección contra la modificación o destrucción inadecuada de la información

Asegurar el acceso y uso oportuno y confiable de la información



# PILARES DE SEGURIDAD DE LA INFORMACION



## Ejemplo:

Si a usted le abren las puertas de su automóvil sin que usted suministre las llaves, entonces el atacante le impacto la variable:

**CONFIDENCIALIDAD**

Pero si le hurtan el reproductor MP3/DVD el atacante impacto la variable:

**INTEGRIDAD**

Finalmente si le hurtan el carro la variable afectada es

**DISPONIBILIDAD**

# PILARES DE SEGURIDAD DE LA INFORMACIÓN

## Propiedades

## Ataque

Confidencialidad

Modificación: Web defacement

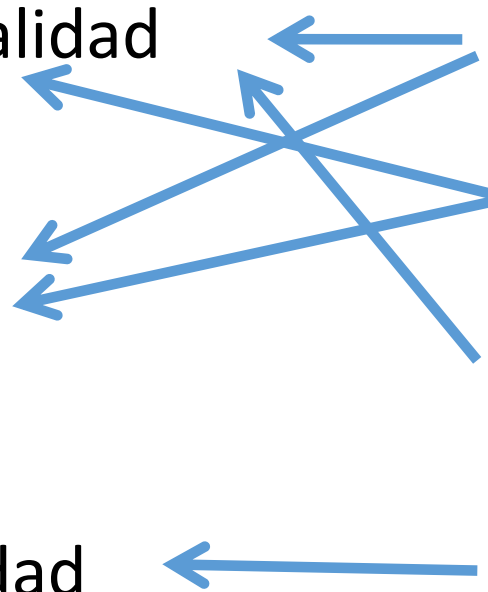
Integridad

Fabricación: Insertar nuevo usuario

Interceptación: Keylogger

Disponibilidad

Interrupción: DoS



# PILARES DE SEGURIDAD DE LA INFORMACIÓN

## Modificación:

También llamados **webdefacement** buscan comprometer la confidencialidad y la integridad del sistema, por ejemplo cuando un atacante modifica la página web de una organización sin previa autorización

## Fabricación:

Comprometen la integridad del sistema por ejemplo al insertar un nuevo usuario en el sistema operativo

## Interrupción:

Comprometen la propiedad Disponibilidad un ejemplo serian los ataques de denegación de servicios o DoS.

## Interceptación:

Un elemento no autorizado consigue un acceso a un determinado objeto









# ¿Qué es una norma ISO?

ISO es la Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales.

Se conoce por ISO tanto a la Organización como a las normas establecidas por la misma para estandarizar los procesos de producción y control en empresas y organizaciones internacionales.

**ISO 27017  
2015** Control de la seguridad de la información en la nube

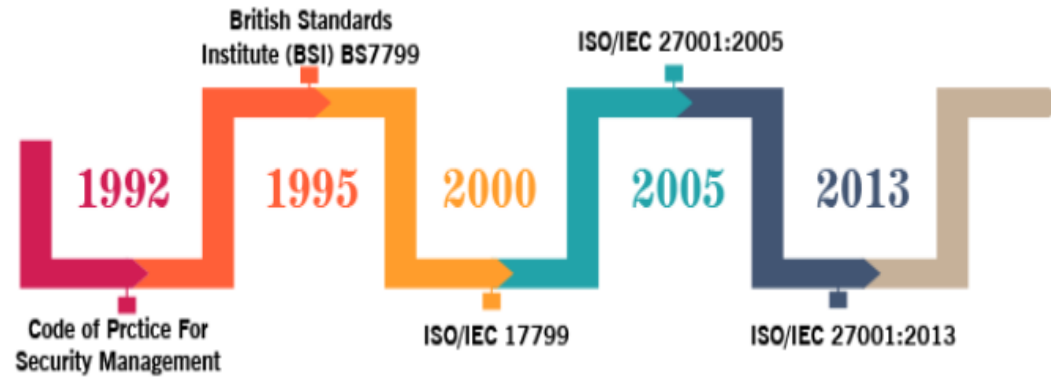
**ISO 27018  
2019** Requisitos para la protección de la información de personal en la Nube

CALIDAD	MEDIO AMBIENTE	RIESGOS Y SEGURIDAD	RESPONSABILIDAD SOCIAL
			
ISO 9001	ISO 14001	ISO 45001	SA 8000
ISO 9004	ISO 50001	ISO 22000	ISO 26000
ISO IEC 17025		ISO 22301	
ISO TS 16949		ISO 27001	
Sistemas Integrados de Gestión		ISO 28000	
		ISO 31000	
		ISO 39001	
		ISO 19600	

# ESTANDARES ISO

- **ISO 27000 SERIES**
- **ISO 27001:** Establecimiento, Implementación, Control y mejora del ISMS. Sigue el PDCA (Plan, Do, Check, Act)
- **ISO 27002:** Se ha sustituido la ISO 17799. Proporciona consejos prácticos sobre cómo implementar controles de seguridad. Utiliza 10 dominios para dirigir ISMS.
- **ISO 27004:** Proporciona métricas para medir el éxito de ISMS
- **ISO 27005:** Un enfoque basado en normas para la gestión de riesgos
- **ISO 31000** Un enfoque basado en normas para la gestión de riesgos  
**nos gestionar los riesgos – de cualquier tipo – en las organizaciones**

# ISO 27001-2005



2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005:  
Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

ISO/IEC 27001:2005		ISO/IEC 27001:2013
NUMERO DE CONTROLES		
133	114	94 Se Mantienen 39 Eliminados 20 Nuevos
DOMINIOS DE SEGURIDAD		
11	14	3 DOMINIOS NUEVOS
REQUISITOS DE GESTION		
102	130	18 REQ-GEST NUEVOS



## QUE ES UN SGSI

- Sistema de Gestion de seguridad de la Información
- Un **Sistema de Gestión de la Seguridad de la Información (SGSI)** es un conjunto de políticas de administración de la información. El término se denomina en Inglés «Information Security Management System» (ISMS).
- El término SGSI es utilizado principalmente por la **ISO/IEC 27001**, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission.



# INTRODUCCIÓN

- **GENERALIDADES**

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple.

[https://www.youtube.com/watch?v=zJhHZl3MB\\_U](https://www.youtube.com/watch?v=zJhHZl3MB_U)

<https://www.youtube.com/watch?v=FOXyXuEtjME>



# INTRODUCCIÓN

- **ENFOQUE BASADO EN PROCESOS**

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización.



- **ENFOQUE BASADO EN PROCESOS**

Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades.

Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso

constituye directamente la entrada del proceso siguiente.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un “enfoque basado en procesos”.

# ENFOQUE BASADO EN PROCESOS

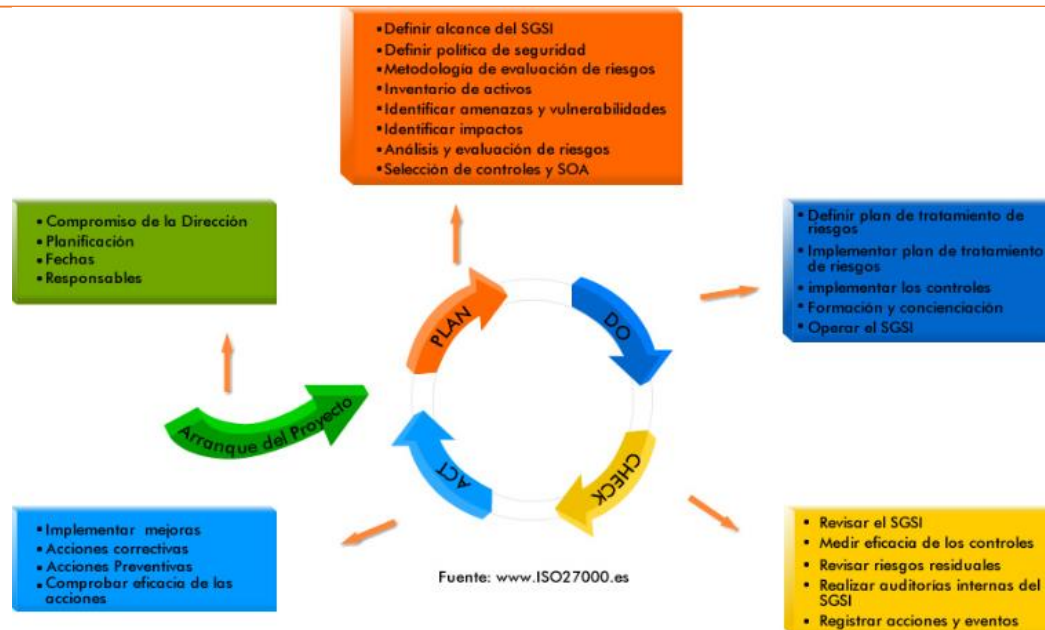
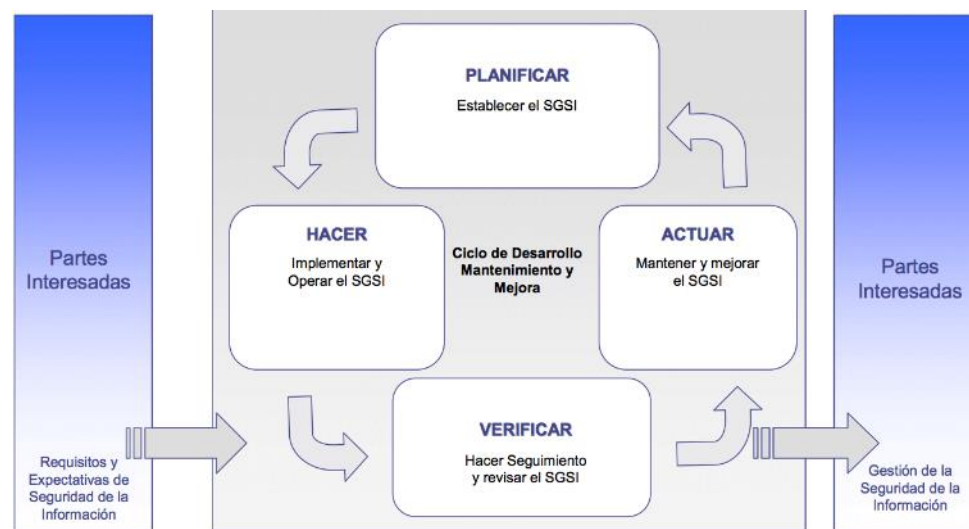
comprender los requisitos de seguridad de la información del negocio,

implementar y operar controles para manejar los riesgos de seguridad de la información de una organización.

c) el seguimiento y revisión del desempeño y eficacia del SGSI, y  
d) la mejora continua basada en la medición de objetivos.

# MODELO DE PROCESO PHVA

## “Planificar-Hacer-Verificar-Actuar” PHVA





# COMPATIBILIDAD CON OTROS SISTEMAS DE GESTIÓN

Se define como el conjunto de elementos relacionados o que interactúan que permiten implantar y alcanzar la política y los objetivos de una organización, en lo que se refiere a aspectos diversos como pueden ser los de calidad, medio ambiente, seguridad y salud, u otras disciplinas

## Ventajas de integrar Sistemas de Gestión

- **Políticas y objetivos alineados**
- **Se simplifica la estructura organizativa.**
- **Se reducen los esfuerzos necesarios para implementar los sistemas.**
- **Mantenimiento del sistema optimizado.**
- **Mejora de la comunicación interna y con los clientes.**



# COMPATIBILIDAD CON OTROS SISTEMAS DE GESTIÓN

## SISTEMA DE GESTIÓN INTEGRADO (SGI)



# TÉRMINOS Y DEFINICIONES

- **Aceptación Del Riesgo** - [Guía ISO/IEC 73:2002]
- **Activo** [NTC 5411-1:2006]
- **Análisis De Riesgo** [Guía ISO/IEC 73:2002]
- **C.I.D.** [NTC 5411-1:2006]
- **Evaluación del riesgo** [Guía ISO/IEC 73:2002]
- **Evento de seguridad de la información** [ISO/IEC TR 18044:2004]



# TÉRMINOS Y DEFINICIONES

## DECLARACIÓN DE APLICABILIDAD

(SoA por las siglas en inglés de Statement of Applicability), un documento que si bien es un requisito de documentación en el estándar ISO/IEC 27001.

Control	Aplicable	Descripción	Justificación	Documentación	Responsable
A.5.1.1 Documentar la política de seguridad de la información	Si	La política de seguridad de la información, aprobada por la alta dirección, en efecto desde el 21 de diciembre de 2008. Una copia fue enviada a todos los empleados y partes interesadas. La versión oficial esta disponible en la intranet	Proveer las directrices para seguridad de la información y el apoyo de la dirección, según los requisitos de negocio y las leyes y reglamentos	Politica2014.doc	Oficial de Seguridad de la Información
A.5.1.2 Revisión de la política de seguridad de la información	Si	La política de seguridad de la información es revisada anualmente en la reunión de revisión de la Dirección la resolución formal se extiende por otro año, En caso de cambios importantes, puede realizarse una revisión durante el año	Asegurar que la política de seguridad de la información se mantiene hasta la fecha y permanece alineada con los objetivos de la organización	1. Procedimiento revisión por la dirección-312PR 2. Politica2014.doc 3. Actas de reunión	Oficial de Seguridad de la Información
A.6.2.2. El tele trabajo	No	-----	Nuestra organización no hace uso del tele trabajo	No hay documento	Director de TI



# EJERCICIO

## DECLARACIÓN DE APLICABILIDAD

# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ESTABLECIMIENTO DEL SGSI : Es el detalle del SGSI, su alcance, sus activos, las tecnologías y justificación de Exclusiones, para esto es necesario tener en cuenta los siguientes pasos:

1. Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos,
2. Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología



# FACES PARA LA CREACION DE UNA POLITICA DE SEGURIDAD



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Consideraciones para una adecuada PSI.

Un análisis de  
Riesgos Informático  
(Valoración de  
activos)

Involucre a las  
áreas responsables  
de los activos

Comunique a Todo  
el personal.

Métodos de  
divulgación  
(Awareness)

Involucre a la Alta  
Gerencia





# Ejemplos de Política de SI

[https://www.mintic.gov.co/gestionti/615/articulos-5482\\_G2\\_Politica\\_General.pdf](https://www.mintic.gov.co/gestionti/615/articulos-5482_G2_Politica_General.pdf)



<https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy>

<https://iso27002.wiki.zoho.com/5-1-1-Documento-de-pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html>



# EJERCICIO

REALIZAR UN POLITICA DE SEGURIDAD DE LA INFORMACION

# EJERCICIO

Uno de los trabajos de un profesional en Seguridad de la Información es elaborar una Política de Seguridad

1. Objetivos Claros
2. Responsabilidades
3. Alcance de la Política
4. Control de la Información
5. Sanciones de No cumplimiento

Una PSI es una forma de Comunicarse con los usuarios... Siempre hay que tener en cuenta que la Seguridad comienza y termina con personas.

# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## RIESGOS

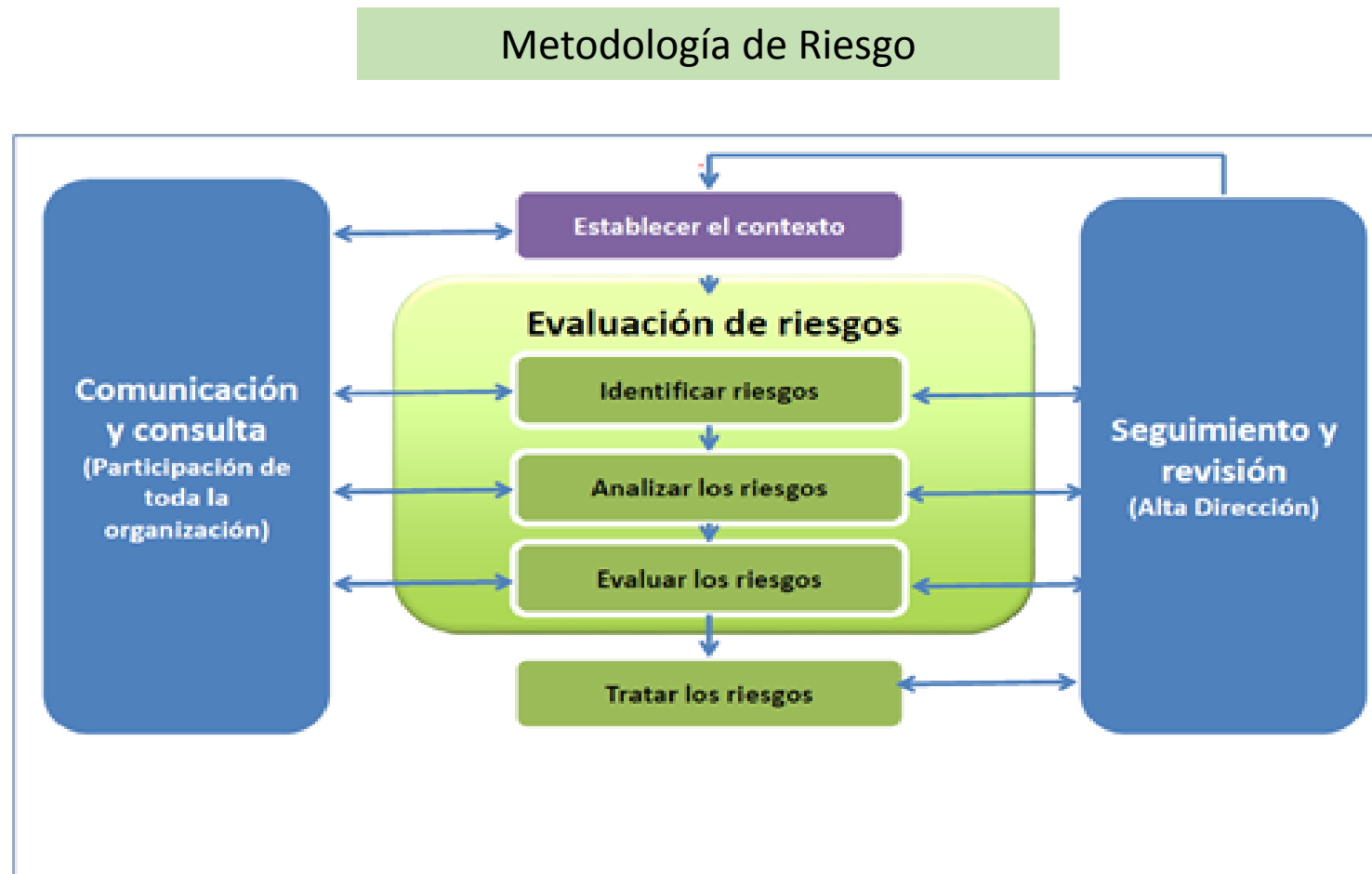


# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- **RIESGO** : La combinación de la probabilidad de un evento y su consecuencia.
- **Amenazas** : La amenaza puede definirse como aquel peligro latente
- **Aceptar Riesgo**: La empresa decide convivir con el Riesgo.
- **Impacto** : Se entienden las derivaciones que puede ocasionar.
- **Probabilidad** : La probabilidad es una medida de la certidumbre asociada a un suceso o evento futuro y suele expresarse como un número entre 0 y 1 (o entre 0 % y 100 %).
- **ISO 31000:2018 de Gestión de Riesgos**



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## Metodología de Riesgo

### IDENTIFICAR LOS ACTIVOS

En este proceso se requiere identificar, valorar y clasificar los activos de información más importantes del negocio y así darles el tratamiento adecuado

### IDENTIFICAR LAS AMENAZAS

Es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad

### IDENTIFICAR LAS VULNERABILIDADES

Es una debilidad que se encuentra en un activo o en un control y que puede ser explotada por una o más amenazas

### IDENTIFICAR LOS IMPACTOS

Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## VALORACION DE ACTIVOS

Proceso	Activo de Información	Atributos									Atributos			Valor del activo
		C			I			D			C	I	D	
		Atributo 1	Atributo 2	Atributo 3	Atributo 1	Atributo 2	Atributo 3	Atributo 1	Atributo 2	Atributo 3				
Proceso 1	Activo 1	5	3	1	3	4	2	3	1	4	3.0	3.0	2.7	2.89
	Activo 2	4	5	4	3	4	3	5	5	4	4.3	3.3	4.7	4.11
	Activo 3	2	3	1	5	3	3	5	3	3	2.0	3.7	3.7	3.11
	Activo 4	3	1	3	1	3	2	3	2	5	2.3	2.0	3.3	2.56
	Activo 5	3	2	1	3	1	3	4	3	4	2.0	2.3	3.7	2.67
	Activo 6	3	3	3	3	3	3	3	3	3	3.0	3.0	3.0	3.00
	Activo 7	1	5	5	3	4	4	5	1	3	3.7	3.7	3.0	3.44



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## GESTIÓN DEL RIESGO

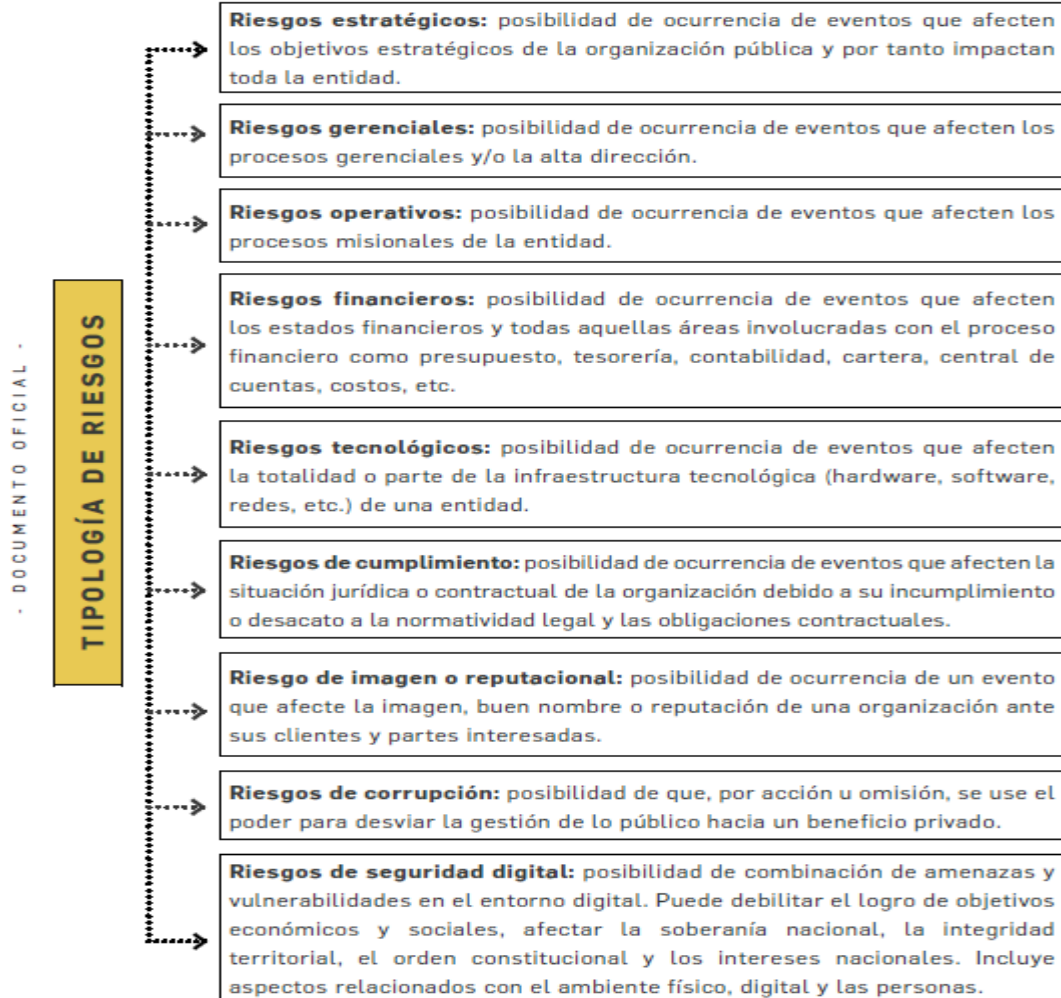


# Gestión de Riesgo - Metodología

- Matriz de Riesgo
  - Productos o servicios
  - Procesos - Activos
  - Amenazas
  - Vulnerabilidades
  - Probabilidad de ocurrencia
  - Impacto
  - Nivel de riesgo > 2
  - Tratamiento del riesgo
    - Mitigar
    - Aceptar
    - Transferir
    - Eliminar
  - Proyecto
  - Nuevo nivel de riesgo  $\leq 2$
- Medición de la eficacia

IMPACTO	Muy Alto	3	3	4	5	5
	Alto	3	3	3	4	5
	Moderado	2	3	3	3	4
	Bajo	1	2	3	3	3
	Minimo	1	1	2	3	3
		Extremada mente improbable	Muy improbable	Probable	Muy probable	Extremada mente probable
		PROBABILIDAD				

# Tipologías de Riesgos



- **Riesgo:** Riesgo acorde al tipo de Riesgo.
- **Descripción:** El escenario en el cual se visualiza la materialización del riesgo de seguridad de la información
- **Causas:** Motivos o circunstancias por las cuales se puede ocasionar el Riesgo de seguridad de la información
- **Consecuencias:** Descripción del impacto causado.
- **Factor de Riesgo:** los definidos por la metodología de riesgo operativo: Infraestructura, tecnología, recursos humanos, procesos y acontecimientos externos.

# Tratamiento de Riesgo

El proceso de tratamiento de riesgos consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo.



Aplicar los controles

Aceptar los riesgos

Transferir riesgos

Aseguradoras,  
proveedores

**RIOBAMBA**  
INSTITUTO VENEZOLANO DE TRANSITO

Anexo 4  
Riobamba, \_\_\_\_ de \_\_\_\_ del 201\_\_

**ACEPTACIÓN DE RIESGOS**

Yo, \_\_\_\_\_, Aspirante al cargo de Agente Civil de Tránsito, en conocimiento de la organización y funcionamiento de la Escuela de Formación de Oficiales y Trozas de la Comisión de Tránsito del Estado, institución responsable de la formación de los Agentes Civiles de Tránsito, con plena conciencia del nivel de exigencia y esfuerzo físico que deberá otorgar en el proceso de formación profesional, de manera libre y voluntaria, he escogido cursar el proceso de formación de Agente Civil de Tránsito, y que al logro del perfil profesional, frente a las nuevas exigencias científicas policiales de Tránsito, presentará altos niveles de riesgo.

**EN CONSECUENCIA:**  
Acepto los riesgos de todo naturaleza a los que por las singulares características de la formación profesional me someteré durante mi permanencia en calidad de Aspirante a Agente Civil de Tránsito del Estado.

Declaro, conocer y admitir las disposiciones legales y reglamentarias que rigen la permanencia dentro de la institución como Aspirante a Agente Civil de Tránsito, hasta mi graduación.

Para constancia de mi compromiso y responsabilidad firmo:

(Firma del aspirante)  
(Apellidos y nombres del aspirante)  
CI (Número de Cédula de Ciudadanía del aspirante)



# EJERCICIO

REALIZAR UN ANALISIS DE LOS RIESGOS

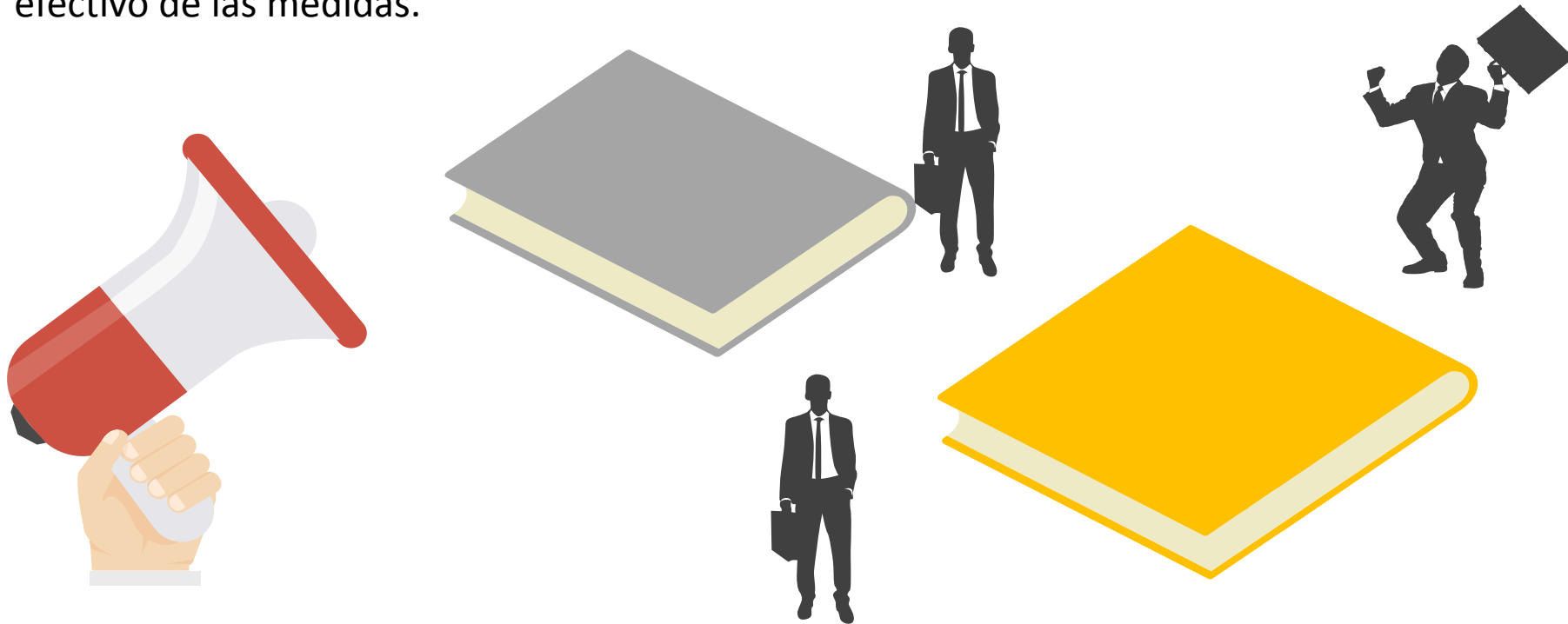
# EJERCICIO

- Escenario1 : Caída de Base de datos del Core de la Empresa
- Escenario 2 : Perdida de comunicación con Dispositivos Externos.
  - **Descripción:** El escenario en el cual se visualiza la materialización del riesgo de seguridad de la información
  - **Causas:** Motivos o circunstancias por las cuales se puede ocasionar el Riesgo de seguridad de la información
  - **Consecuencias:** Descripción del impacto causado.
  - **Tipo de Riesgo**



# Gestión Cultura

El proceso de gestión de la cultura provee el conocimiento acerca de la seguridad de información, a medida que el personal progresa en el desarrollo de la cultura, la necesidad de la misma es interiorizada y su rol es desarrollado. Así, al desarrollar el rol, el personal comienza a actuar de forma más segura y a utilizar las medidas implementadas. Dentro del proceso se incluyen etapas como: sensibilización, entendimiento, uso efectivo de las medidas.



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## FORMACIÓN Y DE TOMA DE CONCIENCIA,

### **Certified Information Security Manager®)**

Esta es una certificación expedida por ISACA ([www.isaca.org](http://www.isaca.org)) y es un programa de certificación desarrollado para gerentes de la seguridad de la información o personas que tengan responsabilidades asociadas con la administración de la seguridad de la información en una organización.

Information Security Governance (21%)

Risk Management (21%)

Information Security Program(me) Management (21%)

Information Security Management (24%)

Response Management (13%)





# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## FORMACIÓN Y DE TOMA DE CONCIENCIA,

### **Cybersecurity Nexus (CSX)**

*El examen de Cybersecurity Fundamentals comprueba un conocimiento base a través de cinco áreas principales:*

Conceptos en Ciberseguridad.

Principios en Arquitecturas de Ciberseguridad.

Ciberseguridad de redes, sistemas, aplicaciones, y datos.

Las implicaciones desde el punto de vista de seguridad de la adopción de tecnologías emergentes.

Respuesta a incidentes.



# AUDITORÍAS INTERNAS

## Auditoría es:

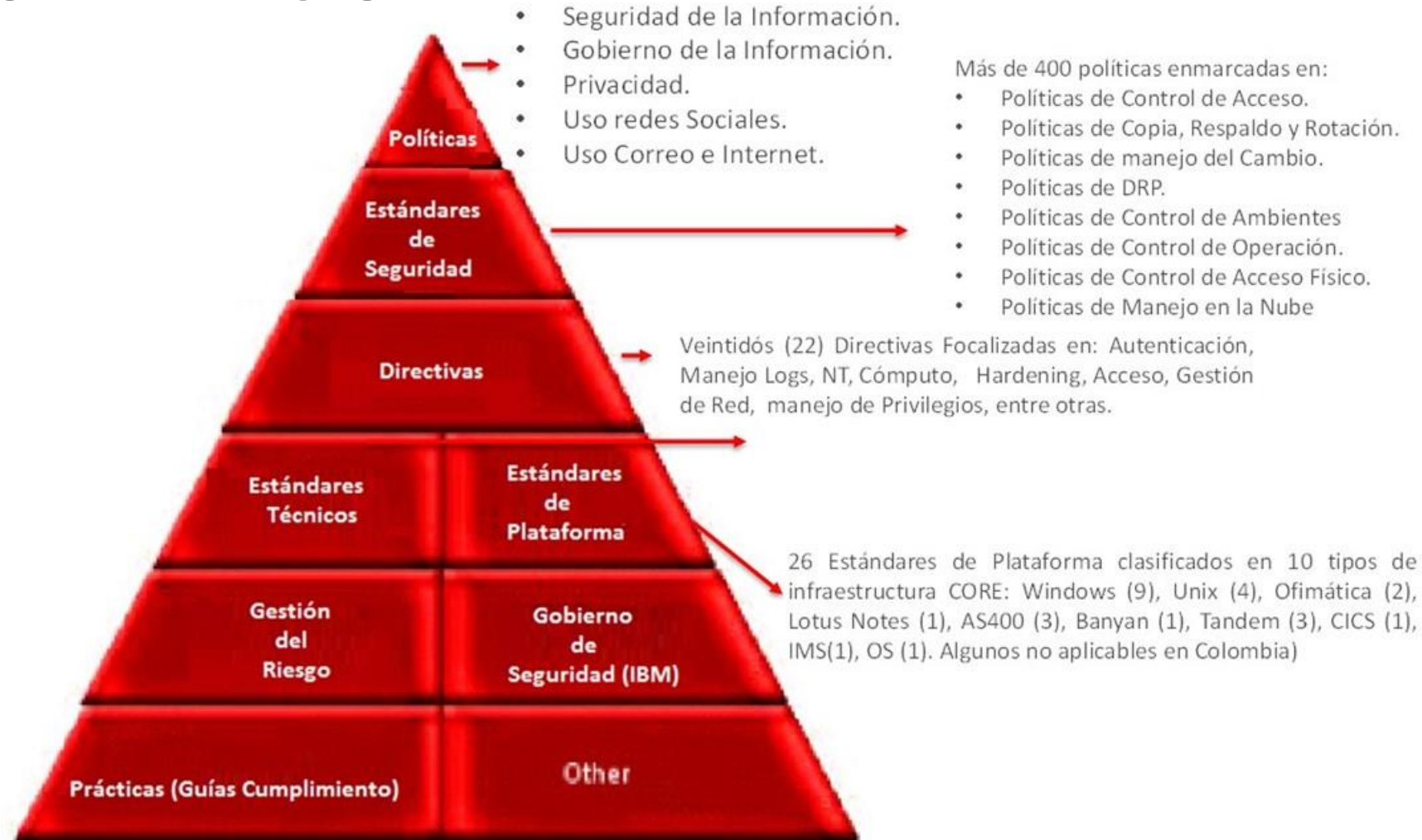
Un examen crítico que se realiza con el fin de evaluar la **eficacia y eficiencia** de una sección, un organismo, una entidad, o un sistema de Gestión de Seguridad de la Información.



**La Auditoría Informática** la podemos definir como el conjunto de **procedimientos y técnicas** para **evaluar** y controlar un sistema informático con el fin de **constatar si sus actividades son correctas y de acuerdo a las normativas informáticas** y generales prefijadas en la organización.



# DOCUMENTACIÓN



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## RESPONSABILIDAD DE LA DIRECCIÓN

Efectuando las revisiones



Brindando los recursos



vulnerabilidades o amenazas  
no tratadas adecuadamente



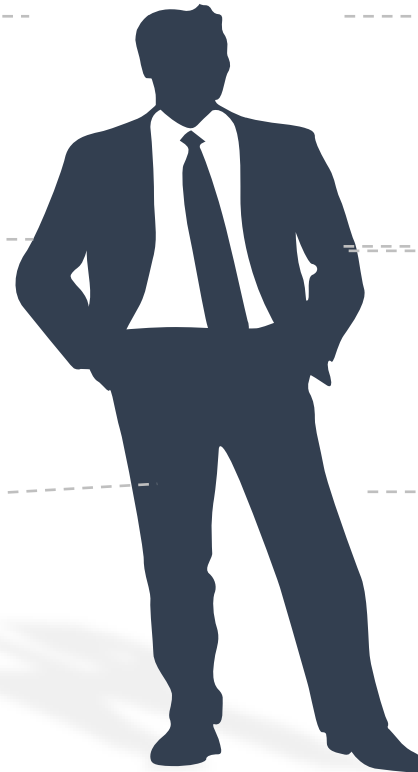
Realizan Auditorías Internas



Criterios para aceptación de  
Riesgos



Estado de las acciones  
Correctivas



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## NORMATIVAS APLICABLES



Bogotá D.C., 14 de julio de 2011



**LEY 1273 DE 2009**



**Circular 052 de 2007 (SFC)  
Circular Básica Jurídica (C.E.  
029/14)**



**Ley 1581 de 2012**

Existen estándares internacionales que ayudan a enfrentarse a este problema, por ejemplo:

- ISO/IEC JTC 1/SC 27 Técnicas de seguridad para tecnologías de la información.
- IEC/SC 65C/WG 13 Redes industriales. Ciberseguridad.
- ISO TC 292/WG 2 Continuidad y resiliencia de las organizaciones.
- UNE-EN ISO 22313:2015 Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices.
- UNE-EN ISO 22301:2015 Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones.



**Ley 527 de 1999 - COMERCIO  
ELECTRÓNICO**



**Circular Externa 007 de 2018  
Gestión de la seguridad de la  
información y la ciberseguridad**

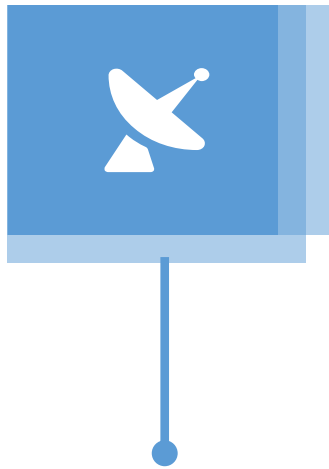


**PCI DSS. (industria de tarjetas de pago)**



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## LEY 1273 DE 2009



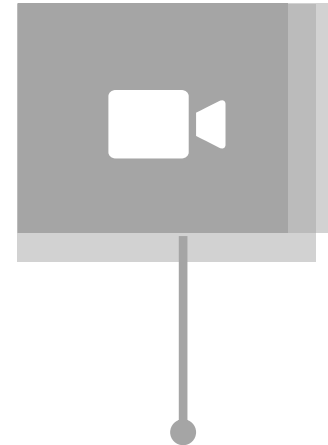
Artículo 269A: Acceso abusivo a un sistema informático

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación



Artículo 269C: Interceptación de datos informáticos.

Artículo 269D: Daño Informático



Artículo 269E: Uso de software malicioso

Artículo 269F: Violación de datos personales



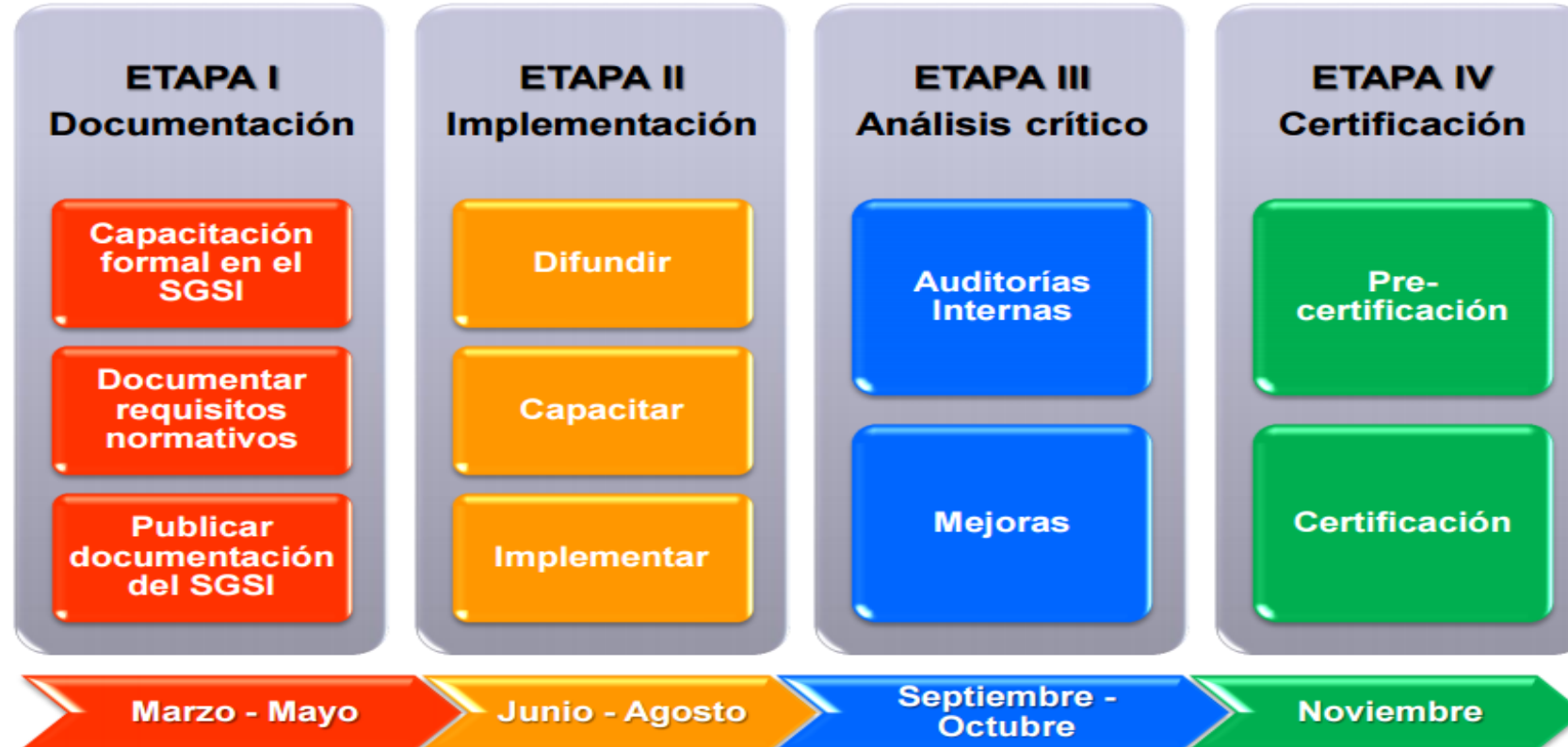
Artículo 269G: Suplantación de sitios web para capturar datos personales.

Artículo 269I: Hurto por medios informáticos y semejantes



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## IMPLEMENTACIÓN Y DISEÑO EN UN PROCESO DE CERTIFICACIÓN



# PREGUNTAS

