



**CAPACITACIÓN USACH**  
UNIVERSIDAD DE SANTIAGO DE CHILE

# FUNDAMENTOS DE ISO 27.002:2022

---

## Sesión N°3 – Conociendo la ISO 27.002:2022

# Agenda

- Caracterización de controles
- Definiciones y clasificaciones de controles
- Definiciones de la ISO 27.002
- Lo nuevo en ISO 27.002:2022

## Profesor del Curso - Carlos Lobos de Medina



- Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postulado en Seguridad Computacional y Gestión de Procesos de Negocios de la Universidad de Chile.
- Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.
- Director de los Programas de Ciberseguridad de Capacitación USACH.

 [carlos.lobos@usach.cl](mailto:carlos.lobos@usach.cl)

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



# Caracterización de controles



# Caracterización de controles

¿Que controles deberíamos tener implementados en las personas?



- Antes de la Contratación
- Durante la Contratación
- Termino de la Contratación

# Caracterización de controles - Equipamiento

¿Que controles deberíamos tener implementados en equipamiento?

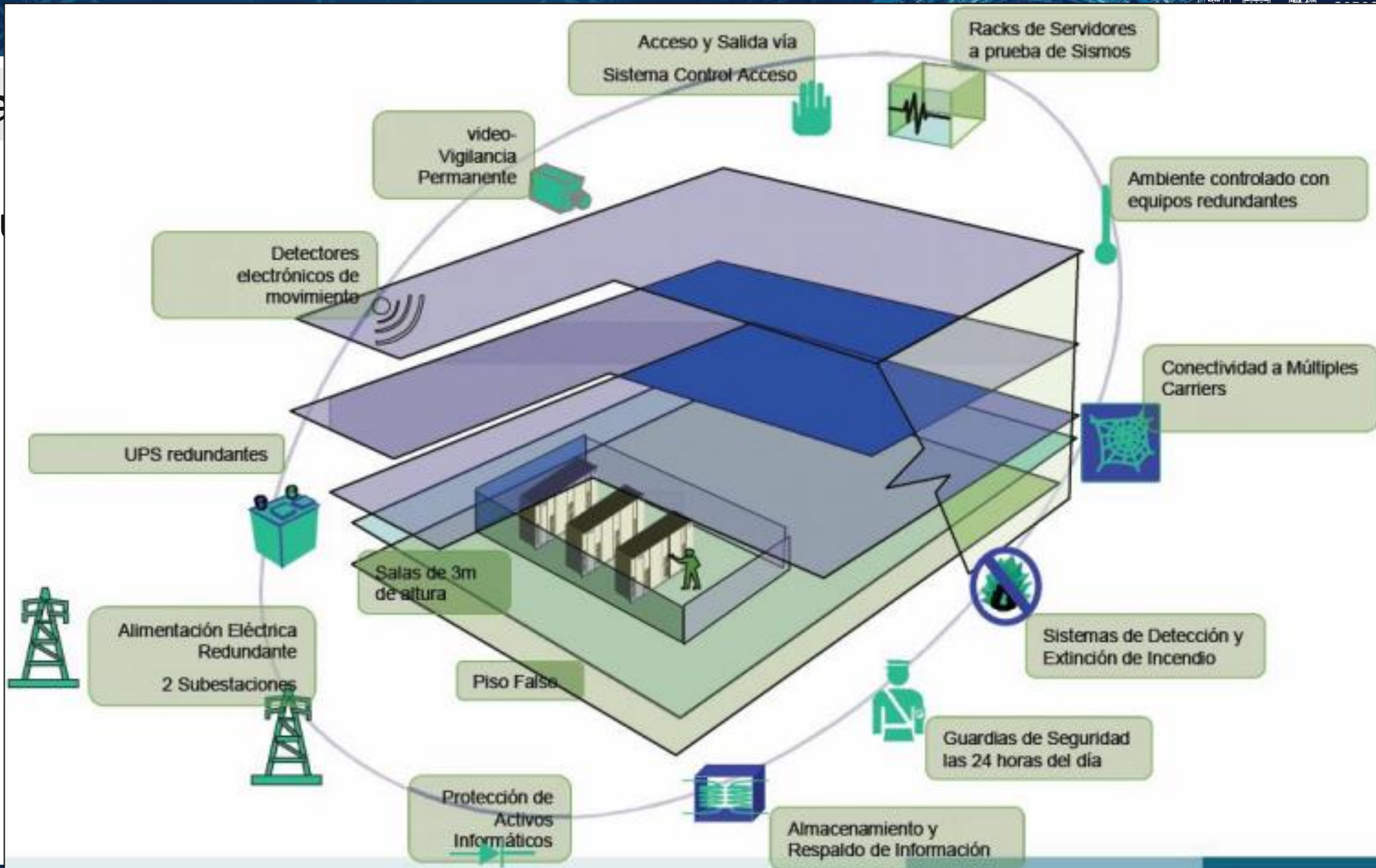


- Controles de Personas
- Controles Lógicos
- Controles Físicos
- Controles Organizacionales



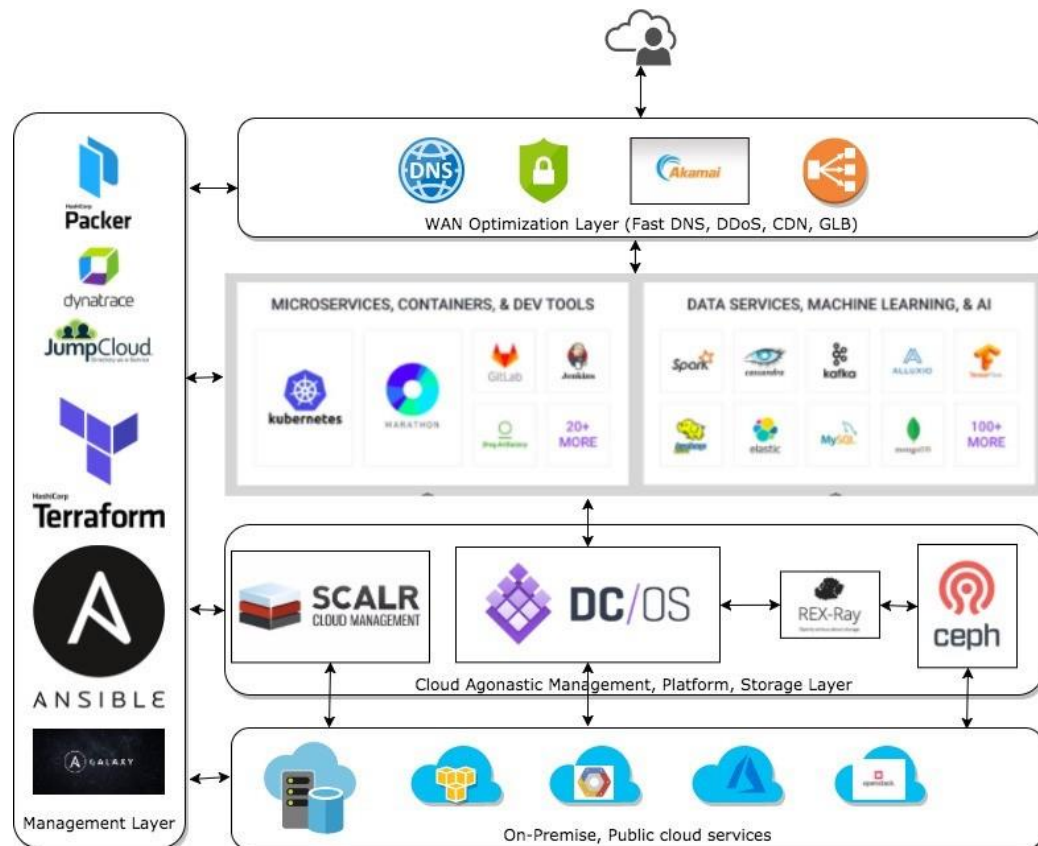
Carac

¿Q



# Caracterización de controles – Desarrollo

¿Que controles deberíamos tener implementados en el Desarrollo?













- Para la Confidencialidad
- Para la Integridad
- Para la Disponibilidad



# Caracterización de controles – Amenazas/Vulnerabilidades

¿Que controles deberíamos tener implementados en A/V?

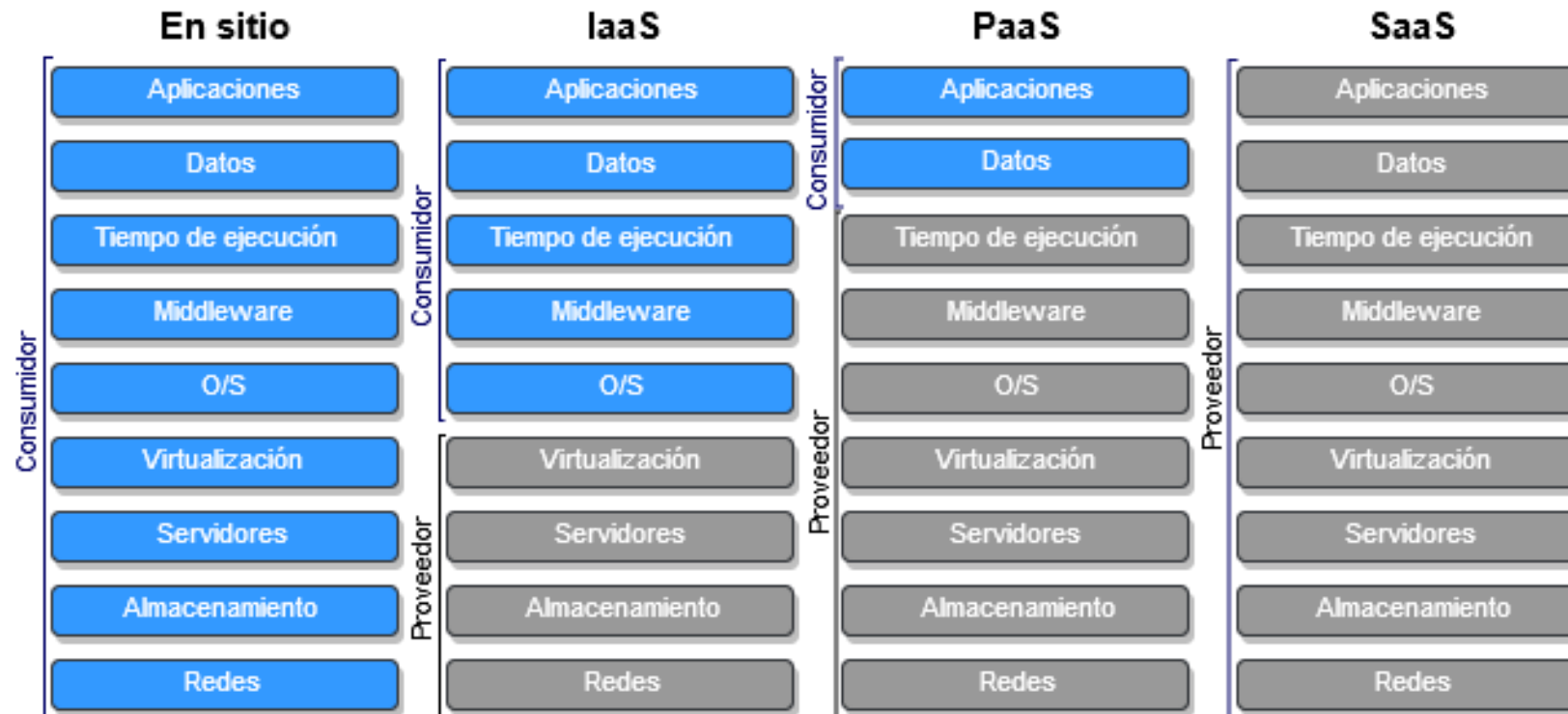
Types of Cybersecurity Threats		Malware	Phishing
			
Spear Phishing	Man in the Middle Attack	Denial of Service Attack	SQL Injection
			
Zero-day Exploit	Advanced Persistent Threats	Ransomware	DNS Attack
			

- De Gobierno
- De Detección
- De Protección
- De Respuesta
- De Recuperación

# Caracterización de controles – Servicios

¿Que controles deberíamos tener implementados en Servicios?

## Separación de responsabilidades



# Consideraciones



## Aspectos Positivos:

- Buena visión de controles necesarios.
- Muchos controles implementados.
- Con adecuado nivel técnico.



## Aspectos Negativos:

- No hay recursos.
- No hay capacidades ni competencias.
- Poco conocimiento de categorías.
- Ni hay formalización.
- No hay alineamiento con buenas prácticas.



# Definiciones y clasificaciones de controles



# Contexto de Controles

Los controles se diseñan para brindar una garantía razonable de que se logren los objetivos del negocio

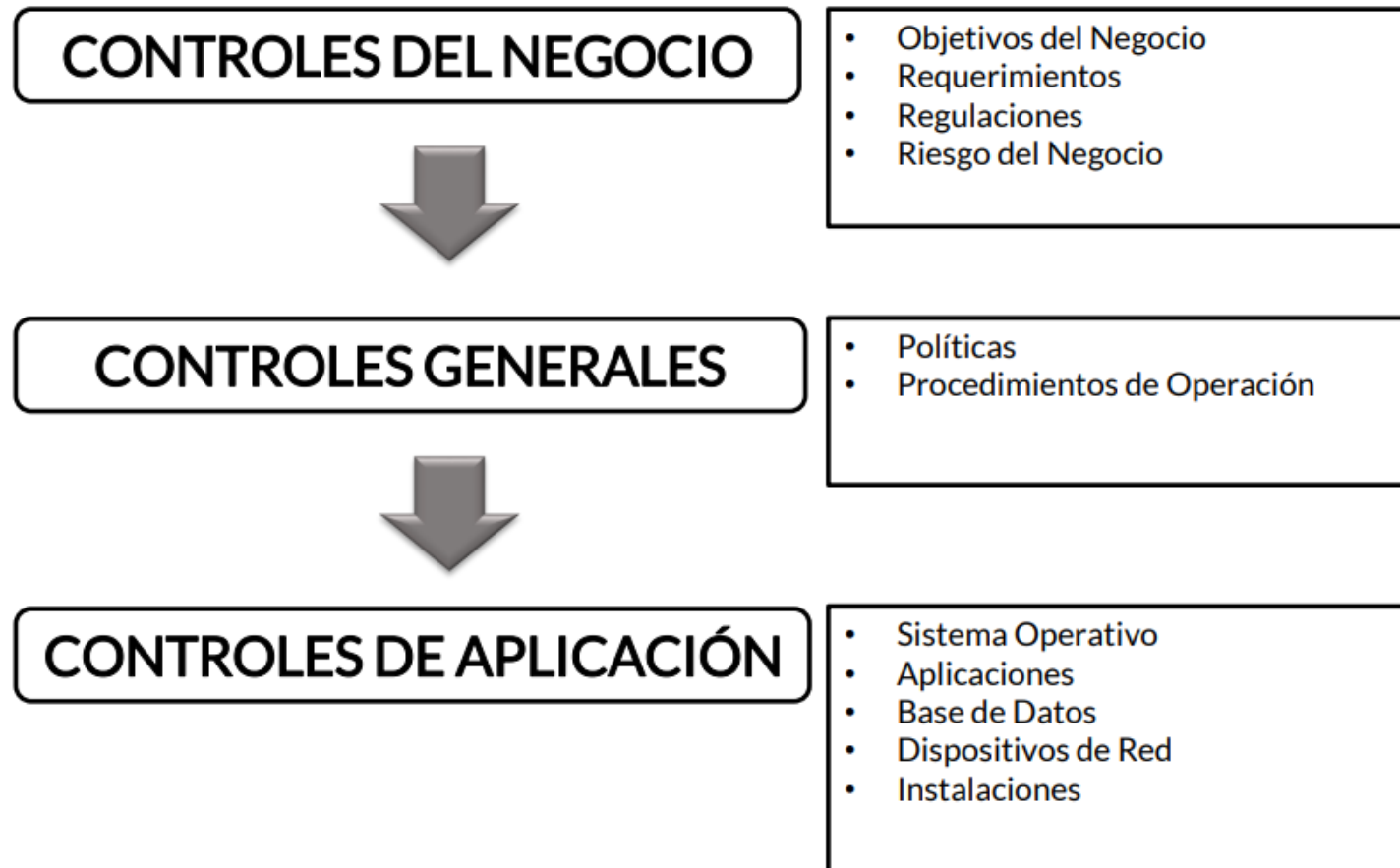


Los controles se diseñan para brindar una garantía razonable de que eventos no deseados puedan evitarse, detectarse y/o corregirse



Los controles posibilitan la disminución de los riesgos del negocio

# Alcance de Controles



Fuente: Manual de Preparación de Examen CRISK 2021



# Categorías de Controles

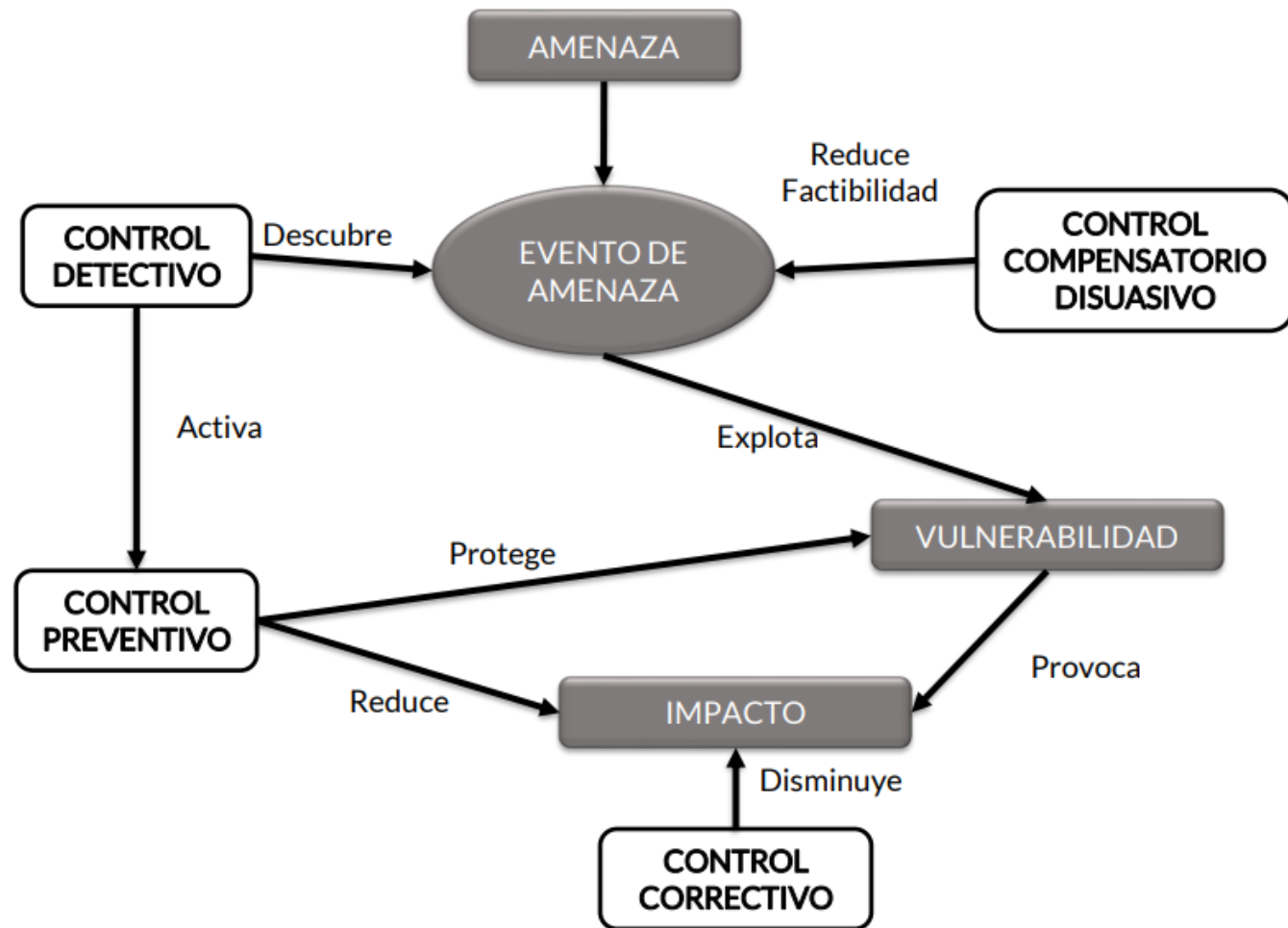
CONTROLES COMPENSATORIOS

CONTROLES CORRECTIVOS

CONTROLES DETECTIVOS

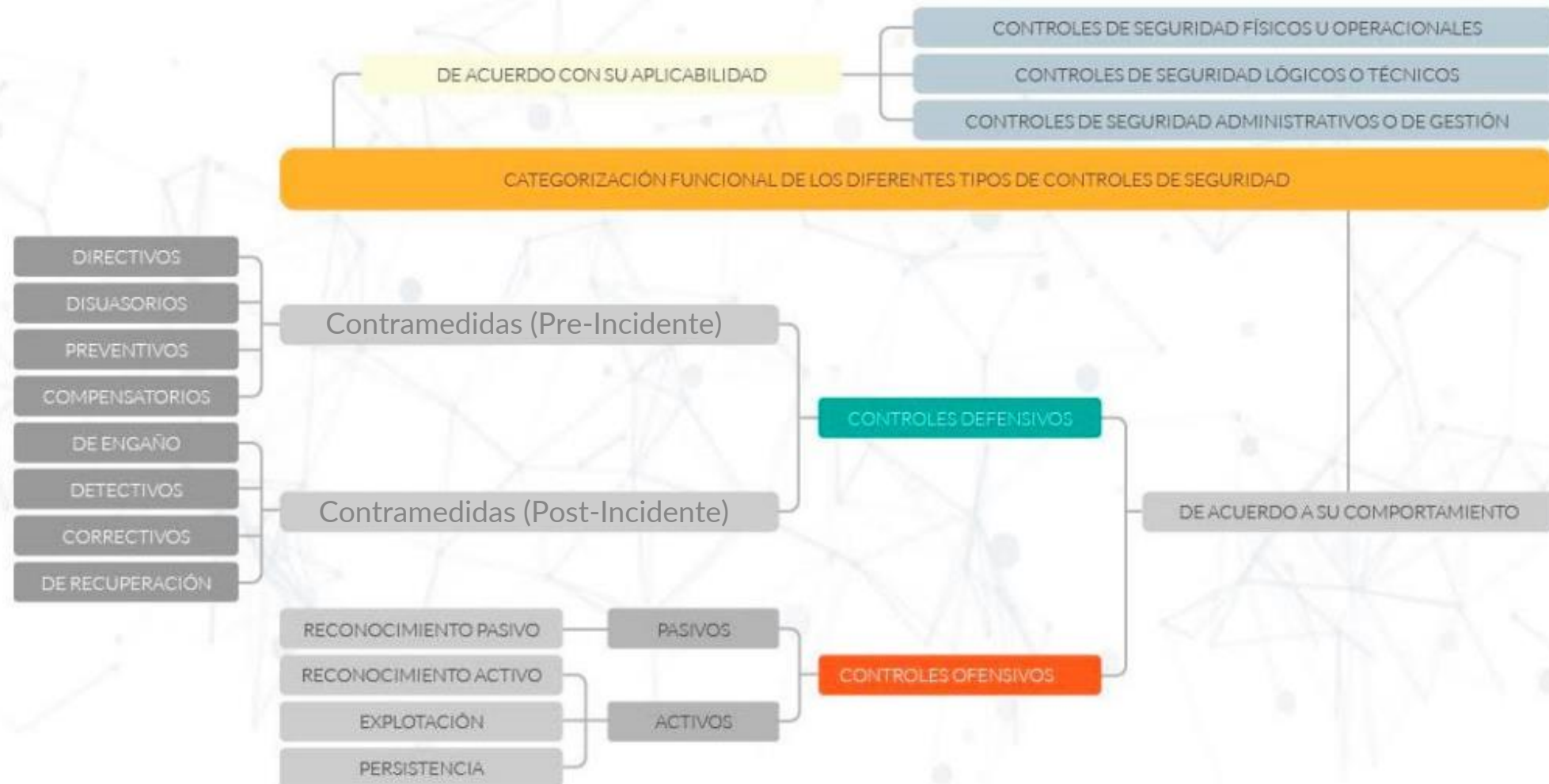
CONTROLES DISUASIVOS

CONTROLES PREVENTIVOS



Fuente: Manual de Preparación de Examen CRISK 2021

# Categorías de Controles - NIST



# Consideraciones

- Un entorno de control considerará:
  - Controles funcionales (Organizacionales, Personas, Físicos, Tecnológicos)
  - Controles de acuerdo a su naturaleza (Defensiva, Preventiva)
  - Controles de acuerdo a su tipo (Preventivo, Correctivo, Detectivo)
  - Controles de acuerdo al CID (Confidencialidad, Integridad, Disponibilidad)
  - Controles de acuerdo a función (Identificar, Proteger, Detectar, Responder, Recuperar)
- La importancia de clasificar los controles radica en el establecimiento de responsabilidades y determinar las reales capacidades del entorno de control en términos de las diversas clasificaciones.



# Definiciones desde la ISO 27.002



# ISO 27002 – Controles de Seguridad de la Información

- Es la norma más relevante en términos de la definición de controles de seguridad de la información, ciberseguridad y privacidad.
- Basado en las mejores prácticas internacionales, es el mayor marco de referencia para la adopción de controles y extensiones en distintos ámbitos de aplicación.
- Provee los lineamientos para la implementación de objetivos de control y controles.
- Es clave para la adopción de ISO 27001.

## Consideraciones desde ISO 27002 (1 de 4)

- “Los recursos empleados en la implementación de controles se deberían equilibrar contra el probable daño al negocio que puede surgir de los problemas de seguridad en la ausencia de estos controles.” (ISO 27002:2013)



No deben ser más costosos que lo que se busca proteger.....Eficiencia.



Deben proteger en la medida que la organización los requiera.....Eficacia.



## Consideraciones desde ISO 27002 (2 de 4)

- “Los controles se pueden seleccionar a partir de esta norma o de otros conjuntos de controles, o bien se pueden diseñar nuevos controles para cumplir con las necesidades específicas según sea necesario.” (ISO 27002)



Se seleccionan los controles relevantes para la organización..... No son todos obligatorios.



Pueden establecer controles adicionales a los de la norma..... Hay controles más allá de la norma.

## Consideraciones desde ISO 27002 (3 de 4)

- “La selección de los controles depende de las decisiones organizacionales en base a la gestión de riesgos y estará sujeta a toda la legislación y normativa nacional e internacional pertinente.” (ISO 27002:2013)



**El enfoque de riesgos es clave en la selección de controles ..... Ayuda a priorizar**



**Debería implementar controles que mitiguen riesgos de mayor impacto y probabilidades de ocurrencia.**

## Consideraciones desde ISO 27002 (4 de 4)

- “Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifican un riesgo.” (ISO 27002:2013)



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

Un entorno de control considerará:

- Controles funcionales (Organizacionales, Personas, Físicos, Tecnológicos)
- Controles de acuerdo a su naturaleza (Defensiva, Preventiva)
- Controles de acuerdo a su tipo (Preventivo, Correctivo, Detectivo)
- Controles de acuerdo al CID (Confidencialidad, Integridad, Disponibilidad)
- Controles de acuerdo a función (Identificar, Proteger, Detectar, Responder, Recuperar)

## Por último

- La ISO 27.002 es el estándar de referencia para la implementación de controles de ciberseguridad, seguridad de la información y privacidad y cuenta con numerosas extensiones:
  - 27.017 de seguridad en la nube
  - 27.019 para el sector energía
  - 27.701 en materia de privacidad y protección de datos
  - 27.799 para el sector salud
  - ....
- La capacidad de adaptación a contextos específicos la hace en una norma capaz de integrarse a diversos dominios de aplicación de una excelente forma.



# Lo nuevo en ISO 27.002:2022



**CAPACITACIÓN USACH**  
UNIVERSIDAD DE SANTIAGO DE CHILE

FUNDAMENTOS DE NOMBRE DE CURSO



DIPLOMADO  
CIBERSEGURIDAD

# Principales Cambios

- La nueva versión de la ISO 27.002:2022 trae consigo importantes cambios, siendo los más representativos:
  - El cambio de nombre
  - La incorporación de nuevos términos y definiciones
  - La nueva estructura de temas de seguridad de la información
  - La nueva estructura de atributos de los controles
  - Cambios en controles desde la versión ISO 27.002:2013
- Un cambio importante adicional es la disminución de los controles, pasando de 114 en la versión 2013 a 93 en la versión 2022.

## Sobre el Cambio de Nombre

- Mucho más amplio en el contexto de desarrollo, puesto que esta en un comité más especializado, incluyendo temas de ciberseguridad y protección de la privacidad como ejes claves.

### **ISO/IEC 27002:2013**

Information technology — Security techniques — Code of practice for information security controls



### **ISO/IEC DIS 27002**

Information security, cybersecurity and privacy protection — Information security controls

# Nuevos Términos y Definiciones

- En total define 37 términos, entre los cuales se incluyen algunos generales y ya definidos en ISO 27.000.
- En total incorpora 16 nuevos términos, buscando establecer un alcance más amplio en elementos propios de la ciberseguridad, la gestión de evidencia electrónica, la gestión de PII y privacidad, la gestión de incidentes y la gestión de la continuidad del negocio.

<b>Cadena de custodia (IS 27.050)</b>	<b>Información confidencial</b>	<b>Disrupción (ISO 22.301)</b>	<b>Endpoint</b>	<b>Brecha de seguridad de la información</b>	<b>Personal</b>	<b>información de identificación personal (PII) (ISO 29.100)</b>	<b>PII principal (ISO 29.100)</b>
<b>Procesador de PII (ISO 29.100)</b>	<b>Evaluación del impacto de la privacidad (ISO 29.134)</b>	<b>Punto objetivo de recuperación (RPO) (ISO 27.031)</b>	<b>Tiempo objetivo recuperación (RTO) (ISO 27.031)</b>	<b>Regla</b>	<b>Información sensitiva</b>	<b>Política específica</b>	<b>Usuario</b>



# Cambios en la estructura

- Un cambio radical con respecto a la versión anterior es la reestructuración de los 14 dominios de controles definidos en ISO 27.002:2013 en torno a 4 grandes temas:
  - Controles Organizacionales (37 controles)
  - Controles de Personas (8 controles)
  - Controles Físicos (14 controles)
  - Controles Tecnológicos (34 controles)
- Esta clasificación de funciones es mucho más simple que la provista por la versión 2013 de la norma, la cual se encuentra mucho más orientada al contexto de aplicación del control (organizacional, personas, físicos y tecnológicos).

# Estructura de Atributos

- Uno de los aspectos relevantes que proporciona la norma para cada control son cinco atributos, los cuales establecen sub clasificaciones del atributo que permiten caracterizar al control, a modo de ejemplo se presentan los primeros tres controles del tema de controles organizacionales definidos en la nueva versión de la norma.

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
<a href="#">5.1</a>	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
<a href="#">5.2</a>	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience
<a href="#">5.3</a>	Segregation of duties	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance	#Governance_and_Ecosystem

# Nuevos Controles – Versión ISO 27.002:2022

- En total se definen 11 nuevos controles, los cuales corresponden a:
  - 5.7 Inteligencia de Amenazas
  - 5.23 Seguridad de la información para el uso de servicios en la nube
  - 5.30 Preparación de las TIC para la continuidad del negocio
  - 7.4 Monitoreo de la seguridad física
  - 8.9 Gestión de la configuración
  - 8.10 Eliminación de la información
  - 8.11 Enmascaramiento de datos
  - 8.12 Prevención de la fuga de datos
  - 8.16 Monitoreo de actividades
  - 8.22 Filtrado Web
  - 8.28 Codificación Segura

## Reordenamiento y eliminación de controles

- La fusión y definición de controles es uno de los aspectos más llamativos, la incorporación de 11 nuevos controles y el reordenamiento de más de 54 controles para definir 23 controles nuevos.
- Esto nos permite contar con una norma con definiciones mucho más actualizadas, más alineada a los contextos de ciberseguridad, protección de la privacidad y gestión de incidencias, y con una mayor simplicidad en controles de gestión de activos, control de acceso e identidades, seguridad física, seguridad en las operaciones y seguridad en el software, lo cual permite a la norma ser mucho más comprensible y aplicable.
- Solo un control fue eliminado desde la versión 2013, el cual corresponde al 11.2.5 Retirada de materiales propiedad de la empresa.



## Mayor información

- Artículo detallado sobre los cambios de ISO 27.002
  - <https://www.linkedin.com/pulse/iso-270022021-conoce-los-principales-cambiosde-la-lobos-de-medina/?trackingId=aVHjpNxBs56SBcUoAjoZaw%3D%3D>
  - <https://diplomadociberseguridad.com/2020/12/28/iso-27-0022021-conoce-losprincipales-cambios-de-la-nueva-norma/>
- Información general de controles y nuevas características (EXCEL)
  - <https://diplomadociberseguridad.com/2020/12/28/iso-27-0022021-conoce-losprincipales-cambios-de-la-nueva-norma/>

# Consultas



■ Carlos Lobos de Medina

 [carlos.lobos@usach.cl](mailto:carlos.lobos@usach.cl)

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



**CAPACITACIÓN USACH**  
UNIVERSIDAD DE SANTIAGO DE CHILE

# FUNDAMENTOS DE ISO 27.002:2022

---

## Sesión N°3 – Conociendo la ISO 27.002:2022