



# Introducción al Sistema de Gestión de Seguridad de la Información (Sesiones 03 y 04)

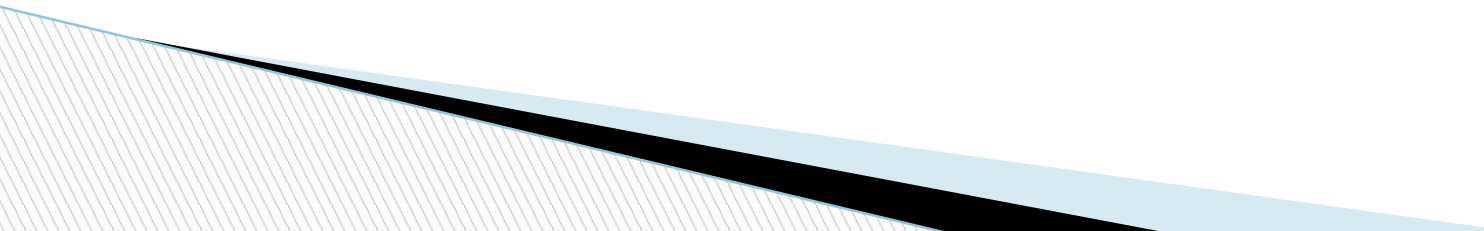
Gestión de Seguridad de la información  
Semestre 2023I

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación al tratamiento de los riesgos y establecimiento de objetivos de seguridad de la información.

# Algunos ejemplos adicionales de la sesión anterior

Documentación del SGSI de empresa del rubro de servicios de seguridad y la información:

- Contexto de Organización
  - Alcance
  - Objetivos del SGSI
  - Política de Seguridad
- 

# Gestión de los riesgos



# Conceptos y Definiciones ¿Qué es un riesgo?

“Efecto de la incertidumbre sobre la consecución de objetivos

- *Nota 1: Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.*
- *Nota 2: Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).*
- *Nota 3: Con frecuencia el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias o una combinación de ambos.*
- *Nota 4: Con frecuencia, el riesgo se expresa en términos de la combinación de las consecuencias un suceso y de su probabilidad.*
- *Nota 5: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.*

# Conceptos y Definiciones ¿Qué es un riesgo?

- “El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos, que ocasione pérdida o daño a los activos. El impacto o la severidad relativa del riesgo es proporcional al valor del daño o pérdida para el negocio y a la frecuencia estimada de la amenaza”

Fuente: Guidelines for the Management of IT Security (International Organization for Standardization)

- “La posibilidad de que algo suceda que impactará en los objetivos. Se mide en términos de consecuencias y probabilidad.”

Fuente: Australian/ New Zealand Standard AS/ NZS 4360 Risk Management

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

# Conceptos y Definiciones

- Activo: Algo de valor (tangible o intangible) que merece protegerse.
- Amenaza: Una causa potencial de un incidente no deseado que puede resultar en daño para un sistema u organización.
- Vulnerabilidad: Cualquier debilidad que pueda ser aprovechada por una amenaza.
- Evento: Un incidente o situación que ocurre en un lugar particular en un intervalo de tiempo particular.

# Opciones de Respuesta a los Riesgos

- ¿Cuánto invertir para mitigar el riesgo?
  - Depende del valor de lo que quiero proteger
  - Depende de la probabilidad de que ocurra el evento



vs





# Opciones de Respuesta a los Riesgos

## Ejemplo:

- Riesgo de pérdida total del centro de cómputo producido por un terremoto.
- Datos:
  - ✓ Valor total del C. Cómputo: US\$1M
  - ✓ De acuerdo a estadísticas en la zona geográfica donde se ubica el C. Cómputo, se produce un terremoto superior a grado 8 cada 10 años.
- Pregunta: ¿Cuánto debería invertir como máximo anualmente en un seguro contra pérdida del centro de cómputo?

# Opciones de Respuesta a los Riesgos

Impacto: US\$1M

Probabilidad =  $1/10 = 0.1$

Pérdida Esperada Anual (ALE) = Impacto x Probabilidad

Pérdida Esperada Anual =  $\text{US\$1M} \times 0.1 = \text{US\$100K}$

Por lo tanto anualmente no debería invertir en un seguro más de US\$100K

Si invierto más, estaré pagando más de lo que me costará construir e implementar C. Cómputo nuevo.

# Opciones de Respuesta a los Riesgos

- Se cuenta con cuatro opciones para responder a los riesgos (MATE):
  - Mitigar el Riesgo
  - Aceptar el Riesgo
  - Transferir el Riesgo
  - Evitar el Riesgo

# Opciones de tratamiento de riesgos

## Mitigar el Riesgo

- La mitigación del riesgo significa que se tomaron medidas para reducir ya sea frecuencia (probabilidad) o el impacto (daño o perjuicio) de un riesgo.
  - Podría requerir el uso de varios controles hasta que éste alcance niveles de aceptación o tolerancia del riesgo.
- Ejemplos de mitigación de riesgos:
  - Implementar nuevos controles técnicos, de gestión u operativos que reduzcan la probabilidad o el impacto de evento adverso
  - Instalar un nuevo sistema de control de accesos
  - Implementar políticas o procedimientos operativos
  - Desarrollar un plan de respuesta a incidentes y un plan de continuidad de negocios eficaces
  - Utilizar controles compensatorios

# Opciones de Respuesta a los Riesgos

## Aceptar el Riesgo

- Es una decisión consciente tomada por la alta gerencia, de reconocer la existencia de un riesgo y conscientemente decidir que el riesgo permanezca (asumir el riesgo) sin (mayores) medidas de mitigación.
  - La Gerencia será responsable por el impacto generado en caso se materialice el riesgo.
- Riesgo Aceptable: Definido como la cantidad de riesgo que la alta gerencia ha determinado que está dentro de los límites aceptables o permisibles.
  - No es lo mismo que ignorar el riesgo, lo cual es una falla para identificar o reconocer la existencia de un riesgo.

# Opciones de Respuesta a los Riesgos

## ...Aceptar el Riesgo

- Ejemplos de aceptación del riesgo:
  - Se prevé que un determinado proyecto no podrá implementar una funcionalidad requerida por el negocio para la fecha planificada. La Gerencia puede decidir aceptar el riesgo y continuar con el proyecto.
  - Un riesgo en particular que es calificado como extremadamente raro (ocurrencia muy poco probable) tiene consecuencias catastróficas, y las medidas para mitigar dicho riesgo son prohibitivas. La Gerencia podría decidir aceptar dicho riesgo.
- La aceptación del riesgo está basada muchas veces en un riesgo mal calculado.
- El nivel de riesgo y el impacto pueden cambiar constantemente, por lo que las revisiones periódicas son necesarias.

# Opciones de Respuesta a los Riesgos

## Transferir / Compartir el Riesgo

- La transferencia del riesgo es una decisión de reducir la pérdida compartiendo el riesgo con otra organización (Ej. Adquisición de un seguro)
- Proyectos compartidos con otras organizaciones son otro ejemplo
- Las decisiones de transferencia de riesgo deben ser revisadas con regularidad

# Opciones de Respuesta a los Riesgos

## Evitar el Riesgo

- Evitar el riesgo significa evitar las actividades o condiciones que dan lugar al riesgo
  - Se aplica cuando no hay otra respuesta adecuada al riesgo
- Ejemplos de evitación<sup>(\*)</sup> del riesgo
  - Reubicar el centro de cómputo lejos de una región con riesgos naturales importantes.
  - Rechazar participar en un proyecto muy grande cuando se observa una muy alta probabilidad de fracaso.
  - Rechazar participar en un proyecto que se basará en sistemas complicados y obsoletos, porque no se cuenta con un aceptable grado de confianza que el proyecto entregue algo útil / viable.
  - Decidir no utilizar cierta tecnología paquete de software ya que impediría una expansión futura.
  - Rechazar abrir sucursales en países con alta probabilidad de estatización o alto nivel de inseguridad

(\*) Evitación: Acción y efecto de evitar – Diccionario RAE

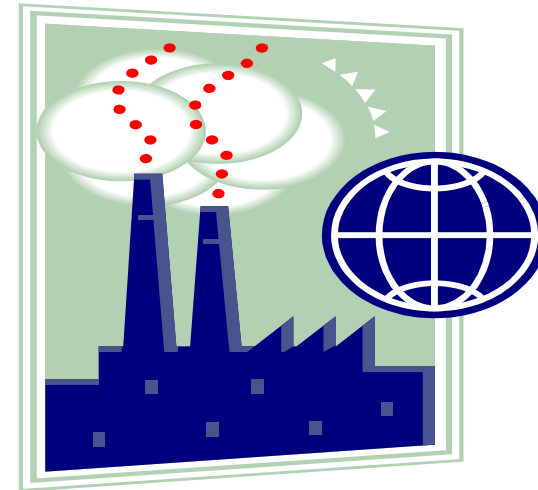


# Visión General de la Gestión de Riesgos

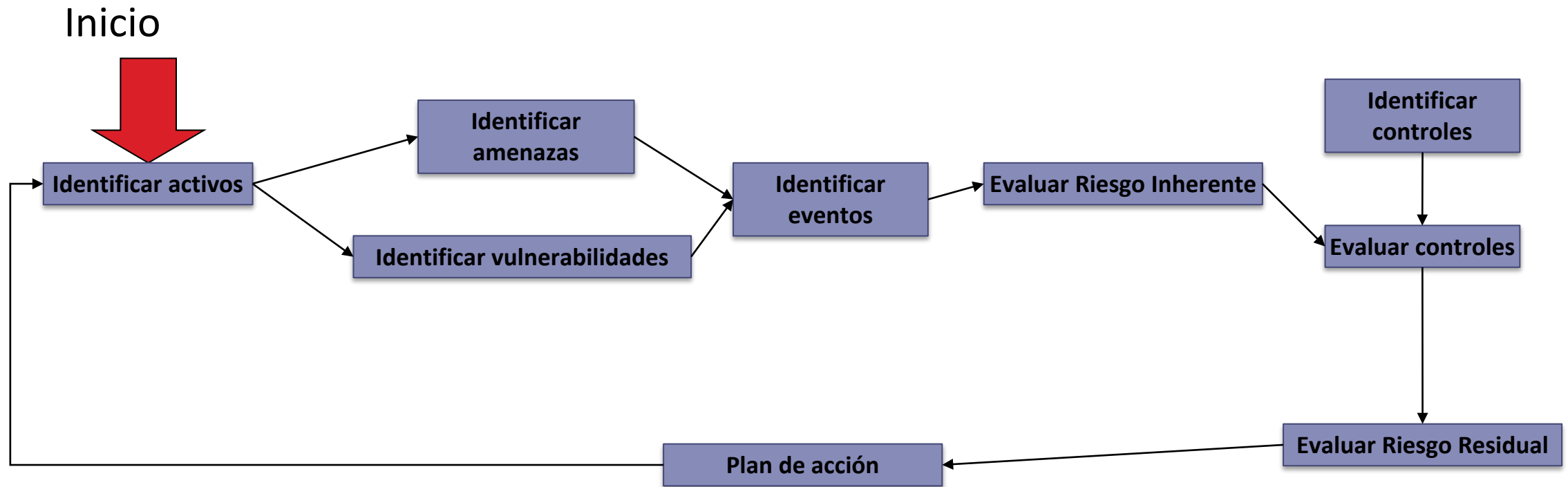
- El proceso de asegurar que el impacto de las amenazas que explotan la vulnerabilidades esté dentro de los límites y costos aceptables.
- Los riesgos deben ser gestionados de manera que no impacten materialmente los procesos de negocio.
- El riesgo es inherente en todas las actividades de negocio.
- Foco específico en la gestión de riesgos de la información desde una perspectiva de seguridad.

# Riesgo Inherente y Riesgo Residual

- Riesgo inherente: Riesgo presente en el curso normal de las actividades de negocio.
- Riesgo residual: Los riesgos después de implementar los controles.



# Marco General de Gestión de Riesgos de la Seguridad de la Información

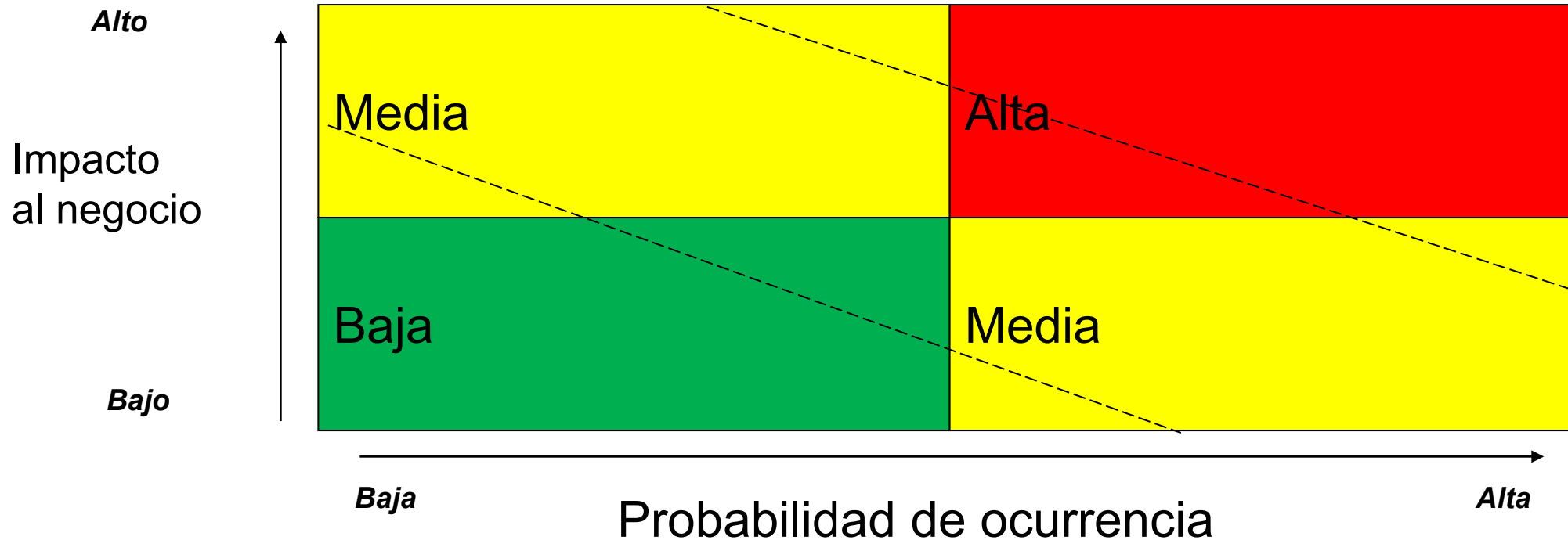


# Análisis Básico del Riesgo

- La clasificación del riesgo implica la evaluación de dos componentes:
  - La posibilidad de que ocurra pérdida o daño (probabilidad de ocurrencia)
  - La magnitud y el efecto del impacto financiero o de otro tipo de dicha ocurrencia (impacto en el negocio).
- Foco inicial en Riesgos Altos (Probabilidad Alta de Ocurrencia y Alto Impacto en el Negocio).
- Se necesita balancear el costo de implementar controles contra los riesgos identificados

# Análisis Básico del Riesgo

## Clasificación del riesgo



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

# Paso 1 Caracterización del Sistema

- Recopilar información de los activos de información:
  - Información y datos
  - Hardware
  - Software
  - Servicios
  - Documentos
  - Personal
- Entregable: Inventario de activos

<https://www.youtube.com/watch?v=THnQ2FH7NtU>

Ej. Activos UNAD: [http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321\\_paso\\_1\\_inventario\\_de\\_activos.html](http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html)

# Paso 2 Identificación de Amenazas

- Cualquier circunstancia o evento con el potencial de causar un recurso de información.
- Identificar amenazas a recursos críticos de TI.
- Amenazas a considerar:
  - Errores
  - Daño/ ataque malicioso
  - Eventos naturales (inundaciones, terremotos, etc.)
  - Fraude
  - Robo
  - Falla del equipo/ software
- Entregable: Declaración de Amenazas conteniendo la lista de amenazas que podrían explotar las vulnerabilidades del sistema.

Ej. Amenazas UNAD: [http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3231\\_identificacin\\_de\\_amenazas.html](http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3231_identificacin_de_amenazas.html)

# Paso 3- Identificación de Vulnerabilidades

- Las vulnerabilidades son características de los recursos de información que pueden ser explotadas por una amenaza para causar da
- Ejemplos:
  - Accesos no removidos en los sistemas de empleados cesados.
  - El firewall permite telnet entrante con cuentas hábiles de invitados.
- Entregable: Lista de vulnerabilidades.

[https://www.youtube.com/watch?v=ZrEpV2Xp8\\_k](https://www.youtube.com/watch?v=ZrEpV2Xp8_k)



# Paso 3- Identificación de Vulnerabilidades

Para la identificación de vulnerabilidades se puede emplear:

- port scanning;
- SNMP scanning;
- Enumeración y captura de banners;
- wireless enumeration;
- vulnerability scanning;
- host evaluation;
- network device analysis;
- password compliance testing;
- application- specific scanning;
- network sniffing.

# Paso 3- Identificación de Vulnerabilidades

La vulnerabilidad puede ser:

- Vulnerabilidad administrativa. Defectos en políticas, procedimientos o actividades de seguridad.
- Vulnerabilidad física. Defectos físicos, geográficos, de personal o en los controles relacionados.
- Vulnerabilidad técnica. Defectos en los controles lógicos de los sistemas de la organización (routers mal configurados, puertas traseras en los programas, contraseñas débiles, etc.).

# Paso 4– Análisis de Control

- Analizar los controles que han sido implementados, o planeados para implementación en el sistema bajo revisión.
- Controles preventivos:
  - Identificación y autenticación
  - Control de acceso a recursos
- Controles detectivos:
  - Logs de eventos de seguridad
- Entregable: Lista de controles utilizados para el sistema de TI.

Ej. Controles Red Hat: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html>

# Paso 5- Determinación de Probabilidad

- Identificar la probabilidad de que la vulnerabilidad potencial pueda ser explotada en el contexto de un ambiente de amenazas.
- Se necesita evaluar:
  - Fuente de amenazas.
  - Naturaleza de las vulnerabilidades.
  - Existencia y efectividad de los controles.
- Definir en términos de *Alto/ Medio/ Bajo*:
  - Alto: Fuente de la amenaza (p.e. un hacker) es capaz de explotar vulnerabilidades (p.e. tiene exploits) y los controles no son efectivos.
- Entregable: Clasificación de probabilidades.

# Paso 6- Análisis del Impacto

- El propósito de este paso es determinar el impacto adverso resultante de la explotación exitosa de una vulnerabilidad.
- Se requiere la clasificación de la información en términos de confidencialidad, integridad y disponibilidad.
- Evaluar el impacto basado en la pérdida de confidencialidad, integridad y disponibilidad.
- Entregable: Declaración de Impacto (Alto, Medio o Bajo)

## Paso 6 Clasificación de Información

- Identificar a los propietarios de la información.
- Utilizar métodos sencillos de clasificación.
- Considerar agrupación de activos de información:

<u>ACTIVO</u>	<u>CONFIDENCIALIDAD</u>	<u>INTEGRIDAD</u>	<u>DISPONIBILIDAD</u>
Datos de clientes	Alta	Alta	Baja

# Paso 6- Impacto de las Amenazas en el Negocio

- La evaluación se basa principalmente en la pérdida de confidencialidad, integridad o disponibilidad de la información.
- Impactos específicos en el negocio incluyen:
  - Pérdida de dinero (efectivo o crédito).
  - Incumplimiento de la ley.
  - Pérdida de reputación/ prestigio/ vergüenza (web defacement).
  - Peligro potencial para el personal o los clientes.
  - Pérdida de confianza.
  - Pérdida de oportunidades de negocio.
  - Reducción en el desempeño/ eficiencia operativos.
  - Interrupción de las actividades del negocio.

# Paso 7 Determinación del Riesgo

- Evaluar el nivel de riesgos de TI.
- La determinación del riesgo para un par amenaza/ vulnerabilidad particular puede ser expresada como una función de:
  - La probabilidad de que una determinada fuente de amenazas intente explotar una determinada vulnerabilidad.
  - La magnitud del impacto en caso de que una fuente de amenazas explote exitosamente las vulnerabilidades.
  - La idoneidad de controles de seguridad planificados o existentes para reducir o eliminar riesgos.
- Entregable: Declaración de niveles de riesgos expresados como Alto / Medio / Bajo.

<https://www.youtube.com/watch?v=g7EPuzN5Awg>

[http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material\\_taller\\_gestion\\_de\\_riesgo.pdf](http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf)



# Paso 8- Recomendaciones de Control

- Se identifican los controles que mitigan o eliminan los riesgos identificados a las operaciones de la organización.
- El objetivo de los controles recomendados es reducir el nivel de riesgo a sistema TI y su información a un nivel aceptable.
- Entregable: Plan de Tratamiento de Riesgos

# Apetito, Tolerancia y Capacidad

- **Apetito de Riesgo** es el nivel de riesgo que la empresa está dispuesta a aceptar en el logro de sus metas.
- **Tolerancia al Riesgo** es el nivel aceptable de variación en relación a la concesión de un objetivo.
- **Capacidad de Riesgo** es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.



# Cláusula 6: Planificación

- 6.1 Acciones para tratar los riesgos y oportunidades
- 6.2 Objetivos de Seguridad de la Información y planificación para Conseguirlos

# Cláusula 6: Planificación

## 6.1 Acciones para tratar los riesgos y oportunidades

Al planificar el SGSI, la organización debe considerar los aspectos mencionados en el numeral 4.1 y los que figuran en el 4.2, y determinar los riesgos y oportunidades que necesitan ser tratados para:

- a. Asegurar que el SGSI pueda lograr los resultados esperados;
- b. Prevenir o reducir efectos indeseados y
- c. Lograr la mejora continua.

La organización debe planificar:

- d. Las Acciones que traten estos riesgos y oportunidades, y
- e. La forma de:
  - 1. Integrar estas acciones en los procesos del SGSI
  - 2. Evaluar la eficacia de estas acciones

# Cláusula 6: Planificación

## 6.1.2 Evaluación de los riesgos de Seguridad de la Información (ERSI)

La organización debe definir un proceso de ERSI que:

- a. Establezca y mantenga criterios de riesgo de seguridad de la información que incluyan:
  - 1. Los criterios de aceptación de los riesgos
  - 2. Los criterios para realizar las ERSI
- b. Se asegure que al realizar nuevamente una ERSI se obtengan resultados consistentes, válidos y comparables.

# Cláusula 6: Planificación

## ...6.1.2 Evaluación de los riesgos de Seguridad de la Información (ERSI)

- c. Identifique los riesgos de seguridad de la información
  - 1. Aplicando el proceso de ERSI para identificar riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad, de la información dentro del alcance del SGSI.
  - 2. Identificando a los propietarios de los riesgos
- d. Analice los riesgos de S.I.
  - 1. Evaluando las consecuencias potenciales que resultarían si se materializan los riesgos identificados
  - 2. Evaluar la probabilidad realista de la ocurrencia de los riesgos identificados
  - 3. Determinar los niveles de riesgo

# Cláusula 6: Planificación

## ...6.1.2 Evaluación de los riesgos de Seguridad de la Información (ERSI)

- e. Evalúe los riesgos de Seguridad de la Información:
  - 1. Comparar los resultados del análisis de riesgo vs los criterios establecidos
  - 2. Priorizar los riesgos para su tratamiento

***La Organización deberá conservar información documentada del proceso de ERSI***

# Cláusula 6: Planificación

## 6.1.3 Información de Tratamiento de Riesgos de Seguridad

La organización debe definir y aplicar un proceso de tratamiento de los riesgos de S.I. para:

- a. Seleccionar opciones de tratamiento adecuadas teniendo en cuenta los resultados de la evaluación de riesgos;
- b. Determinar los controles que sean necesarios para poner en práctica las opciones de tratamiento de riesgos elegida;
- c. Comparar los controles determinados en el punto anterior, con los del Anexo “A”.



# Cláusula 6: Planificación

## ...6.1.3 Información de Tratamiento de Riesgos de Seguridad

- d. Elaborar una Declaración de Aplicabilidad que incluya los controles necesarios y la justificación tanto de las inclusiones, así como de las exclusiones de los controles del Anexo “A”.
- e. Formular un plan de tratamiento de riesgos de S.I.
- f. Obtener del propietario del riesgo, la aprobación del plan de tratamiento, y la aceptación de los riesgos residuales.

***La organización debe conservar información documentada del proceso de tratamiento de riesgos***

# Cláusula 6: Planificación

## 6.2 Objetivos de Seguridad de la Información y Planificación para Lograrlos

La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Los objetivos de seguridad de la información deben:

- a. Ser consistente con la Política de S.I.
- b. Ser medibles (si es posible)
- c. Ser comunicados, y
- d. Ser actualizados según corresponda

***La organización debe conservar información documentada sobre los objetivos de seguridad de la información***

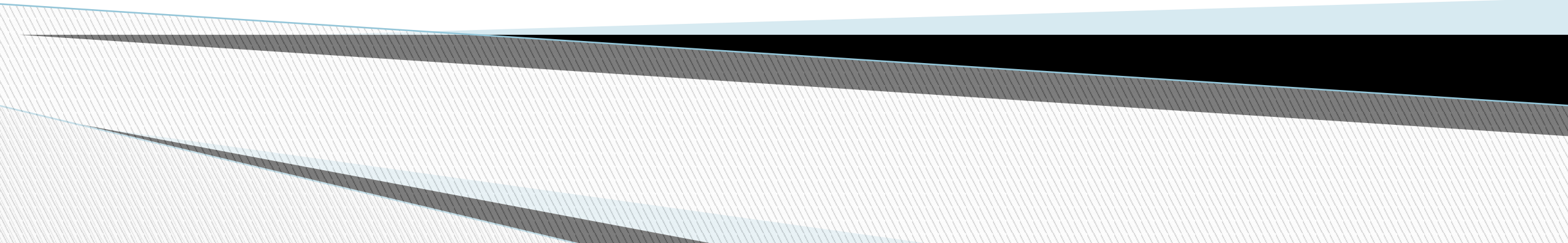
# Cláusula 6: Planificación

...6.2 Objetivos de Seguridad de la Información y Planificación para Lograrlos

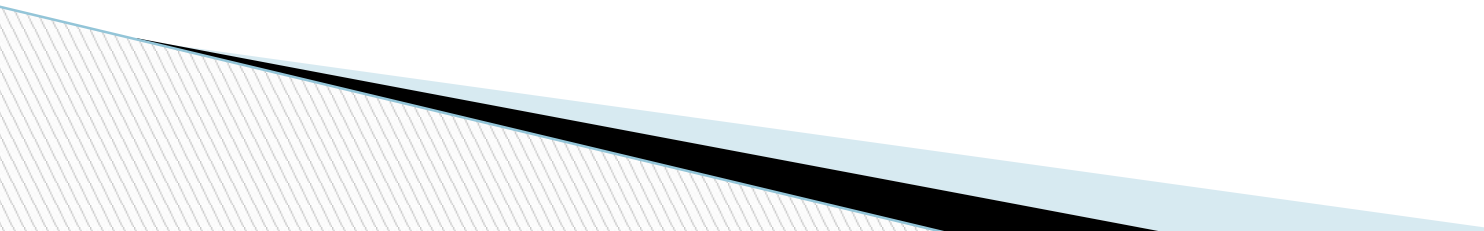
Al planificar cómo alcanzar sus objetivos de seguridad de la información, la organización debe determinar:

- a. Lo que se hará.
- b. Qué recursos requerirá
- c. Quién será responsable
- d. Cuándo se completará
- e. La forma en que se evaluará los resultados.

# Repaso: Planificación



# Repasemos

1. ¿Cuáles son los componentes básicos que permiten clasificar los riesgos?
  2. ¿Qué opciones existen para el tratamiento de los riesgos? Ejemplos.
  3. ¿Qué información exige la norma documentar en esta cláusula?
- 



# Funcionamiento del SGSI (sesión 10)

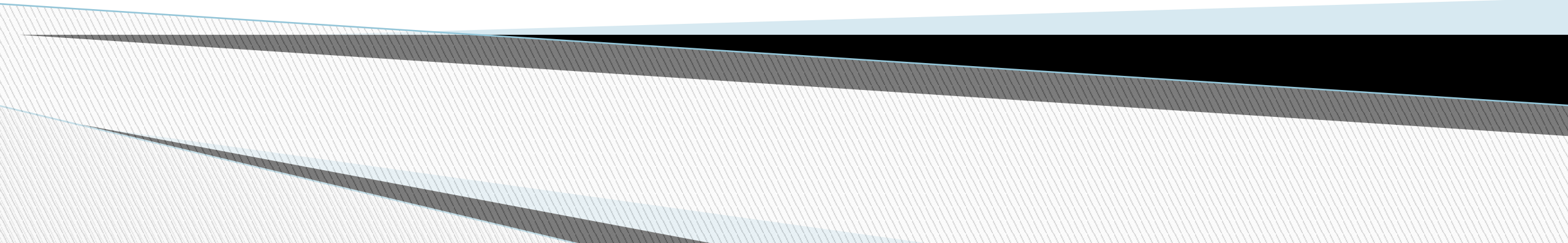
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

# **Anexo “A”**

## **Controles**





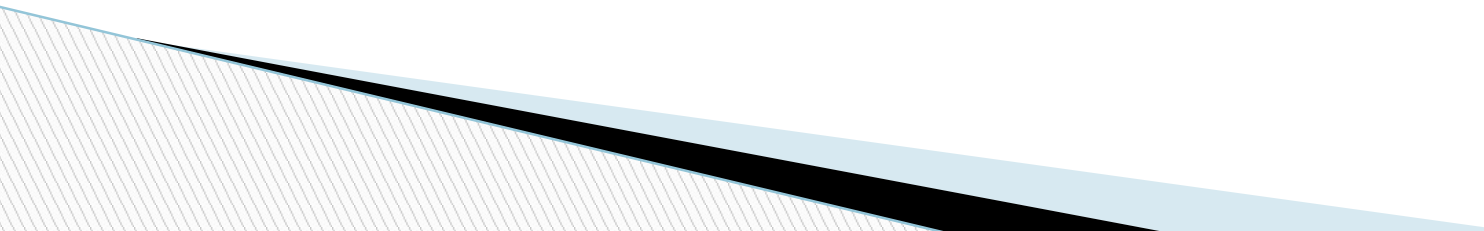
# A.8 Controles tecnológicos

## 8.18 Uso de programas de utilidad privilegiados

- Considerar lo siguiente para el uso de programas utilitarios que pudieran ser capaces de anular los controles del sistema
  - a. usar procedimientos de identificación, autenticación y autorización para los programas utilitarios;
  - b. separar los programas utilitarios de las aplicaciones de software;
  - c. limitar la utilización de programas utilitarios al número mínimo de usuarios autorizados y de confianza;
  - d. la autorización para el uso especial de los programas utilitarios;

# A.8 Controles tecnológicos

## 8.18 Uso de programas de utilidad privilegiados

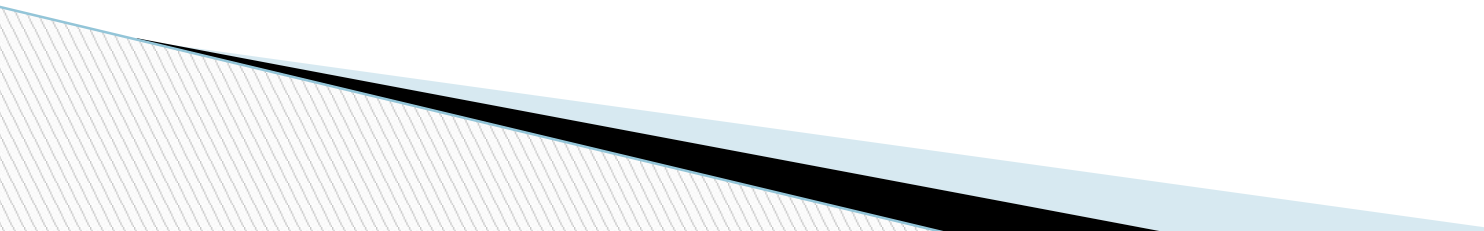
- e. limitar la disponibilidad de los programas utilitarios, por ejemplo, para la autorización de un cambio no autorizado;
  - f. el registrar el uso de programas utilitarios;
  - g. la definición y documentación de los niveles de autorización para los programas utilitarios;
  - h. la eliminación o desactivación de todos los programas utilitarios innecesarios;
  - i. no poner programas utilitarios a disposición de usuarios que tienen acceso a las aplicaciones en sistemas donde se requiere separación de funciones.
- 

# A.8 Controles tecnológicos

## 8.19 Instalación de software en sistemas operativos

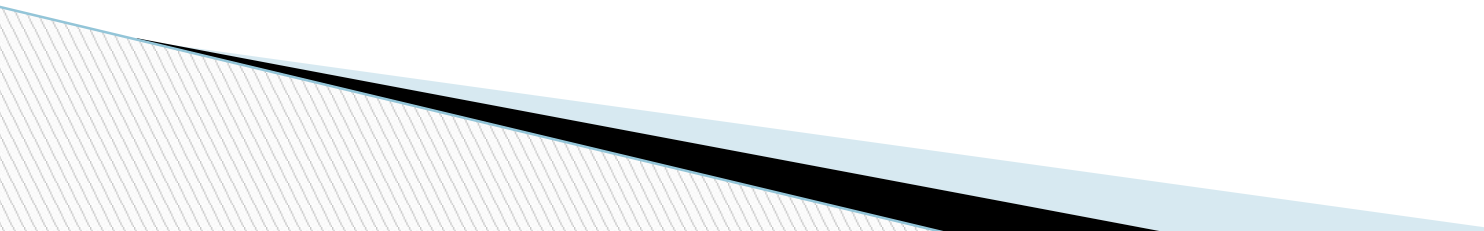
*Deberían implantarse procedimientos para controlar la instalación de software en los sistemas operacionales*

*Considerar lo siguiente:*

- a. Actualización de software únicamente por administradores entrenados y autorizados
  - b. Sistemas en producción no deberían tener código de desarrollo ni compiladores
  - c. Los sistemas operacionales deben implantarse luego de pruebas exhaustivas (utilidad, seguridad, efecto sobre otros sistemas y usuarios)
- 

# A.8 Controles tecnológicos

## 8.19 Instalación de software en sistemas operativos

- d. Control de la configuración y documentación del sistema
  - e. Antes de cambios considerar una estrategia de roll back (vuelta atrás)
  - f. Registro de auditoría de los cambios efectuados
  - g. Mantener la versión anterior como contingencia
- 

# A.8 Controles tecnológicos

## 8.20 Seguridad de las redes

*Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.*

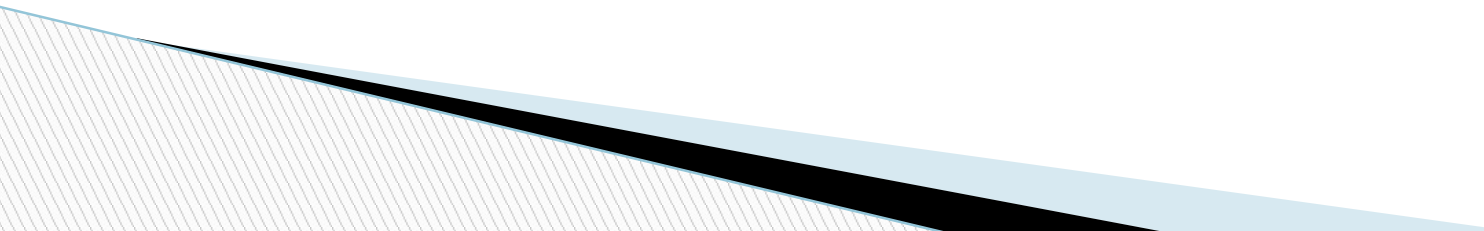
La red debe estar adecuadamente administrada y controlada, con el fin de protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usa la red, incluida la información en tránsito.

## A.8 Controles tecnológicos

### 8.21 Seguridad de los servicios de red

*Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.*

Las características de seguridad, los niveles de servicio, y los requerimientos de administración de todos los servicios de red deben ser identificados e incluidos en los acuerdos con los diferentes proveedores de servicios de red, bien sean internos o externos.



# A.8 Controles tecnológicos

## 8.22 Segregación de redes

*Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.*

Los controles para segregar grupos de dispositivos de información, usuarios y sistemas de información deben ser los adecuados para la organización.

.



## A.8 Controles tecnológicos

### 8.23 Filtro web

*El acceso a sitios web externos debe ser gestionado para reducir la exposición a contenido malicioso.*



# A.8 Controles tecnológicos

## 8.24 Uso de la criptografía

Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad e/o integridad de la información.

*Debería desarrollarse e implantarse una política sobre el uso de controles criptográficos para la protección de información.*

Cuando se desarrolla una política criptográfica se debería considerar:

- a. Qué tipo de información requerirá cifrado
- b. basado en una evaluación de riesgo, el tipo del algoritmo de cifrado requerido;

# A.8 Controles tecnológicos

## 8.24 Uso de la criptografía

*Debería desarrollarse e implantarse una política sobre el uso de controles criptográficos para la protección de información.*

Cuando se desarrolla una política criptográfica se debería considerar:

- a. Qué tipo de información requerirá cifrado
- b. basado en una evaluación de riesgo, el tipo del algoritmo de cifrado requerido;

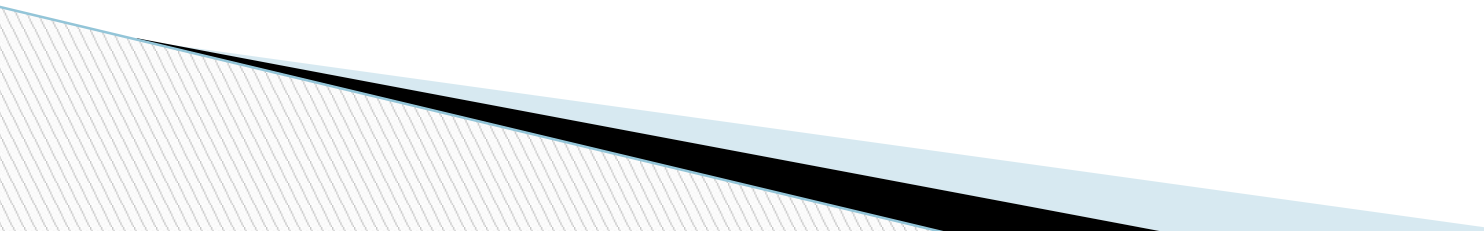
# A.8 Controles tecnológicos

## 8.24 Uso de la criptografía

- c. cifrado para protección de información transportada por medio de dispositivos móviles o removibles, o a través de líneas de comunicación;
- d. gestión de claves, incluyendo:
  - i. métodos para tratar la protección de claves criptográficas
  - ii. y la recuperación de información cifrada en el caso de claves perdidas, comprometidas o dañadas;
- e. funciones y responsabilidades, por ejemplo quien es responsable de:
  - i. la implementación de la política;
  - ii. la gestión de la clave, incluyendo la generación de la clave.

# A.8 Controles tecnológicos

## 8.24 Uso de la criptografía

- f. las normas a ser adoptadas para la implementación eficaz en todas partes de la organización (qué solución es utilizada para qué proceso de negocio);
  - g. el impacto de usar información cifrada, sobre los controles que se basan en la inspección de contenido (por ejemplo la detección de software malicioso).
- 

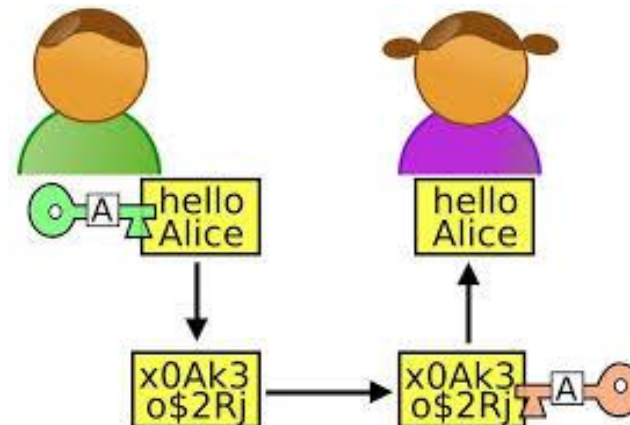
# A.8 Controles tecnológicos

## 8.24 Uso de la criptografía

Considerar las regulaciones y restricciones nacionales aplicables en diferentes partes del mundo.

Los controles criptográficos pueden usarse, por ejemplo, para:

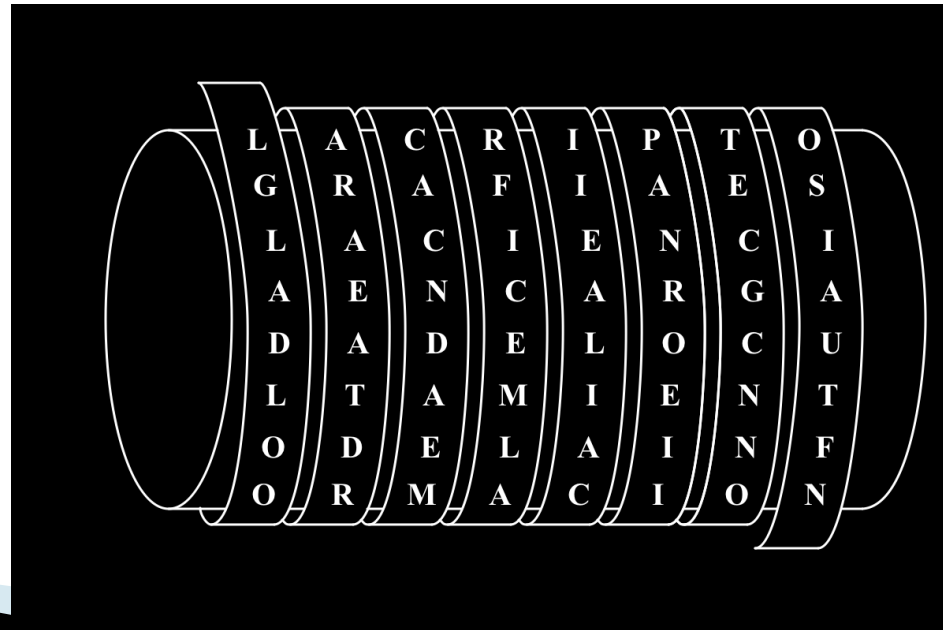
- ✓ Confidencialidad: Información crítica o sensible
- ✓ Integridad
- ✓ No repudio
- ✓ Autenticación



# A.8 Controles tecnológicos

## 8.24 Uso de la criptografía

- La decisión para aplicar técnicas criptográficas debe provenir de un proceso de evaluación de riesgos y selección de controles.
- Buscar asesoría de un especialista

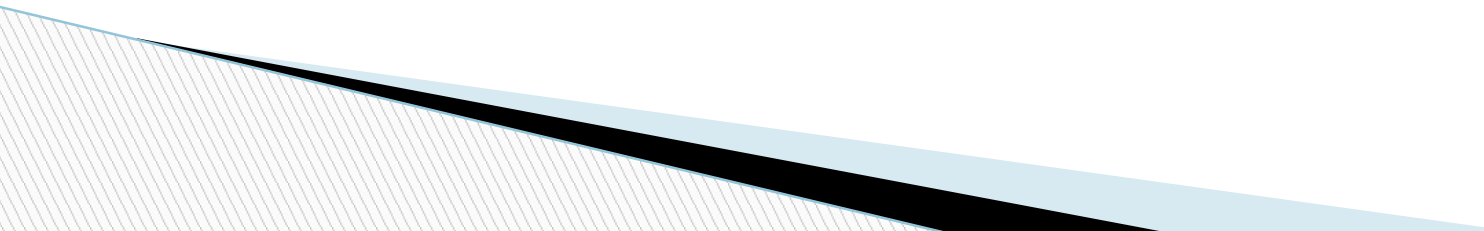


## A.8 Controles tecnológicos

### 8.25 Ciclo de vida de desarrollo seguro

Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.

Deben existir reglas de seguridad de acuerdo a las necesidades de la organización para ser aplicadas durante las diversas etapas del ciclo del desarrollo de software.

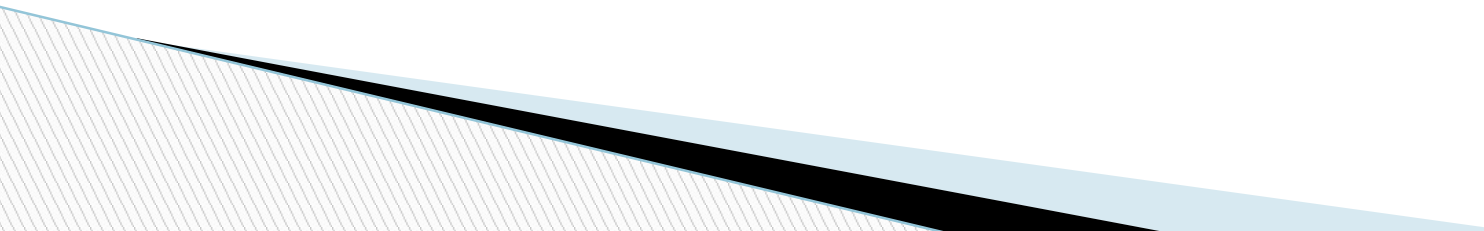


## A.8 Controles tecnológicos

### 8.26 Requisitos de seguridad de las aplicaciones

La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.

Los datos disponibles, procesados o transmitidos a través de un sistema público, deben encontrarse protegidos para asegurar su integridad y prevenir modificaciones no autorizadas de cualquier origen.





## A.8 Controles tecnológicos

### 8.26 Requisitos de seguridad de las aplicaciones

La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.

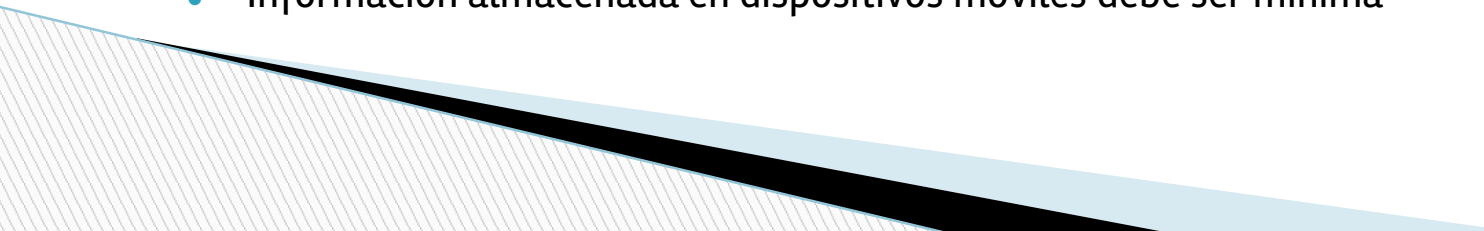
Los datos involucrados en transacciones en línea, están protegidos para prevenir transmisiones de información incompletas; desvío o modificación no autorizados del mensaje, así como divulgación no autorizada y también para evitar la duplicación o reproducción de parte o totalidad del mensaje.

# A.8 Controles tecnológicos

## 8.27 Arquitectura de sistemas seguros y principios de ingeniería

Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información.

Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información, tales como por ejemplo:

- Modelo de permisos mínimos
  - Seguimiento de las tecnologías utilizadas para el desarrollo
  - Accesos a los sistemas deben ser validados
  - Protocolos para cifrar las comunicaciones
  - Información almacenada en dispositivos móviles debe ser mínima
- 

# A.8 Controles tecnológicos

## 8.28 Codificación segura

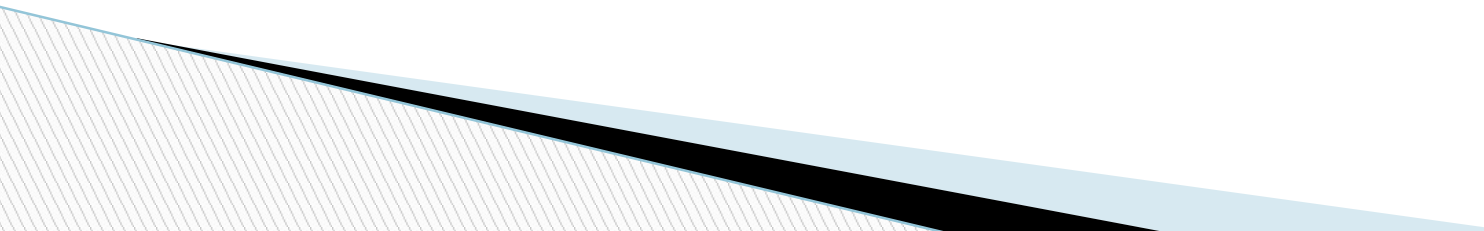
Principios de codificación segura deben ser aplicados al desarrollo de software. Es decir, conjuntos de reglas y pautas para reducir las vulnerabilidades y errores de seguridad durante el desarrollo.

## A.8 Controles tecnológicos

### **8.29 Pruebas de seguridad en el desarrollo y la aceptación**

Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad.

Se deben probar todas las funcionalidades de seguridad establecidas en el requerimiento, durante las diferentes fases del desarrollo.

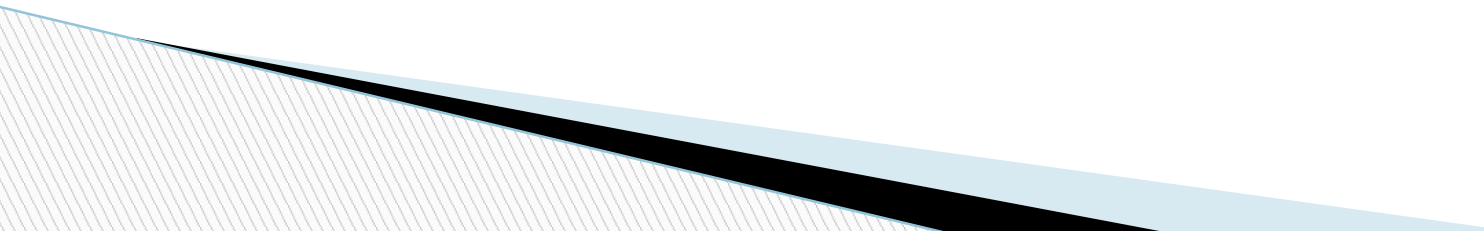


## A.8 Controles tecnológicos

### 8.29 Pruebas de seguridad en el desarrollo y la aceptación

Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas.

Se analizan, diseñan y programan el detalle de las pruebas de aceptación para sistemas nuevos o actualizados, aplicando criterios metodológicos de certificación según las necesidades de la organización.

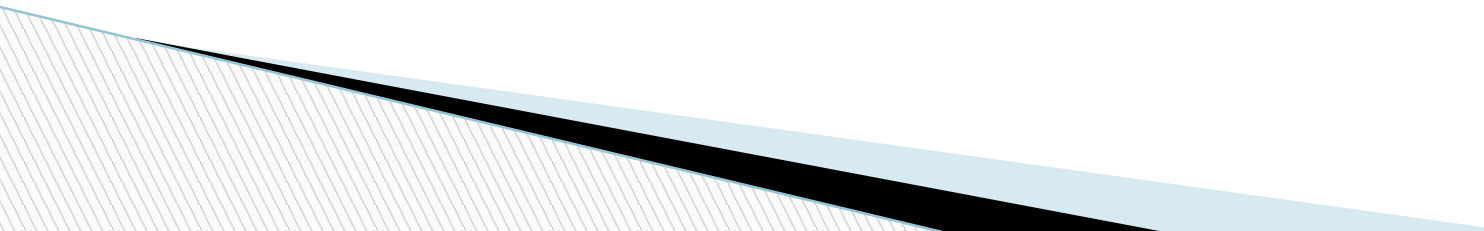


## A.8 Controles tecnológicos

### 8.30 Desarrollo externalizado

La organización debe supervisar y monitorear la actividad del desarrollo del sistema tercerizado.

El desarrollo de software realizado en esquema de outsourcing, debe estar supervisado y monitoreado por la organización previa a la solicitud del requerimiento y después de aprobado el trabajo.



## A.8 Controles tecnológicos

### 8.31 Separación de los entornos de desarrollo, prueba y producción

*Los ambientes para desarrollo, prueba y producción deberían separarse para reducir los riesgos de acceso no autorizado o los cambios al entorno operacional.*

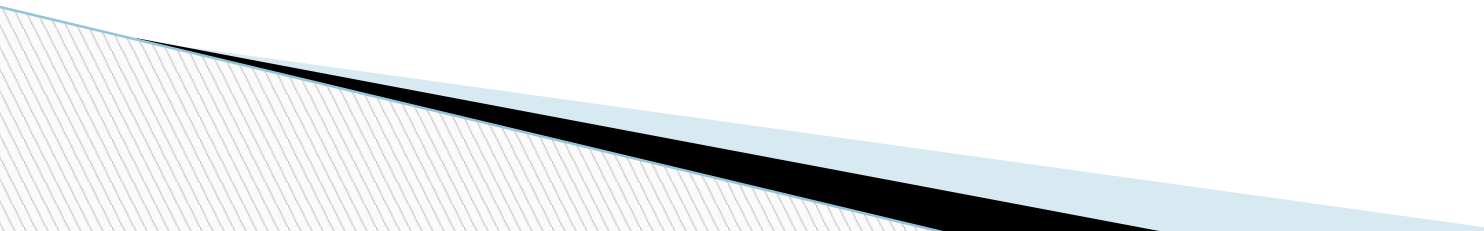
Deberían mantenerse separados los entornos de desarrollo, pruebas y producción.

Los siguientes puntos deberían considerarse:

- a. deberían definirse y documentarse las reglas para transferir el software del ambiente de desarrollo al de operación;
- b. el software de desarrollo y el de producción deberían, si es posible, funcionar en sistemas y procesadores diferentes, y en dominios o directorios distintos;

# A.8 Controles tecnológicos

## 8.31 Separación de los entornos de desarrollo, prueba y producción

- c. probar los cambios en un ambiente de pruebas o ensayos, antes de ser transferidos a producción; las pruebas no deberían hacerse en los sistemas en producción, salvo en circunstancias excepcionales;
  - d. los compiladores, editores y otras herramientas de desarrollo no deberían accederse desde los sistemas en producción;
  - e. emplear cuentas de usuario diferentes para los sistemas en producción y prueba;
  - f. los datos sensibles no deberían copiarse en el ambiente del sistema de prueba, a menos que se proporcionen controles equivalentes.
- 

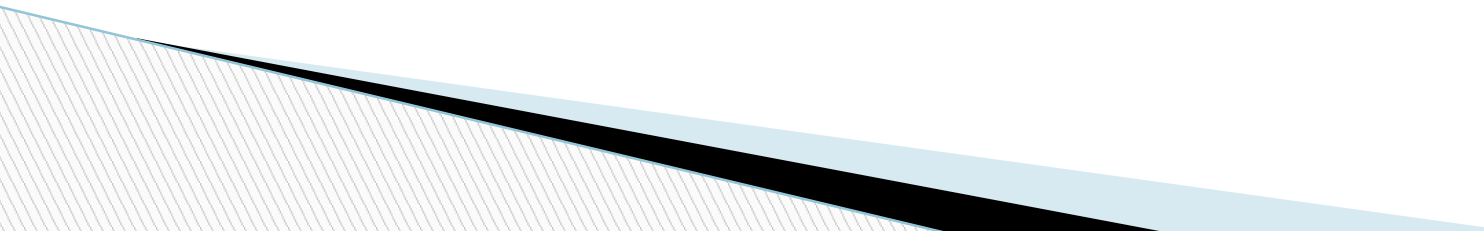


## A.8 Controles tecnológicos

### **8.31 Separación de los entornos de desarrollo, prueba y producción**

Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.

El ambiente de desarrollo debe ser adecuadamente protegido durante el ciclo completo de análisis, diseño y codificación, incluyendo las etapas de integración con otras actividades de desarrollo.



# A.8 Controles tecnológicos

## 8.32 Gestión del cambio

*Deberían controlarse los cambios en la organización, los procesos de negocio, los sistemas e instalaciones de procesamiento de información que afecten a la seguridad de la información.*

En particular deberían considerarse los siguientes elementos:

- a. identificación y registro de cambios significativos;
- b. planificación y pruebas de los cambios;
- c. evaluación de los impactos potenciales de tales cambios;
- d. procedimiento formal de aprobación para los cambios propuestos;
- e. verificación de que se han cumplido los requisitos de seguridad;
- f. comunicación de los detalles del cambio a todas las partes pertinentes;
- g. procedimientos de vuelta atrás (*fallback*)
- h. *proceso de cambios de emergencia*

# A.8 Controles tecnológicos

## 8.32 Gestión del cambio

Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.

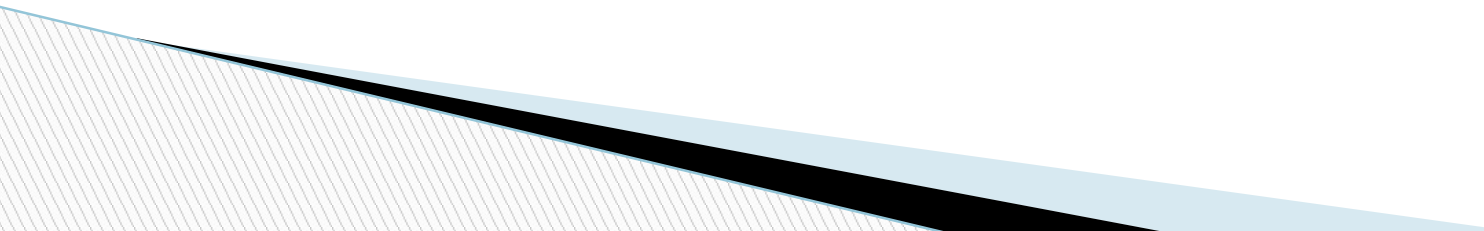
Se diseñan y aplican adecuados procedimientos formales de control de cambios para controlar la implementación de cualquier modificación a los sistemas.

## A.8 Controles tecnológicos

### 8.32 Gestión del cambio

Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.

Cuando se reemplazan, modifican o re-configuran los sistemas operativos, todas las aplicaciones críticas del negocio deben ser revisadas y certificadas para garantizar que no se produzca un impacto adverso en las operaciones o la seguridad de información en la organización.

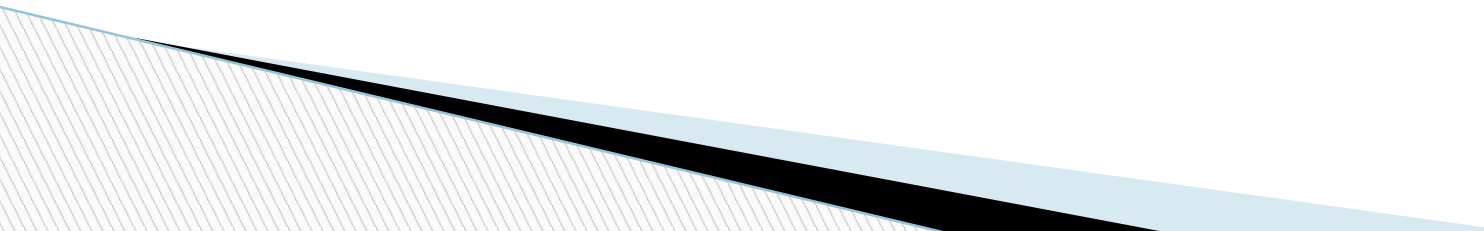


# A.8 Controles tecnológicos

## 8.32 Gestión del cambio

Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.

Las modificaciones de los paquetes de software deben ser controladas y restringidas, limitadas a los cambios necesarios y todos los cambios serán estrictamente supervisados para validar el cumplimiento de las políticas de seguridad de información de la organización.



## A.8 Controles tecnológicos

### 8.33 Gestión del cambio

Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa.

Los datos de prueba del sistema deben ser seleccionados cuidadosamente, protegidos y controlados para prevenir cualquier uso indebido.

## **A.8 Controles tecnológicos**

### **8.34 Protección de los sistemas de información durante las pruebas de auditoría**

Se debe planificar y gestionar adecuadamente las pruebas de auditoría realizadas sobre los sistemas a fin de reducir el riesgo de afectar su operatividad.



# Funcionamiento del SGSI (sesión 10)

Gestión de Seguridad de la información  
Semestre 2023-II

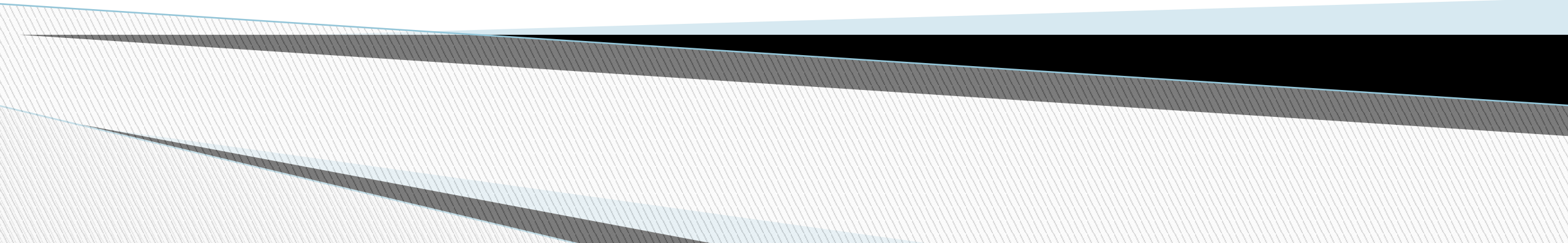


# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

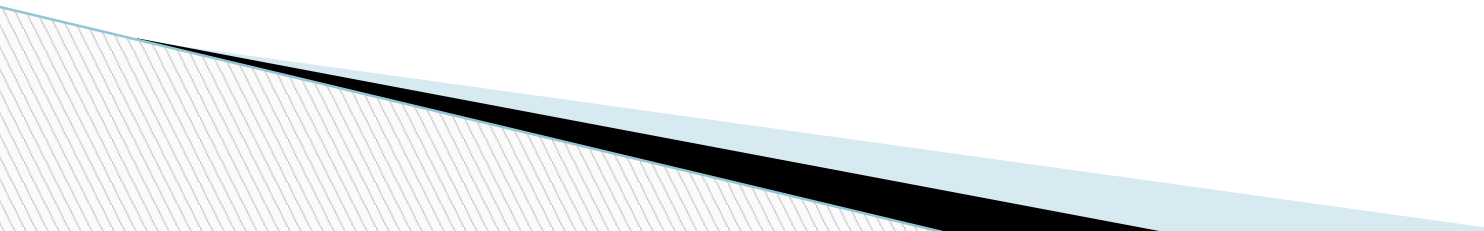
# **Anexo “A”**

## **Controles**



# A.8 Controles tecnológicos

## 8.1 Dispositivos de punto final del usuario

- Debería adoptarse una política y medidas de seguridad de apoyo para gestionar los riesgos introducidos por el uso de dispositivos móviles.
  - Especial cuidado para garantizar que la información de negocios no se vea comprometida.
  - La política de dispositivos móviles debería tener en cuenta los riesgos de trabajar con dispositivos móviles en entornos desprotegidos.
- 

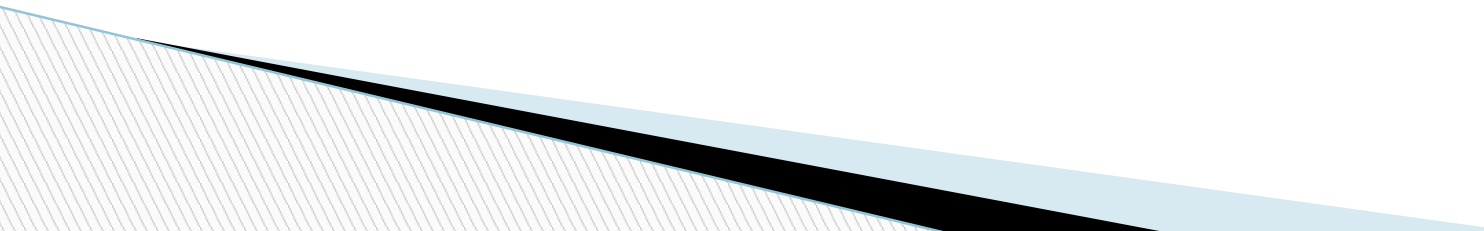
# A.8 Controles tecnológicos

## 8.1 Dispositivos de punto final del usuario

- La política de dispositivos móviles debería considerar:
  - a) el registro de los dispositivos móviles;
  - b) los requisitos de protección física;
  - c) la restricción de instalación de software;
  - d) los requisitos de las versiones de software de los dispositivos móviles
  - e) la restricción de la conexión a los servicios de información;
  - f) los controles de acceso,
  - g) técnicas criptográficas;
  - h) protección contra software malicioso;
  - i) desactivación, eliminación o bloqueo a distancia;
  - j) copias de seguridad;

# A.8 Controles tecnológicos

## 8.1 Dispositivos de punto final del usuario

- Cuidados para uso en lugares públicos y áreas no protegidas (criptografía)
  - Protección física contra robo (Ej. Cadenas de seguridad, en cajones con llave, no dejar juntos token y equipos, etc.)
  - Concienciar al personal sobre los riesgos
  - Protocolos de seguridad inalámbricos
  - Respaldo de información en dispositivos móviles
- 

# A.8 Controles tecnológicos

## 8.1 Dispositivos de punto final del usuario

*Los usuarios deberían asegurarse que los equipos desatendidos tienen la protección apropiada.*

Advertir a usuarios sobre los requisitos y procedimientos de seguridad para proteger equipamiento desatendido

Advertir a usuarios sobre:

- a. terminar sesiones activas o bloquear el equipo;
- b. cerrar sesión de aplicaciones o de servicios de red cuando ya no sea necesario;
- c. asegurar a las computadoras o dispositivos móviles de uso no autorizado mediante una clave de bloqueo o un control equivalente

# A.8 Controles tecnológicos

## 8.2 Derechos de acceso privilegiados

- Debería controlarse la asignación de derechos de acceso privilegiados a través de un proceso formal de autorización de acuerdo con la política de control de acceso. Considerar los siguientes pasos:
  - a. Identificar a los usuarios a los que es necesario asignar acceso privilegiado a cada sistema o proceso; Ej. sistema operativo, base de datos y cada aplicación.
  - b. los derechos de acceso privilegiados deberían asignarse a usuarios sobre la base de necesidad de uso, basados en el requisito mínimo para sus roles funcionales;

# A.8 Controles tecnológicos

## 8.2 Derechos de acceso privilegiados

- c. Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los derechos de acceso privilegiados no deberían otorgarse hasta que el proceso de autorización no sea completado;
- d. Definir requisitos para la expiración de los derechos de acceso
- e. los derechos de acceso privilegiados deberían asignarse a una *ID de usuario diferente de la utilizada para las actividades regulares del negocio*. Las actividades regulares del negocio no deberían ser desempeñadas desde las cuentas privilegiadas;



# A.8 Controles tecnológicos

## 8.2 Derechos de acceso privilegiados

- f. deberían revisarse regularmente las competencias de los usuarios para con los derechos de acceso privilegiados, a fin de verificar si se encuentran alineadas con sus funciones;
- g. deberían establecerse y mantenerse procedimientos específicos para evitar el uso no autorizado de ID de usuarios de administración genéricos.
- h. mantenerse la confidencialidad de la contraseña (Ej. cambio periódico de contraseñas y cambio a la brevedad cuando un usuario privilegiado deja o cambia de trabajo).

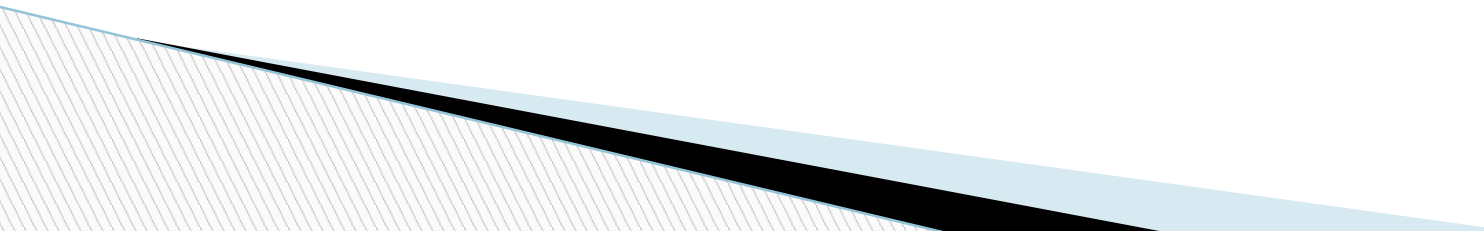
# A.8 Controles tecnológicos

## 8.3 Restricción del acceso a la información

- Las restricciones de acceso deberían basarse en los requisitos de negocio y estar de acuerdo con la política de control de acceso.
- Debería considerarse:
  - a. proveer menús para controlar el acceso a las funciones del sistema de aplicaciones;
  - b. controlar los datos que pueden ser accedidos por un usuario particular;
  - c. controlar los derechos de acceso de los usuarios, por ejemplo leer, escribir, borrar y ejecutar;

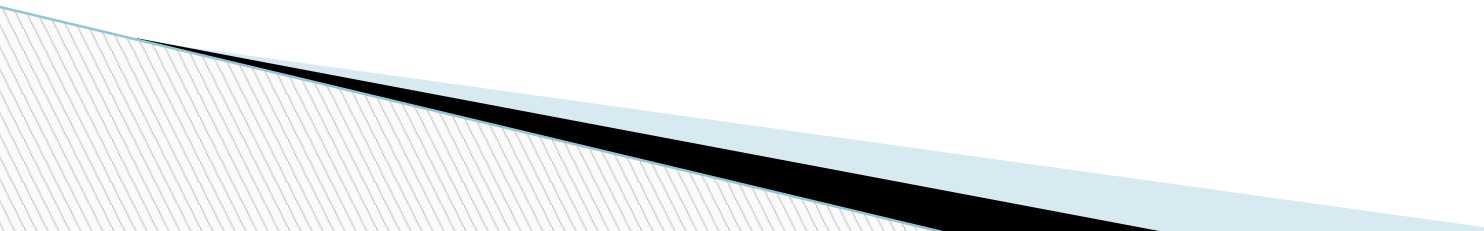
# A.8 Controles tecnológicos

## 8.3 Restricción del acceso a la información

- d. controlar los derechos de acceso de otras aplicaciones;
  - e. limitar la información contenida en las salidas;
  - f. proporcionar controles de acceso físico o lógico para aislar las aplicaciones sensibles, datos de aplicación o sistemas.
- 

# A.8 Controles tecnológicos

## 8.4 Acceso al código fuente

- El acceso al código fuente de programas debería ser estrictamente controlado, para prevenir la introducción de una funcionalidad no autorizada, evitar cambios involuntarios, así como a mantener la confidencialidad de la propiedad intelectual valiosa.
  - Para el código fuente de programas, esto puede lograrse mediante el almacenamiento centralizado, controlado de dicho código, preferiblemente en las bibliotecas de programas fuentes.
- 

# A.8 Controles tecnológicos

## 8.4 Acceso al código fuente

- Considerar las siguientes directrices para controlar el acceso a la biblioteca de programas fuente:
  - a. de ser posible, las bibliotecas de programas fuente no deberían mantenerse en los sistemas en producción;
  - b. el código fuente de programas y las bibliotecas de programas fuente deberían gestionarse según procedimientos establecidos;
  - c. el personal de apoyo debería tener acceso restringido a bibliotecas fuente de programas;
  - d. la actualización de bibliotecas de programas fuente y artículos asociados, y la entrega de programas fuente a programadores sólo debería realizarse después de que la autorización ha sido recibida;

# A.8 Controles tecnológicos

## 8.4 Acceso al código fuente

- e. los listados de programas deberían mantenerse en un entorno seguro;
- f. debería mantenerse un registro de auditoría de todos los accesos a bibliotecas fuentes de programas;
- g. el mantenimiento y la copia de bibliotecas fuente de programas deberían estar sujetos a procedimientos estrictos de control de cambio.

Si el código fuente del programa va a ser publicado, deberían considerarse controles adicionales para ayudar a conseguir garantías sobre su integridad (por ejemplo, la firma digital).

# A.8 Controles tecnológicos

## 8.5 Autenticación segura

- Debería elegirse una técnica de autenticación adecuada para corroborar la identidad declarada de un usuario.
- Cuando se requiere una fuerte autenticación y verificación de la identidad, deberían utilizarse métodos alternativos / complementarios a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, señales o medios biométricos.
- El procedimiento para iniciar sesión en un sistema o aplicación debería ser diseñado para minimizar la de acceso no autorizado. Por lo tanto, el proceso de inicio de sesión (*logon*) debería divulgar el mínimo de información sobre el sistema o aplicación, de manera de evitar proveer a un usuario no autorizado con asistencia innecesaria.

# A.8 Controles tecnológicos

## 8.5 Autenticación segura

- Un buen procedimiento de inicio de sesión (*log-on*) debería:
  - a. no mostrar identificación del sistema o aplicación hasta que termine el proceso de inicio de sesión;
  - b. desplegar un mensaje genérico advirtiendo que el sistema debería accederse solamente por usuarios autorizados;
  - c. no ofrecer mensajes de ayuda durante el proceso de inicio de sesión (*log-on*) que puedan guiar a usuarios no autorizados;
  - d. validar la información de inicio de sesión (*log-on*) sólo tras rellenar todos sus datos de entrada. Si se produce una condición de error, el sistema no debería indicarse qué parte de esos datos es correcta o incorrecta;



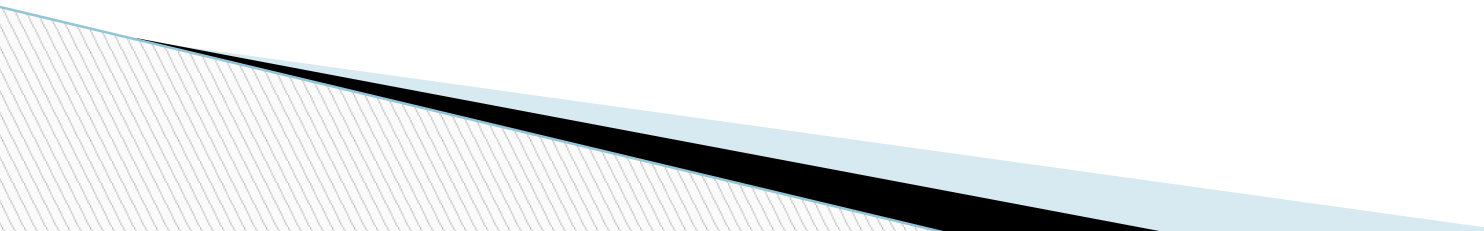
# A.8 Controles tecnológicos

## 8.5 Autenticación segura

- e. proteger contra intentos de inicio de sesión por fuerza bruta;
- f. registrar los intentos fallidos y exitosos de conexión;
- g. ejecutar un evento de seguridad si se detecta una posible violación fallida o exitosa de los controles de inicio de sesión;
- h. mostrar la siguiente información tras completar una conexión con éxito:
  - i. fecha y hora de la anterior inicio de sesión (*log-on*) realizada con éxito;
  - ii. detalles de cualquier intento de conexión fallido desde el momento de la última conexión realizada con éxito.

# A.8 Controles tecnológicos

## 8.5 Autenticación segura

- i. no mostrar la contraseña que está siendo ingresada;
  - j. no transmitir contraseñas en texto claro por la red;
  - k. cancelar sesiones inactivas después de un período de inactividad definido, especialmente en las ubicaciones de alto riesgo, tales como en las áreas públicas o en los dispositivos móviles;
  - l. restringir los tiempos de conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidades para el acceso no autorizado. (Ej. Realización de fraude luego del horario regular de trabajo)
- 

# A.8 Controles tecnológicos

## 8.6 Gestión de la capacidad

El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.

# A.8 Controles tecnológicos

## 8.7 Protección contra el malware

*Los controles de detección, prevención y recuperación para proteger ante software malicioso deberían ser implementados, combinados con el conocimiento correspondiente del usuario.*

La protección ante software malicioso debería basarse en el empleo de sistemas de detección y reparación, en la conciencia de la seguridad, y en apropiados controles de acceso al sistema y gestión de cambios.

Las siguientes directrices deberían considerarse:

- a. prohibición del uso de software no autorizado
- b. controles que previenen o detectan el uso de software no autorizado;
- c. controles que previenen o detectan el uso de sitios web maliciosos;

# A.8 Controles tecnológicos

## 8.7 Protección contra el malware

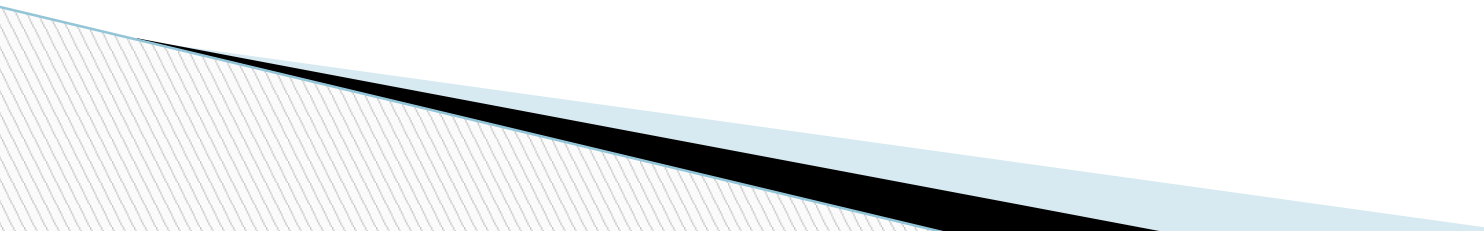
- d. indicar medidas de seguridad a adoptar al obtener archivos y software por redes externas.
- e. reducción de las vulnerabilidades técnicas
- f. revisiones regulares del contenido de datos y software que soportan los procesos críticos del negocio;
- g. la instalación y actualización regular de software para detección de software malicioso.
- h. Procedimientos de gestión de software para detección de soft. malic.
- i. Planes de recuperación, incluyendo el aislamiento de entornos críticos
- j. Información de peligros a través de listas o páginas web

# A.8 Controles tecnológicos

## 8.8 Gestión de las vulnerabilidades técnicas

*Debería obtenerse en forma regular información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información en uso, debería evaluarse la exposición de la organización a tales vulnerabilidades, y deberían tomar medidas apropiadas para abordar el riesgo asociado.*

*Considerar lo siguiente:*

- a. Manejo de parches
  - b. Definición de recursos para identificación de vulnerabilidades
  - c. Cronograma para levantamiento de vulnerabilidades
- 

# A.8 Controles tecnológicos

## 8.8 Gestión de las vulnerabilidades técnicas

- d. Probar el parche antes de su aplicación
- e. Priorizar la reducción de vulnerabilidades
- f. Vincular la gestión de incidentes con el manejo de vulnerabilidades

# A.8 Controles tecnológicos

## 8.9 Gestión de la configuración

Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.



# A.8 Controles tecnológicos

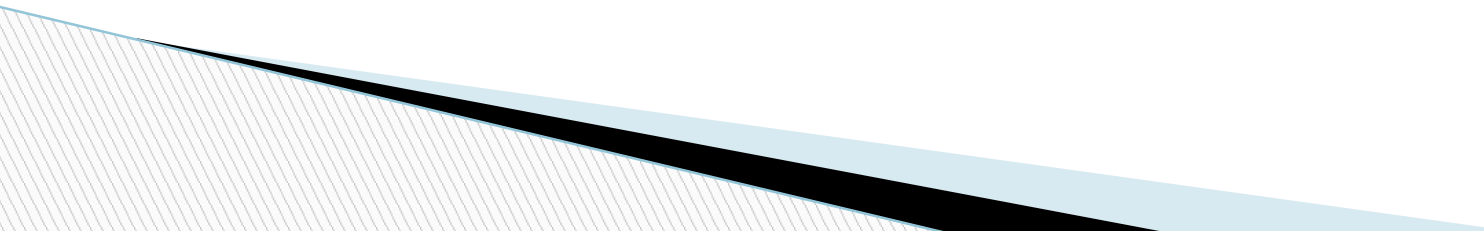
## 8.10 Eliminación de información

La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.

## A.8 Controles tecnológicos

### 8.11 Enmascaramiento de datos

El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.



# A.8 Controles tecnológicos

## 8.12 Prevención de la fuga de datos

Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

## A.8 Controles tecnológicos

### 8.13 Información de respaldo

*Deberían hacerse regularmente copias de respaldo de la información y del software y probarse regularmente acorde con la política de respaldo aceptada.*

Definir una política de respaldo, incluyendo los requisitos de protección y retención.

Mantener copias de respaldo en instalaciones adecuada para asegurar la recuperación en caso de desastre.

# A.8 Controles tecnológicos

## 8.13 Información de respaldo

Elaborar un plan de respaldo, considerando:

- Grado (completo, diferencial) y frecuencia de respaldo
- Almacenamiento en lugar apartado y seguro
- Protección ambiental y física de copias de respaldo
- Probar copias para asegurar funcionamiento
- En caso de información confidencial, cifrar copia de respaldo

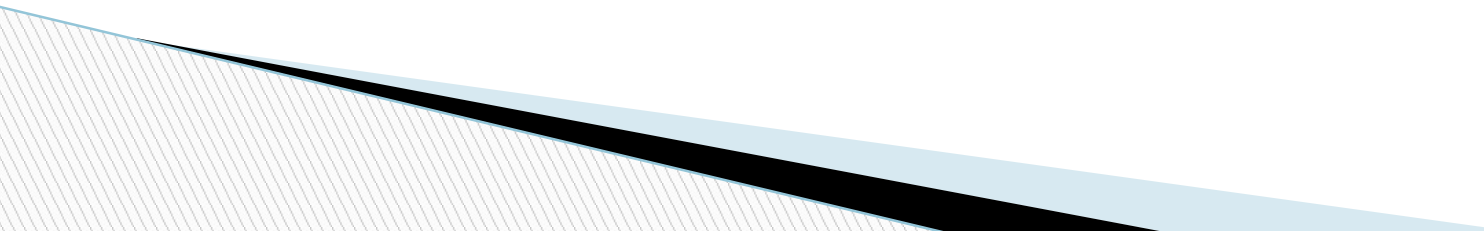
Establecer procedimientos de generación de copias, monitoreo, acciones en caso de falla, etc.



## A.8 Controles tecnológicos

### 8.14 Redundancia de las instalaciones de tratamiento de la información

*Deberían implantarse las instalaciones de procesamiento de información con la redundancia suficiente para cumplir con los requisitos de disponibilidad.*

- Identificar los requisitos para la disponibilidad de los sistemas de información. Cuando la disponibilidad no puede ser garantizada mediante la arquitectura existente de los sistemas, deberían considerarse los componentes o las arquitecturas redundantes.
  - Las redundancias deben ser probadas
  - Considerar los riesgos asociados a la aplicación de redundancias (Integridad, confidencialidad).
- 

# A.8 Controles tecnológicos

## 8.15 Registro


*Los registros de eventos que registran actividades del usuario, excepciones, fallas y eventos de seguridad de la información deberían ser producidos, mantenidos y revisados regularmente.*

Los registros de eventos deberían incluir, cuando corresponda:

- a. ID de usuario;
- b. actividades del sistema;
- c. fechas, horarios y detalles de los eventos clave, por ejemplo, inicio y cierre de sesión;
- d. identidad o ubicación del dispositivo, si es posible, y el identificador del sistema;

# A.8 Controles tecnológicos

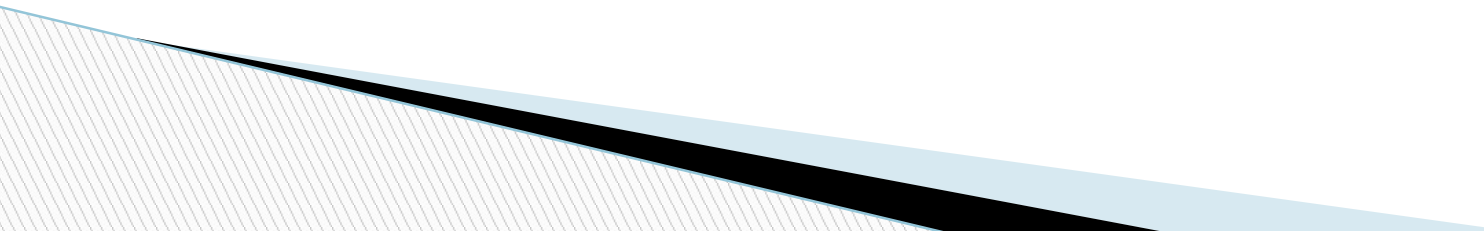
## 8.15 Registro

- e. registros de intentos de acceso al sistema exitosos y rechazados;
  - f. cambios en la configuración del sistema;
  - g. uso de utilidades y aplicaciones del sistema;
  - h. archivos accedidos y tipo de acceso;
  - i. direcciones y protocolos de red;
  - j. alarmas lanzadas por el sistema de control de acceso;
  - k. activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y sistemas de detección de intrusos;
- 



# A.8 Controles tecnológicos

## 8.15 Registro

- l. registros de las transacciones realizadas por los usuarios en las aplicaciones.
  - El registro de eventos establece las bases para los sistemas de control automatizados, que son capaces de generar informes consolidados y alertas en la seguridad del sistema.
  - Los registros podrían contener información confidencial
  - Restringir el acceso a borrar y deshabilitar los registros de ser posible a los administradores
- 

# A.8 Controles tecnológicos

## 8.15 Registro

*Los medios de registro y la información de registros deberían protegerse contra su alteración y acceso no autorizado.*

Considerar controles para evitar:

- a. Cambios en la configuración de registros (qué se registra)
- b. Edición o eliminación de registros
- c. Pérdida de registros por falta de espacio de almacenamiento o sobre-escritura

Definir criterios de retención de registros



## A.8 Controles tecnológicos

### 8.15 Registro

*Las actividades del administrador y operador del sistema deberían registrarse y los registros deberían protegerse y revisarse regularmente.*

Es necesario proteger y revisar los registros para verificar que el personal con cuentas privilegiadas no altere los registros.

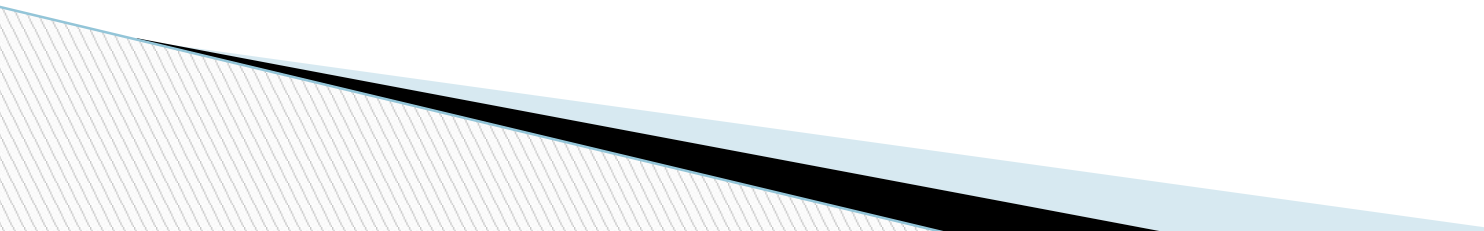
# A.8 Controles tecnológicos

## 8.16 Actividades de seguimiento

Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.

# A.8 Controles tecnológicos

## 8.17 Sincronización de relojes

- Los registros inexactos restarán credibilidad y consistencia a las pruebas (*Ej. Investigación de correo electrónico*)
  - Servidores externos para sincronización (Ej. Ntp.org, times.windows.com, etc.)
  - Protocolo de sincronización (Ej. NTP)
- 



# Funcionamiento del SGSI (sesión 9)

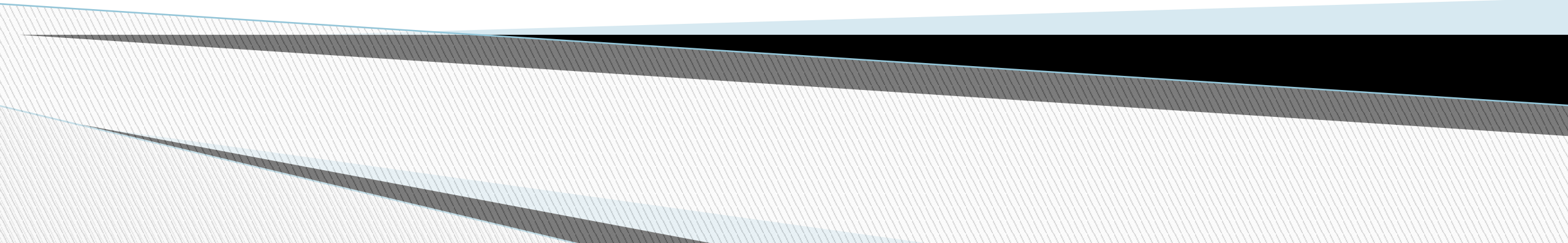
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

# **Anexo “A”**

## **Controles**





# A.7 Controles físicos

## 7.1 Perímetro de seguridad física

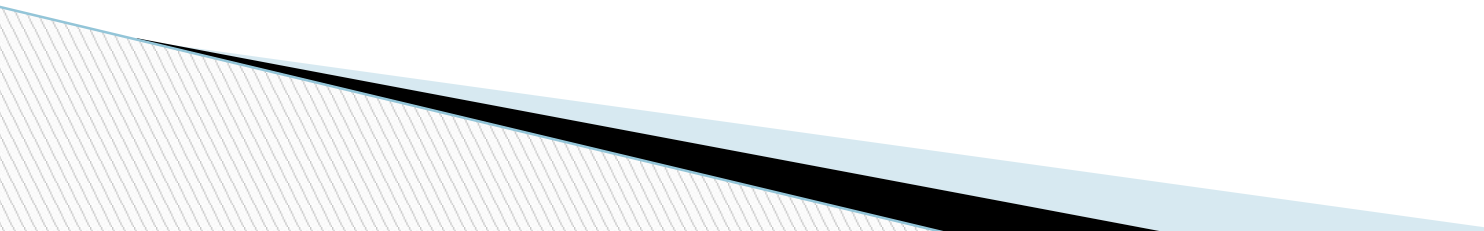
*Deberían definirse y utilizarse los perímetros de seguridad para proteger las áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.*

Debería considerarse lo siguiente:

- a. la ubicación y la resistencia de cada uno de los perímetros deberían depender de los requisitos de la seguridad de los activos y de los resultados de una evaluación de riesgos;
- b. Solidez física de muros, pisos y paredes, puertas reforzadas para evitar acceso no autorizado (p.e. vallas, alarmas, cerraduras, etc.). Ventanas de pisos bajos deberían estar bloqueadas cuando no tienen custodia; considerar protección externa principalmente en pisos bajos.

# A.7 Controles físicos

## 7.1 Perímetro de seguridad física

- c. debería haber un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio; restringirse sólo al personal autorizado;
  - d. donde sea aplicable, deberían construirse barreras físicas para evitar el acceso físico no autorizado y la contaminación del entorno;
  - e. todas las puertas contra incendios del perímetro de seguridad deberían tener alarma, ser supervisadas y probadas conjuntamente con las paredes para establecer el nivel requerido de resistencia de acuerdo a las normas (incluyendo protección contra el fuego).
- 

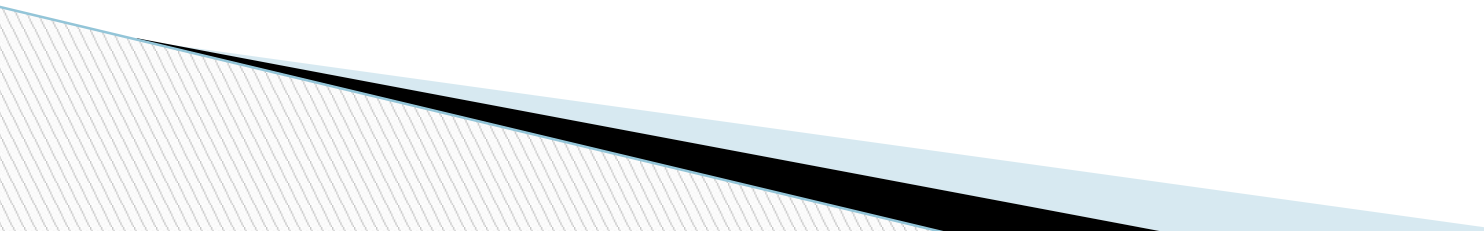
# A.7 Controles físicos

## 7.1 Perímetro de seguridad física

- f. Considerar sistemas de detección de intrusos adecuados y probar regularmente para cubrir todas las puertas externas y ventanas accesibles; las áreas desocupadas deberían contar con alarmas siempre; también debería proporcionarse protección para otras áreas, por ejemplo, sala de computadoras o cuartos de comunicaciones;
- g. las instalaciones de procesamiento de información gestionadas por la organización deberían separarse físicamente de aquellas gestionadas por terceras partes.

# A.7 Controles físicos

## 7.1 Perímetro de seguridad física

- múltiples barreras brindan protección adicional, pues la falla de una barrera no significará que la seguridad se vea comprometida
  - un área segura puede ser una oficina cerrada, o varios cuartos rodeados por una barrera física continua interna de seguridad. Las barreras adicionales y los perímetros para controlar el acceso físico pueden ser necesarios entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad.
  - consideraciones especiales en los edificios donde funcionan múltiples organizaciones.
  - adaptarse a las circunstancias técnicas y económicas de la organización, según se establece en la evaluación de riesgos.
- 

# A.7 Controles físicos

## 7.2 Entrada física

*Las áreas de seguridad deberían estar protegidas por controles de entrada apropiados que aseguren que sólo se permite el acceso de personal autorizado.*

Considerar lo siguiente:

- a. la fecha y hora de entrada y salida de visitantes deberían restringirse, y todos los visitantes deberían supervisarse a menos que su acceso se haya aprobado previamente; el acceso debería concederse sólo para propósitos específicos, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia. La identidad de los visitantes debería ser autenticada

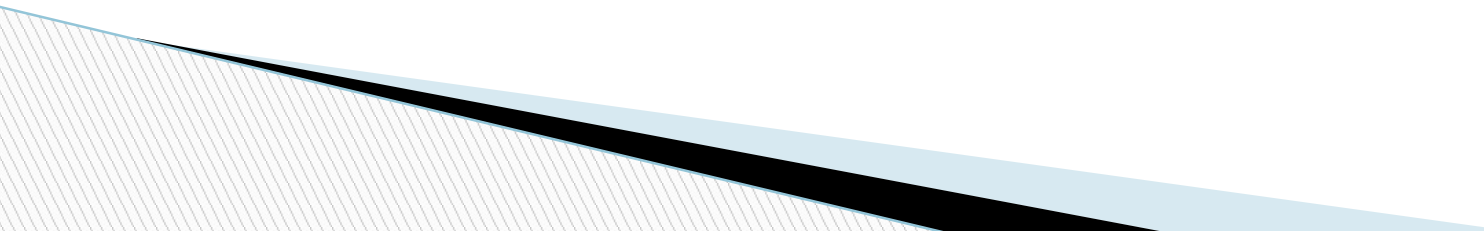
# A.7 Controles físicos

## 7.2 Entrada física

- b. el acceso a las áreas donde se procesa o se almacena la información sensible debería ser restringido sólo a las personas autorizadas mediante la implementación de controles de acceso, p.e. mediante la implementación de un mecanismo de fuerte autenticación
- c. debería mantenerse libro de registro físico o electrónico de auditoría;
- d. debería requerirse a todos los empleados, contratistas y partes externas usar algún tipo de identificación visible. Reportar cualquier incumplimiento.

# A.7 Controles físicos

## 7.2 Entrada física

- e. el acceso del personal de soporte de terceras partes a las áreas seguras o a las instalaciones sensibles de procesamiento de la información debe otorgarse sólo cuando sea requerido; este acceso debería ser autorizado y supervisado;
  - f. los derechos de acceso a las áreas seguras deberían ser regularmente revisados y actualizados, y revocados cuando sea necesario.
- 

# A.7 Controles físicos

## 7.2 Entrada física

*Los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones deberían controlarse, y si es posible, aislarlos de instalaciones de procesamiento de la información para evitar el acceso no autorizado.*

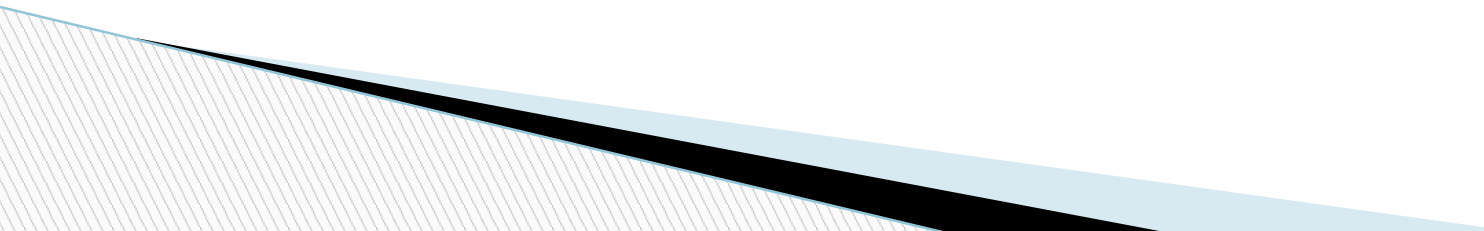
Considerar lo siguiente:

- a. debería restringirse el acceso al área de entrega y carga desde el exterior únicamente al personal autorizado e identificado;
- b. el área de entrega y carga debería diseñarse para que los suministros puedan cargarse y descargarse sin que el personal de depósito tenga acceso a otras zonas del edificio;



# A.7 Controles físicos

## 7.2 Entrada física

- d. el material entrante debería inspeccionarse y examinarse en busca de explosivos, químicos u otros materiales peligrosos,
  - e. el material entrante debería registrarse de acuerdo con el procedimiento de gestión de activos al entrar en el lugar;
  - f. cuando sea posible, los envíos entrantes y salientes deberían separarse físicamente
  - g. el material entrante debería inspeccionarse para saber si hay pruebas de manipulación indebida.
- 

# A.7 Controles físicos

## 7.3 Asegurar las oficinas, salas e instalaciones

*Debería diseñarse y aplicarse la seguridad física para oficinas, despachos e instalaciones.*

Considerar lo siguiente:

- a. las instalaciones claves deberían situarse de manera de evitar el acceso público;
- b. cuando corresponda, los edificios deberían ser discretos y dar el mínimo indicio de su propósito, cuando sea posible, sin dar muestras obvias, fuera o dentro del edificio, que identifiquen la presencia de las actividades de procesamiento de la información;

# A.7 Controles físicos

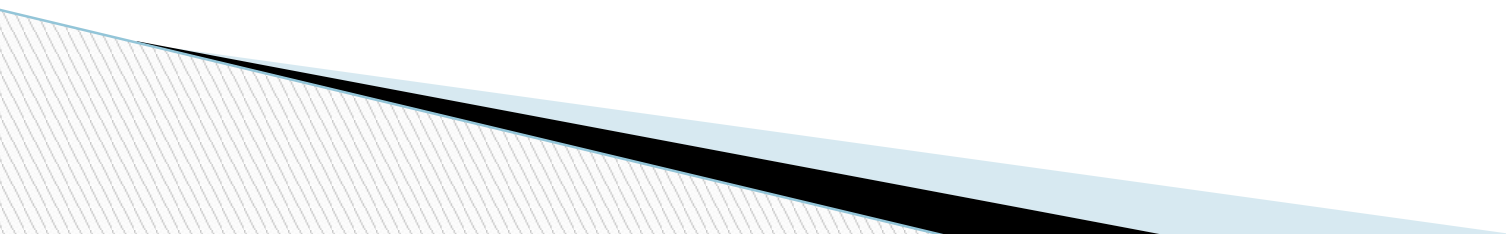
## 7.3 Asegurar las oficinas, salas e instalaciones

- c. las instalaciones deberían estar configuradas para evitar que la información confidencial o las actividades sean visibles y audibles desde el exterior. Cuando corresponda, debería considerarse el blindaje electromagnético.

## **A.7 Controles físicos**

### **7.4 Asegurar las oficinas, salas e instalaciones**

Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.

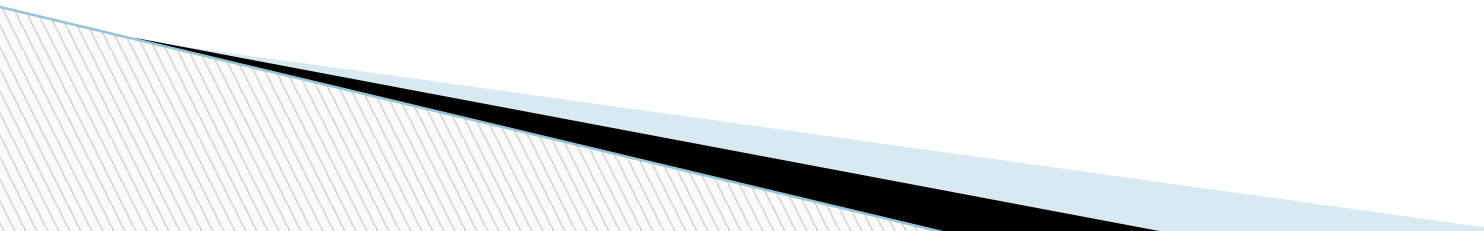


## A.7 Controles físicos

### 7.5 Protección contra las amenazas físicas y medioambientales

*Deberían diseñarse y aplicarse protección física contra desastres naturales, ataques maliciosos o accidentes.*

Debería obtenerse asesoramiento especializado sobre cómo evitar los daños causados por incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o artificiales.




# A.7 Controles físicos

## 7.6 Trabajar en zonas seguras

*Deberían diseñarse y aplicarse procedimientos para trabajar en áreas seguras*

Considerar lo siguiente:

- a. el personal sólo debería conocer la existencia de un área segura, o de sus actividades, si lo necesitara para su trabajo;
  - b. debería evitarse el trabajo no supervisado en áreas seguras
  - c. las áreas seguras desocupadas deberían cerrarse y controlarse
  - d. no debería permitirse la presencia de equipos de fotografía, video, audio u otras formas de registro, salvo autorización expresa.
- 

# A.7 Controles físicos

## 7.7 Escritorio y pantalla despejados

*Debería adoptarse una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.*

Tener en cuenta la clasificación de la información, requisitos legales y contractuales, los aspectos culturales y de riesgo de la organización.

Considerar:

- a. la información sensible o crítica del negocio, contenida por ejemplo en medios de almacenamiento electrónicos o en papel, debería asegurarse bajo llave, especialmente cuando la oficina está vacía;

# A.7 Controles físicos

## 7.7 Escritorio y pantalla despejados

- b. las computadoras y terminales deberían protegerse con un mecanismo de bloqueo de pantalla, cuando está desatendida.
- c. debería prevenirse el uso no autorizado de fotocopadoras y otras tecnologías de reproducción (por ejemplo escáneres, cámaras digitales). Considerar el uso de clave para impresión.
- d. documentación conteniendo información clasificada o sensible debería retirarse de las impresoras inmediatamente.



# A.7 Controles físicos

## 7.8 Ubicación y protección de los equipos

*El equipamiento debería ubicarse o protegerse para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.*

Considerar lo siguiente:

- a. el equipamiento debería situarse de manera de minimizar el acceso innecesario a las áreas de trabajo;
- b. las instalaciones de procesamiento de la información que manejan datos sensibles deberían colocarse cuidadosamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso.

# A.7 Controles físicos

## 7.8 Ubicación y protección de los equipos

- c. las instalaciones de almacenamiento deberían asegurarse para evitar el acceso no autorizado;
- d. los elementos que requieran protección especial deberían aislarse para reducir el nivel general de protección requerida;
- e. deberían adoptarse controles para reducir al mínimo el riesgo de amenazas físicas potenciales, tales como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética, y vandalismo;

# A.7 Controles físicos

## 7.8 Ubicación y protección de los equipos

- f. definir restricciones para comer, beber, y fumar en proximidad de las instalaciones de procesamiento de la información;
- g. las condiciones ambientales, tales como temperatura y humedad, deberían supervisarse para verificar que las mismas no afectan negativamente el funcionamiento de las instalaciones
- h. deberían colocarse pararrayos sobre todos los edificios y deberían aplicarse filtros de protección contra rayos a todas las líneas entrantes de energía y de comunicaciones;

# A.7 Controles físicos

## 7.8 Ubicación y protección de los equipos

- i. debería considerarse el uso de métodos de protección especial, como las cubiertas de teclados, para el equipamiento ubicado en entornos industriales;
- j. debería protegerse el equipamiento que procese información sensible para reducir al mínimo el riesgo de fuga de información debido a la emanación electromagnética.

# A.7 Controles físicos

## 7.9 Ubicación y protección de los equipos

*Deberían aplicarse medidas de seguridad a los activos fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de las mismas.*

- El uso de cualquier equipamiento que almacene o procese información fuera de las instalaciones de la organización, debería autorizarse por la Dirección. Esto se aplica a los equipamientos de la organización y al equipamiento de propiedad privada utilizado en nombre de la organización.

Considerar lo siguiente:

- a. los equipos y soportes que contengan datos con información y sean sacados de su entorno habitual no deberían dejarse desatendidos en sitios públicos;

# A.7 Controles físicos

## 7.9 Ubicación y protección de los equipos

- b. deberían observarse siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos;
- c. los controles para las ubicaciones fuera de los locales , tales como el trabajo en el domicilio, el teletrabajo y los sitios temporales deberían determinarse mediante una evaluación de los riesgos y aplicarse los controles convenientes según sea apropiado, por ejemplo, gabinetes para archivos con cerradura, una política de escritorios limpios, controles de acceso a las computadoras y comunicaciones seguras con la oficina (ver la Norma ISO/IEC 27033 Seguridad en Redes);

# A.7 Controles físicos

## 7.9 Ubicación y protección de los equipos

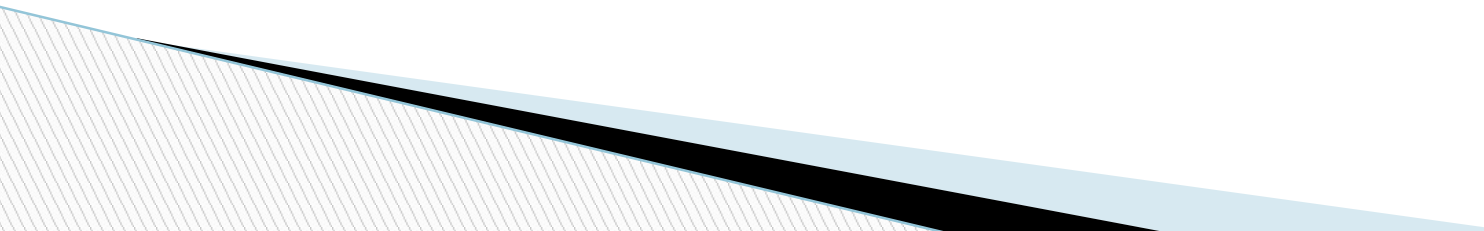
- d. cuando el equipamiento de fuera de las instalaciones es transferido entre diferentes personas o partes externas, debería mantenerse un registro que defina la cadena de custodia para el equipamiento, incluyendo como mínimo, los nombres y las organizaciones de aquellos que son responsables del equipamiento.

Notas:

- Los riesgos, por ejemplo, los daños, hurto o espionaje, pueden variar considerablemente entre las locaciones.
- El equipamiento de almacenamiento y procesamiento de la información comprende todo tipo de computadoras personales, organizadores, teléfonos móviles, tarjetas inteligentes, documentos u otros, que se lleven al domicilio o fuera del lugar habitual de trabajo.

# A.7 Controles físicos

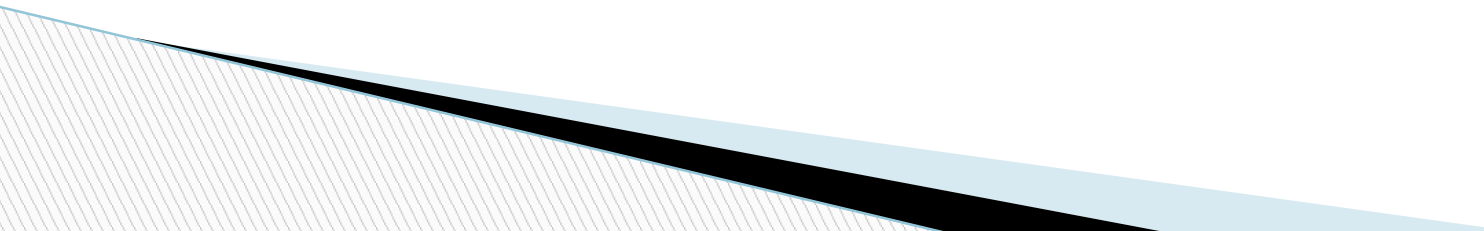
## 7.10 Medios de almacenamiento

- Considerar:
    - a) si ya no son necesarios, los contenidos de los medios reutilizables que deberían retirarse de la organización deberían hacerse irrecuperables;
    - b) cuando sea necesario y práctico, se debería requerirse autorización para los medios a retirar de la organización y debería mantenerse un registro de dichas extracciones, a fin de mantener un registro de auditoría;
    - c) todos los medios deberían almacenarse en un entorno seguro, de acuerdo con las especificaciones del fabricante;
- 



# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- d) si la confidencialidad o la integridad de los datos son consideraciones importantes, deberían utilizarse técnicas criptográficas para proteger los datos en los medios extraíbles;
  - e) para mitigar el riesgo de degradación de los medios mientras se necesitan los datos almacenados, los datos deberían transferirse a medios nuevos antes de convertirse en ilegibles;
  - f) deberían almacenarse varias copias de los datos valiosos en un medio independiente para reducir aún más el riesgo del daño o pérdida de los datos coincidentes;
- 

# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- Deberían establecerse procedimientos formales para la eliminación segura de los medios para minimizar el riesgo de fuga de información confidencial.
- Los procedimientos para la eliminación segura de los medios que contienen información confidencial deberían ser proporcionales a la sensibilidad de esa información.
- Considerar:
  - a) los medios que contienen información confidencial deberían almacenarse y eliminarse de forma segura, por ejemplo, mediante incineración o trituración, o el borrado de datos para su uso por otra aplicación dentro de la organización;

# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- b) establecer procedimientos para identificar los elementos que puedan requerir la eliminación segura;
- c) mas sencillo es obligar a que medios sean recopilados y eliminados de forma segura, en lugar de tratar de separar los elementos sensibles;
- d) En caso de emplear servicios de empresas especializadas, tener cuidado en su selección (controles y experiencia adecuados)
- e) la eliminación de los elementos sensibles debería registrarse a fin de mantener un registro de auditoría.

*(Ej. Degausser, borrado con datos aleatorios)*

# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- Considerar el efecto de agregación
- Los dispositivos dañados que contienen datos sensibles pueden requerir una evaluación de riesgos para determinar si los elementos deberían ser destruidos físicamente en lugar de ser enviados para su reparación o descarte

# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- Deberían considerarse las siguientes directrices para proteger a los medios que contienen información que es transportada:
  - a) transportes o mensajeros confiables;
  - b) debería acordarse con la dirección una lista de mensajeros autorizados;
  - c) deberían desarrollarse procedimientos para verificar la identificación de los mensajeros;

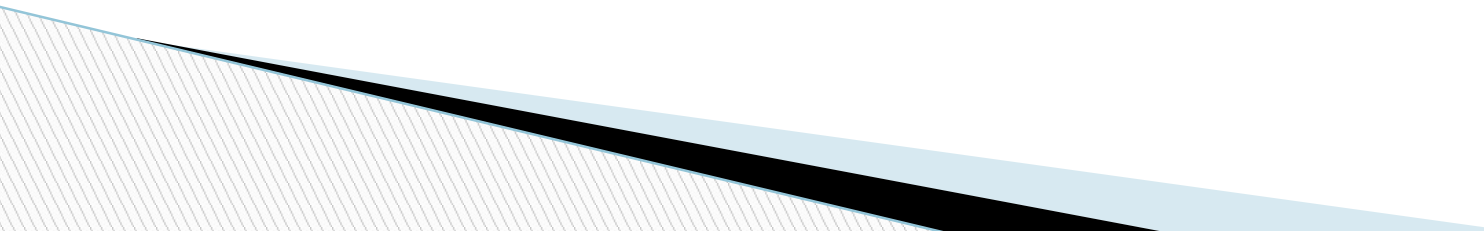
# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- d) consideraciones del embalaje el embalaje (daño físico, factores ambientales – calor, la humedad o los campos electromagnéticos)
- e) mantener registros para identificar el contenido de los medios, la protección aplicada así como el registro de los tiempos de transferencia a los guardias y la recepción en el destino.

# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- La información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte físico, por ejemplo, al enviar los medios a través del servicio postal o por mensajería.
  - Cuando la información confidencial en los medios no se encuentra cifrada, debería considerarse la protección física adicional de los medios.
- 

# A.7 Controles físicos

## 7.10 Medios de almacenamiento

*Los equipamientos, la información o el software no deberían retirarse de las instalaciones de la organización sin autorización previa.*

Considerar lo siguiente:

- a. deberían identificarse aquellos empleados y usuarios de terceras partes que tengan autoridad para permitir el retiro de activos fuera de los locales de la organización;
- b. debería fijarse los límites de tiempo para el equipamiento retirado y verificar el cumplimiento del retorno;
- c. debería registrarse tanto la salida del equipamiento del local, como el retorno del mismo;



# A.7 Controles físicos

## 7.10 Medios de almacenamiento

- Considerar controles de inspección para detectar y prevenir el ingreso no autorizado a las instalaciones, de dispositivos de grabación, armas, etc. Los individuos deberían estar en conocimiento de que estas instancias de inspección serán llevadas a cabo, y las mismas deberían realizarse solamente con la autorización apropiada según los requisitos legales y reguladores.

# A.7 Controles físicos

## 7.11 Servicios de apoyo

*Debería protegerse el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causados por fallas en los servicios de apoyo.*

Los elementos de soporte (por ejemplo, la electricidad, las telecomunicaciones, el agua potable, el gas, el alcantarillado, la ventilación y el aire acondicionado) deberían:

- a. cumplir con las especificaciones del fabricante de los equipamientos y con los requisitos legales locales;
- b. Evaluar su capacidad para cumplir con el crecimiento del negocio y las interacciones con otros elementos de soporte;
- c. ser inspeccionados y probados regularmente para asegurar su buen funcionamiento;

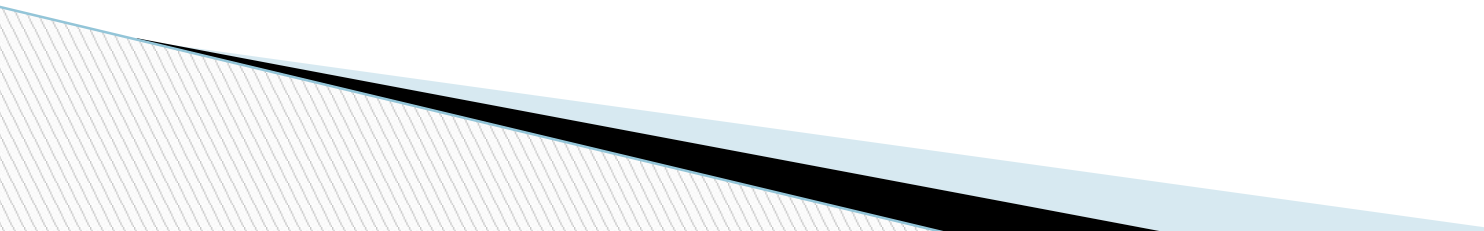
# A.7 Controles físicos

## 7.11 Servicios de apoyo

- d. si es necesario, implementar alarmas para detectar fallos de funcionamiento;
- e. si es necesario, tener múltiples canales con diversos enrutamientos físicos.

# A.7 Controles físicos

## 7.11 Servicios de apoyo

- Deberían proporcionarse alumbrado y comunicaciones de emergencia.
  - Los interruptores y las válvulas de emergencia para cortar el suministro de energía, agua, gas u otros servicios públicos deberían ubicarse cerca de las salidas de emergencia o de las salas de máquinas.
  - Se puede obtener redundancia adicional para la conectividad de redes mediante múltiples rutas de más de un proveedor de servicios públicos.
- 

# A.7 Controles físicos

## 7.12 Seguridad del cableado

*El cableado de energía y de telecomunicaciones que transporta datos o servicios de información de soporte debería protegerse contra interceptación, interferencia o daños.*

Considerar lo siguiente:

- a. las líneas de energía y telecomunicaciones en instalaciones de procesamiento de la información deberían ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa;
- b. los cables de energía deberían separarse de los cables de comunicaciones para evitar interferencias;

# A.7 Controles físicos

## 7.12 Seguridad del cableado

- c. entre los controles adicionales a considerar para los sistemas sensibles o críticos se incluyen:
  - i. instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección;
  - ii. uso de escudos electromagnéticos para proteger los cables;
  - iii. iniciar barridos técnicos e inspecciones físicas contra dispositivos no autorizados conectados a los cables;
  - iv. acceso controlado a los paneles de conexión (*patcheras*) y a las salas de cable.

# A.7 Controles físicos

## 7.13 Mantenimiento de los equipos

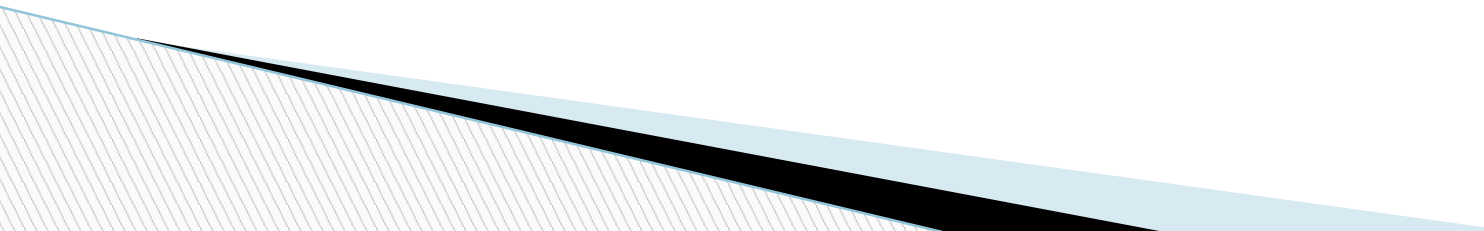
*El equipamiento debería mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.*

Considerar lo siguiente:

- a. el equipamiento debería mantenerse de acuerdo a las recomendaciones del proveedor;
- b. sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y el mantenimiento a los equipos;
- c. deberían mantenerse registros de todos los fallos, así como de todo el mantenimiento preventivo y correctivo;
- d. deberían implantarse controles apropiados cuando el equipamiento sea dispuesto para mantenimiento (confidencialidad de la información).

## A.7 Controles físicos

### 7.13 Mantenimiento de los equipos

- e. debería cumplirse con todos los requisitos impuestos por pólizas de seguros;
  - f. antes de poner el equipamiento nuevamente en funcionamiento, debería ser inspeccionado para asegurar que el equipamiento no ha sido manipulado y no tiene un mal funcionamiento.
- 



## A.7 Controles físicos

### 7.14 Eliminación segura o reutilización de los equipos

*Todo aquel equipamiento que contenga medios de almacenamiento debería revisarse para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su disposición final o reutilización.*

- Los equipamientos deberían revisarse para asegurar que los medios de almacenamiento estén contenidos antes de su eliminación o reutilización.
- Los dispositivos de almacenamiento con información sensible o con derechos de autor deberían destruirse físicamente o la información debería destruirse, suprimirse o sobrescribirse usando técnicas para hacer que la información original no sea recuperable, en lugar de utilizar las funciones de borrado o formateado rápido.

# A.7 Controles físicos

## 7.14 Eliminación segura o reutilización de los equipos

Además del borrado seguro del disco, todo el cifrado del disco reduce el riesgo de divulgación de información confidencial cuando los equipamientos son eliminados o redistribuidos, siempre que:

- a. el proceso de cifrado sea lo suficientemente fuerte y cubra todo el disco (incluyendo el espacio no asignado, los archivos de intercambio, etc.);
- b. las claves del cifrado son lo suficientemente largas como para resistir los ataques de fuerza bruta;
- c. las claves del cifrado se mantienen confidenciales (por ejemplo, nunca son almacenadas en el mismo disco).



# Funcionamiento del SGSI (sesión 8)

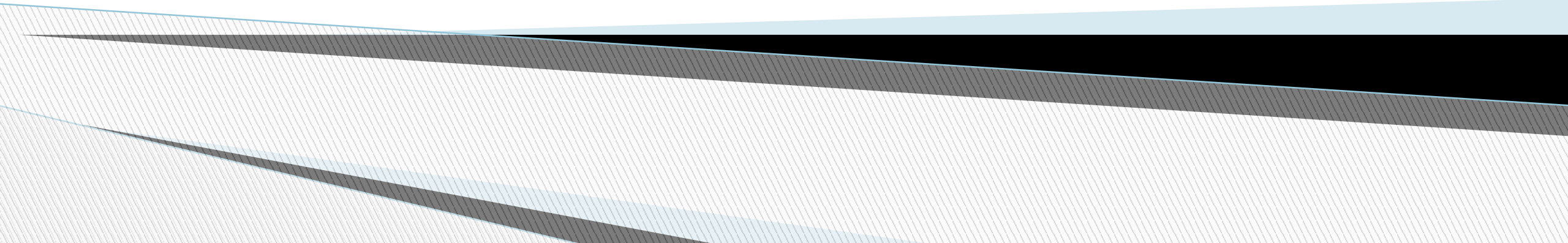
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

# **Anexo “A”**

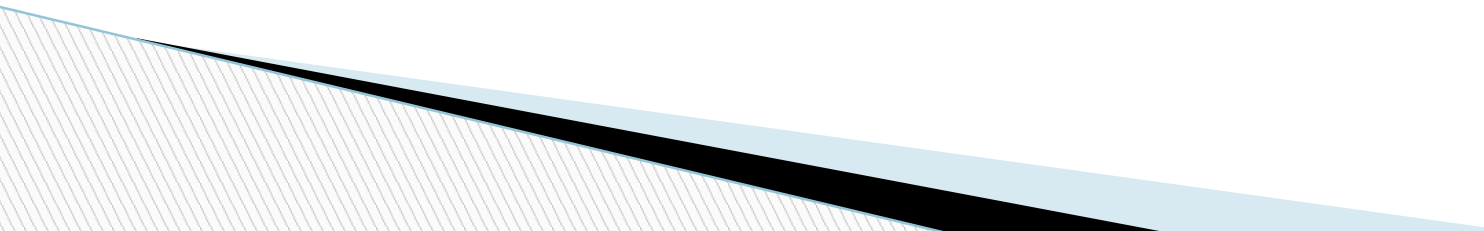
## **Controles**



## **A.6 Controles de personas**

### **6.1 Comprobaciones de verificación de antecedentes**

Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos percibidos.



## A.6 Controles de personas

### 6.2 Términos y condiciones para el empleo

Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.

## A.6 Controles de personas

### **6.3 Educación, entrenamiento y conciencia de seguridad de la información**

El personal de la organización y las partes interesadas relevantes deben recibir la concienciación, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.



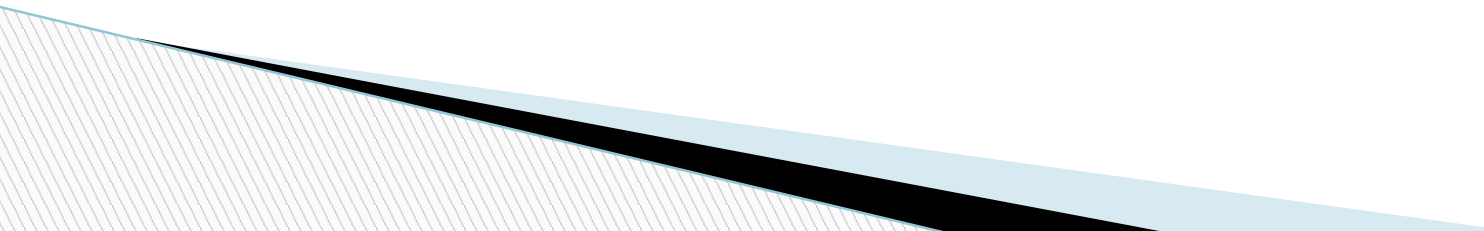
## A.6 Controles de personas

### 6.4 Proceso disciplinario

Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

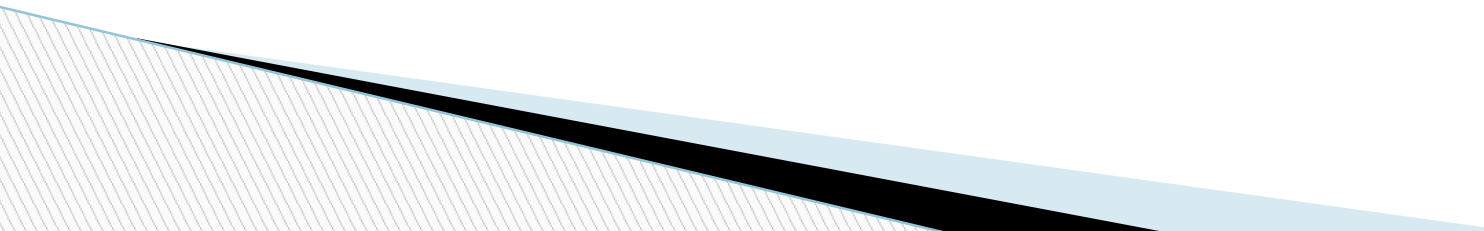
## A.6 Controles de personas

### 6.5 Responsabilidades después de la terminación o cambio de empleo

- La comunicación de las responsabilidades en la desvinculación debería incluir los requisitos de seguridad de la información y las responsabilidades legales.
  - Las responsabilidades del acuerdo de confidencialidad, deberían continuar por un período de tiempo definido luego de la desvinculación, de ser aplicable.
- 

# A.6 Controles de personas

## 6.5 Responsabilidades después de la terminación o cambio de empleo

- El contrato debería contener las responsabilidades y deberes que permanecen válidos aún luego de la desvinculación.
  - RR.HH. generalmente es responsable por el proceso de desvinculación y coordina con el supervisor del trabajador para gestionar los aspectos de seguridad de la información.
  - En el caso de un contratista, este proceso de responsabilidad en la finalización puede ser llevado a cabo por el tercero de conformidad con el contrato entre la organización y la tercera parte.
- 

# A.6 Controles de personas

## 6.5 Responsabilidades después de la terminación o cambio de empleo

*Otros temas en la terminación:*

- *Definir qué se hará con la información del usuario. ¿El propietario del proceso / información decidirá qué se hace con ella?*
- *¿Sus accesos a sistemas serán asignados a otros usuarios?*
- *¿Qué se hace con la información personal del usuario? (Ej. Correo electrónico, información personal en computador, etc.)*

## A.6 Controles de personas

### 6.6 Confidencialidad y no divulgación de acuerdos

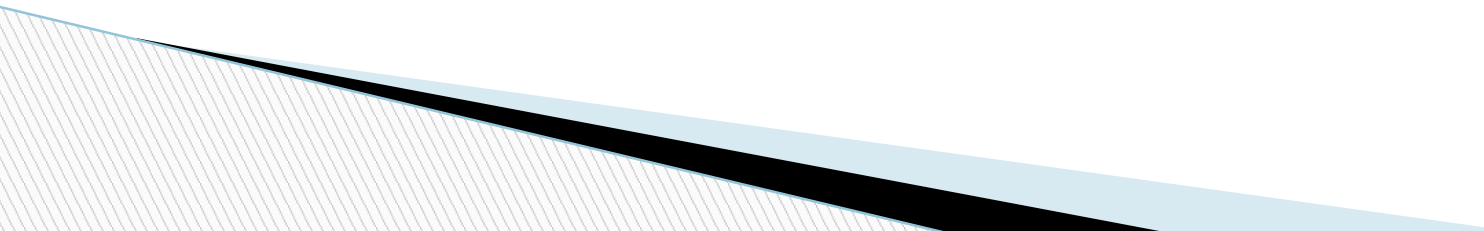
*Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.*

Los acuerdos de confidencialidad y no revelación deben reflejar las necesidades de la organización, documentarse y revisarse periódicamente tanto en las relaciones con sus colaboradores como con proveedores, socios estratégicos, reguladores, etc.

# A.6 Controles de personas

## 6.7 Trabajo remoto

Considerar aspectos como:

- Seguridad física del lugar de teletrabajo
  - Seguridad de las comunicaciones
  - ¿Se permitirá almacenamiento en dispositivo remoto?
  - Amenazas de acceso no autorizado por otras personas
  - Derechos de propiedad intelectual / Licencias de software
  - Legislación en cuanto a acceso a equipos privados
  - Protección de software malicioso
- 

# A.6 Controles de personas

## 6.8 Informes de eventos de seguridad de la información

*Los eventos de seguridad de la información deberían reportarse a través de los canales de gestión apropiados, lo más rápidamente posible.*

Responsabilidad de empleados y contratistas de reportar eventos de seguridad, y conocer el procedimiento de reporte.

Estas situaciones incluyen:

- Control ineficaz de la seguridad
- Violación de confidencialidad, integridad o disponibilidad
- Errores humanos
- Incumplimientos a la política de seguridad
- Cambios no controlados
- Mal funcionamiento de sistemas
- Violaciones de acceso

## A.6 Controles de personas

### **6.8 Informes de eventos de seguridad de la información**

Los desperfectos u otros comportamientos anómalos del sistema pueden ser un indicador de un ataque a la seguridad o de una violación real a la seguridad y por lo tanto, debería siempre reportarse como un evento de seguridad de la información.

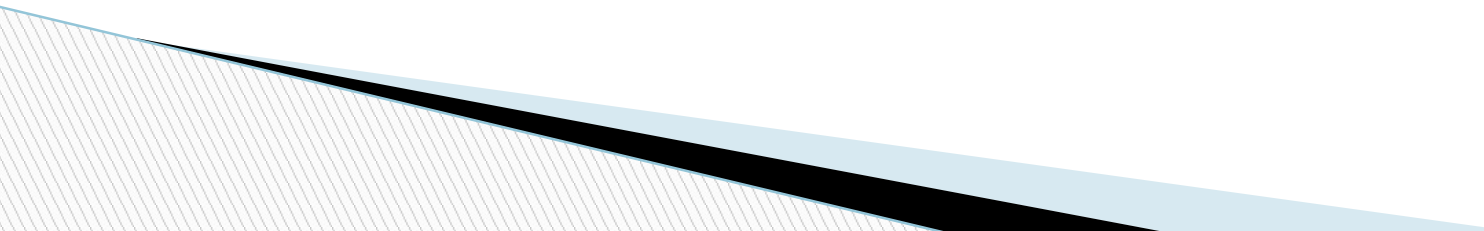


## A.6 Controles de personas

### 6.8 Informes de eventos de seguridad de la información

*A todos los empleados y contratistas de sistemas y de los servicios de información se les debería requerir observar y reportar cualquier debilidad de seguridad de la información vista o de la que se sospecha en relación a los sistemas o servicios.*

Los empleados y los contratistas deberían ser advertidos de no intentar probar presuntas debilidades de seguridad. Las pruebas de las debilidades pueden ser interpretadas como un posible mal uso del sistema, y podrían causar daños también al sistema o servicio de información y resultar en la responsabilidad legal para la persona que realiza la prueba.





# Funcionamiento del SGSI (sesión 7)

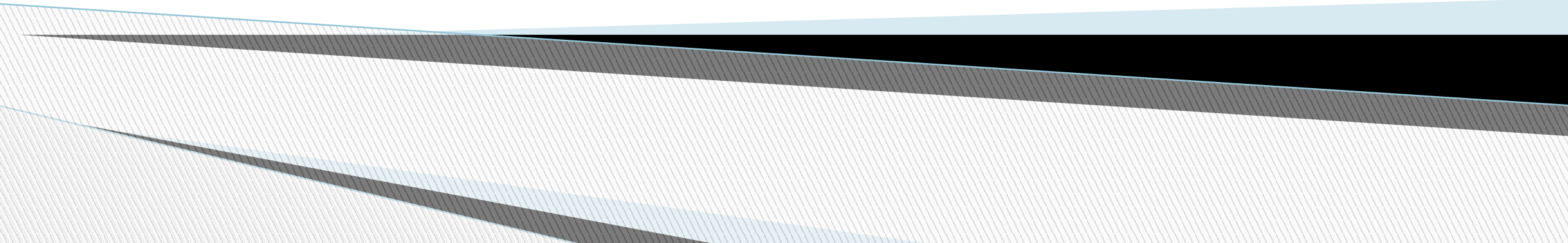
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

# **Anexo “A”**

## **Controles**

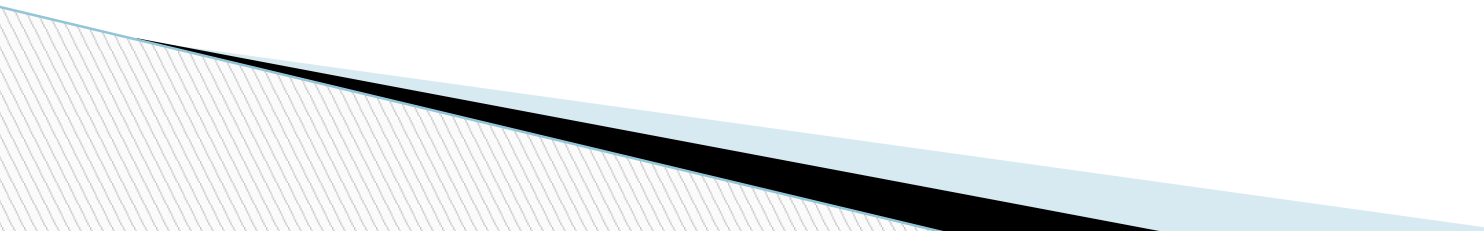


# A.5 Controles organizacionales

## 5.26 Respuesta a los incidentes de seguridad de la información

*Los incidentes de seguridad de la información deberían tener respuesta de acuerdo con los procedimientos documentados.*

La respuesta debería incluir:

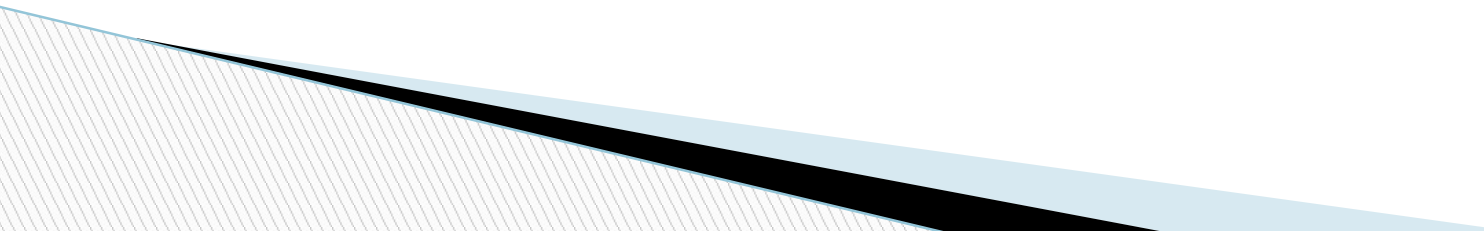
- a) la recopilación oportuna de evidencia
  - b) la realización de análisis forenses
  - c) escalamiento, según corresponda;
  - d) garantizar que todas las actividades de respuesta son registradas adecuadamente;
  - e) comunicar los datos relevantes del incidente a las partes que correspondan;
  - f) tratar las debilidades de seguridad de la información encontradas;
- 

## A.5 Controles organizacionales

### **5.27 Aprender de los incidentes de seguridad de la información**

*El conocimiento obtenido a partir del análisis y la resolución de los incidentes de seguridad de la información debería utilizarse para reducir la probabilidad o el impacto de futuros incidentes.*

Deberían existir mecanismos para permitir que los costos de los incidentes de seguridad de la información sean cuantificados y controlados. La información obtenida de evaluación de los incidentes de seguridad de la información debería utilizarse para identificar los incidentes recurrentes o de alto impacto.

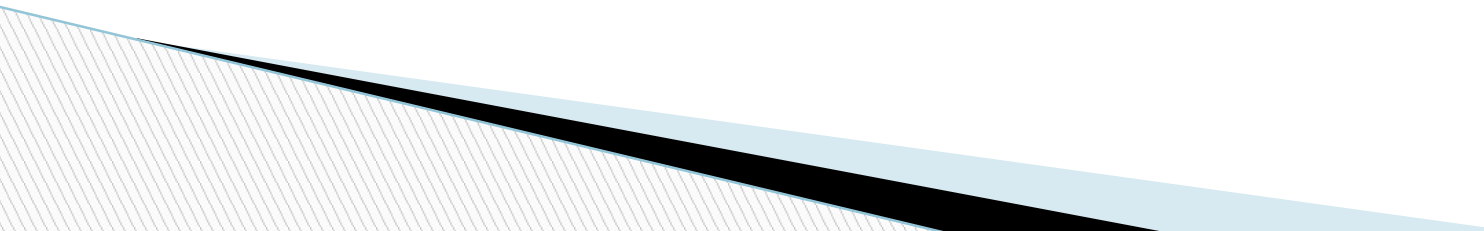


# A.5 Controles organizacionales

## 5.27 Aprender de los incidentes de seguridad de la información

La evaluación de incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de futuras ocurrencias, o para ser tomada en cuenta en el proceso de revisión de la política de seguridad.

Con el debido cuidado de los aspectos de confidencialidad, se pueden incluir escenarios de incidentes reales de seguridad de la información en la capacitación de la sensibilización del usuario, como ejemplos de lo que podría suceder, cómo responder a estos incidentes y cómo evitarlos en el futuro.



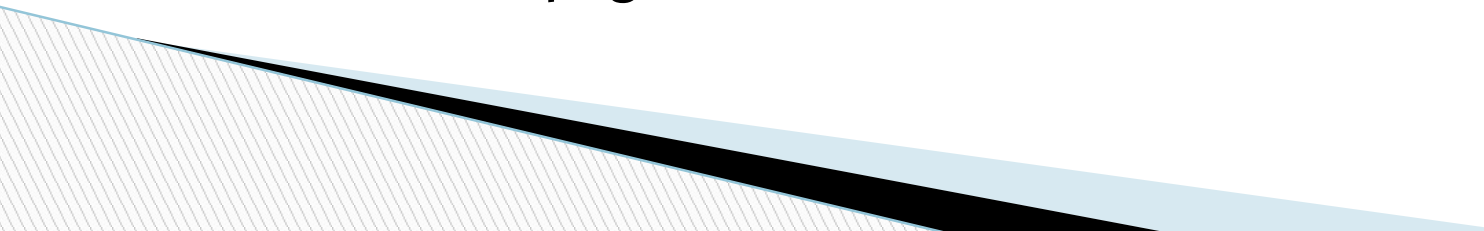
# A.5 Controles organizacionales

## 5.28 Recolección de evidencia

*La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.*

Deberían desarrollarse y seguirse procedimientos internos al tratar con evidencia para los propósitos de acción disciplinaria y legal.

En general, estos procedimientos de evidencia deberían proporcionar procesos de identificación, recolección, adquisición y conservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendido o apagado.





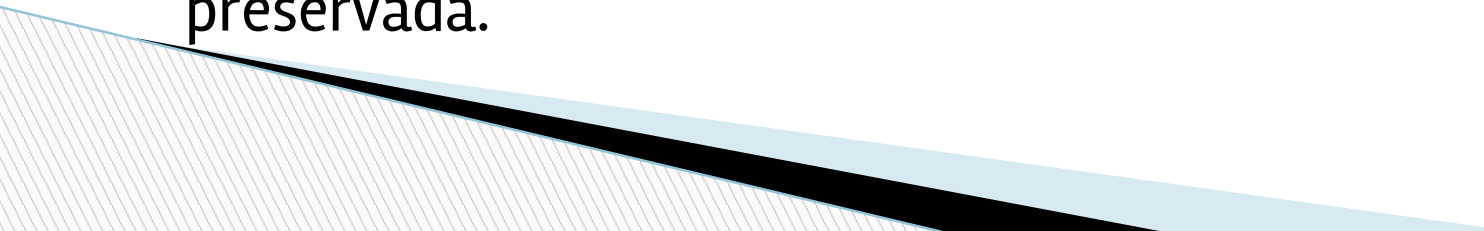
# A.5 Controles organizacionales

## 5.28 Recolección de evidencia

Los procedimientos deberían tener en cuenta:

- a) la cadena de custodia;
- b) la seguridad de la evidencia;
- c) la seguridad del personal;
- d) las funciones y responsabilidades del personal involucrado;
- e) la competencia del personal;
- f) la documentación;

Cuando sea factible, debería buscarse la certificación u otros medios pertinentes de la calificación del personal y las herramientas, con el fin de fortalecer el valor de la evidencia preservada.



# A.5 Controles organizacionales

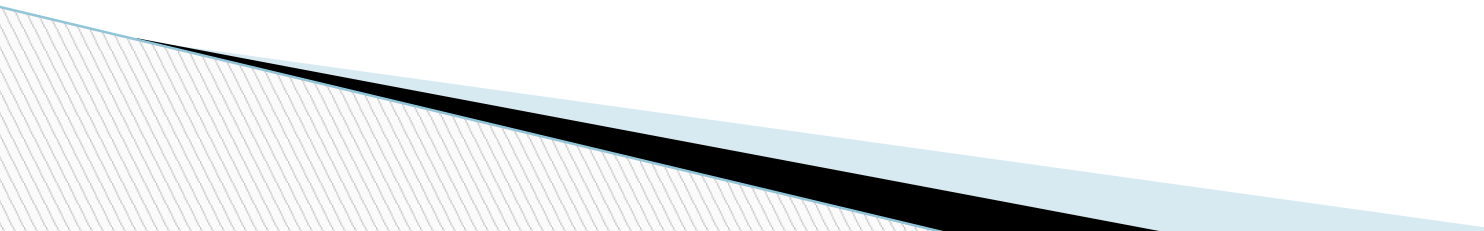
## 5.28 Recolección de evidencia

La evidencia forense puede trascender los límites organizacionales o jurisdiccionales. En tales casos, debería asegurarse que la organización tiene derecho a recopilar la información requerida como evidencia forense. Deberían considerarse los requisitos de las distintas jurisdicciones para maximizar las posibilidades de admisión de la evidencia en todas las jurisdicciones pertinentes.

# A.5 Controles organizacionales

## 5.28 Recolección de evidencia

Procesos:

- La identificación es el proceso que implica la búsqueda, el reconocimiento y la documentación de las posibles evidencias.
  - La recolección es el proceso de reunir los elementos físicos que podrían
  - contener evidencia potencial.
  - La adquisición es el proceso de crear una copia de los datos dentro de un conjunto definido.
  - La preservación es el proceso de mantener y salvaguardar la integridad y el estado original de la evidencia potencial.
- 

# A.5 Controles organizacionales

## 5.28 Recolección de evidencia

Cuando se detecta un evento de seguridad de la información por primera vez, puede que no sea obvio si el evento va a resultar o no en una acción judicial. Por lo tanto, existe el peligro de que las evidencias necesarias sean destruidas intencionalmente o accidentalmente antes de se de cuenta de la gravedad del incidente. Es recomendable involucrar a un abogado o la policía a principios de cualquier acción legal contemplada y buscar asesoramiento sobre las evidencias requeridas.

La Norma ISO/IEC 27037 proporciona directrices para la identificación, recolección, adquisición y preservación de evidencia digital.




## A.5 Controles organizacionales

### 5.29 Seguridad de la información durante la interrupción

*La organización debería determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o un desastre.*

Deberían determinarse los requisitos de seguridad de la información al planificar la continuidad del negocio y la recuperación ante desastres, esto evitará trabajo adicional innecesario.

En caso de no existir una planificación formal, se puede realizar un análisis BIA (Análisis de Impacto en el Negocio) para determinar los requisitos de seguridad necesarios en situaciones adversas.



# A.5 Controles organizacionales

## 5.29 Seguridad de la información durante la interrupción

*La organización debería establecer, documentar, implantar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.*

Una organización debería asegurarse que:

- a) se establezca una estructura de gestión adecuada para, mitigar y responder a un evento disruptivo utilizando personal con la autoridad, experiencia y competencia necesarias;
- b) se desarrollen y aprueben los planes documentados, los procedimientos de respuesta y recuperación.

# A.5 Controles organizacionales

## 5.29 Seguridad de la información durante la interrupción

La organización debería establecer:

- a) Controles de seguridad dentro de los procesos de recuperación.
- b) Procesos para mantener la seguridad de la información en una situación adversa
- c) Controles compensatorios para los controles de seguridad que no pueden ser mantenidos durante una situación adversa

# A.5 Controles organizacionales

## 5.29 Seguridad de la información durante la interrupción

*La organización debería verificar los controles establecidos e implementados de la continuidad de la seguridad de la información a intervalos regulares, con el fin de asegurar que sean válidas y efectivas en situaciones adversas.*

- Asegurarse que los planes y controles definidos para ser aplicados en un contexto de continuidad, se mantengan actualizados (cambios organizacionales, procesos, técnicos, etc.)
- Se debería probar los procedimientos de continuidad a fin de verificar que son eficaces, válidos y permiten mantener el nivel de seguridad requerido



## A.5 Controles organizacionales

### **5.30 Preparación de las TIC para la continuidad de la actividad**

*La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.*

# A.5 Controles organizacionales

## 5.31 Requisitos legales, reglamentarios y contractuales

*Todos los requisitos legales, estatutarios, reglamentarios, contractuales relevantes y el enfoque de la organización para cumplirlos deberían ser explícitamente identificados, documentados, y actualizados para cada sistema de información y para la organización.*

- La Gerencia es responsable de identificar todas las leyes aplicables a su organización a fin de cumplir con los requisitos para su tipo de negocio. Si la organización realiza negocios en otros países, la Gerencia debería considerar el cumplimiento en todos los países pertinentes.

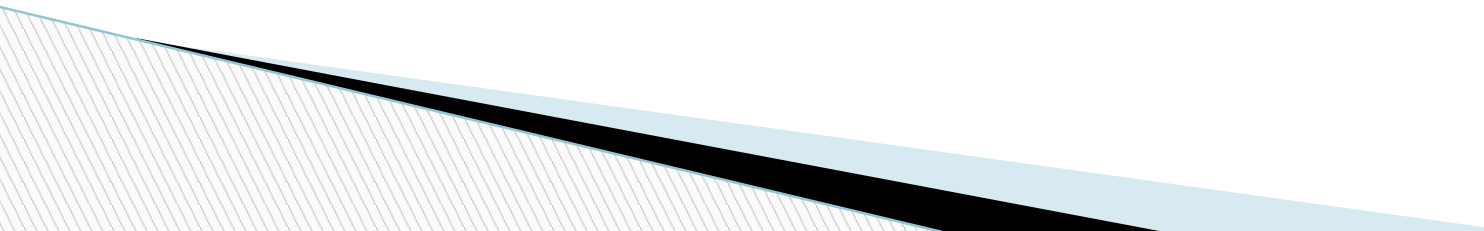
## A.5 Controles organizacionales

### 5.31 Requisitos legales, reglamentarios y contractuales

*Deberían utilizarse controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones relevantes.*

Deberían considerarse para el cumplimiento de los acuerdos, las leyes, y las regulaciones relevantes, incluyendo restricciones en la importación o en la exportación de hardware y de software para realizar funciones criptográficas o que incluyen éstas.

Mediante el asesoramiento jurídico debería intentarse asegurar el cumplimiento de leyes y regulaciones pertinentes. Antes que la información cifrada o los controles criptográficos sean trasladados a otro país, también debería tenerse en cuenta el asesoramiento jurídico.



# A.5 Controles organizacionales

## 5.32 Derechos de propiedad intelectual

*Deberían implantarse procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales relacionados sobre los derechos de propiedad intelectual y el uso de los productos de software patentados.*

Debería considerarse lo siguiente:

- Publicar política de cumplimiento de derechos de propiedad intelectual
- Adquirir software de fuentes conocidas
- Concienciar al personal, medidas disciplinarias
- Incluir en registro de activos el atributo de propiedad intelectual

# A.5 Controles organizacionales

## 5.32 Derechos de propiedad intelectual

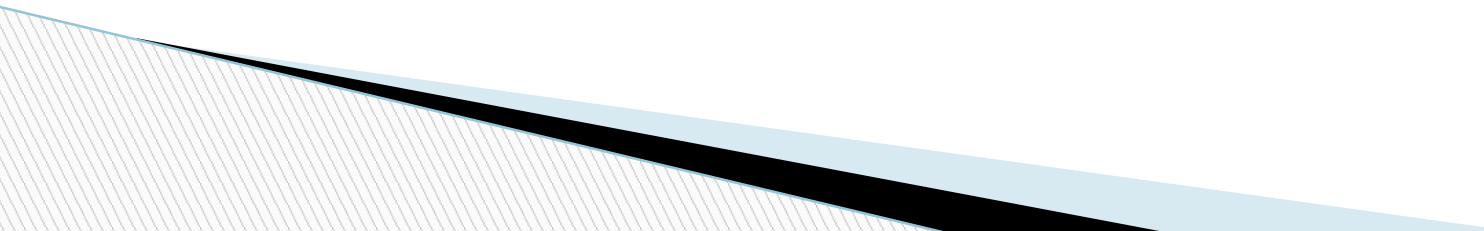
- Mantener documentación que acredite las licencias
- Implantar controles para no sobrepasar la cantidad de licencias
- Efectuar revisiones
- Procedimientos de eliminación de software
- Cumplir términos de uso de software
- No realizar copias no permitidas (software ni documentos)

Los derechos de propiedad intelectual incluyen software o documentos con derecho de copia, derechos de diseño, marcas registradas, patentes y código fuente licenciado.

## A.5 Controles organizacionales

### 5.32 Derechos de propiedad intelectual

Los productos de software propietario se suelen entregar con un contrato de licencia que especifica términos y condiciones del licenciamiento, por ejemplo, limitar el uso de los productos a máquinas específicas o limitar la generación de copias únicamente a finalidades de respaldo. La importancia y la concienciación de los derechos de propiedad intelectual deberían comunicarse al personal para el software desarrollado por la organización.



# A.5 Controles organizacionales

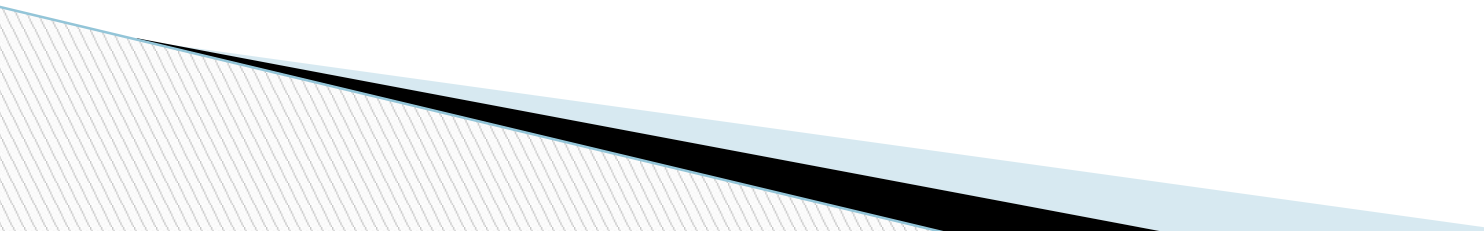
## 5.33 Protección de los registros

*Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada de acuerdo con los requisitos legislativos, reglamentarios, contractuales y del negocio.*

- Considerar la clasificación definida en la organización
- Los registros se deberían categorizar según el tipo, como por ejemplo: registros contables, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, cada uno de los cuales con los detalles de plazos de retención y medios de almacenamiento, como por ejemplo, papel, microfichas, medios magnéticos u ópticos.

# A.5 Controles organizacionales

## 5.33 Protección de los registros

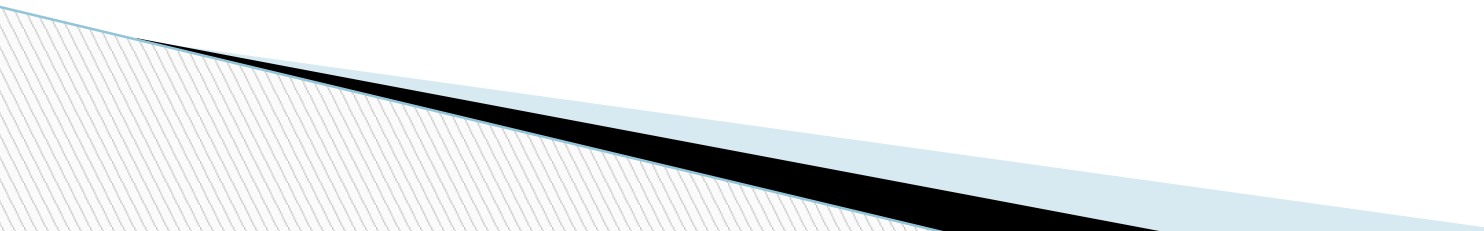
- Asegurarse de guardar llaves criptográficas
  - Considerar la posibilidad de deterioro de los medios utilizados para almacenar los registros
  - El sistema de almacenamiento elegido debe cumplir los requisitos de tiempo y forma de su recuperación
  - El sistema de almacenamiento deberá identificar los registros y periodo de retención, así como permitir su destrucción cuando ya no sean necesarios.
- 



# A.5 Controles organizacionales

## 5.33 Protección de los registros

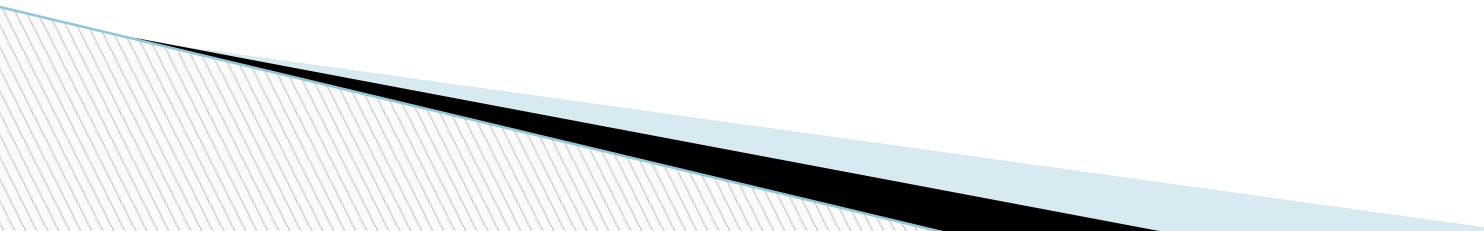
Establecer:

- Directrices de retención almacenamiento y tratamiento
  - Calendario de retenciones
  - Inventario de fuentes de información
- 

# A.5 Controles organizacionales

## 5.34 Privacidad y protección de la información personal

*La privacidad y protección de los datos personales deben ser aseguradas tal como lo requiere la legislación y regulación relevante donde sea aplicable.*

- Establecer política de protección de datos personales
  - Considerar Ley de Protección de Datos Personales (en Perú) y leyes similares en varios otros países.
  - La Norma ISO/IEC 29100 proporciona un marco de alto nivel para la protección de los datos personales dentro de los sistemas de información y de tecnología de la comunicación.
- 

# A.5 Controles organizacionales

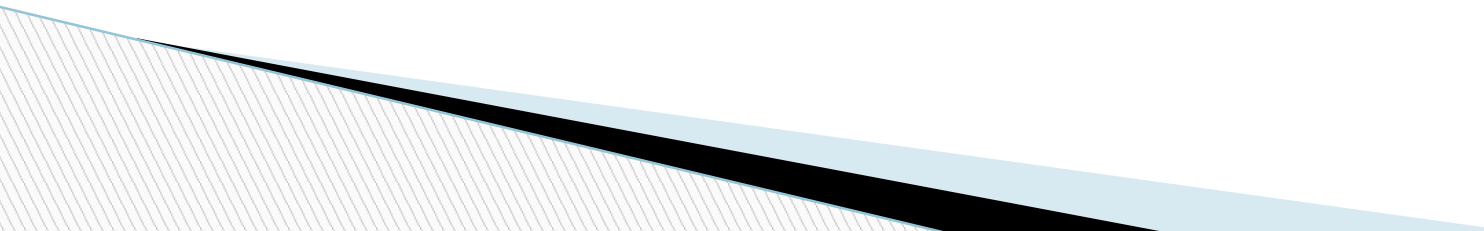
## 5.35 Revisión independiente de la seguridad de la información

*El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información) deberían revisarse de forma independiente a intervalos planificados o cuando se producen cambios significativos.*

- La dirección debe asegurar una revisión independiente
- Dicha revisión debería realizarse por personas independientes del área bajo revisión, Ej.: la función de auditoría interna, un administrador independiente o una organización de tercera parte especializada en ese tipo de revisiones. Las personas que llevan a cabo estas revisiones deberían tener las habilidades y experiencia apropiadas.

# A.5 Controles organizacionales

## 5.35 Revisión independiente de la seguridad de la información

- Resultados de evaluación deben documentarse y comunicarse
  - De ser aplicable la dirección deberá tomar acciones correctivas
  - Las Normas ISO/IEC 27007 “Directrices para auditar sistemas de gestión de seguridad de la información” e ISO/IEC TR 27008 “Directrices para los auditores de los controles de seguridad de la información” también proporcionan directrices para realizar la revisión independiente.
- 

## A.5 Controles organizacionales

### 5.36 Cumplimiento de las políticas, reglas y normas de seguridad de la información

*La Gerencia debería revisar regularmente el cumplimiento del procesamiento de la información y los procedimientos dentro de su área de responsabilidad con las políticas de seguridad apropiadas, las normas, y cualquier otro requisito de seguridad*

Si se detectan incumplimientos la gerencia debería:

- a) identificar las causas del incumplimiento;
- b) implementar las acciones correctivas apropiadas;
- c) revisar la acción correctiva tomada, para comprobar su eficacia e identificar las deficiencias y debilidades.

# A.5 Controles organizacionales

## 5.36 Cumplimiento de las políticas, reglas y normas de seguridad de la información

*Los sistemas de información deberían revisarse regularmente para verificar el cumplimiento con las políticas y las normas de seguridad de la información de la organización.*

- Preferiblemente utilizar herramientas especializadas
- Alternativamente personal experimentado puede efectuar revisiones manuales
- En caso de pruebas de intrusión, considerar cuidados pertinentes
- La revisión del cumplimiento también comprende, por ejemplo, pruebas de intrusión y evaluación de vulnerabilidades
- La Norma ISO/IEC TR 27008 proporciona orientación específica con respecto a las revisiones de cumplimiento técnico.

# A.5 Controles organizacionales

## 5.37 Procedimientos operativos documentados

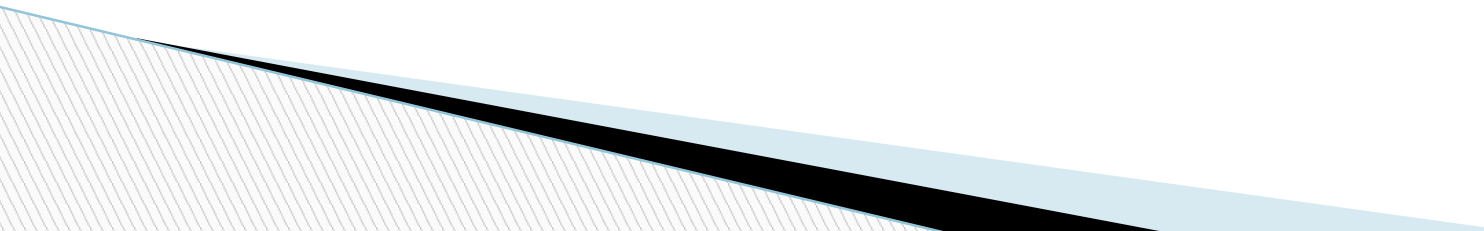
*Los procedimientos de operación deberían documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.*

Deberían elaborarse procedimientos documentados para las actividades del sistema asociadas con las instalaciones de comunicaciones y de procesamiento de información, tales como procedimientos de arranque y apagado del computador, respaldo, mantenimiento de equipos, manejo de medios, sala de cómputos, utilización de correo, y seguridad.

# A.5 Controles organizacionales

## 5.37 Procedimientos operativos documentados

Los procedimientos operacionales deberían especificar las instrucciones de funcionamiento, incluyendo:

- a. la instalación y configuración de los sistemas;
  - b. respaldo;
  - c. interdependencias entre sistemas, tiempos de comienzo y finalización de tareas;
  - d. instrucciones para el manejo de errores
  - e. contactos de soporte y escalamiento
- 



# A.5 Controles organizacionales

## 5.37 Procedimientos operativos documentados

- f. instrucciones para manipulación de salidas y medios especiales Ej. papelería especial o la gestión de salidas confidenciales
- g. procedimientos de reinicio y recuperación del sistema
- h. la gestión de las pistas de auditoría (logs)
- i. procedimientos de monitoreo

Los procedimientos de operación deben estar documentados, y contar con una adecuada gestión de cambios.





# Funcionamiento del SGSI (sesión 6)

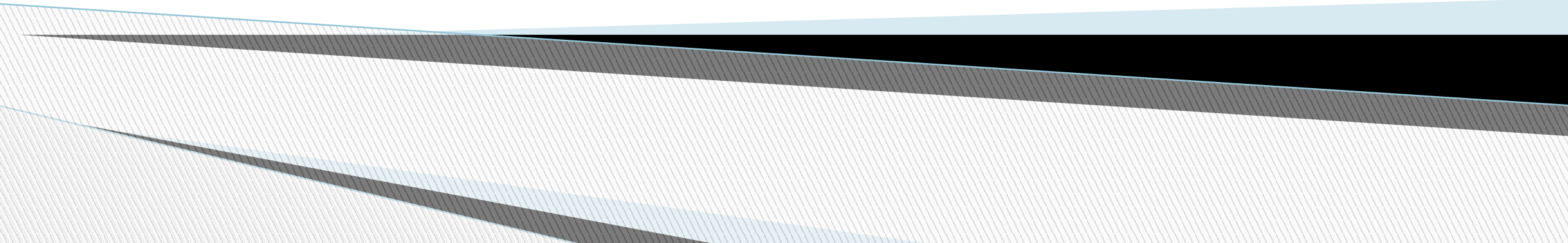
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

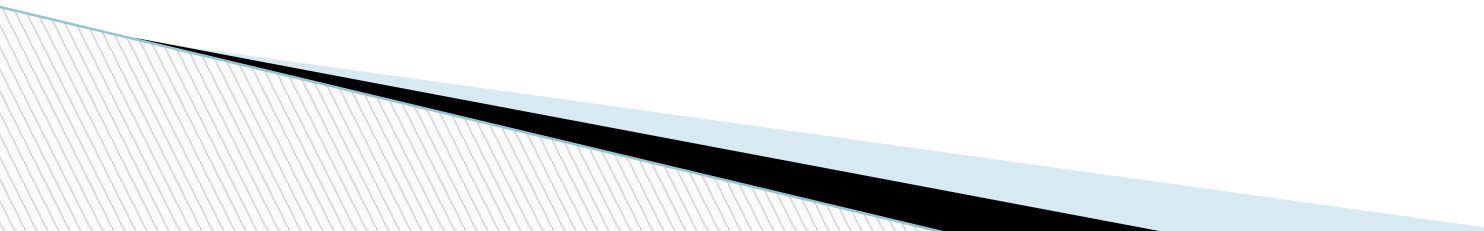
# **Anexo “A”**

## **Controles**



# A.5 Controles organizacionales

## 5.11 Retorno de activos

- El proceso de finalización debería formalizarse e incluir la devolución de todos los activos físicos y electrónicos previamente de la organización. (Ej. Laptops, celulares, tablets, discos duros externos, etc.)
  - En los casos en que un empleado o usuario de tercera parte adquiere equipos de la organización o utiliza su propio equipo, deberían seguirse procedimientos para garantizar que toda la información pertinente sea transferida a la organización y borrada de forma segura del equipo.
- 

# A.5 Controles organizacionales

## 5.11 Retorno de activos

- En los casos en que un empleado o usuario de una tercera parte tiene información de que es importante para la Organización, la información debería documentarse y transferirse a la organización.
- *En algunas organizaciones para evitar la destrucción deliberada de la información / o la sustracción de la misma, se toman algunas acciones tales como:*
  - *Primero se retira los accesos al usuario al sistema y luego se le comunica su cese.*
  - *Copia de toda de la información del usuario antes de la comunicación*
  - *Una vez comunicado el cese el trabajador es acompañado para recoger sus pertenencias y verificar que no dañe los activos de información, etc.*

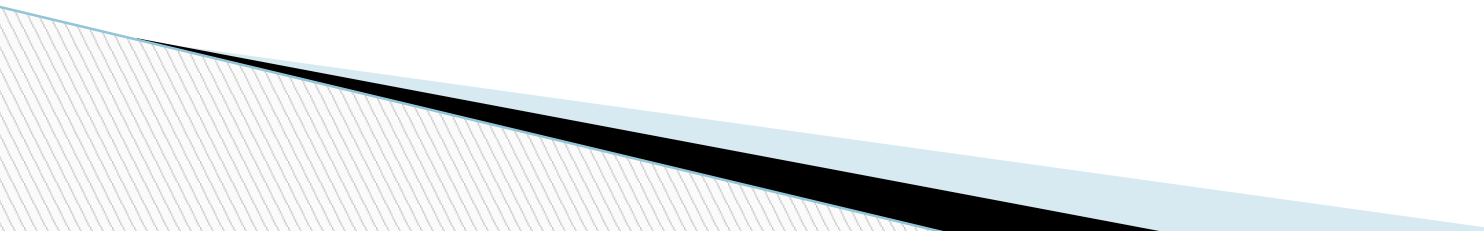
# A.5 Controles organizacionales

## 5.11 Retorno de activos

- Durante el período de aviso de finalización, la organización debería controlar la copia no autorizada de la información pertinente (por ejemplo, propiedad intelectual) por los empleados y contratistas que desean renunciar.
- *Ej. Copia de toda la base de datos de clientes mediante cinta de respaldo.*
- *Sustracción de información en medios removibles*
- *Envío de información mediante correo electrónico,*
- *Sustracción de información impresa, etc...*

# A.5 Controles organizacionales

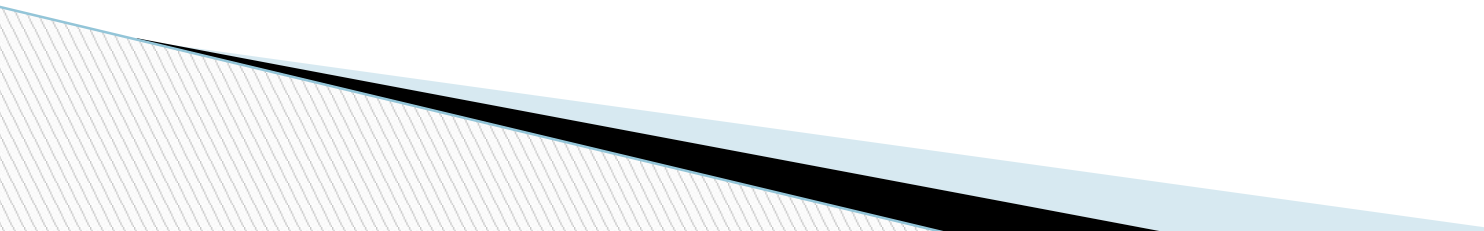
## 5.12 Clasificación de la Información

- La clasificación y los controles de protección asociados a la información deberían tener en cuenta las necesidades del negocio y requisitos legales.
  - Los propietarios de los activos de información son responsables de su clasificación.
  - El esquema de clasificación debería incluir las convenciones para la clasificación y los criterios para la revisión de la clasificación en el tiempo. El nivel de protección en el esquema debería evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad y cualquier otro requisito para la información considerada.
  - Alineamiento con la política de control de acceso
- 



# A.5 Controles organizacionales

## 5.12 Clasificación de la Información

- Cada nivel debería tener un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.
  - El esquema debería ser consistente en toda la organización para que todos clasifiquen la información y los activos relacionados de la misma manera, tengan un entendimiento común de los requisitos de protección y apliquen la protección adecuada.
  - Los resultados de la clasificación deberían indicar el valor de los activos en función de su sensibilidad y criticidad para la organización, por ejemplo, en términos de confidencialidad, integridad y disponibilidad.
- 

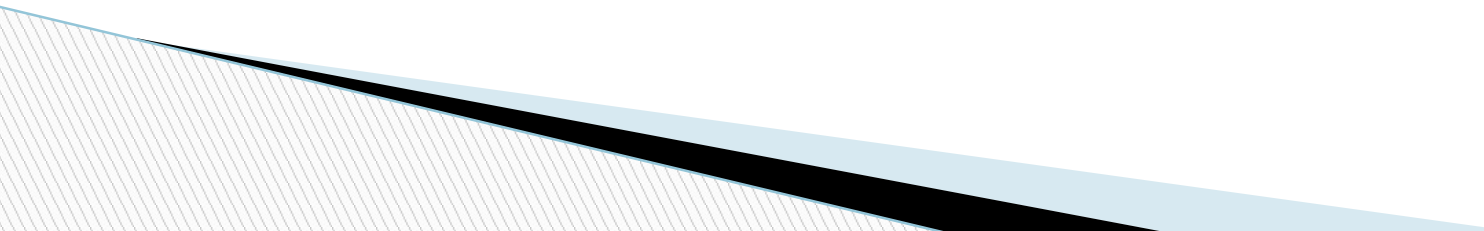
# A.5 Controles organizacionales

## 5.12 Clasificación de la Información

- Los resultados de la clasificación deberían actualizarse de acuerdo con los cambios de su valor, sensibilidad y criticidad durante su ciclo de vida.
- La clasificación les ofrece a las personas que tratan con información, una indicación concisa de cómo manejarla y protegerla. La creación de grupos de información con necesidades de protección similares y la especificación de los procedimientos de seguridad de la información que se aplican a toda la información en cada grupo, facilitan esto.

# A.5 Controles organizacionales

## 5.12 Clasificación de la Información

- La información suele dejar de tener importancia o criticidad tras cierto tiempo, por ejemplo, cuando se ha hecho pública.
  - Sobre-clasificación conllevaría a la implementación de controles innecesarios
  - Infra-clasificación puede poner en peligro el logro de los objetivos del negocio.
- 

# A.5 Controles organizacionales

## 5.12 Clasificación de la Información

- Un ejemplo de un esquema de clasificación de confidencialidad de la información se podría basar en cuatro niveles, de la siguiente manera:
  - a) la divulgación no causa ningún daño;
  - b) la divulgación causa menor incomodidad o inconveniencia operativa menor;
  - c) la divulgación tiene un impacto significativo a corto plazo en las operaciones o los objetivos tácticos;
  - d) la divulgación tiene un grave impacto en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización.

# A.5 Controles organizacionales

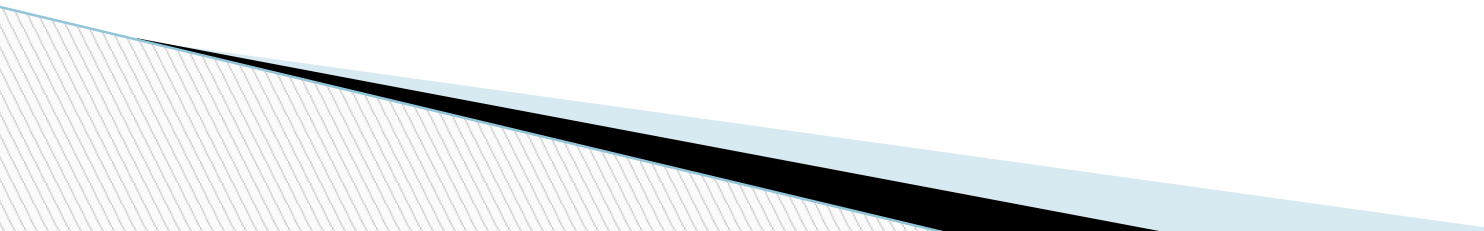
## 5.12 Clasificación de la Información

*Ejemplos:*

*Clasificación Militar:*

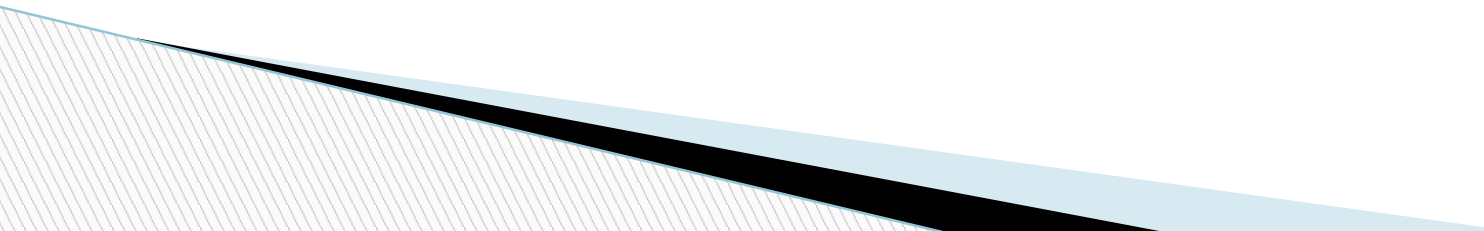
- *Estrictamente Secreta*
- *Secreta*
- *Confidencial*
- *Reservada*

*Clasificación simple del sector privado*

- *Confidencial*
  - *De uso Interno*
  - *Pública*
- 

# A.5 Controles organizacionales

## 5.13 Etiquetado de Información

- El etiquetado debería reflejar el esquema de clasificación. Las etiquetas deberían reconocerse fácilmente.
  - Los procedimientos deberían proporcionar orientación sobre dónde y cómo se adjuntan las etiquetas, considerando cómo se accede a la información o se gestionan los activos, en función de los tipos de medios.
  - Los procedimientos pueden definir casos en los que se omite el etiquetado, Ej. información no confidencial.
  - Los empleados y los contratistas deberían estar al tanto de los procedimientos del etiquetado.
- 

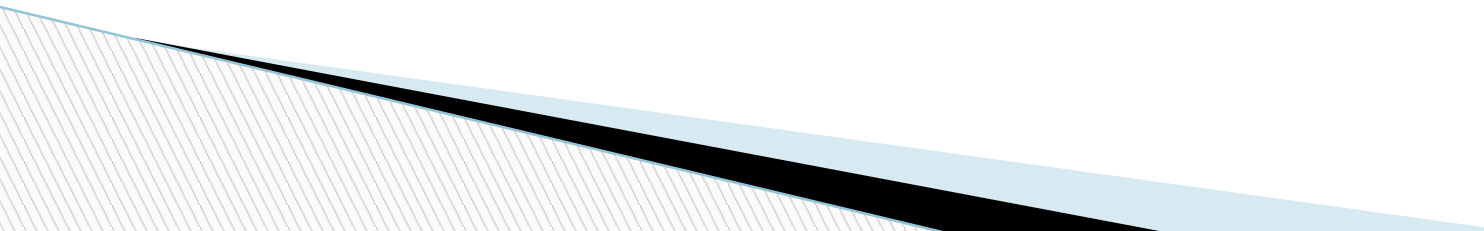
# A.5 Controles organizacionales

## 5.13 Etiquetado de Información

- Los reportes de los sistemas que contienen información clasificada como sensible o crítica debería llevar una etiqueta adecuada de clasificación.
- El etiquetado de la información y sus activos relacionados, a veces, pueden tener efectos negativos. Los activos clasificados son más fáciles de identificar y por lo tanto, objeto de robo por parte de los atacantes internos o externos.

# A.5 Controles organizacionales

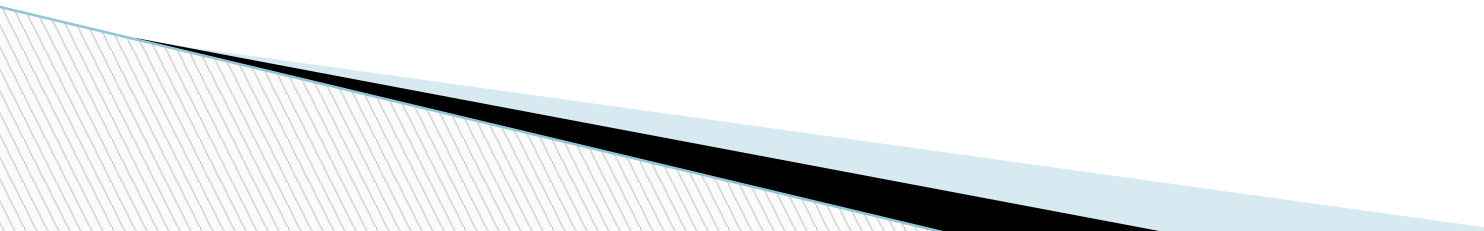
## 5.14 Transferencia de información

- Establecer una política formal de intercambio, procedimientos y controles para proteger la transferencia de información a través de los servicios de comunicación.
  - Se establecen acuerdos para el intercambio de información y software dentro de la organización y con organizaciones externas.
  - Proteger adecuadamente la información sensible de la organización, involucrada en la mensajería electrónica.
- 



# A.5 Controles organizacionales

## 5.15 Control de acceso

- Los propietarios de los activos deberían determinar las reglas de control de acceso, los derechos y las restricciones para las funciones específicas de los usuarios con respecto a sus activos con el nivel de detalle requerido por los riesgos asociados.
  - Los controles de acceso son tanto lógicos como físicos, y éstos deberían considerarse en forma conjunta.
  - Comunicar claramente a los usuarios y proveedores los criterios especificados para el control de accesos.
- 

# A.5 Controles organizacionales

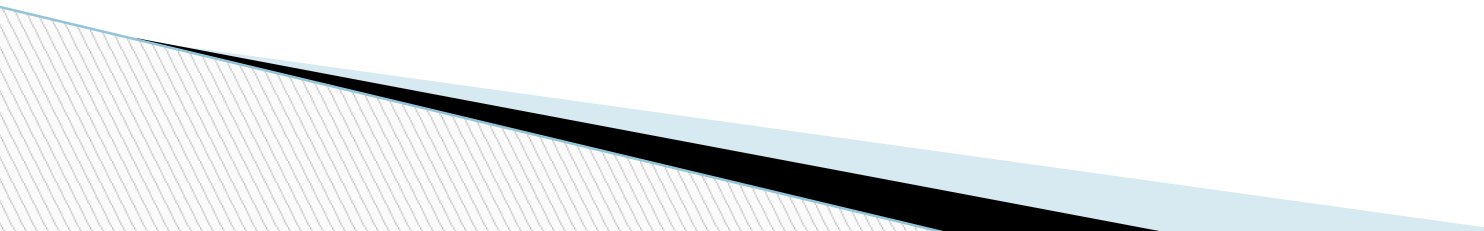
## 5.15 Control de acceso

La política debería tener en cuenta lo siguiente:

- a. requisitos de seguridad de aplicaciones de negocio;
- b. políticas para autorización y distribución de la información, Ej. los niveles de seguridad y clasificación de la información;
- c. consistencia entre los derechos de acceso y las políticas de clasificación de la información de los diferentes sistemas y redes;
- d. legislación relevante y obligaciones contractuales con respecto a la limitación de acceso a los datos o servicios;

# A.5 Controles organizacionales

## 5.15 Control de acceso

- e. Segregación de los roles de control de acceso, Ej. Solicitud, autorización, administración
  - f. Requisitos formales de pedidos de acceso;
  - g. revisión periódica de derechos de acceso;
  - h. remoción de derechos de acceso;
  - i. archivo de los registros de todos los eventos importantes relativos al uso y a la gestión de las identidades del usuario y la autenticación
  - j. roles con acceso privilegiado.
- 

# A.5 Controles organizacionales

## 5.15 Control de acceso

- Las reglas de control de acceso deberían ser soportadas por procedimientos formales y responsabilidades definidas
- El control de acceso basado en roles es un enfoque utilizado exitosamente por muchas organizaciones para vincular los derechos de acceso con los roles de negocios.
- Dos de los principios frecuentes de la política de control de accesos:
  - a. necesidad de saber
  - b. necesidad de utilizar

# A.5 Controles organizacionales

## 5.15 Control de acceso

- Debería formularse una política relativa al uso de redes y servicios de red. Esta política debería cubrir:
  - a. las redes y servicios de red a los cuales es permitido acceder;
  - b. los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red;
  - c. los controles y procedimientos para proteger el acceso
  - d. los medios utilizados para acceder a las redes y servicios de red (Ej: VPN o redes inalámbricas);
  - e. requisitos de autenticación
  - f. El monitoreo del uso de los servicios de red.

# A.5 Controles organizacionales

## 5.15 Control de acceso

- La política sobre el uso de servicios de red debería ser coherente con la política de control de acceso de la organización
- Conexiones no autorizadas o inseguras a servicios de red pueden afectar a toda la organización.
- Este control es particularmente importante para conexiones de red a aplicaciones sensibles o críticas del negocio o de usuarios en ubicaciones de alto riesgo, Ej. áreas públicas o externas.

# A.5 Controles organizacionales

## 5.16 Gestión de identidad

- El proceso de gestión de ID de usuarios debería incluir:
  - a. utilización de la identificación única de usuario (*IDs*) *para permitir que los usuarios queden* vinculados y sean responsables de sus acciones; el uso de identificadores de grupo, debería permitirse solamente cuando sea necesario por razones de negocio u operativas, y deberían ser aprobadas y documentadas;
  - b. desactivación o eliminación inmediata los IDs de los usuarios que han dejado la organización;
  - c. eliminación o desactivación periódica de IDs de usuarios innecesarias

# A.5 Controles organizacionales

## 5.16 Gestión de identidad

- Proporcionar o revocar el acceso a la información o a las instalaciones de procesamiento de información es, por lo general, un procedimiento de dos pasos:
  - a. asignar y habilitar, o revocar el ID de usuario;
  - b. proporcionar o revocar los derechos de acceso a dicho ID de usuario



# A.5 Controles organizacionales

## 5.17 Información de autenticación

- El proceso debería incluir los siguientes requisitos:
  - a. debería requerirse a los usuarios la firma de una declaración para mantener la información de autenticación personal secreta
  - b. Asignación inicial de una información de autenticación temporal que debe ser cambiada por el usuario en el primer uso
  - c. deberían establecerse procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación secreta nueva, sustitutiva o temporal;

# A.5 Controles organizacionales

## 5.17 Información de autenticación

- d. la información de autenticación temporal debería proporcionarse a los usuarios de forma segura; Ej. El uso de terceros o mensajes de correo electrónico sin proteger (texto sin cifrar) debería evitarse;
- e. la información de autenticación secreta temporal debería ser única para cada individuo y no debería ser fácil de adivinar;
- f. los usuarios deberían confirmar la recepción de la información de autenticación secreta;

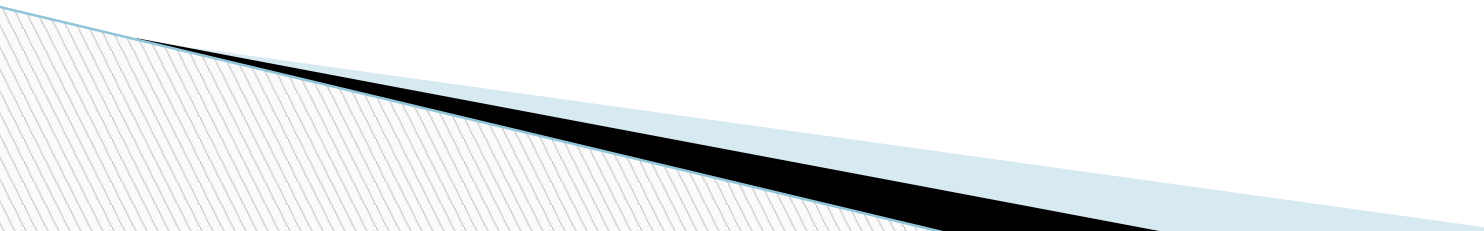
# A.5 Controles organizacionales

## 5.17 Información de autenticación

Las contraseñas son un tipo de información de autenticación secreta comúnmente utilizadas y son un medio común para verificar la identidad del usuario. Otros tipos de información de autenticación secreta son claves criptográficas y otros datos almacenados en señales de hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación.

# A.5 Controles organizacionales

## 5.17 Información de autenticación

- Todos los usuarios deberían ser advertidos sobre:
    - a. mantener en secreto la información de autenticación confidencial, asegurando que no se divulga a otras partes, incluidas las personas de autoridad;
    - b. evitar mantener un registro (por ejemplo, en papel, archivo de software o dispositivo de mano) de la información de autenticación secreta, salvo que pueda almacenarse de forma segura y el método de almacenamiento haya sido aprobado (por ejemplo, repositorio de contraseñas);
- 

# A.5 Controles organizacionales

## 5.17 Información de autenticación

- Todos los usuarios deberían ser advertidos sobre:
  - c. cambiar la información de autenticación secreta siempre que existan indicios de su posible compromiso;
  - d. Criterios para la selección de contraseñas:
    - i. fáciles de recordar;
    - ii. no se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc.;
    - iii. no vulnerables a ataques tipo diccionario (es decir, que no consistan en palabras incluidas en diccionarios);
    - iv. libres de caracteres idénticos sucesivos ya sean todos numéricos o alfabéticos;
    - v. si es temporal, cambiadas en el primer inicio de sesión.

# A.5 Controles organizacionales

## 5.17 Información de autenticación

- e. no compartir la información de autenticación secreta del usuario individual;
- f. garantizar una adecuada protección de las contraseñas cuando las mismas son utilizadas como información de autenticación secreta en procedimientos de inicio de sesión automático y luego almacenadas; (también para contraseñas de autenticación entre aplicaciones)

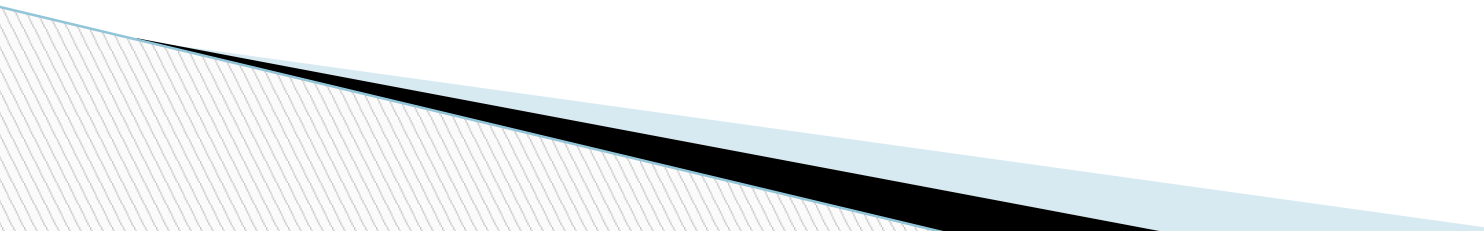
# A.5 Controles organizacionales

## 5.17 Información de autenticación

- Los servicios de *Single Sign On* o de otras herramientas de gestión de la información de autenticación secreta, reduce la cantidad de información de autenticación secreta que los usuarios están obligados a proteger y por lo tanto puede aumentar la eficacia de este control.
- Sin embargo, estas herramientas también pueden aumentar el impacto de la divulgación de la información de autenticación secreta.

# A.5 Controles organizacionales

## 5.17 Información de autenticación

- Un sistema de gestión de contraseñas debería:
    - a. requerir el uso de contraseñas e identificaciones de usuario (*IDs individuales con el fin de* establecer responsabilidades;
    - b. permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para evitar errores al introducirlas;
    - c. imponer la selección de contraseñas de calidad;
    - d. forzar a los usuarios el cambio de contraseñas temporales en su primer inicio de sesión (*log-on*);
- 



# A.5 Controles organizacionales

## 5.17 Información de autenticación

- Un sistema de gestión de contraseñas debería:
  - e. requerir los cambios de contraseña periódicos, y según sea necesario;
  - f. mantener un registro de las anteriores contraseñas utilizadas y, evitar su reutilización;
  - g. no mostrar las contraseñas en la pantalla cuando se están introduciendo;
  - h. almacenar archivos de contraseñas en lugares diferentes de los datos del sistema de aplicaciones;
  - i. almacenar y transmitir las contraseñas en forma protegida.

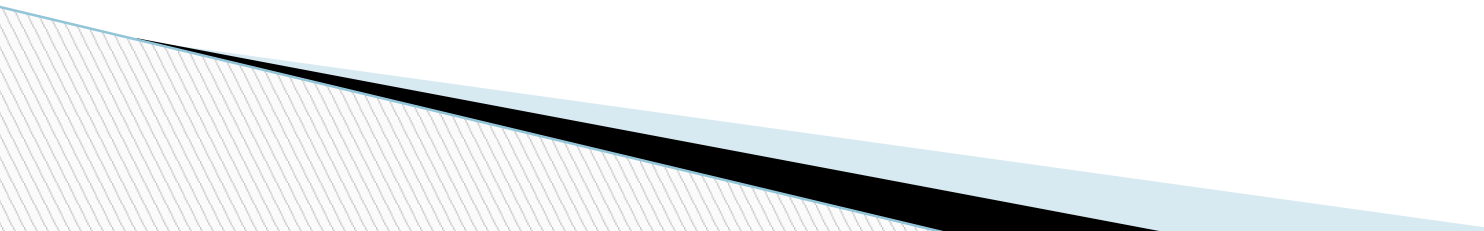
# A.5 Controles organizacionales

## 5.18 Derechos de acceso

- El proceso de gestión para asignar o revocar los derechos de acceso concedidos al ID de usuario debería incluir:
  - a. la obtención de la autorización del propietario del sistema o servicio de información
  - b. la verificación de que el nivel de acceso concedido cumple las políticas de acceso y la segregación de funciones;
  - c. la garantía de que los derechos de acceso no se encuentren activados (por ejemplo, por los proveedores del servicio) antes de que se completen los procedimientos de autorización;

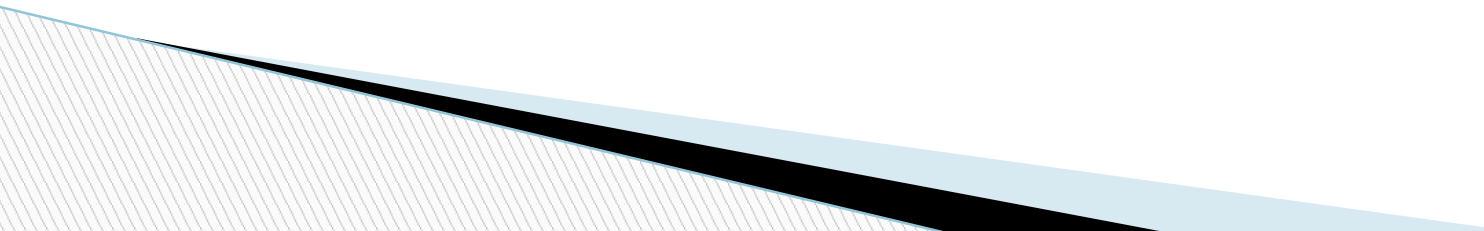
# A.5 Controles organizacionales

## 5.18 Derechos de acceso

- d. el mantenimiento de un registro central de los derechos de acceso concedidos a un ID de usuario para acceder a los sistemas y servicios de la información;
  - e. Adecuación de los derechos de acceso de los usuarios que han cambiado de funciones o puestos de trabajo y eliminar o bloquear inmediatamente los derechos de acceso de los usuarios que han abandonado la organización;
  - f. la revisión periódica de los derechos de acceso con los propietarios de los sistemas o servicios de la información.
- 

# A.5 Controles organizacionales

## 5.18 Derechos de acceso

- Debería considerarse la posibilidad de establecer los roles de acceso estándar para las funciones típicas del negocio. (Ej. Tesorero, Asistente de cuentas por cobrar, Comprador, Administrador de presupuesto, Auditor, etc.)
  - Las solicitudes y las revisiones de acceso son más fáciles de gestionar a nivel de tales roles que a nivel de los derechos particulares.
  - Considerar la posibilidad de incluir cláusulas en los contratos (personal y terceros) que especifiquen sanciones si se intenta el acceso no autorizado.
- 

# A.5 Controles organizacionales

## 5.18 Derechos de acceso

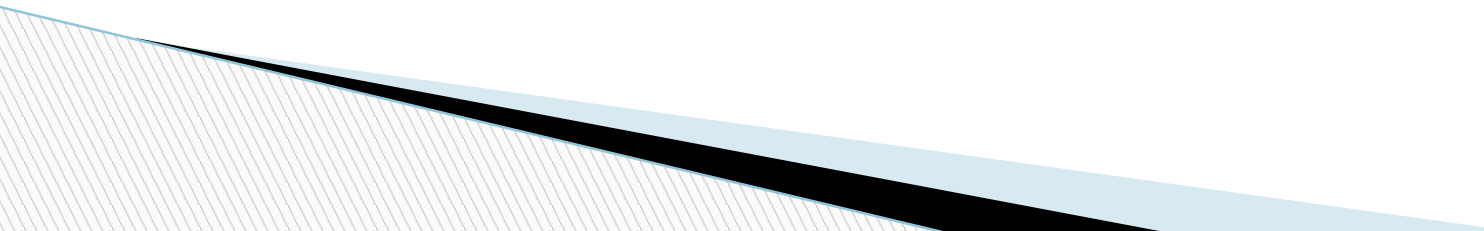
- La revisión de los derechos de acceso debería considerar lo siguiente:
  - a. los derechos de acceso de usuarios deberían revisarse a intervalos regulares, y luego de cualquier cambio, tal como una promoción, una degradación, o terminación del empleo;
  - b. Accesos privilegiados requieren una revisión con mayor frecuencia.
  - c. los cambios en las cuentas privilegiadas deberían registrarse para su revisión periódica.

Este control compensa las posibles debilidades en la ejecución de los controles.



# A.5 Controles organizacionales

## 5.18 Derechos de acceso

- Cuando se produce una desvinculación, los derechos de acceso de un individuo a la información y los activos asociados con instalaciones de procesamiento de información y servicios deberían eliminarse o suspenderse.
  - En caso de cambio de puesto, los cambios en la relación laboral deberían ser reflejados en la remoción de todos los derechos de acceso que no fueron aprobados para el nuevo puesto (incluyendo acceso físico y lógico)
  - La remoción o el ajuste se pueden hacer mediante la eliminación o la revocación o el reemplazo de las claves, tarjetas de identificación, etc.
- 

# A.5 Controles organizacionales

## 5.18 Derechos de acceso

- Cualquier documentación que identifique los derechos de acceso de los empleados y contratistas debería reflejar la eliminación o el ajuste de los derechos de acceso. Si un empleado o usuario de tercera parte que se marcha ha conocido las contraseñas para ID de usuarios que permanecen activos, estas deberían cambiarse al momento de la desvinculación o cambio de cargo, contrato o acuerdo. (Ej. Especial cuidado en cese de colaboradores con cuentas privilegiadas y cuentas grupales)

# A.5 Controles organizacionales

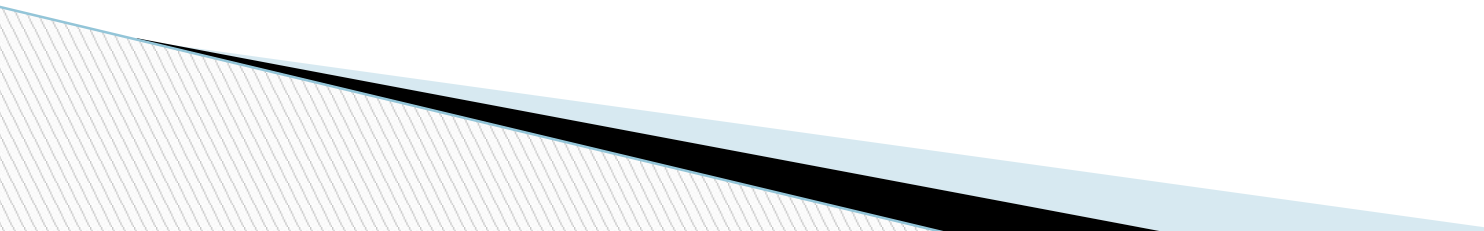
## 5.18 Derechos de acceso

- Los derechos de acceso a la información y los activos, deberían reducirse o eliminarse antes de que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo tales como:
  - a. si la desvinculación o cambio es iniciado por el empleado, contratista, o por la dirección y la razón de la desvinculación;
  - b. las responsabilidades actuales del empleado, parte usuaria de tercera parte o cualquier otro usuario;
  - c. el valor de los activos accesibles



# A.5 Controles organizacionales

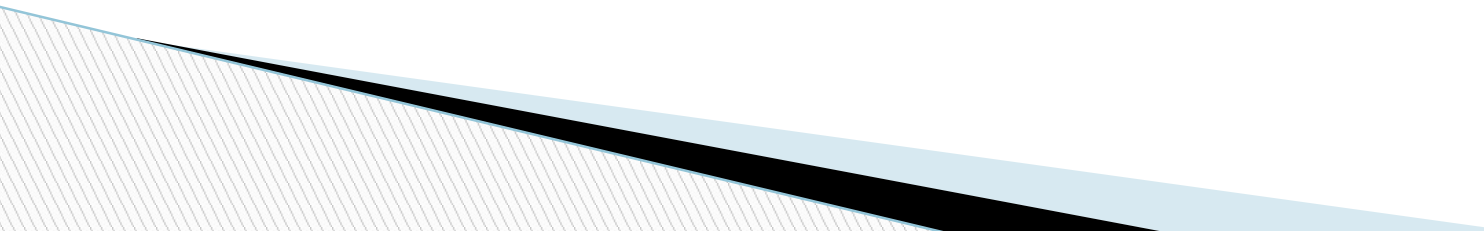
## 5.18 Derechos de acceso

- Notificar al personal sobre el cese del trabajador para que no continúe compartiendo información con él. Verificar que se haya retirado de los grupos de comunicación (Ej. Cuenta de correo personal en comunicaciones grupales).
  - En caso de despido el trabajador contrariado podría dañar información o sabotear equipamiento.
  - En casos de personas que renuncian o son despedidas, podrían estar tentados a llevarse información para uso futuro.
- 

## A.5 Controles organizacionales

### 5.19 Seguridad de la información en la relación con proveedores

Las organizaciones deberían establecer una política para controlar el acceso del proveedor a la información, incluyendo los procesos y procedimientos a ser implementados por:

- la organización
  - el proveedor
- 

# A.5 Controles organizacionales

## 5.19 Seguridad de la información en la relación con proveedores

- ✓ Identificar y registrar los tipos de proveedores a quien la organización permite acceder a su información (servicios de TI, logística, financieros, auditores externos, etc.)
- ✓ Establecer tipos de acceso por tipo de proveedor
- ✓ Procedimientos para monitorear el cumplimiento de las normas de seguridad por parte de los proveedores
- ✓ Controles de integridad sobre la información proporcionada
- ✓ Obligaciones para proteger la información
- ✓ Gestión de incidentes

# A.5 Controles organizacionales

## 5.20 Abordar la seguridad de la información en los acuerdos con proveedores

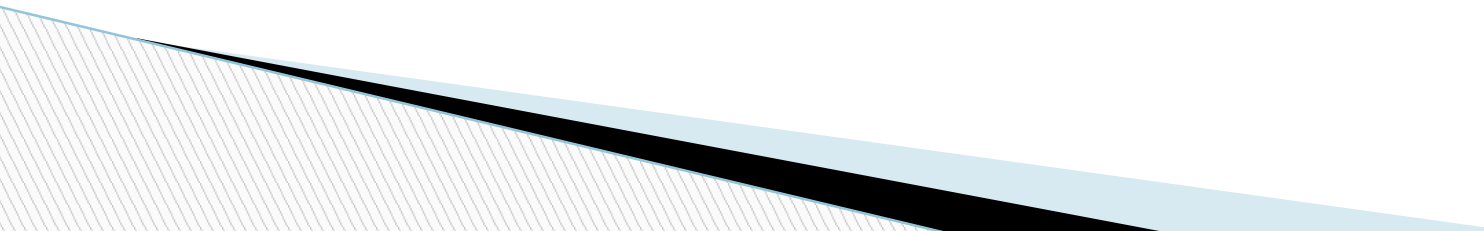
Deberían establecerse y documentarse acuerdos con los proveedores para asegurar el entendimiento de las obligaciones respecto a la seguridad de la información.

Debería tenerse en cuenta lo siguiente:

- a) descripción de la información a ser proporcionada/accedida y los métodos;
- b) criterios de clasificación de la información;

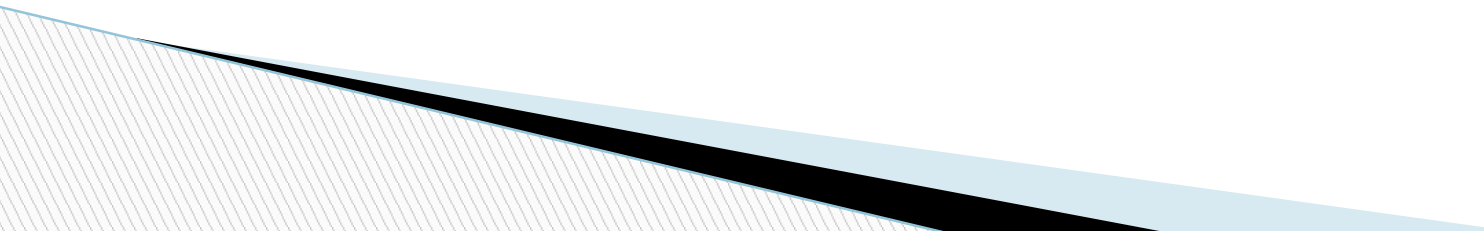
# A.5 Controles organizacionales

## 5.20 Abordar la seguridad de la información en los acuerdos con proveedores

- c) los requisitos legales y reglamentarios;
  - d) Controles a implementar por cada parte (acceso, evaluación de desempeño, la supervisión, etc.)
  - e) lista explícita del personal autorizado
  - f) políticas de seguridad de la información relevantes;
  - g) procedimientos de gestión de incidentes;
  - h) requisitos de selección (si es aplicable);
  - i) el derecho a auditar;
- 

# A.5 Controles organizacionales

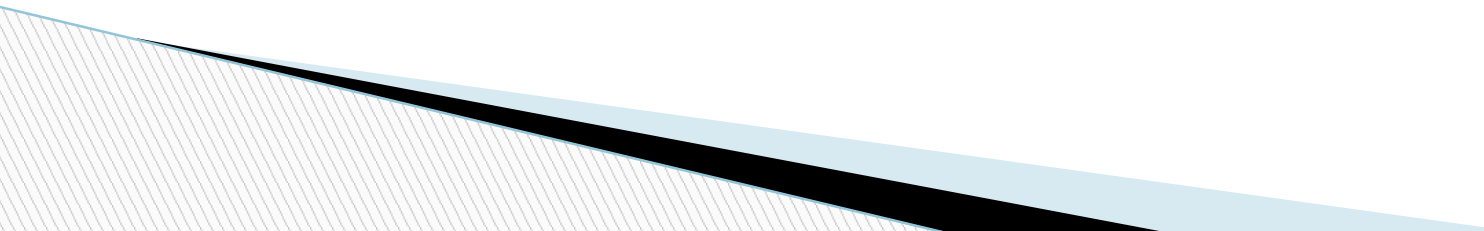
## 5.20 Abordar la seguridad de la información en los acuerdos con proveedores

- j) la resolución de problemas y conflictos;
  - k) informe periódico del proveedor sobre la efectividad de los controles y la corrección problemas;
  - l) Obligación del proveedor de cumplir con los requisitos de seguridad de la organización.
- 

# A.5 Controles organizacionales

## 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

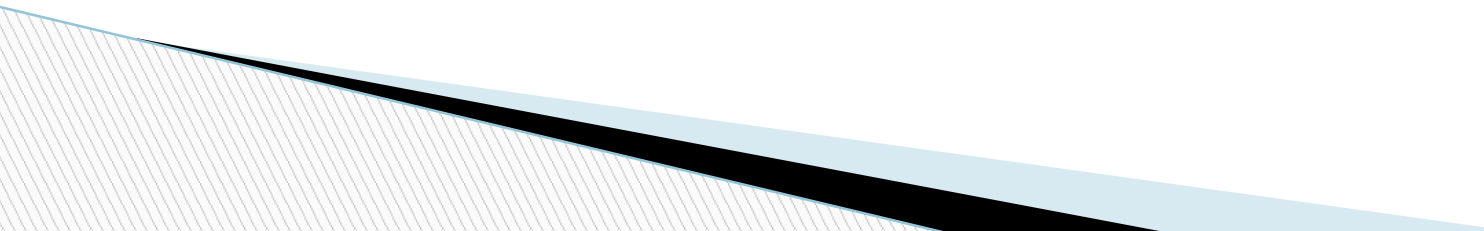
Deberían considerarse los siguientes temas:

- Requisitos de seguridad de los productos proporcionados
  - Proveedor será responsable de cumplimiento de requisitos de seguridad por parte de subcontratistas y sus propios proveedores
  - Identificación de componentes críticos del servicio o producto
  - Rastreo de componentes en la cadena
  - Garantías
- 

# A.5 Controles organizacionales

## 5.22 Seguimiento, revisión y gestión de cambios de los servicios de proveedores

El seguimiento y la revisión de los servicios de proveedores deberían asegurar el cumplimiento de los términos y condiciones de seguridad de la información de los acuerdos, y que los incidentes y los problemas de la seguridad de la información estén manejados correctamente.

- Niveles de desempeño
  - Informes del servicio y reuniones de evaluación
  - Auditorías y seguimiento a problemas reportados
  - Reportes de incidentes de seguridad
  - Capacidad de servicio del proveedor
- 



# A.5 Controles organizacionales

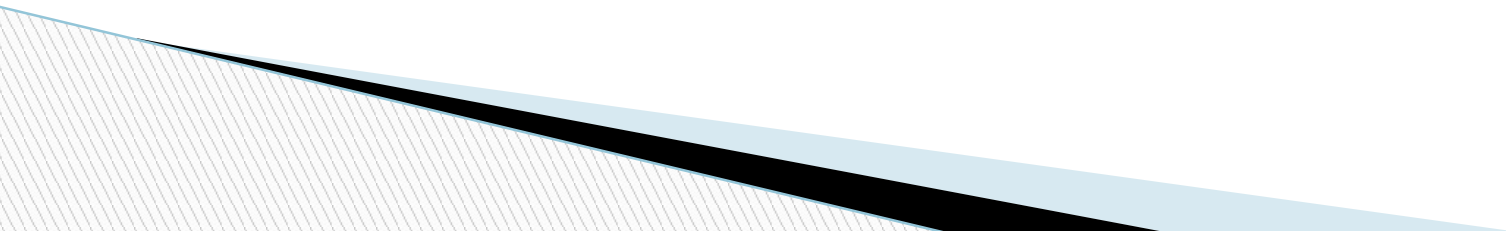
## **5.22 Seguimiento, revisión y gestión de cambios de los servicios de proveedores**

Los cambios a la prestación de servicios de los proveedores, incluyendo mantenimiento y mejora de las políticas, procedimientos y controles existentes de la seguridad de la información, deberían gestionarse teniendo en cuenta la criticidad de la información, sistemas, y procesos de negocios involucrados y la reevaluación de riesgos.

# A.5 Controles organizacionales

## **5.23 Seguridad de la información para el uso de servicios en la nube**

Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización



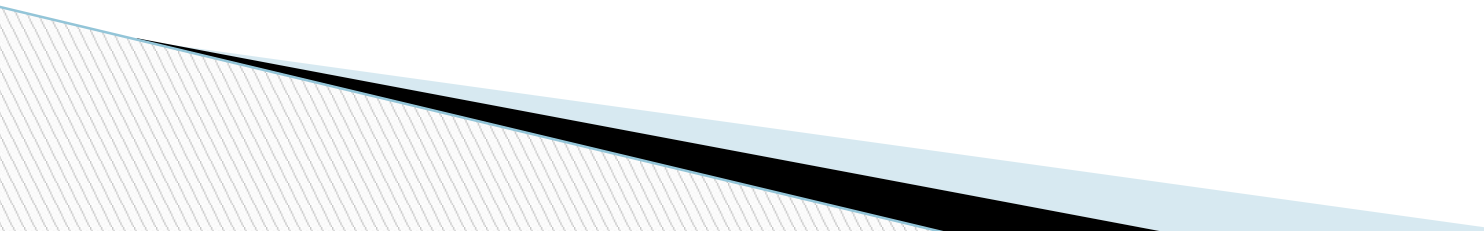
# A.5 Controles organizacionales

## 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

El seguimiento y la revisión de los servicios de proveedores deberían asegurar el cumplimiento de los términos y condiciones de seguridad de la información de los acuerdos, y que los incidentes y los problemas de la seguridad de la información estén manejados correctamente.

Deberían establecerse procedimientos y responsabilidades para:

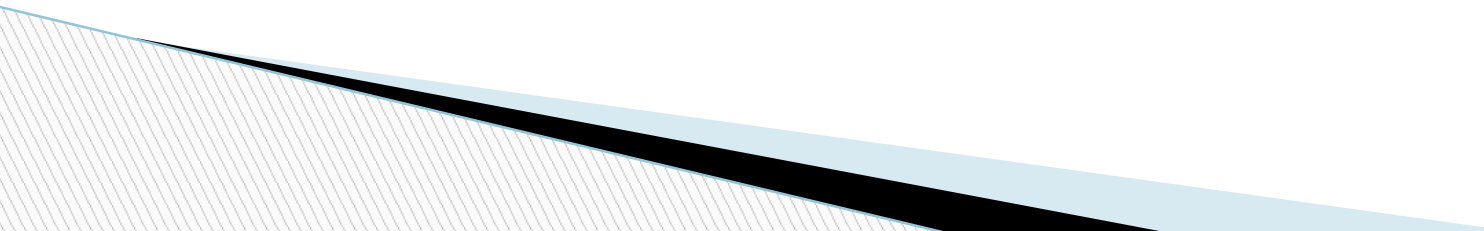
- Planificación y respuesta a incidentes
  - Supervisión, detección y análisis de incidentes
  - Registro de incidentes
- 

# A.5 Controles organizacionales

## 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

- Manejo de evidencia
- Evaluación de debilidades
- Respuesta, escalamiento y comunicaciones durante incidentes

Asegurar:

- Competencia del personal
  - Establecimiento de punto de contacto
  - Contacto con entidades externas
- 

# A.5 Controles organizacionales

## 5.25 Evaluación y decisión sobre eventos de seguridad de la información

El punto de contacto debería evaluar cada evento de seguridad de la información y decidir si debería ser clasificado como un incidente de seguridad de la información.

En los casos en que la organización tiene un equipo de respuesta a incidentes de seguridad de la información (ISIRT, por sus siglas en inglés, information security incident response team), la evaluación y la decisión pueden ser enviadas al ISIRT para su confirmación o reevaluación.

Los resultados de la evaluación y la decisión deberían registrarse en detalle con el fin de futura referencia y verificación.





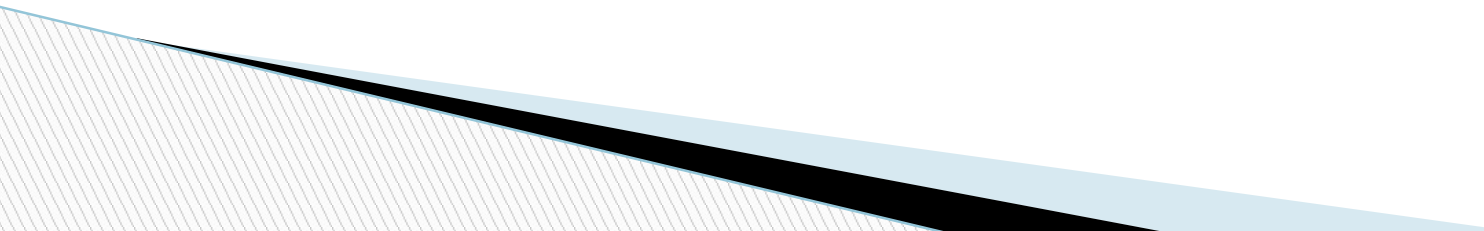
# Funcionamiento del SGSI (sesión 5)

Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

El estudiante conocerá los requisitos de la norma en relación a operación, evaluación del desempeño y mejora del SGSI.

# Cláusula 8: Operación

- 8.1 Planificación y Control Operacional
  - 8.2 Evaluación de Riesgos de Seguridad de la información
  - 8.3 Tratamiento de Riesgos de Seguridad de la Información
- 



# Cláusula 8: Operación

## 8.1 Planificación y Control Operacional

- La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1. La organización también debe implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2.
- La organización **debe mantener información documentada para asegurar que los procesos se han llevado a cabo de acuerdo a lo planificado.**

# Cláusula 8: Operación

## ... 8.1 Planificación y Control Operacional

- La organización debe controlar los cambios planeados y revisar los resultados
- Los procesos tercerizados deben ser controlados.

# Cláusula 8: Operación

## 8.2 Evaluación de Riesgos de Seguridad de la Información

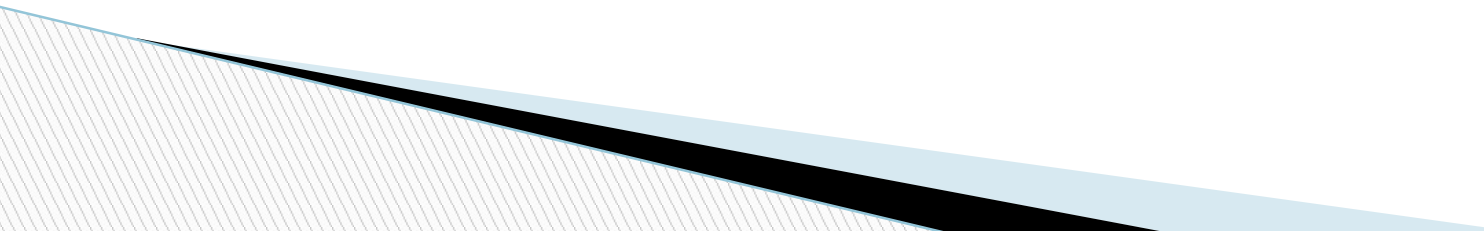
- La organización debe realizar evaluaciones de riesgos de S.I. en intervalos planificados y cuando ocurran cambios significativos, tomando en cuenta los criterios establecidos en 6.1.2a
- La organización **debe mantener información documentada de los resultados de las evaluaciones de riesgos de S.I.**

# Cláusula 8: Operación

## 8.3 Tratamiento de Riesgos de Seguridad de la Información

- La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.
- La organización **debe mantener información documentada de los resultados del tratamiento de riesgos de S.I.**

# Cláusula 9: Evaluación del Desempeño

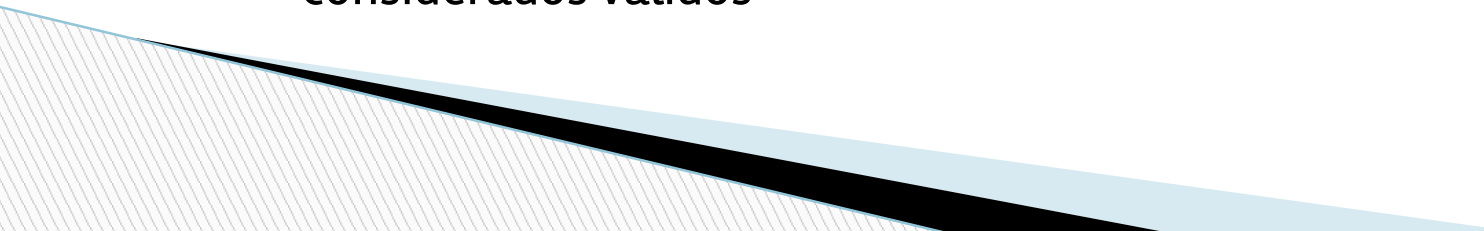
- 9.1 Monitoreo Medición, Análisis y Evaluación
  - 9.2 Auditoría Interna
  - 9.3 Revisión por la Gerencia
- 

# Cláusula 9: Evaluación del Desempeño

## 9.1 Monitoreo Medición, Análisis y Evaluación

- La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del SGSI
- La organización debe determinar:
  - a. Qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información
  - b. Los métodos para monitoreo, medición, análisis y evaluación, para asegurar resultados válidos

Nota: Los métodos deben proporcionar resultados comparables y reproducibles para ser considerados válidos



# Cláusula 9: Evaluación del Desempeño

## ...9.1 Monitoreo Medición, Análisis y Evaluación

- c. Cuándo debe ser realizado
- d. Quién debe monitorear y medir
- e. Cuándo los resultados deben ser analizados y evaluados
- f. Quién debe analizar esos resultados

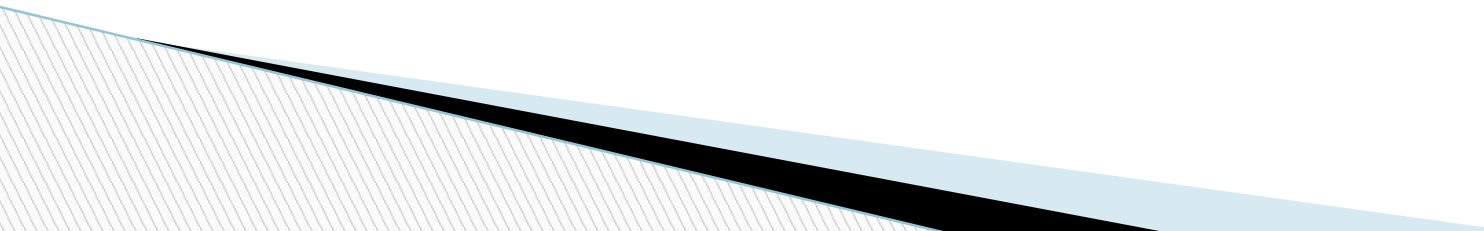
La organización **debe mantener información documentada apropiada como evidencia del monitoreo y resultados de medición**



# Cláusula 9: Evaluación del Desempeño

## 9.2 Auditoría Interna

La organización debe conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

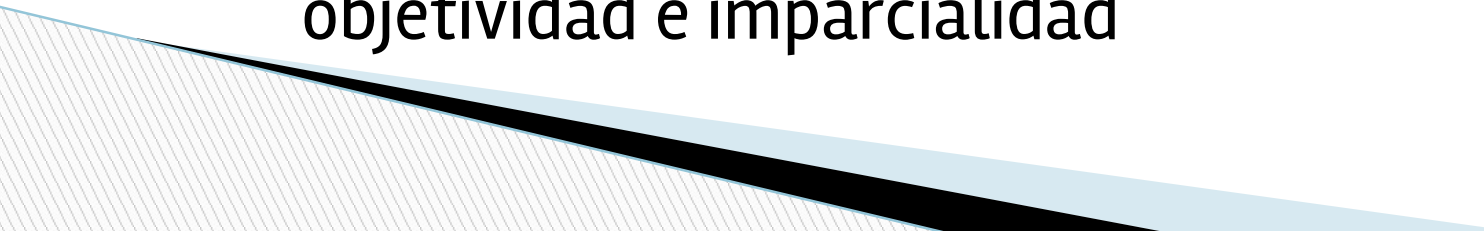
- a. Está en conformidad con los requisitos de la organización para su SGSI, y los requisitos de esta norma.
  - b. Está efectivamente implementado y mantenido
- 



# Cláusula 9: Evaluación del Desempeño

## ...9.2 Auditoría Interna

La organización debe:

- c. Planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos. Los programas de auditoría deben considerar la importancia de los procesos y resultados de auditorías previas.
  - d. Definir criterios y alcance de cada auditoría
  - e. Seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad
- 

# Cláusula 9: Evaluación del Desempeño

## ...9.2 Auditoría Interna

La organización debe:

- f. Asegurar que los resultados se reporten a los niveles relevantes
- g. Retener evidencias de los programas y resultados de la auditoría

# Cláusula 9: Evaluación del Desempeño

## 9.3 Revisión por la Gerencia

La alta gerencia debe revisar el SGSI de la organización a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.

Esto debe incluir:

- a. Estado de acciones en relación a revisiones anteriores
- b. Cambios en asuntos externos e internos que son relevantes al SGSI
- c. Retroalimentación sobre el desempeño de S.I. , incluyendo: No conformidades y acciones correctivas, resultados del monitoreo y medición, resultados de auditoría y cumplimiento de objetivos de S.I.

# Cláusula 9: Evaluación del Desempeño

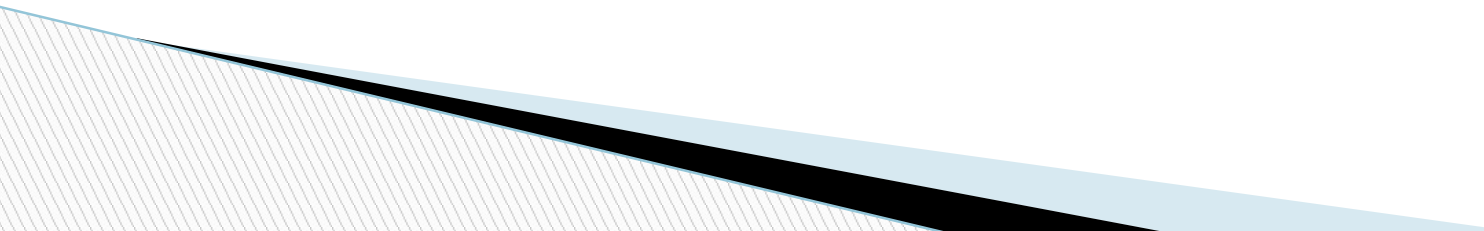
## ...9.3 Revisión por la Gerencia

- d. Retroalimentación de partes interesadas
- e. Resultados de la evaluación de riesgos y estado de su plan de tratamiento
- f. Oportunidades para la mejora continua

La organización **debe reterner información documentada como evidencia de los resultados de revisiones por parte de la gerencia.**



# Cláusula 10: Mejora

- 10.1 No conformidades y Acción Correctiva
  - 10.2 Mejora Continua
- 

# Cláusula 10: Mejora

## 10.1 No conformidades y Acción Correctiva

- Cuando ocurre una no conformidad, la organización debe:
  - a. Reaccionar a la no conformidad y, según sea aplicable: Tomar acción para controlarla y corregirla; y ocuparse de las consecuencias.
  - b. Evaluar la necesidad de acciones para eliminar las causas: Revisando la no conformidad, determinando las causas y determinando si existen no conformidades similares.
  - c. Implementar cualquier acción necesaria
  - d. Revisar la eficacia de las acciones tomadas
  - e. Hacer cambios al SGSI si fuera necesario.

# Cláusula 10: Mejora

## ...10.1 No conformidades y Acción Correctiva

- La organización debe mantener información documentada como evidencia de:
  - f. La naturaleza de las no conformidades y cualquier acción subsiguiente tomada
  - g. Los resultados de cualquier acción correctiva

# Cláusula 10: Mejora

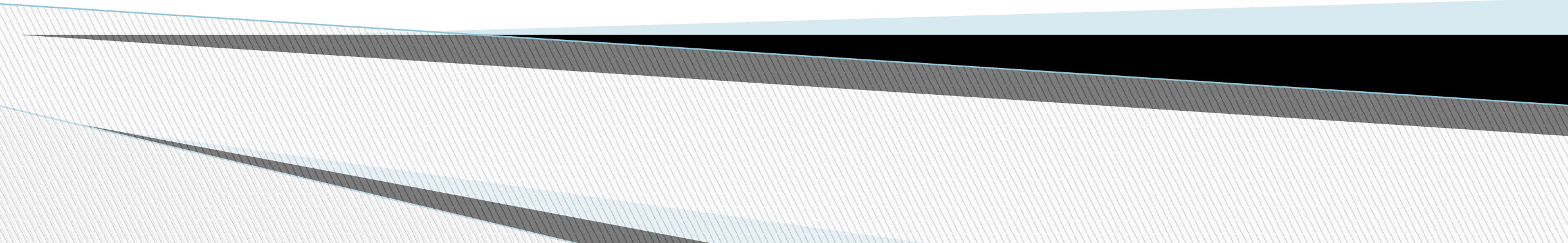
## 10.2 Mejora Continua

- La organización debe mejorar continuamente la conveniencia, adecuación, y efectividad del sistema de gestión de seguridad de la información.



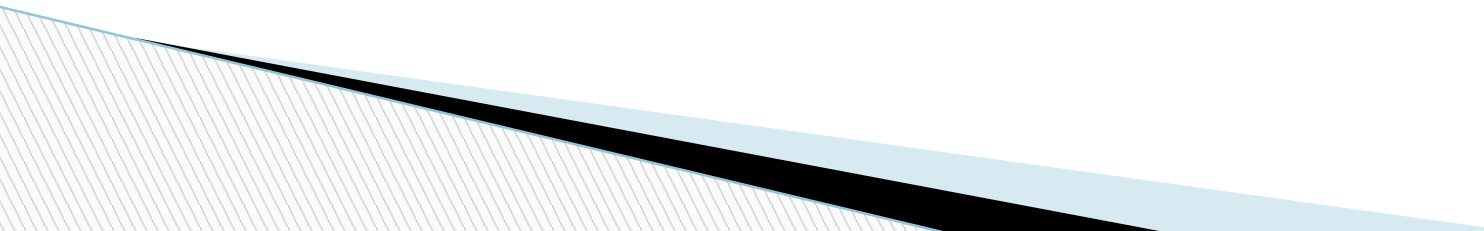
# **Anexo “A”**

## **Controles**



# A.5 Controles organizacionales

## 5.1 Políticas de seguridad de la información

- Aprobadas por el más alto nivel de la organización posible
  - Deben abordar: Estrategia de negocios, normativa y entorno
  - Deben contener: Objetivos de S.I., Asignación de responsabilidades, proceso para manejo de desviaciones
  - Debe ser comunicada a partes relevantes y estar disponible
- 

# A.5 Controles organizacionales

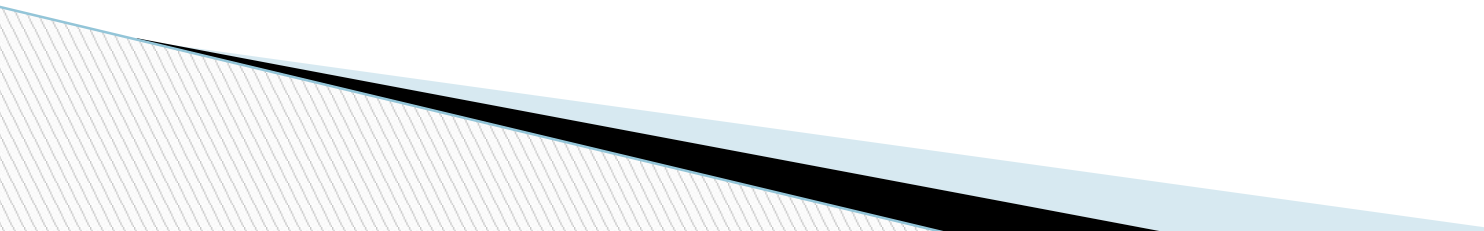
## 5.1 Políticas de seguridad de la información

La Política General de Seguridad de la Información será soportada por otras políticas de menor nivel, abocadas a temas más específicos, así por ejemplo:

- a) control de acceso
- b) clasificación (y manejo) de la información
- c) seguridad física y ambiental
- d) temas finales orientados al usuario, tales como:
  - 1) uso aceptable de activos
  - 2) escritorio y pantalla limpios
  - 3) transferencia de información
  - 4) dispositivos móviles y teletrabajo
  - 5) restricciones a las instalaciones y uso del software, etc.

# A.5 Controles organizacionales

## 5.1 Políticas de seguridad de la información

- Las políticas de seguridad de la información deberían revisarse a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas.
  - Cada política debería tener un propietario con responsabilidad de gestión aprobada para el desarrollo, la revisión y la evaluación de las políticas
- 

# A.5 Controles organizacionales

## 5.2 Roles y responsabilidades en seguridad de la información

- Deberían identificarse las responsabilidades para protección de activos individuales y para realización de procesos específicos de seguridad de la información.
- Responsabilidades de Gestión de Riesgos, aceptación de riesgos residuales
- Los responsables pueden delegar tareas, pero siguen siendo los responsables.
- Personal debe ser competente en sus tareas
- Asignar responsabilidades de coordinación de seguridad con terceros

# A.5 Controles organizacionales

## 5.3 Segregación de funciones

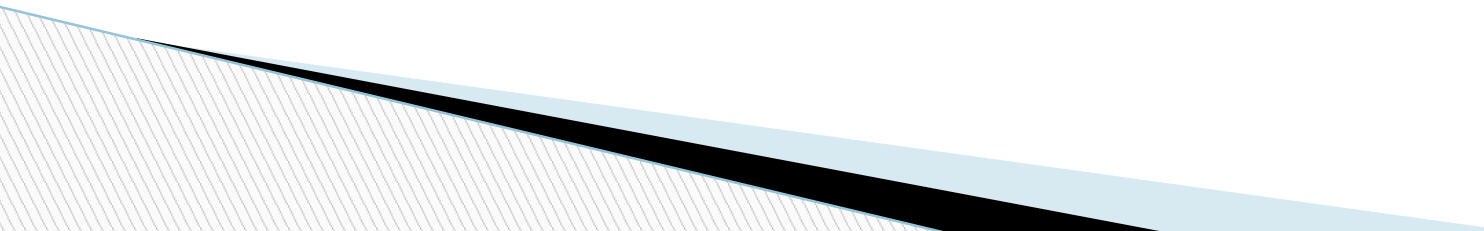
- La segregación de funciones es un método para manejar los conflictos de intereses y las posibilidades de fraude.
- Restringe el poder asignado a un individuo
- Coloca barreras para prevenir el fraude que puede ser efectuado por una sola persona.
- En caso de colusión, el fraude igual se podrá realizar



# A.5 Controles organizacionales

## 5.3 Segregación de funciones

Algunos ejemplos:

- El que otorga accesos  $\neq$  Revisa periódicamente los accesos
  - El que ejecuta la tarea  $\neq$  Realiza la medición de rendimiento (métrica)
  - El que define los roles  $\neq$  Asigna los roles y accesos
  - Programador  $\neq$  Ejecuta pases a producción de cambios
  - Personal de Desarrollo  $\neq$  Autoriza pases a producción
  - Contraseñas compartidas para accesos críticos (Cuentas de superusuario, acceso a bóvedas, etc.)
- 

## **A.5 Controles organizacionales**

### **5.4 Responsabilidades de la gerencia**

La gerencia exigirá a empleados y proveedores cumplir con las políticas y procedimientos de seguridad establecidos por la organización.

Asegurar que las responsabilidades y autoridades relevantes para la seguridad se hayan asignado y comunicado formalmente.

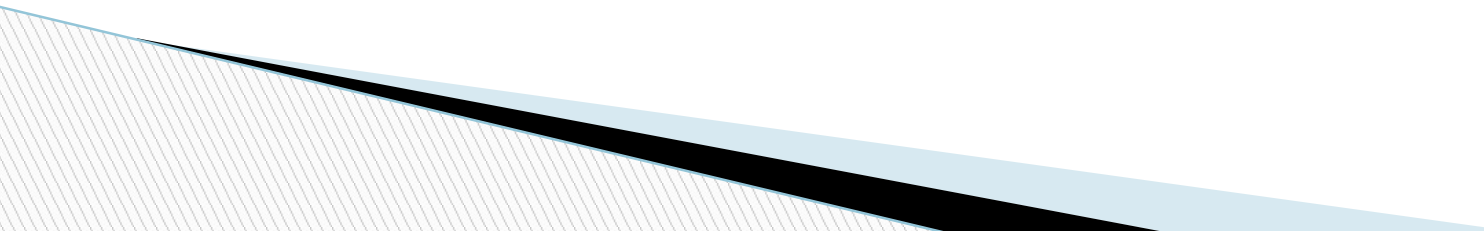




# A.5 Controles organizacionales

## 5.5 Contacto con autoridades

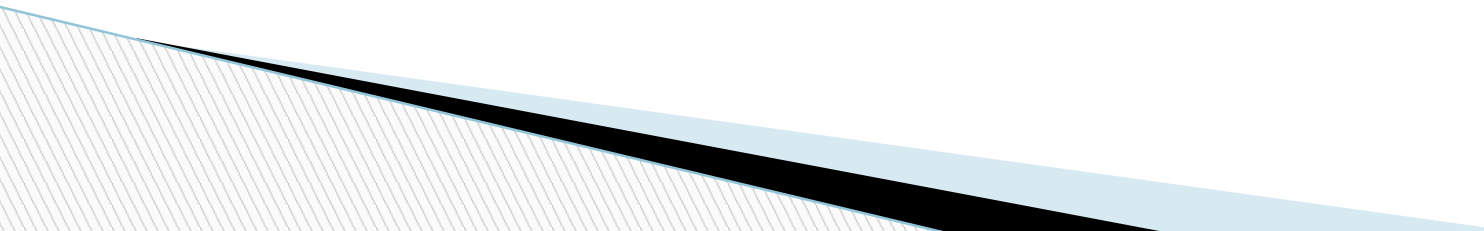
Algunos ejemplos:

- Policía, División de Delitos Informáticos de la Policía Nacional (DIVINDAT)
  - Bomberos
  - Defensa Civil
  - Dirección General de Protección de Datos Personales
- 

# A.5 Controles organizacionales

## 5.6 Contacto con grupos de interés especializados

Algunos ejemplos:


- Foros de Seguridad
  - Proveedores de software: Sistemas Operativos, aplicaciones (alertas de seguridad, notificaciones de parches, etc.)
  - Proveedores de servicios:
    - Comunicaciones
    - Antivirus
    - herramientas de seguridad
    - consultores, etc.
- 

# A.5 Controles organizacionales

## 5.7 Inteligencia de amenazas

La información relacionada con las amenazas a la seguridad de la información debe ser recopilada y analizada para producir inteligencia sobre las amenazas.

Ejemplos:

- Recibir la inteligencia de amenazas de foros y fuentes de intercambio de información.
  - Identificar y documentar las amenazas, tanto internas como externas.
  - Recopilar y correlacionar datos de los eventos de múltiples fuentes.
- 

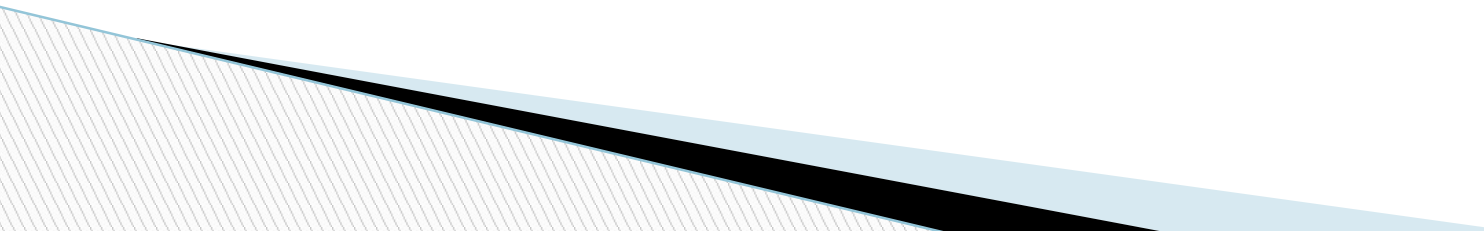
# A.5 Controles organizacionales

## 5.8 Seguridad de Información en Gestión de Proyectos

- La seguridad de la información debería integrarse en el método de gestión de proyectos de la organización para garantizar que los riesgos de seguridad de la información son identificados y tratados como parte de un proyecto.
- Los métodos de gestión de proyectos en uso deberían exigir que:
  - a) los objetivos de seguridad de la información sean incluidos en los objetivos del proyecto;
  - b) una evaluación de riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto para identificar los controles necesarios;
  - c) la seguridad de la información es parte de todas las fases de la metodología del proyecto aplicada.

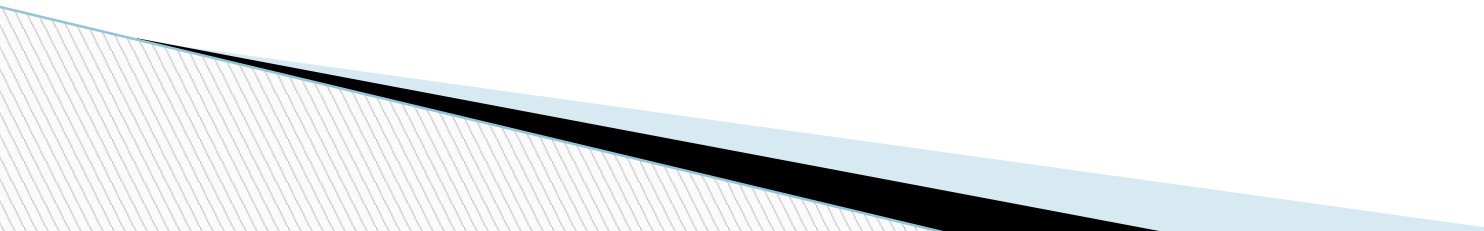
# A.5 Controles organizacionales

## 5.9 Inventario de información y otros activos asociados

- La documentación debería mantenerse en inventarios dedicados o existentes, según corresponda.
  - El inventario de activos debería ser exacto, actualizado, consistente y alineado con otros inventarios.
  - Para cada uno de los activos identificados, debería asignarse un propietario y debería identificarse la clasificación.
  - Los inventarios de activos ayudan a garantizar que se logra la protección eficaz, pero también pueden ser requeridos para otros propósitos, como por ejemplo por razones de salud y seguridad, financieras o de seguros (gestión de activos).
- 

# A.5 Controles organizacionales

## 5.9 Inventario de información y otros activos asociados

- Se debe asignar oportunamente la propiedad de los activos
  - La propiedad debería asignarse cuando los activos son creados o cuando son transferidos a la organización.
  - El propietario de los activos debería ser responsable de la correcta gestión de un activo durante todo el ciclo de vida de los activos.
- 

# A.5 Controles organizacionales

## 5.9 Inventario de información y otros activos asociados

El propietario del activo debería:

- a) asegurar que los activos son inventariados;
- b) asegurar que los activos son clasificados y protegidos adecuadamente;
- c) definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso;
- d) garantizar el manejo adecuado cuando el activo es eliminado o destruido.

# A.5 Controles organizacionales

## 5.9 Inventario de información y otros activos asociados

- El propietario identificado no necesariamente tiene ningún derecho de propiedad sobre el activo.
- Las tareas rutinarias pueden ser delegadas, por ejemplo, a un guardia que vigile el activo diariamente, pero la responsabilidad continua siendo del propietario.
- En sistemas de información complejos, puede resultar útil designar un grupo de activos, los cuales actúan en forma conjunta para proveer un servicio particular. En este caso, el propietario del servicio es responsable por la entrega del mismo, incluido el funcionamiento de sus activos.



# A.5 Controles organizacionales

## 5.10 Uso aceptable de la información y otros activos asociados

- Los empleados y los usuarios de terceras partes (Ej. Consultores) que utilizan o tienen acceso a los activos de la organización deberían ser conscientes de los requisitos de seguridad de la información de la organización.
- Deberían responsabilizarse del uso de los recursos de procesamiento de la información y de cualquier uso llevados a cabo bajo su responsabilidad.
- *Recomendable elaborar una Política de uso Aceptable de Activos de Información cubriendo aspectos básicos que deben conocer los empleados y terceros, tales como: Uso del correo electrónico, Uso de Internet, Acceso a sistemas de información de la Organización, uso de dispositivos móviles, etc...*



# **Introducción al Sistema de Gestión de Seguridad de la Información (Sesión 03)**

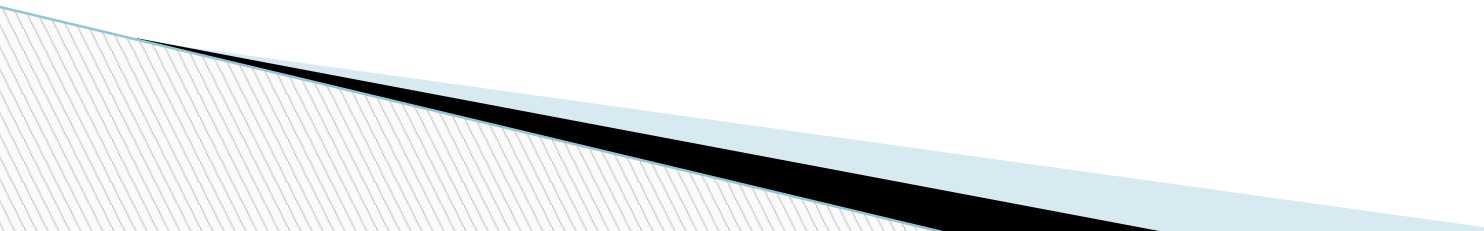
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

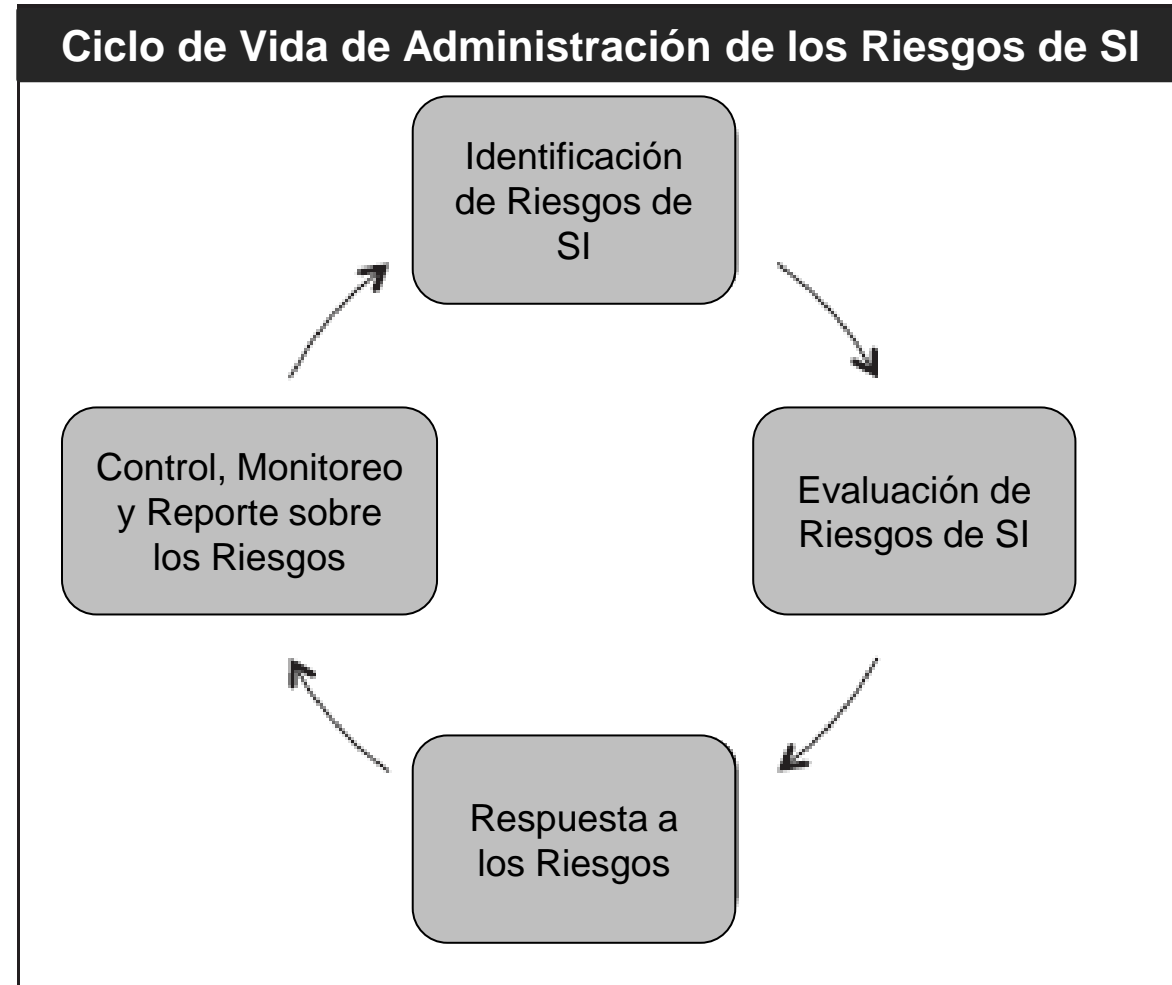
El estudiante conocerá los requisitos de la norma en relación al tratamiento de los riesgos y establecimiento de objetivos de seguridad de la información.

# Algunos ejemplos adicionales de la sesión anterior

Documentación del SGSI de empresa del rubro de servicios de seguridad de la información:

- Contexto de Organización
  - Alcance
  - Objetivos del SGSI
  - Política de Seguridad
- 

# Gestión de los riesgos



# Conceptos y Definiciones – ¿Qué es un riesgo?

“Efecto de la incertidumbre sobre la consecución de objetivos”

- *Nota 1: Un efecto es una desviación, positiva o negativa, respecto a lo previsto.*
- *Nota 2: Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).*
- *Nota 3: Con frecuencia el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias o una combinación de ambos.*
- *Nota 4: Con frecuencia, el riesgo se expresa en términos de la combinación de las consecuencias de un suceso y de su probabilidad.*
- *Nota 5: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.*

# Conceptos y Definiciones – ¿Qué es un riesgo?

- “El potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos, que ocasione pérdida o daño a los activos. El impacto o la severidad relativa del riesgo es proporcional al valor del daño o pérdida para el negocio y a la frecuencia estimada de la amenaza”

Fuente: Guidelines for the Management of IT Security (International Organization for Standardization)

- “La posibilidad de que algo suceda que impactará en los objetivos. Se mide en términos de consecuencias y probabilidad.”

Fuente: Australian/New Zealand Standard AS/NZS 4360 Risk Management

# Conceptos y Definiciones

- Activo: Algo de valor (tangible o intangible) que merece protegerse.
- Amenaza: Una causa potencial de un incidente no deseado que puede resultar en daño para un sistema u organización.
- Vulnerabilidad: Cualquier debilidad que pueda ser aprovechada por una amenaza.
- Evento: Un incidente o situación que ocurre en un lugar particular en un intervalo de tiempo particular.

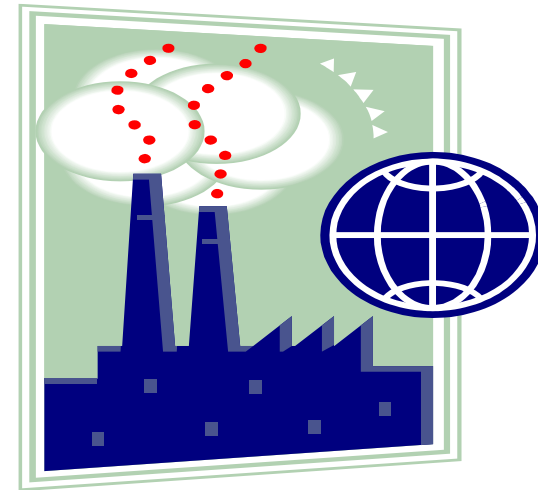


# Visión General de la Gestión de Riesgos

- El proceso de asegurar que el impacto de las amenazas que explotan las vulnerabilidades esté dentro de los límites y costos aceptables.
- Los riesgos deben ser gestionados de manera que no impacten materialmente los procesos de negocio.
- El riesgo es inherente en todas las actividades de negocio.
- Foco específico en la gestión de riesgos de la información desde una perspectiva de seguridad.

# Riesgo Inherente y Riesgo Residual

- Riesgo inherente: Riesgo presente en el curso normal de las actividades de negocio.
- Riesgo residual: Los riesgos después de implementar los controles.

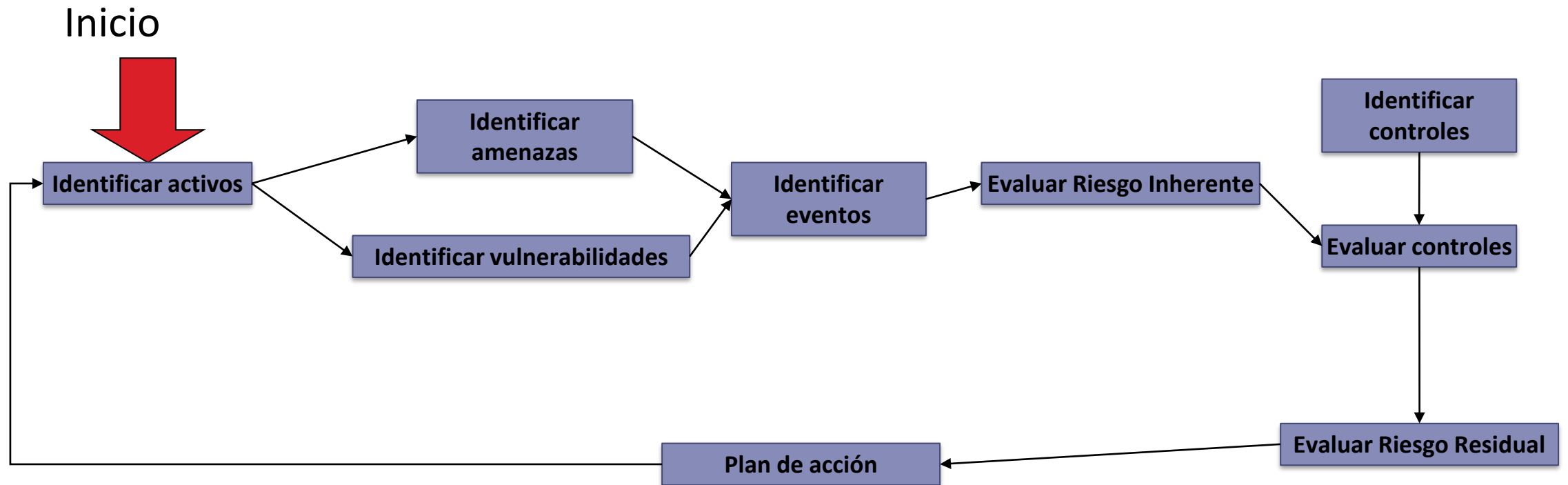


# Apetito, Tolerancia y Capacidad

- **Apetito de Riesgo** es el nivel de riesgo que la empresa está dispuesta a aceptar en el logro de sus metas.
- **Tolerancia al Riesgo** es el nivel aceptable de variación en relación a la concesión de un objetivo.
- **Capacidad** es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.



# Marco General de Gestión de Riesgos de la Seguridad de la Información

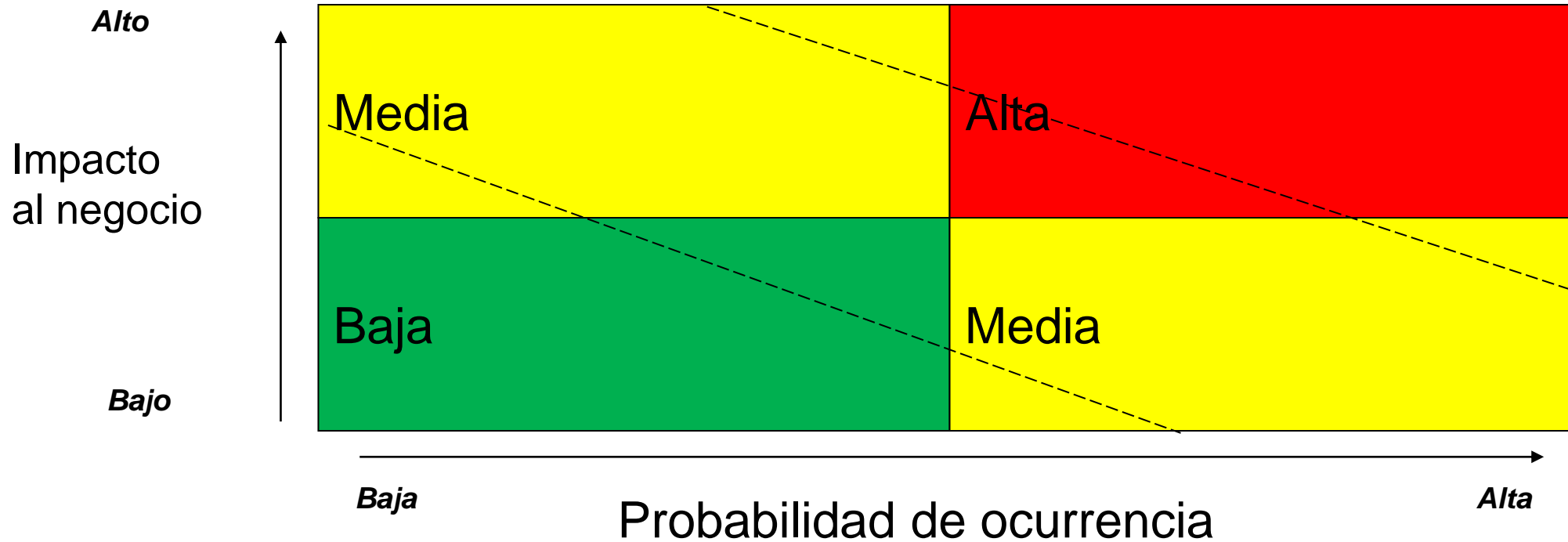


# Análisis Básico del Riesgo

- La clasificación del riesgo implica la evaluación de dos componentes:
  - La posibilidad de que ocurra pérdida o daño (probabilidad de ocurrencia)
  - La magnitud y el efecto del impacto financiero o de otro tipo de dicha ocurrencia (impacto en el negocio).
- Foco inicial en Riesgos Altos (Probabilidad Alta de Ocurrencia y Alto Impacto en el Negocio).
- Se necesita balancear el costo de implementar controles contra los riesgos identificados:
  - También aplica transferir los riesgos vía seguros.

# Análisis Básico del Riesgo

## Clasificación del riesgo



# Paso 1 – Caracterización del Sistema

- Recopilar información del sistema y las redes:
  - Información y datos
  - Hardware
  - Software
  - Servicios
  - Documentos
  - Personal
- Entregable: Comprensión del Sistema de TI.

## Paso 2 – Identificación de Amenazas

- Cualquier circunstancia o evento con el potencial de causar daño a un recurso de información.
- Identificar amenazas a recursos críticos de TI.
- Amenazas a considerar:
  - Errores
  - Daño/ataque malicioso
  - Eventos naturales (inundaciones, terremotos, etc.)
  - Fraude
  - Robo
  - Falla del equipo/software
- Entregable: Declaración de Amenazas conteniendo la lista de amenazas que podrían explotar las vulnerabilidades del sistema.



# Paso 3 – Identificación de Vulnerabilidades

- Las vulnerabilidades son características de los recursos de información que pueden ser explotadas por una amenaza para causar daño.
- Ejemplos:
  - Accesos no removidos en los sistemas de empleados cesados.
  - El firewall permite telnet entrante con cuentas hábiles de invitados.
- Entregable: Lista de vulnerabilidades del sistema.

# Paso 4 – Análisis de Control

- Analizar los controles que han sido implementados, o planeados para implementación en el sistema bajo revisión.
- Controles preventivos:
  - Identificación y autenticación
  - Control de acceso a recursos
- Controles detectivos:
  - Logs de eventos de seguridad
- Entregable: Lista de controles utilizados para el sistema de TI.

# Paso 5 – Determinación de Probabilidad

- Identificar la probabilidad de que la vulnerabilidad potencial pueda ser explotada en el contexto de un ambiente de amenazas.
- Se necesita evaluar:
  - Fuente de amenazas.
  - Naturaleza de las vulnerabilidades.
  - Existencia y efectividad de los controles.
- Definir en términos de Alto/Medio/Bajo:
  - Alto: Fuente de la amenaza (p.e. un hacker) es capaz de explotar vulnerabilidades (p.e. tiene exploits) y los controles no son efectivos.
- Entregable: Clasificación de probabilidades.

# Paso 6 – Análisis del Impacto

- El propósito de este paso es determinar el impacto adverso resultante de la explotación exitosa de una vulnerabilidad.
- Se requiere la clasificación de la información en términos de confidencialidad, integridad y disponibilidad.
- Evaluar el impacto basado en la pérdida de confidencialidad, integridad o disponibilidad.
- Entregable: Declaración de Impacto (Alto, Medio o Bajo)

## Paso 6 – Clasificación de Información

- Identificar a los propietarios de la información.
- Utilizar métodos sencillos de clasificación.
- Considerar agrupación de activos de información:

<u>ACTIVO</u>	<u>CONFIDENCIALIDAD</u>	<u>INTEGRIDAD</u>	<u>DISPONIBILIDAD</u>
Datos de clientes	Alta	Alta	Baja

# Paso 6 – Impacto de las Amenazas en el Negocio

- La evaluación se basa principalmente en la pérdida de confidencialidad, integridad o disponibilidad de la información. Impactos específicos en el negocio incluyen:
  - Pérdida de dinero (efectivo o crédito).
  - Incumplimiento de la ley.
  - Pérdida de reputación/prestigio/vergüenza (web defacement).
  - Peligro potencial para el personal o los clientes.
  - Pérdida de confianza.
  - Pérdida de oportunidades de negocio.
  - Reducción en el desempeño/eficiencia operativos.
  - Interrupción de las actividades del negocio.

# Paso 7 – Determinación del Riesgo

- Evaluar el nivel de riesgos de TI.
- La determinación del riesgo para un par amenaza/ vulnerabilidad particular puede ser expresada como una función de:
  - La probabilidad de que una determinada fuente de amenazas intente explotar una determinada vulnerabilidad.
  - La magnitud del impacto en caso de que una fuente de amenazas explote exitosamente las vulnerabilidades.
  - La idoneidad de controles de seguridad planificados o existentes para reducir o eliminar riesgos.
- Entregable: Declaración de niveles de riesgos expresados como Alto / Medio / Bajo.

## Paso 8 – Recomendaciones de Control

- Se identifican los controles que mitigan o eliminan los riesgos identificados a las operaciones de la organización.
- El objetivo de los controles recomendados es reducir el nivel de riesgo al sistema TI y su información a un nivel aceptable.
- Entregable: Recomendaciones de controles y soluciones alternativas para mitigar riesgos.



# Paso 8 – Riesgo Residual

- Mitigación del riesgo:
  - Identificar e implementar controles.
  - Seguro contra la ocurrencia del riesgo.
- La aceptación del riesgo residual depende de:
  - La política organizacional (Apetito y tolerancia).
  - La identificación y la medición del riesgo.
  - La incertidumbre en el enfoque mismo de la valoración de riesgos.
  - Costo y efectividad de la implementación

# Paso 9 – Documentación de Resultados

- Reporte de evaluación de riesgos:
  - Describe amenazas y vulnerabilidades.
  - Describe niveles de riesgo.
  - Brinda recomendaciones para la implementación de controles.

# Opciones de Respuesta a los Riesgos

- ¿Cuánto invertir para mitigar el riesgo?
  - Depende del valor de lo que quiero proteger
  - Depende de la probabilidad de que ocurra el evento



vs



# Opciones de Respuesta a los Riesgos

Ejemplo:

- Riesgo de pérdida total del centro de cómputo producido por un terremoto.
- Datos:
  - ✓ Valor total del C. Cómputo: US\$1M
  - ✓ De acuerdo a estadísticas en la zona geográfica donde se ubica el C. Cómputo, se produce un terremoto superior a grado 8 cada 10 años.
- Pregunta: ¿Cuánto debería invertir como máximo anualmente en un seguro contra pérdida del centro de cómputo?

# Opciones de Respuesta a los Riesgos

Impacto: US\$1M

Probabilidad =  $1/10 = 0.1$

Pérdida Esperada Anual (ALE) = Impacto x Probabilidad

Pérdida Esperada Anual =  $\text{US\$1M} \times 0.1 = \text{US\$100K}$

Por lo tanto anualmente no debería invertir en un seguro más de US\$100K

Si invierto más, estaré pagando más de lo que me costará construir e implementar C. Cómputo nuevo.

# Opciones de Respuesta a los Riesgos

- Se cuenta con cuatro opciones para responder a los riesgos (MATE):
  - Mitigar el Riesgo
  - Aceptar el Riesgo
  - Transferir el Riesgo
  - Evitar el Riesgo

# Opciones de Respuesta a los Riesgos

## Mitigar el Riesgo

- La mitigación del riesgo significa que se tomaron medidas para reducir ya sea la frecuencia (probabilidad) o el impacto (daño o perjuicio) de un riesgo.
  - Podría requerir el uso de varios controles hasta que éste alcance niveles de aceptación o tolerancia del riesgo.
- Ejemplos de mitigación de riesgos:
  - Implementar nuevos controles técnicos, de gestión u operativos que reduzcan la probabilidad o el impacto de evento adverso
  - Instalar un nuevo sistema de control de accesos
  - Implementar políticas o procedimientos operativos
  - Desarrollar un plan de respuesta a incidentes y un plan de continuidad de negocios eficaces
  - Utilizar controles compensatorios

# Opciones de Respuesta a los Riesgos

## Aceptar el Riesgo

- Es una decisión consciente tomada por la alta gerencia, de reconocer la existencia de un riesgo y conscientemente decidir que el riesgo permanezca (asumir el riesgo) sin (mayores) medidas de mitigación.
  - La Gerencia será responsable por el impacto generado en caso se materialice el riesgo.
- Riesgo Aceptable: Definido como la cantidad de riesgo que la alta gerencia ha determinado que está dentro de los límites aceptables o permisibles.
  - No es lo mismo que ignorar el riesgo, lo cual es una falla para identificar o reconocer la existencia de un riesgo.



# Opciones de Respuesta a los Riesgos

## ...Aceptar el Riesgo

- Ejemplos de aceptación del riesgo:
  - Se prevé que un determinado proyecto no podrá implementar una funcionalidad requerida por el negocio para la fecha planificada. La Gerencia puede decidir aceptar el riesgo y continuar con el proyecto.
  - Un riesgo en particular que es calificado como extremadamente raro (ocurrencia muy poco probable) tiene consecuencias catastróficas, y las medidas para mitigar dicho riesgo son prohibitivas. La Gerencia podría decidir aceptar dicho riesgo.
- La aceptación del riesgo está basada muchas veces en un riesgo mal calculado.
- El nivel de riesgo y el impacto pueden cambiar constantemente, por lo que las revisiones periódicas son necesarias.

# Opciones de Respuesta a los Riesgos

## Transferir / Compartir el Riesgo

- La transferencia del riesgo es una decisión de reducir la pérdida compartiendo el riesgo con otra organización (Ej. Adquisición de un seguro)
- Proyectos compartidos con otras organizaciones son otro ejemplo
- Las decisiones de transferencia de riesgo deben ser revisadas con regularidad

# Opciones de Respuesta a los Riesgos

## Evitar el Riesgo

- Evitar el riesgo significa evitar las actividades o condiciones que dan lugar al riesgo
  - Se aplica cuando no hay otra respuesta adecuada al riesgo
- Ejemplos de evitación<sup>(\*)</sup> del riesgo
  - Reubicar el centro de cómputo lejos de una región con riesgos naturales importantes.
  - Rechazar participar en un proyecto muy grande cuando se observa una muy alta probabilidad de fracaso.
  - Rechazar participar en un proyecto que se basará en sistemas complicados y obsoletos, porque no se cuenta con un aceptable grado de confianza que el proyecto entregue algo útil / viable.
  - Decidir no utilizar cierta tecnología paquete de software ya que impediría una expansión futura.
  - Rechazar abrir sucursales en países con alta probabilidad de estatización o alto nivel de inseguridad

(\*) Evitación: Acción y efecto de evitar – Diccionario RAE

# Cláusula 6: Planificación

- 6.1 Acciones para tratar los riesgos y oportunidades
- 6.2 Objetivos de Seguridad de la Información y planificación para Conseguirlos

# Cláusula 6: Planificación

## 6.1 Acciones para tratar los riesgos y oportunidades

Al planificar el SGSI, la organización debe considerar los aspectos mencionados en el numeral 4.1 y los que figuran en el 4.2, y determinar los riesgos y oportunidades que necesitan ser tratados para:

- a. Asegurar que el SGSI pueda lograr los resultados esperados;
- b. Prevenir o reducir efectos indeseados y
- c. Lograr la mejora continua.

La organización debe planificar:

- d. Las Acciones que traten estos riesgos y oportunidades, y
- e. La forma de:
  - 1. Integrar estas acciones en los procesos del SGSI
  - 2. Evaluar la eficacia de estas acciones

# Cláusula 6: Planificación

## 6.1.2 Evaluación de los riesgos de Seguridad de la Información (ERSI)

La organización debe definir un proceso de ERSI que:

- a. Establezca y mantenga criterios de riesgo de seguridad de la información que incluyan:
  - 1. Los criterios de aceptación de los riesgos
  - 2. Los criterios para realizar las ERSI
- b. Se asegure que al realizar nuevamente una ERSI se obtengan resultados consistentes, válidos y comparables.

# Cláusula 6: Planificación

## ...6.1.2 Evaluación de los riesgos de Seguridad de la Información (ERSI)

- c. Identifique los riesgos de seguridad de la información
  - 1. Aplicando el proceso de ERSI para identificar riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad, de la información dentro del alcance del SGSI.
  - 2. Identificando a los propietarios de los riesgos
- d. Analice los riesgos de S.I.
  - 1. Evaluando las consecuencias potenciales que resultarían si se materializan los riesgos identificados
  - 2. Evaluar la probabilidad realista de la ocurrencia de los riesgos identificados
  - 3. Determinar los niveles de riesgo

# Cláusula 6: Planificación

...6.1.2 Evaluación de los riesgos de Seguridad de la Información (ERSI)

- e. Evalúe los riesgos de Seguridad de la Información:
  - 1. Comparar los resultados del análisis de riesgo vs los criterios establecidos
  - 2. Priorizar los riesgos para su tratamiento

***La Organización deberá conservar información documentada del proceso de ERSI***



# Cláusula 6: Planificación

## 6.1.3 Información de Tratamiento de Riesgos de Seguridad

La organización debe definir y aplicar un proceso de tratamiento de los riesgos de S.I. para:

- a. Seleccionar opciones de tratamiento adecuadas teniendo en cuenta los resultados de la evaluación de riesgos;
- b. Determinar los controles que sean necesarios para poner en práctica las opciones de tratamiento de riesgos elegida;
- c. Comparar los controles determinados en el punto anterior, con los del Anexo “A”.

# Cláusula 6: Planificación

## ...6.1.3 Información de Tratamiento de Riesgos de Seguridad

La organización debe definir y aplicar un proceso de tratamiento de los riesgos de S.I. para:

- d. Elaborar una Declaración de Aplicabilidad que incluya los controles necesarios y la justificación tanto de las inclusiones, así como de las exclusiones de los controles del Anexo “A”.
- e. Formular un plan de tratamiento de riesgos de S.I.
- f. Obtener del propietario del riesgo, la aprobación del plan de tratamiento, y la aceptación de los riesgos residuales.

***La organización debe conservar información documentada del proceso de tratamiento de riesgos***

# Cláusula 6: Planificación

## 6.2 Objetivos de Seguridad de la Información y Planificación para Lograrlos

La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Los objetivos de seguridad de la información deben:

- a. Ser consistente con la Política de S.I.
- b. Ser medibles (si es posible)
- c. Ser comunicados, y
- d. Ser actualizados según corresponda

***La organización debe conservar información documentada sobre los objetivos de seguridad de la información***

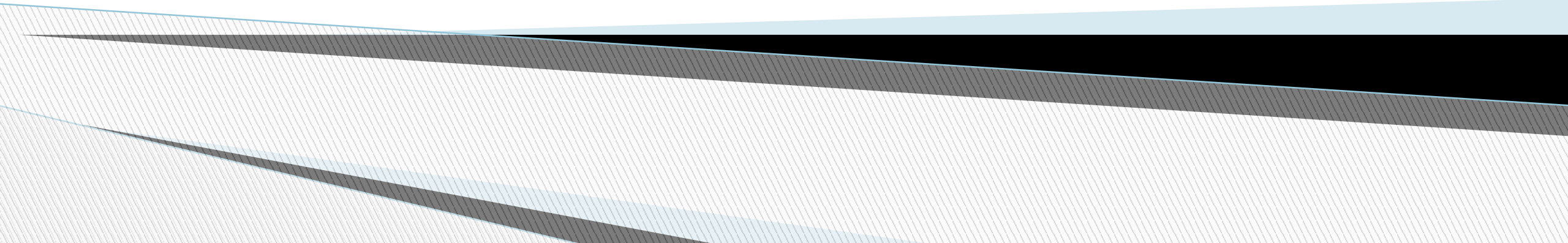
# Cláusula 6: Planificación

...6.2 Objetivos de Seguridad de la Información y Planificación para Lograrlos

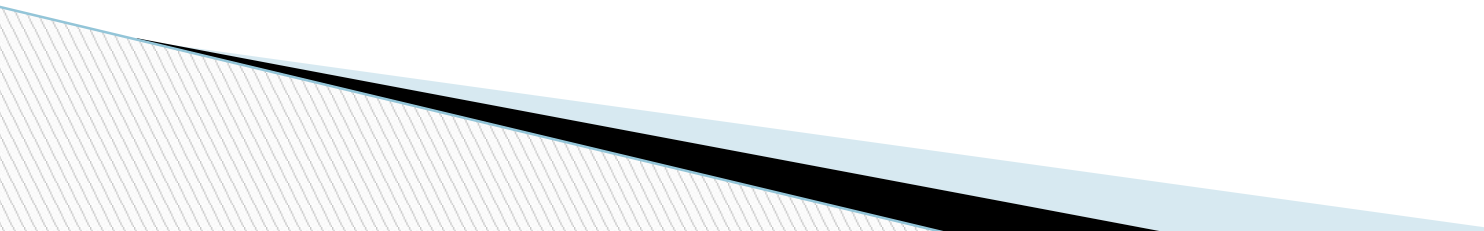
Al planificar cómo alcanzar sus objetivos de seguridad de la información, la organización debe determinar:

- a. Lo que se hará.
- b. Qué recursos requerirá
- c. Quién será responsable
- d. Cuándo se completará
- e. La forma en que se evaluará los resultados.

# Repaso: Planificación



# Repasemos

1. ¿Qué opciones existen para el tratamiento de los riesgos? Ejemplos.
  2. ¿Qué información exige la norma documentar en esta cláusula?
- 



# **Introducción al Sistema de Gestión de Seguridad de la Información (Sesión 02)**

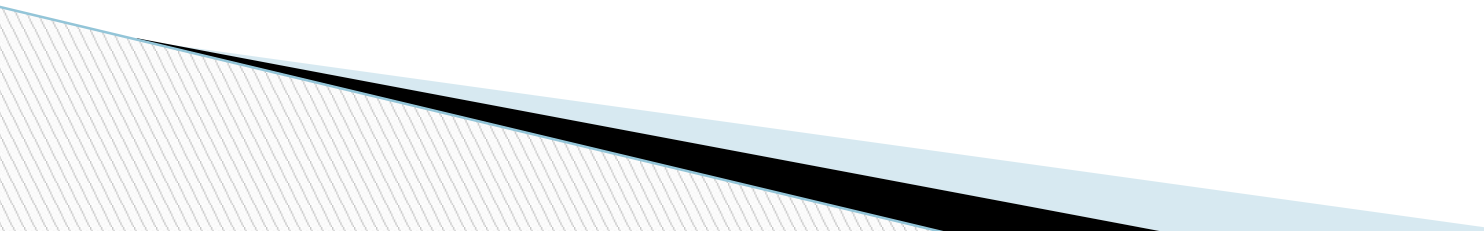
Gestión de Seguridad de la información  
Semestre 2023-II

# Logro de la sesión

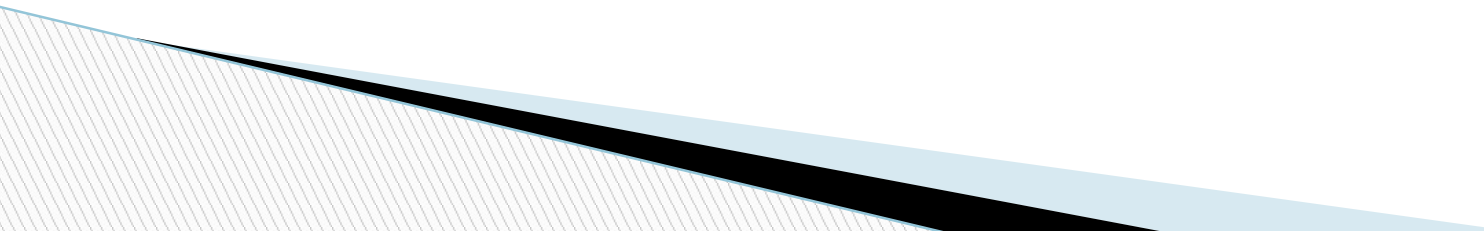
El estudiante conoce la estructura de la norma ISO 27001 y comprende la importancia de definir adecuadamente el contexto y alcance como base para una implementación exitosa y alineada a los objetivos de la Organización



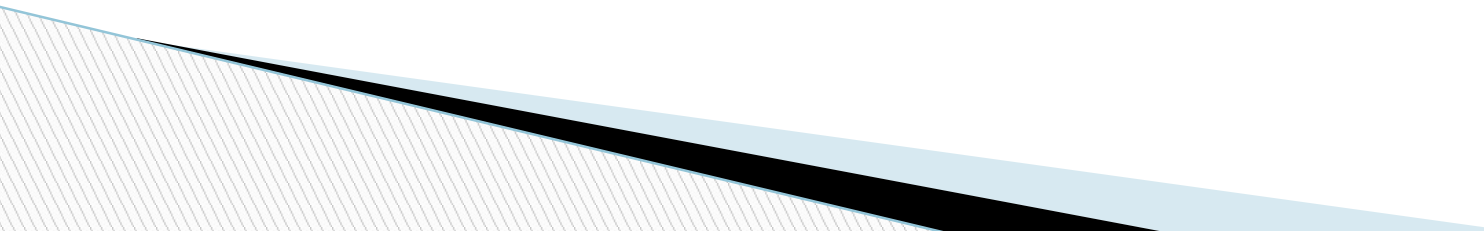
# ISO 27001:2022

- Especifica los requisitos de gestión de un SGSI (cláusula 4 a 10)
  - Los requisitos (cláusulas) son escritos usando el verbo “deberán” en imperativo
  - Anexo “A”: 4 grupos que contienen 93 controles.
  - Una organización puede ser certificada en esta norma.
- 

# ISO 27002:2022

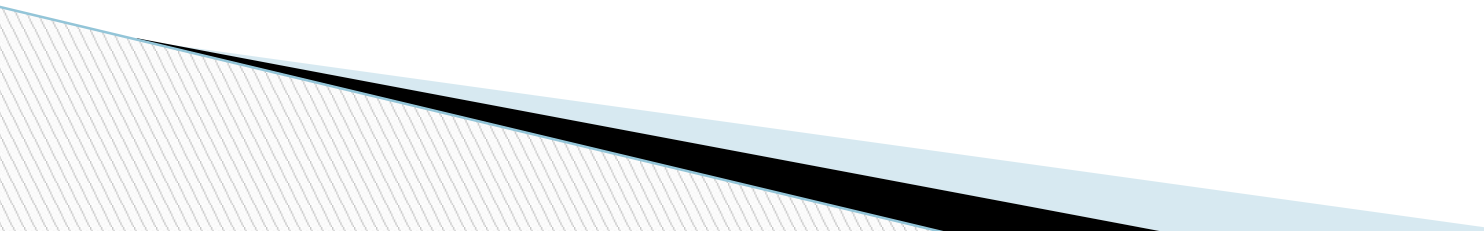
- Guía de buenas prácticas para los controles de seguridad de la información (documento de referencia)
  - Cláusulas escritas con el verbo “debería”
  - Compuesto de 4 grupos y 93 controles
  - Una organización no puede ser certificada en esta norma
- 

# Anexo SL

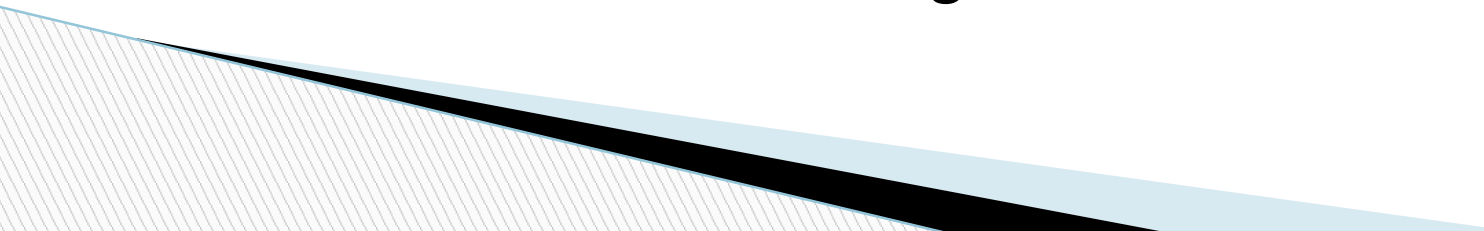
- A lo largo de los años ISO ha publicado muchas normas de sistemas de gestión en temas de calidad y medioambiente, hasta la seguridad de la información y la gestión de la continuidad del negocio. A pesar de compartir elementos comunes, todas las normas ISO de sistemas de gestión tienen diferentes estructuras. Esto, a su vez, da lugar a cierta confusión y dificultades en la fase de implantación.
- 

# Anexo SL

¿Por qué una nueva estructura de alto nivel?

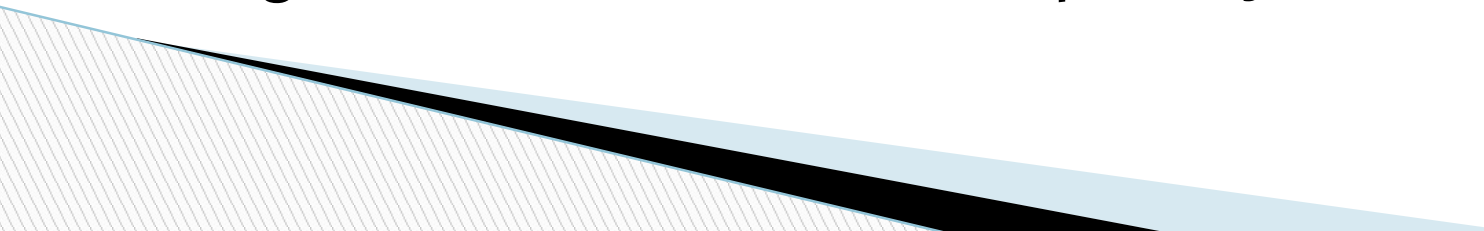
- La mayoría de las organizaciones disponen de más de una norma de sistemas de gestión implantada y certificada. Hacer esto de forma individual ocupa una gran cantidad de tiempo y recursos extras, por lo que existe una clara necesidad de encontrar una forma de integrar y combinar las normas de la mejor manera posible.
  - Cada una de las normas de sistemas de gestión presenta diferentes estructuras, requisitos y terminología, por lo que la integración es un reto.
- 

# Anexo SL

- Ejemplo: El requerimiento “Control de documentos”, en el caso de ISO 9001, se encuentra en la cláusula 4.2.3, mientras que en ISO 14001 se localiza en 4.4.5.
  - Para abordar este problema, ISO desarrolló el Anexo SL – el marco para un sistema de gestión genérico y la estructura para todas las normas de sistemas de gestión nuevas y revisadas de ahora en adelante. Para hacer frente a las necesidades específicas de la industria, los requisitos adicionales de sectores particulares se añadirán a este marco genérico.
- 

# Anexo SL

¿Cómo afecta a las organizaciones?

- Esta estructura de alto nivel se pondrá en marcha en todas las normas de sistemas de gestión nuevas y revisadas para garantizar coherencia y compatibilidad.
  - Con el Anexo SL, los implantadores de sistemas de gestión pueden esperar menos conflictos, duplicidades, confusión y malentendidos que los que se produjeron como consecuencia de las diferentes estructuras de las normas de sistemas de gestión. Los auditores de sistemas de gestión ahora utilizarán un conjunto básico de requisitos genéricos en todas las disciplinas y sectores industriales.
- 

# Anexo SL

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

## Cláusula 1: Objeto y campo de aplicación

El alcance establece los resultados esperados del sistema de gestión. Los resultados son específicos de la industria y deben ser coherentes con el contexto de la organización (cláusula 4).

## Cláusula 2: Referencias normativas

Proporciona detalles sobre las normas de referencia o publicaciones relevantes en relación a la norma concreta.

## Cláusula 3: Términos y definiciones

Detalla términos y definiciones aplicables a la norma específica, además de cualquier otro término y definición relacionado con la norma.

## Cláusula 4: Contexto de la organización

La cláusula 4 consta de cuatro sub-cláusulas::

4.1 Conocimiento de la organización y de su contexto

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

4.3 Determinación del alcance del sistema de gestión de la calidad

4.4 Sistema de gestión

Como punto de partida y referencia del sistema de gestión, la cláusula 4 determina por qué la organización está donde está. Como parte de la respuesta a esta pregunta, la organización debe identificar las cuestiones internas y externas que pueden influir en los resultados esperados, así como a todas las partes interesadas y sus necesidades. También debe documentar su alcance y establecer los límites del sistema de gestión - todo en línea con los objetivos de negocio.

# Anexo SL

## Cláusula 5: Liderazgo

La cláusula 5 consta de tres sub-cláusulas:

- 5.1 Liderazgo y compromiso
- 5.2 Política
- 5.3 Roles, responsabilidades y autoridades en la organización

La nueva estructura hace especial hincapié en el liderazgo, no sólo a la dirección que figuraba en las normas anteriores. Esto quiere decir que la alta dirección tiene ahora una mayor responsabilidad y participación en el sistema de gestión de la organización. Deben integrar los requisitos del sistema de gestión en los procesos de negocio de la organización, asegurar que el sistema de gestión logra los resultados previstos y asignar los recursos necesarios. La alta dirección es también responsable de comunicar la importancia del sistema de gestión y aumentar la toma de conciencia y la participación de los empleados.

## Cláusula 6: Planificación

La cláusula 6 consta de dos sub-cláusulas:

- 6.1 Acciones para tratar riesgos y oportunidades
- 6.2 Objetivos del sistema de gestión y planificación para lograrlos

La cláusula 6 nos proporciona la manera directa de tratar el riesgo. Una vez que la organización ha definido los riesgos y oportunidades en la cláusula 4, tiene que establecer cómo van a ser tratados a través de la planificación. Este enfoque proactivo sustituye a la acción preventiva y reduce la necesidad de acciones correctivas posteriormente. Se pone especial atención también en los objetivos del sistema de gestión. Deben ser medibles, ser objeto de seguimiento, comunicados, coherentes con la política del sistema de gestión y actualizados cuando sea necesario.

## Cláusula 7: Soporte

La cláusula 7 consta de cinco sub-cláusulas:

- 7.1 Recursos
- 7.2 Competencia
- 7.3 Toma de conciencia
- 7.4 Comunicación
- 7.5 Información documentada

Después de abordar el contexto, el compromiso y la planificación, las organizaciones tendrán que analizar el soporte necesario para cumplir con sus metas y objetivos. Esto incluye los recursos, comunicaciones internas y externas, así como la información documentada que reemplaza los términos utilizados anteriormente como documentos, documentación y registros.



# Anexo SL

## Cláusula 8: Operación

La cláusula 8 consta de una sub-cláusula:

### 8.1 Planificación y control operacional

La mayor parte de los requisitos del sistema de gestión se encuentran dentro de esta cláusula. La cláusula 8 aborda tanto los procesos internos como los contratados externamente, mientras que la gestión del proceso global incluye criterios adecuados para el control de estos procesos así como formas de gestionar el cambio planificado y el no previsto.

## Cláusula 9: Evaluación del desempeño

La cláusula 9 consta de tres sub-cláusulas:

### 9.1 Seguimiento, medición, análisis y evaluación

### 9.2 Auditoría interna

### 9.3 Revisión por la dirección

Para dar cumplimiento a éste requisito, las organizaciones deben determinar qué, cómo y cuándo ha de ser supervisado, medido, analizado y evaluado. La auditoría interna también es parte de este proceso para asegurar que el sistema de gestión se ajusta a los requisitos de la organización, así como a los de la norma, y se ha implantado y mantenido con éxito. El último paso, la revisión por la dirección, que analiza si el sistema de gestión es apropiado, adecuado y eficaz.

## Cláusula 10: Mejora

Con dos sub-cláusulas, la cláusula 10 analiza cómo se deben tratar las no conformidades y acciones correctivas:

### 10.1 No conformidad y acción correctiva

### 10.2 Mejora continua

En un mundo empresarial en constante cambio, no todo siempre se lleva a cabo según lo planificado. La cláusula 10 analiza las formas de hacer frente a las no conformidades y acciones correctivas, así como las estrategias de mejora continua.

# Cláusula 4: Contexto de la Organización

4.1 Comprender la Organización y su contexto

4.2 Comprender las Necesidades y Expectativas de las partes interesadas

4.3 Determinar el alcance del SGSI

4.4 Sistema de Gestión de Seguridad de la Información

# Cláusula 4: Contexto de la Organización

## 4.1 Comprender la Organización y su contexto

- La organización debe determinar los aspectos externos e internos relevantes y que afectan su capacidad de lograr los resultados deseados de este SGSI.
- Determinar estas cuestiones se refiere a establecer el contexto externo e interno de la organización considerado en la cláusula 5.3 de la norma ISO 31000:2009

# Cláusula 4: Contexto de la Organización

ISO 31000:2009 – Gestión del Riesgo – Principios y Directrices

Establecimiento del contexto externo:

- El contexto externo es el entorno externo en el cual organización busca conseguir sus objetivos.
- Es importante su comprensión para asegurar que los objetivos e inquietudes de las partes interesadas externas se tienen en cuenta cuando se desarrollan los criterios de riesgo.
- El contexto externo se basa en el contexto a escala de la organización, pero con detalles específicos de requisitos legales y reglamentarios, con las percepciones de las partes interesadas y otros aspectos específicos del alcance del proceso de gestión del riesgo.

# Cláusula 4: Contexto de la Organización

El contexto externo puede incluir, pero no se limita a:

- Entorno social y cultural, político, legal, reglamentario, financiero, tecnológico económico, natural y competitivo, a nivel internacional, nacional, regional o local;
- Los factores y las tendencias clave que tengan impacto en los objetivos de la organización; y
- Las relaciones con las partes interesadas externas, sus percepciones y sus valores

# Cláusula 4: Contexto de la Organización

## Establecimiento del contexto interno:

- El contexto interno es el entorno interno en que la organización busca conseguir sus objetivos.
- El proceso de gestión del riesgo debe estar alineado con la cultura, los procesos, la estructura y la estrategia de la organización.
- Establecer este contexto es importante, ya que:
  - La gestión del riesgo se desarrolla en el contexto de los objetivos de la organización
  - El logro de los objetivos afecta el compromiso, la credibilidad, confianza y valores.

# Cláusula 4: Contexto de la Organización

El contexto interno puede incluir pero no se limita a:

- El gobierno, la estructura de la organización, las funciones y las responsabilidades;
- Las políticas, los objetivos y las estrategias establecidas
- Las aptitudes, entendidas en términos de recursos y conocimientos (por ejemplo: capital, tiempo, personas, procesos, sistemas)
- Las relaciones con las partes internas interesadas
- La cultura de la organización
- Los sistemas de información, los flujos de información, y los procesos de toma de decisiones
- Normas, directrices y modelos adoptados por la organización

# Cláusula 4: Contexto de la Organización

## 4.2 Comprender las Necesidades y Expectativas de las partes interesadas

Se debe definir:

- Las partes interesadas relevantes al SGSI
- Los requisitos de estas partes interesadas (incluyendo requisitos legales, regulatorios y contractuales)



# Cláusula 4: Contexto de la Organización

## 4.3 Determinar el alcance del SGSI

- La organización debe determinar los límites y aplicabilidad del SGSI para establecer su alcance.
- Cuando se determina este alcance, la organización debe considerar los aspectos internos y externos referidos en la sección 4.1:
- Los requisitos referidos en el 4.2
- Las interfases y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones

El alcance debe estar disponible como **información documentada**

# Cláusula 4: Contexto de la Organización

## 4.4 Sistema de Gestión de Seguridad de la Información

- La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI en conformidad con los requisitos de la norma.

# Cláusula 5: Liderazgo

- 5.1 Liderazgo y Compromiso
- 5.2 Política
- 5.3 Roles, Responsabilidades y autoridades organizacionales

# Cláusula 5: Liderazgo

## 5.1 Liderazgo y Compromiso

La alta dirección debe demostrar su liderazgo y compromiso respecto al SGSI

- a. Garantizar que la Política de Seguridad de la Información y los objetivos de seguridad son compatibles con los objetivos de la organización.
- b. Asegurar que los requisitos de seguridad se integren en los procesos del negocio
- c. Asegurar la disponibilidad de recursos requeridos por el SGSI
- d. Comunicar la importancia de una gestión eficaz de la seguridad y cumplimiento de los requisitos del SGSI

# Cláusula 5: Liderazgo

## ... 5.1 Liderazgo y Compromiso

- e. Asegurar que el SGSI alcance el resultado previsto
- f. Dirección y apoyo a las personas para contribuir a la eficacia del SGSI
- g. Promoción de la mejora continua
- h. Apoyando a otras funciones de gestión relevantes para demostrar liderazgo, así como se aplica a sus áreas de responsabilidad

Ejemplo de evidencia: Comunicaciones de la alta gerencia en relación a S.I., autoridad y rango designado al responsable del SGSI, etc.

# Cláusula 5: Liderazgo

## 5.2 Política

La alta dirección debe establecer una política de S.I. que:

- a. Sea adecuada para la organización
- b. Incluya los objetivos de seguridad (ver 6.2)
- c. Compromiso de cumplir con requisitos aplicables
- d. Compromiso de mejora continua
- e. Debe estar disponible como **información documentada**
- f. Comunicada a la organización
- g. Estar disponible a las partes interesadas

Ejemplo de evidencia: Política de Seguridad de Información firmada por Gte. General, comunicada al personal y publicada

# Cláusula 5: Liderazgo

## 5.3 Roles, Responsabilidades y autoridades organizacionales

La alta dirección debe asegurarse que las responsabilidades y autoridades relevantes para la seguridad se hayan asignado y comunicado. Además dar responsabilidad y autoridad para:

- a. Garantizar que el SGSI se ajuste a requisitos de la norma
- b. Informar sobre el rendimiento del SGSI

Ejemplo de evidencia: Organigrama (comunicación de roles), documentación de funciones relevantes, existencia de un comité de S.I., actas del comité, etc.

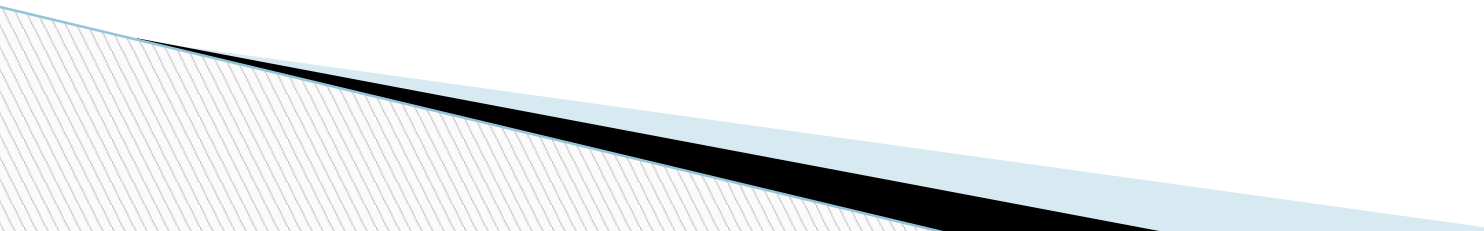
# Cláusula 6: Planificación

- 6.1 Acciones para tratar los riesgos y oportunidades
- 6.2 Objetivos de Seguridad de la Información y planificación para Conseguirlos

( A ser desarrollado a detalle en sesión 4)



# Cláusula 7: Soporte

- 7.1 Recursos
  - 7.2 Competencia
  - 7.3 Concienciación
  - 7.4 Comunicación
  - 7.5 Información Documentada
- 

# Cláusula 7: Soporte

## 7.1 Recursos

La organización debe determinar y proporcionar recursos necesarios para establecimiento, implementación, mantenimiento y mejora continua del SGSI.

Ejemplo de evidencia: Presupuesto asignado

# Cláusula 7: Soporte

## 7.2 Competencia

- a. Determinar competencias necesarias de las personas de la organización cuyo rendimiento puede afectar la seguridad de la información
- b. Educación, capacitación, experiencia
- c. Si es necesario adquirir competencias
- d. Evidencia de las competencias

Ejemplo de evidencia: Currículum del personal a cargo, Certificados de cursos o capacitaciones, Certificaciones, etc.

# Cláusula 7: Soporte

## 7.3 Concienciación

Debe incluir:

- Política
- Contribución a la eficacia del SGSI
- Consecuencias de no cumplir requisitos del SGSI

Ejemplo de evidencia: Plan de capacitación, presentaciones preparadas para las actividades de concienciación, listas de asistencia de personal, etc.

# Cláusula 7: Soporte

## 7.4 Comunicación

La organización debe determinar necesidades de comunicación internas y externas

- a. Qué comunicar
- b. Cuándo
- c. A quién
- d. Quién debe comunicar
- e. Los procesos de comunicación

Ejemplo de evidencia: Declaración de pautas de comunicación

# Cláusula 7: Soporte

## 7.5 Información Documentada

El SGSI debe incluir:

- a. Información documentada requerida por la norma
- b. Información documentada determinada por la organización

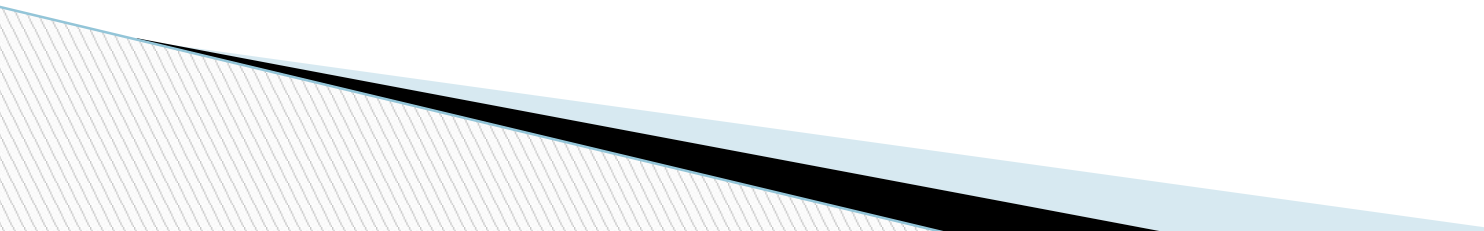
Nota: La extensión puede variar: Tamaño y actividades, complejidad de procesos, competencia de personas

# Cláusula 7: Soporte

## ...7.5 Información Documentada

### *Creación y Actualización:*

La organización debe asegurar:

- a. Identificación y descripción apropiada
  - b. Formato y medios apropiados
  - c. Revisión y Aprobación apropiadas
- 

# Cláusula 7: Soporte

## ...7.5 Información Documentada

### *Información documentada:*

Se debe controlar para asegurar que:

- a. Esté disponible
- b. Esté protegida adecuadamente

La organización debe realizar:

- ✓ Distribución
- ✓ Almacenamiento y preservación
- ✓ Control de cambios
- ✓ Retención y Disposición



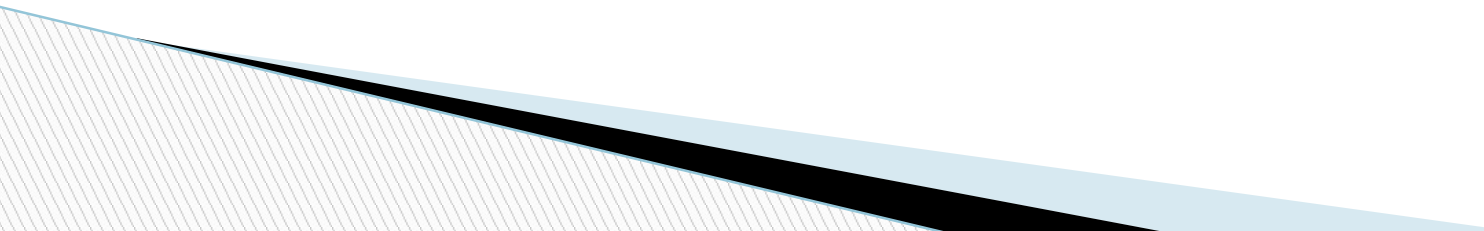
# Ejercicio

Tomando como base las organizaciones trabajadas en la sesión #1, trabaje en grupos para preparar una presentación del contexto de la organización, y el alcance propuesto para implementar un SGSI.

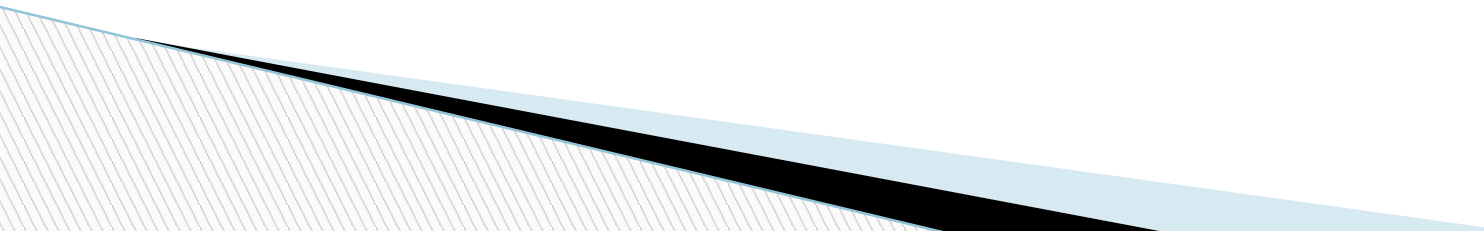
Las presentaciones se realizarán durante las sesiones N°2 y N°3.

- a) Entidad que brinda servicios de Hosting de Servidores / Administración de seguridad de la información
- b) Entidad que brinda servicio de archivo de documentos
- c) Entidad que brinda servicios de reparto de documentos
- d) Entidad que brinda servicios de salud (Ej. Clínica, hospital)
- e) Entidad que brinda servicios de asesoría legal
- f) Entidad financiera
- g) Empresa de telecomunicaciones

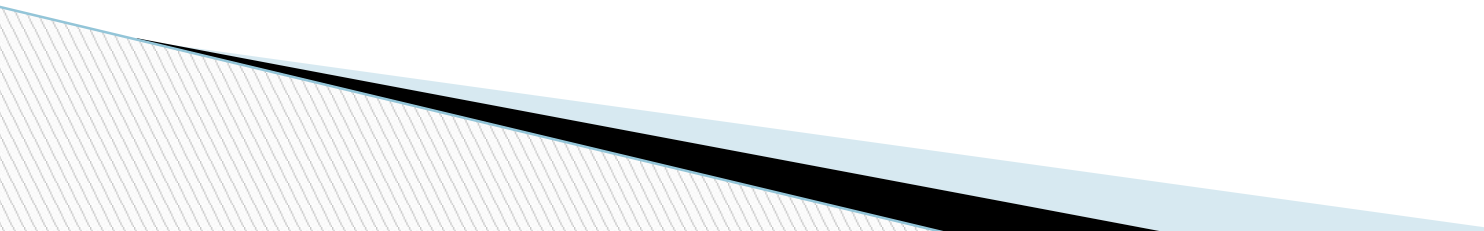
# Cláusula 8: Operación

- 8.1 Planificación y Control Operacional
  - 8.2 Evaluación de Riesgos de Seguridad de la información
  - 8.3 Tratamiento de Riesgos de Seguridad de la Información
- 

# Cláusula 9: Evaluación del Desempeño

- 9.1 Monitoreo Medición, Análisis y Evaluación
  - 9.2 Auditoría Interna
  - 9.3 Revisión por la Gerencia
- 

# Cláusula 10: Mejoras

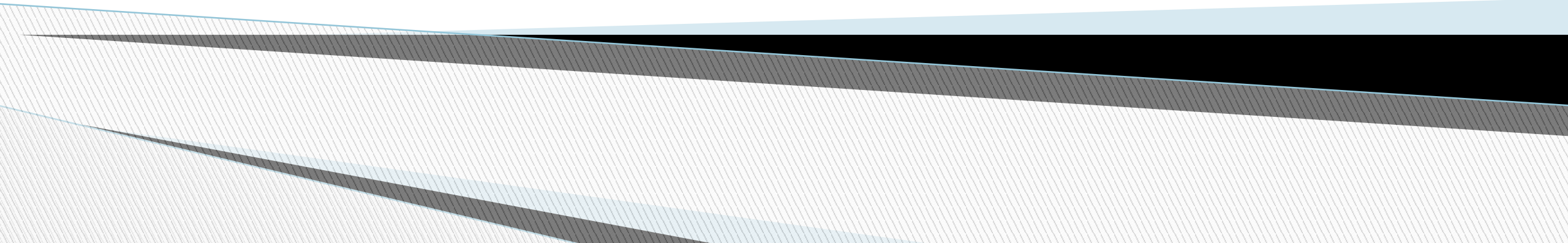
- 10.1 No conformidades y Acción Correctiva
  - 10.2 Mejora Continua
- 

# Secciones de la Norma ISO 27001:2022 (Anexo A)

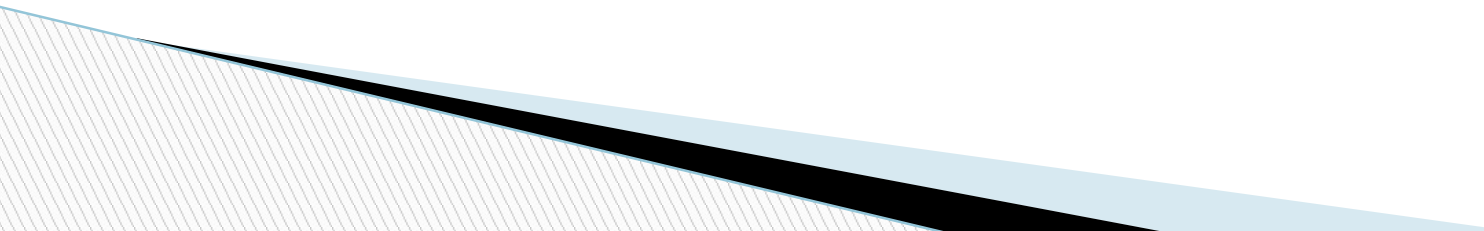
## Controles



# **Repaso: Estructura ISO 27001, Contexto de la Organización y Alcance del SGSI**



# Repasemos

1. ¿Qué es el anexo SL?
  2. ¿Por qué es importante definir el contexto de la organización?
  3. ¿Qué es el alcance de un SGSI? ¿Qué se debería considerar en su definición?
- 



# **Introducción al Sistema de Gestión de Seguridad de la Información (Sesión 01)**

Gestión de Seguridad de la información  
Semestre 2023-II



# Logro de la sesión

El estudiante comprende qué es un Sistema de Gestión de Seguridad de la Información (SGSI), entiende los beneficios de implementar un SGSI para una organización y conoce la familia de normas ISO 27000.

# ¿Qué es un SGSI?



# ¿Qué es un SGSI?

- Un SGSI es un enfoque sistemático para la gestión de la información sensible de la compañía, de tal forma que ésta permanezca segura. Esto incluye personas, procesos y sistemas de TI aplicando un proceso de administración de riesgos.
- Puede ayudar a las pequeñas, medianas y grandes empresas en cualquier sector mantener los activos de información segura.

Fuente: [www.iso.org](http://www.iso.org)



# ¿Qué es un SGSI?

- Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
- Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

Fuente: wikipedia

SGSI: <https://www.youtube.com/watch?v=zV2sfyvfaqik>

# Motivos para implantar un SGSI


¿Por qué implantar un SGSI?:


- ✓ Requisito legal: En Perú, obligatorio para entidades del estado.
- ✓ Requisito corporativo: Ej. Puede ser obligatorio implementarlo por estándar de la oficina principal.
- ✓ Práctica adquirida de la industria: Ej. Los principales competidores están acreditados, no estarlo se vuelve en una desventaja
- ✓ Obtener ventaja estratégica: Ej. Buscar mejorar imagen ante accionistas
- ✓ Para asegurarse de implementar mejores prácticas en Seguridad
- ✓ Etc...

Beneficios SGSI: <https://www.youtube.com/watch?v=6EspTMCxTgM>  
<https://www.youtube.com/watch?v=FgenDtaUhsQ>

# ¿Por qué implantar un SGSI?



Enviar a un amigo 

Descargar Contenido en 

Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL

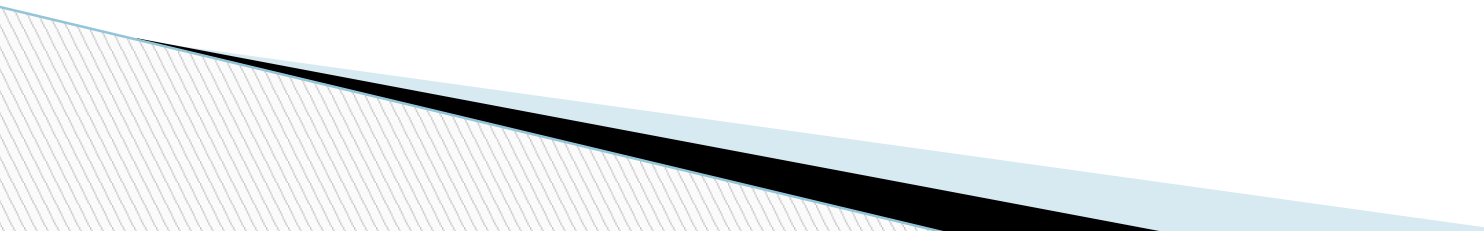
Nº 004-2016-PCM

Lima, 8 de enero de 2016



Norma

# Beneficios de implementar un SGSI

- Reducción de Riesgos
  - Reducción de costos
  - Optimizar recursos e inversiones
  - La seguridad pasa a ser un sistema convirtiéndose en una actividad de gestión, ciclo de vida metódico y controlado.
  - Protección del Negocio
  - Mejora de la competitividad (eficacia / eficiencia)
  - Cumplimiento Legal y Regulatorio
  - Mejora Imagen Corporativa
- 

# Beneficios de implementar un SGSI

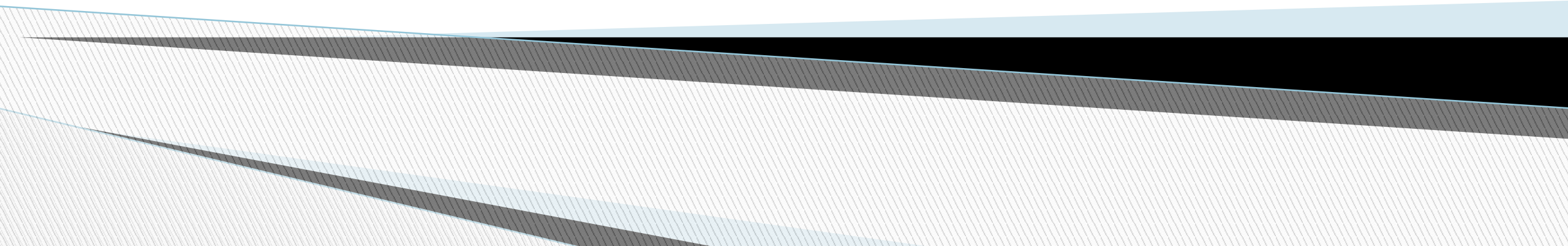
- Demuestra que la alta gerencia está comprometida con la seguridad de la organización, incluyendo la información de sus clientes.
- Enfocada en reducir los riesgos de la información que es valiosa para la organización
- Operaciones optimizadas en la organización dadas las responsabilidades y procesos claramente definidos
- Construye una cultura de seguridad

[https://www.youtube.com/watch?v=Z\\_bzHQCjkH8](https://www.youtube.com/watch?v=Z_bzHQCjkH8)





# **Norma ISO 27001:2022**



# Un poco de historia...

- 1995: La British Standards Institution (BSI) publica la norma BS 7799–1:1995, Mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Eran recomendaciones que no permitían la certificación ni establecía la forma de conseguirla.
- 1998: La BSI publica la norma BS 7799–2:1999: Revisión de la anterior norma. Establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.
- 2000: La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799–1 que dio lugar a la llamada ISO 17799:2000, sin experimentar grandes cambios.

## (...cont) Un poco de historia

2002: Se publicó una nueva versión “BS 7799–2:2002” que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

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

2007: Se publica la nueva versión ISO 27001:2007

2013: Se publica la versión ISO 27001:2013

2022: Se publica la versión ISO 27001:2022

# ISO / IEC 27001 – Gestión de la Seguridad de la Información

- La familia de estándares ISO 27000 ayuda a las organizaciones a mantener seguros los activos de información
- Ayuda a las organizaciones a gestionar la seguridad de los activos, tales como: información financiera, propiedad intelectual, información de los empleados o información confiada a la organización por terceros.
- ISO/IEC 27001 provee los requerimientos para un sistema de gestión de seguridad de la información (SGSI).

# Familia de Normas ISO / IEC 27000

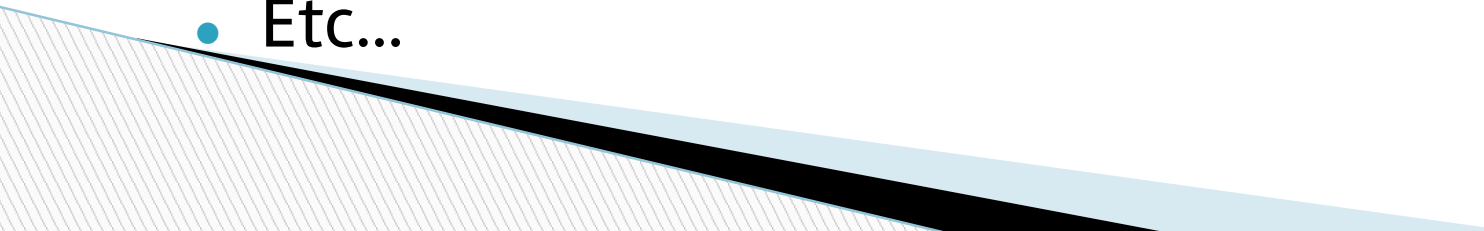


# Familia de Normas ISO / IEC 27000

ISO / IEC	Descripción
27000	Vocabulario Estándar empleado en la familia 27000
27001	Requisitos a cumplir para implantar un SGSI certificable
27002	Código de Buenas Prácticas para la Gestión de la Seguridad
27003	Guía de Implementación
27004	Métricas
27005	Gestión de los Riesgos de Seguridad de la Información
27006	Requisitos a cumplir por organizaciones encargadas de emitir certificaciones
27007	Guía para Auditar los SGSI
27011	Guía de gestión de la Seguridad de la Información específica para Telecomunicaciones
27015	Guía de gestión de la Seguridad de la Información en servicios Financieros
27017	Código de práctica para controles de Seguridad de la Información para cloud services
27031	Guía de Continuidad de Negocio en lo relativo a TI y Comunicaciones
27032	Guía relativa a la Ciberseguridad

# Mantener la certificación también genera:

Recursos requeridos para:

- Auditoría externa anual (costo de auditor, viáticos, personal de la compañía dedicado durante la auditoría, etc.)
  - Auditoría de re-certificación trianual
  - Actualización permanente de la documentación (procedimientos, normas, evidencia de actividades, registros, etc.)
  - Operación de procedimientos y actividades definidas por el SGSI
  - Recursos para la auditoría Interna requerida por el SGSI
  - Actualización de herramientas empleadas y costo asociado
  - Entrenamiento del personal incluido en el alcance (tiempo y costos)
  - Etc...
- 

# Ejercicio

Discuta en grupos por qué sería beneficioso para las siguientes organizaciones implementar y certificar un SGSI ISO 27001 (elija una del grupo celeste y una del grupo verde):

- ✓ Entidad que brinda servicios de Hosting de Servidores / Administración de seguridad de la información
- ✓ Entidad que brinda servicio de archivo de documentos
- ✓ Entidad que brinda servicios de reparto de documentos
- ✓ Entidad que brinda servicios de salud (Ej. Clínica, hospital)
- ✓ Entidad que brinda servicios de asesoría legal
- ✓ Entidad financiera
- ✓ Empresa de telecomunicaciones



# Certificación en ISO/IEC 27001

- Al igual que los otros estándares de sistemas de gestión ISO, la certificación en ISO/IEC 27001 es posible pero no obligatoria. Algunas organizaciones elegirán implementar el estándar para beneficiarse con las mejores prácticas que él contiene, mientras que otras, decidirán que además quieren certificarse para asegurar a los clientes (internos y externos) que sus recomendaciones han sido seguidas.
- La organización ISO no brinda la certificación. La certificación es brindada por organismos externos de certificación.

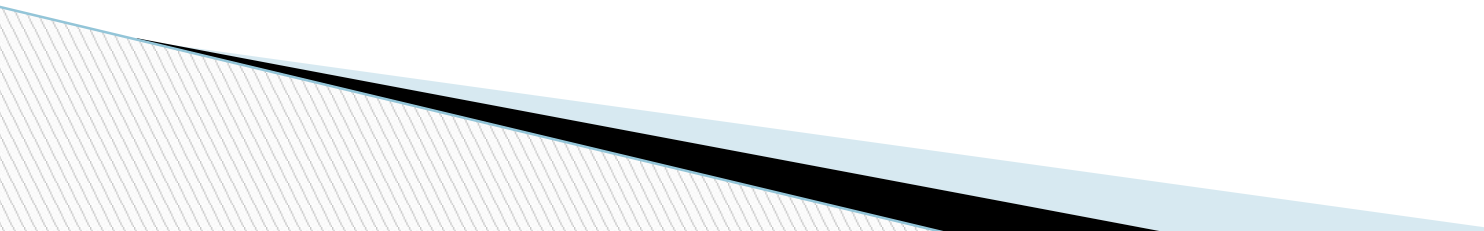
# ¿Quiénes son los organismos externos de certificación?

- El Comité de Evaluación de la Conformidad de ISO (CASCO por sus siglas en inglés) ha producido una serie de estándares relacionados al proceso de certificación, los cuales son empleados por los organismos externos de certificación.
- Cuando se elige a un organismo de certificación se debe:
  - ✓ Analizar y comparar varios organismos de certificación
  - ✓ Verificar si el organismo emplea los estándares CASCO relevantes
  - ✓ Verificar si está acreditado. La acreditación no es obligatoria y no estar acreditado no significa necesariamente que el organismo no es bueno; sin embargo la acreditación provee una confirmación independiente de su competencia. Para encontrar un organismo acreditado se puede consultar en el International Accreditation Forum (IAF)

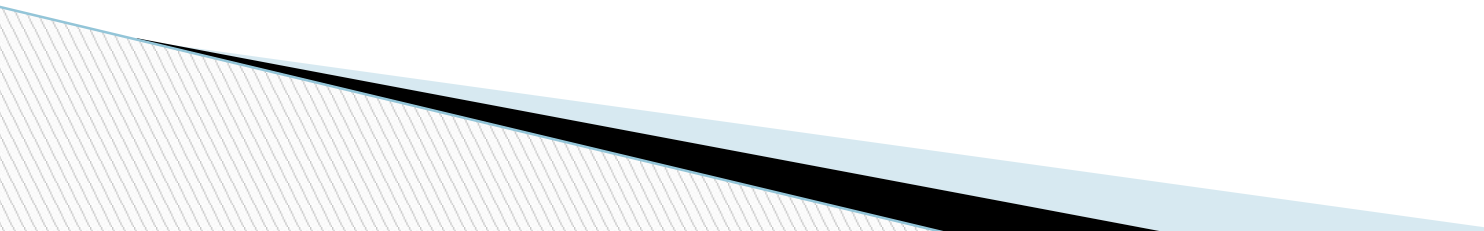
# Secciones de la Norma ISO 27001:2013



# Cláusula 4: Contexto de la Organización

- 4.1 Comprender la Organización y su contexto
  - 4.2 Comprender las Necesidades y Expectativas de las partes interesadas
  - 4.3 Determinar el Alcance del SGSI
  - 4.4 Sistema de Gestión de Seguridad de la Información
- 

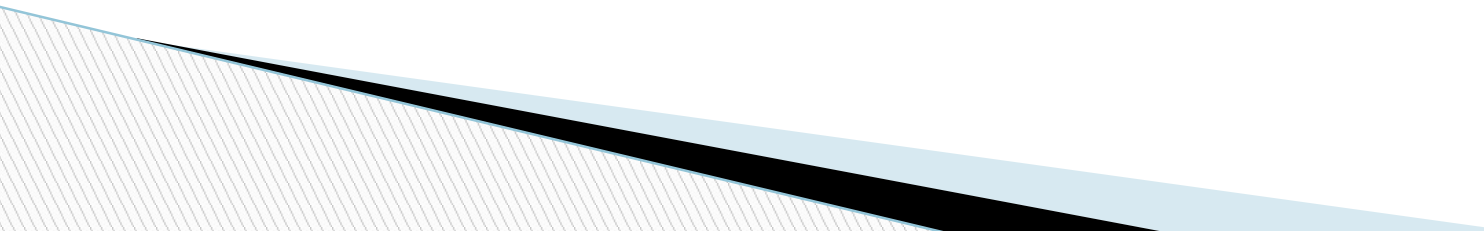
# Cláusula 5: Liderazgo

- 5.1 Liderazgo y Compromiso
  - 5.2 Política
  - 5.3 Roles, Responsabilidades y autoridades organizacionales
- 

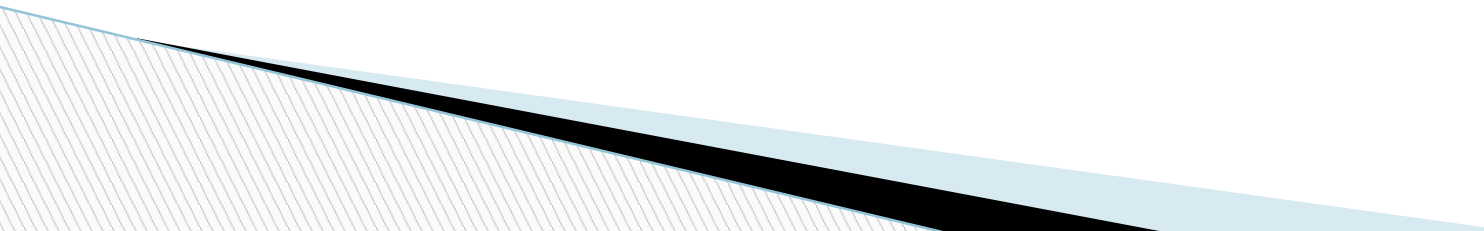
# Cláusula 6: Planificación

- 6.1 Acciones para tratar los riesgos y oportunidades
- 6.2 Objetivos de Seguridad de la Información y planificación para Conseguirlos

# Cláusula 7: Soporte

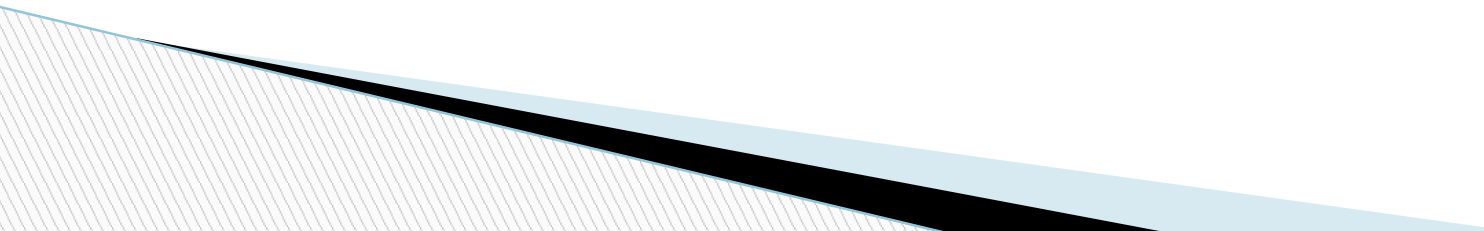
- 7.1 Recursos
  - 7.2 Competencia
  - 7.3 Concienciación
  - 7.4 Comunicación
  - 7.5 Información Documentada
- 

# Cláusula 8: Operación

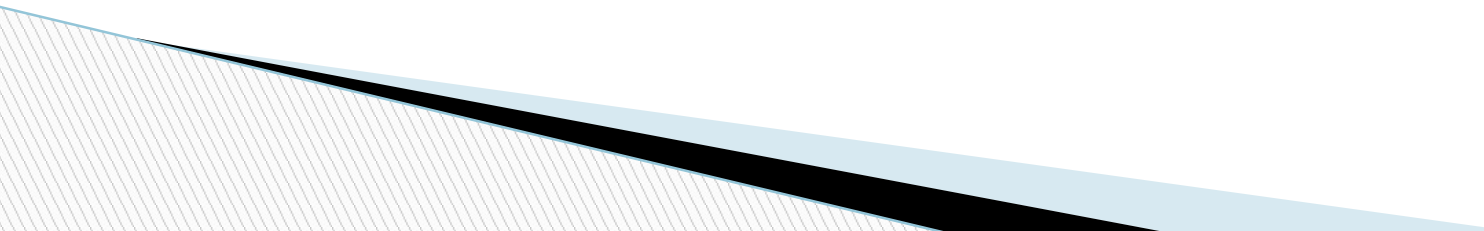
- 8.1 Planificación y Control Operacional
  - 8.2 Evaluación de Riesgos de Seguridad de la información
  - 8.3 Tratamiento de Riesgos de Seguridad de la Información
- 



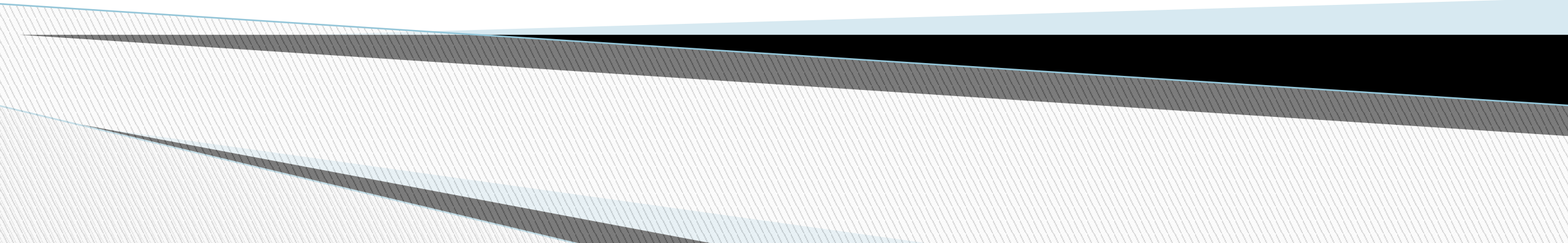
# Cláusula 9: Evaluación del Desempeño

- 9.1 Monitoreo Medición, Análisis y Evaluación
  - 9.2 Auditoría Interna
  - 9.3 Revisión por la Gerencia
- 

# Cláusula 10: Mejoras

- 10.1 No conformidades y Acción Correctiva
  - 10.2 Mejora Continua
- 

# Repaso – SGSI



# Repasemos

¿Qué es un SGSI?

¿Cuáles son los beneficios de implementar un SGSI?

¿Qué es la familia de normas ISO 27000?

¿Qué se requiere para mantener la certificación?

