

## MÓDULO I

### Fundamentos y Marcos de Referencia

---

- Ciberseguridad
- Marcos de referencia
- Seguridad de la información
- Activos y riesgos

# CIBERSEGURIDAD

*Seguridad de la Información en la Era Digital*

---

Componente Formativo · Informática y Redes

Instructora: Bibiana Andrea Grcia

2026

# OBJETIVOS DE APRENDIZAJE

**01**

Comprender los principios básicos de la seguridad de la información y su evolución hacia la ciberseguridad.

**02**

Identificar los marcos de referencia internacionales más utilizados para la gestión de riesgos cibernéticos.

**03**

Analizar los activos de información y aplicar metodologías de valoración según estándares ISO/IEC 27001.

**04**

Desarrollar una postura crítica frente a las políticas de seguridad organizacional.

# CONTENIDO TEMÁTICO

**1** Ciberseguridad: definición y contexto

**2** Marcos de referencia: NIST CSF, ISO 27001, COBIT, HITRUST, CSA

**3** Seguridad de la información: principios CIA

**4** Políticas de seguridad

**5** Estándares y normas

**6** Riesgos y mecanismos de valuación

**7** Activos de información: tangibles e intangibles

**8** Inventario, clasificación y etiquetado de activos

# ¿QUÉ ES LA CIBERSEGURIDAD?

*"La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, métodos de gestión de riesgos, acciones, formación y tecnologías utilizadas para proteger los activos de la organización y los usuarios en el ciberentorno."*

*Unión Internacional de Telecomunicación (UIT), 2010*

## **Protección**

Activos y usuarios en el ciberentorno

## **Gestión**

Políticas, riesgos y controles

## **Alcance**

Dispositivos, redes, comunicaciones, datos

# CONTEXTO Y RELEVANCIA

**La ciberseguridad se ha convertido en estándar y necesidad organizacional**

## **Servicios en Internet**

Uso masivo de conectividad para procesos operativos y de negocio

## **Computación en la Nube**

Migración acelerada que amplía la superficie de ataque

## **Interconexión de Sedes**

Redes extendidas con mayor exposición a amenazas externas

## **Transformación Digital**

Los procesos core del negocio dependen de la tecnología

# MARCOS DE REFERENCIA

## ¿Por qué son necesarios?

Ante el incremento de ataques cibernéticos, los marcos de referencia suministran información valiosa en el diseño de procesos de control y mitigación de riesgos. Son una guía, no una solución definitiva; deben complementarse con análisis de riesgos contextualizado.

**NIST CSF**

**ISO/IEC 27001**

**COBIT**

**HITRUST CSF**

**CSA CCM**

*Seleccione el marco más adecuado a su entorno y complemente con otros según el riesgo identificado.*

# NIST CSF · ISO/IEC 27001:2013

## NIST CSF

- ▶ National Institute of Standards and Technology
- ▶ Marco ampliamente adoptado a nivel internacional
- ▶ Cinco funciones: Identificar · Proteger · Detectar · Responder · Recuperar
- ▶ Aplicable a organizaciones de cualquier tamaño e industria

## ISO/IEC 27001:2013

- ▶ Organización Internacional de Normalización (ISO)
- ▶ Reconocido y respetado internacionalmente
- ▶ Protege confidencialidad, integridad y disponibilidad
- ▶ Filosofía basada en la gestión de riesgos sistematizada

# COBIT · HITRUST CSF · CSA CCM

## COBIT

Desarrollado por ISACA (organización global sin fines de lucro)

Gobierno y control de TI: objetivos, auditoría y gestión

Guía de mejores prácticas para cualquier organización

## HITRUST CSF

Creado por Health Information Trust Alliance

Marco más adoptado en la industria de la salud en EE.UU.

Incluye controles HIPAA y controles ampliados aplicables a cualquier sector

## CSA CCM

Desarrollado por Cloud Security Alliance para proveedores cloud

Controles específicos para entornos de computación en la nube

Se actualiza frecuentemente: riesgos cloud únicos y cambiantes



# SEGURIDAD DE LA INFORMACIÓN

*"Proteger la información y los sistemas de información de acceso, uso, divulgación, alteración, modificación o destrucción no autorizados." —Soriano, M. (2014)*

**Conceptos diferenciados — no son sinónimos:**

## Seguridad de la Información

Protección de la información en cualquier formato y soporte

## Seguridad Informática

Protección de sistemas y equipos informáticos

## Seguridad en la Red

Protección de la infraestructura de comunicaciones y redes

# TRIADA CIA — PRINCIPIOS FUNDAMENTALES

La triada CIA sustenta la seguridad de la información en tres pilares interdependientes:

## C

---

### CONFIDENCIALIDAD

Garantiza que la información sea accesible únicamente a las personas autorizadas. Previene la divulgación no autorizada de datos sensibles.

## I

---

### INTEGRIDAD

Asegura que la información no ha sido alterada, modificada o destruida de forma no autorizada. Garantiza exactitud y completitud.

## A

---

### DISPONIBILIDAD

Garantiza que los sistemas y la información estén accesibles cuando los usuarios autorizados los necesiten. Previene interrupciones del servicio.

# POLÍTICAS DE SEGURIDAD

*"Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa... para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital."*

*Caurin, 2018*

**Una política de seguridad debe responder:**

## ¿Qué?

Qué activos y recursos deben protegerse

## ¿De quién?

Contra qué amenazas y actores maliciosos

## ¿Cómo?

Mecanismos, controles y procedimientos de protección

# ESTÁNDARES Y NORMAS DE REFERENCIA

## ISO/IEC 27000

---

Sistema de administración de seguridad de la información (ISMS). Controla la seguridad bajo gestión administrativa explícita.

## ISO 15408

---

Estándar 'Criterio Común': permite integrar y probar aplicaciones de software de forma segura.

## RFC 2196

---

Memorándum del IETF para políticas y procedimientos de seguridad en sistemas conectados a Internet.

## ISA/IEC 62443

---

Estándar para la seguridad en automatización industrial y sistemas de control. Evolución del ISA-99 (2007).

# RIESGOS Y MECANISMOS DE VALUACIÓN

*"El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico." —Zambrano & Valencia (2017)*

## AMENAZA

Cualquier evento que puede afectar activos de información. Puede ser de origen humano, natural o técnico.

## VULNERABILIDAD

Debilidad en un sistema que puede ser explotada por una amenaza para causar daño.

## RIESGO

Probabilidad  $\times$  Impacto. Se compara con el riesgo límite aceptable; si es inferior, se convierte en riesgo residual.

## RIESGO RESIDUAL

Riesgo que permanece después de aplicar controles. Debe ser aceptado formalmente por la organización.

# ACTIVOS DE INFORMACIÓN

*Según ISO/IEC 27001: "Activo es todo aquello que es importante y que la organización valora, por lo tanto debe protegerse."*

## ACTIVOS TANGIBLES (Materiales)

- ▶ Servidores físicos y equipos de red
- ▶ Equipos informáticos y periféricos
- ▶ Portátiles, tabletas y móviles
- ▶ Pendrives y dispositivos extraíbles
- ▶ Instalaciones y oficinas
- ▶ Personal propio

## ACTIVOS INTANGIBLES (Lógicos)

- ▶ Aplicaciones informáticas (ERP, CRM, etc.)
- ▶ Sistemas operativos
- ▶ Gestores de bases de datos
- ▶ Software de comunicaciones
- ▶ Sistemas de copias de seguridad
- ▶ Suministros y licencias

# INVENTARIO DE ACTIVOS — ISO/IEC 27001

## Actividades del proceso de control de activos:

1

### 1. Identificación

Determinar todos los activos vinculados al cumplimiento de los objetivos organizacionales.

2

### 2. Clasificación

Evaluar confidencialidad, integridad y disponibilidad con niveles: Alta · Media · Baja.

3

### 3. Propiedad

Asignar un responsable/propietario a cada activo del inventario.

4

### 4. Etiquetado

Etiquetar cada activo según el esquema: {Clasif.C} - {Clasif.I} - {Clasif.D}

5

### 5. Valoración

Determinar el valor del activo según el impacto ante una posible afectación.

6

### 6. Tratamiento

Definir controles preventivos, correctivos y de recuperación según el nivel de riesgo.

# CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

Sistema de clasificación basado en tres dimensiones:

## CONFIDENCIALIDAD

**IC / IR / IP / ISC**

---

IC: Información Clasificada  
IR: Información Reservada  
IP: Información Pública  
ISC: Info. Sin Clasificar

## INTEGRIDAD

**A · M · B**

---

A: Alta — información crítica  
M: Media — importante  
B: Baja — impacto reducido

## DISPONIBILIDAD

**1 · 2 · 3**

---

1: Alta — acceso permanente  
2: Media — acceso frecuente  
3: Baja — acceso ocasional

Formato de etiqueta: {Clasif.Confidencialidad} — {Clasif.Integridad} — {Clasif.Disponibilidad}    Ej: IC — A — 1



# METODOLOGÍAS DE VALUACIÓN DE ACTIVOS

La valuación de activos inicia con la identificación, clasificación y asignación de valor. Se recomienda seleccionar la metodología que mejor se ajuste al entorno organizacional:

## MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Desarrollada por el Gobierno de España. Altamente estructurada.

## OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation. Orientada a procesos organizacionales y autoevaluación.

## CRAMM

CCTA Risk Analysis and Management Method. Marco británico basado en identificación y valoración cuantitativa de activos.

## ISO/IEC 27005

Estándar internacional para la gestión de riesgos de seguridad de la información. Complementa la ISO 27001.

# ACTIVIDAD DE APRENDIZAJE — AA1\_EV01

## Producto: Informe del análisis y valuación de activos de información

### Pregunta 1

¿Cuáles son los activos tangibles o intangibles informáticos de su organización vinculados al cumplimiento de los objetivos empresariales?

### Pregunta 2

¿Cómo debe ser la clasificación de los activos en su organización?

### Pregunta 3

¿Qué metodologías o estándares puede utilizar para el proceso de valuación de activos?

# SÍNTESIS DEL COMPONENTE FORMATIVO

**Marcos  
de referencia**

**Seguridad  
de la Info.**

**CIBERSEGURIDAD**

**Políticas y  
Estándares**

**Activos y  
Riesgos**

*La ciberseguridad articula marcos normativos, principios CIA, políticas organizacionales y metodologías de valuación de activos en una gestión integral del riesgo tecnológico.*

# REFERENCIAS BIBLIOGRÁFICAS

Caurin, J. (2018). Políticas de seguridad informática. Emrendepyme.

International Organization for Standardization. (2013). ISO/IEC 27001:2013. Ginebra: ISO.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. NIST. <https://doi.org/10.6028/NIST.CSWP.04162018>

Soriano, M. (2014). Seguridad en redes y seguridad de la información. Universidad Politécnica de Valencia.

Unión Internacional de Telecomunicación. (2010). Resolución 130 (Rev. Guadalajara, 2010). UIT.

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Análisis y gestión de riesgos informáticos. Revista Espacios, 38(49).

ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. ISACA.

Cloud Security Alliance. (2021). Cloud Controls Matrix v4. CSA. <https://cloudsecurityalliance.org>

# ¿Preguntas y reflexiones?

---

*"La educación no cambia el mundo;  
cambia a las personas que van a cambiar el mundo."*

— Paulo Freire

Instructora de Informática · 2025

# RIESGO INFORMÁTICO

## Y MATRIZ DE RIESGOS



Presentado por: Bibiana Andrea Gracia

Es la probabilidad que una amenaza informática se materialice sobre un activo, provocando un impacto que ocasione pérdidas o daños materiales e inmateriales.



## 1.1 Tipos de Riesgo Informático

### ALTO

El impacto sobre la organización puede ocasionar pérdidas o desarticulación de sus procesos core del negocio a muy corto plazo.

### MEDIO

El impacto no es tan evidente en el corto plazo, pero si no se corrige puede generar pérdidas o desarticulación progresiva.

### BAJO

El impacto causa un daño aislado que no perjudica componentes clave de la organización.

*El análisis de riesgos es el primer eslabón de la gestión de la seguridad de la información: permite decidir eliminar, ignorar, transferir o mitigar cada riesgo identificado.*



## 1.2 Matriz de Riesgos Informáticos

### ¿Para qué sirve?

- Identificar activos necesarios para la misión y visión organizacional.
- Conocer las amenazas y la probabilidad de que se materialicen.
- Cuantificar el impacto potencial sobre la organización.
- Seleccionar alternativas de mitigación adecuadas.
- Facilitar una gestión adecuada y sostenida del riesgo.

### Fórmula base

$$\text{Riesgo} = \text{Probabilidad de Amenaza} \times \text{Magnitud del Daño}$$

### Niveles de riesgo



Bajo Riesgo = 1 – 6



Medio Riesgo = 8 – 9



Alto Riesgo = 12 – 16





# Fundamentos: Escala de Valoración

Valor	Nivel	Descripción
1	Insignificante	El evento es altamente improbable o su daño es prácticamente nulo para los activos.
2	Baja	Posibilidad reducida de materialización; el daño, aunque presente, es manejable y controlable.
3	Mediana	Probabilidad moderada de ocurrencia con un impacto considerable en los activos organizacionales.
4	Alta	Probabilidad elevada de materialización con impacto severo, comprometiendo la operación de la entidad.



# Clasificación de Activos en la Matriz

## Confidencial, Privado y Sensitivo

Información cuya divulgación no autorizada compromete la privacidad, la seguridad o los intereses estratégicos de la organización.

## Obligación por Ley / Contrato / Convenio

Activos sujetos a cumplimiento normativo, regulatorio o contractual; su pérdida puede acarrear sanciones legales.

## Costo de Recuperación (Tiempo, Económico, Material, Imagen)

Activos valorados según el esfuerzo requerido para su recuperación: tiempo operativo, inversión económica, reputación e imagen institucional.

*La clasificación determina el impacto potencial y el nivel de importancia del activo para la operación organizacional.*



# Uso y Adaptación de la Matriz

## ¿Cómo se usa?

- Ingresar activos identificados en fases previas (sistemas, equipos, personal).
- Seleccionar clasificación del activo según análisis previo.
- Asignar valor de probabilidad a cada amenaza (1–4).
- La matriz calcula automáticamente el nivel de riesgo.
- Analizar las celdas coloreadas para definir el plan de tratamiento.

## ¿Cómo se adapta?

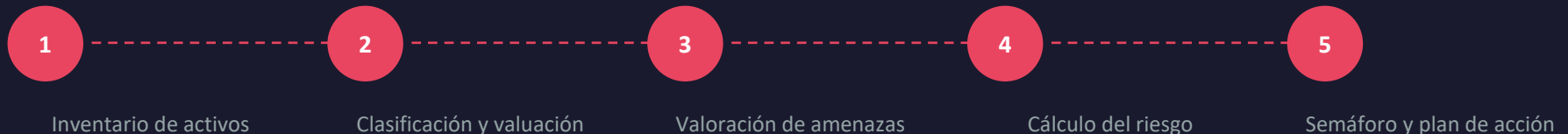
- La colección de amenazas y activos es una aproximación general.
- Ajustar valores de amenazas según la realidad de cada organización.
- Agregar o eliminar activos según inventario propio.
- Recalibrar umbrales de riesgo si el contexto lo requiere.
- Revisar y actualizar periódicamente ante nuevas amenazas.

*"Dependiendo del color de cada celda, podemos sacar conclusiones sobre el nivel de riesgo y las medidas de protección necesarias." (Velázquez Martínez, 2011)*

## EJEMPLO PRÁCTICO

# Construcción de la Matriz de Riesgo Informático

La siguiente secuencia ilustra, paso a paso, cómo una organización del sector tecnológico aplica la metodología de Velázquez Martínez (2011) para identificar, valorar y priorizar sus riesgos informáticos sobre activos de infraestructura crítica.



# Paso 1 & 2 — Inventario y Clasificación de Activos

Activo de Información	Clasificación	Escala de Impacto
Firewall de Borde Zentyl	Costo	4 Alto
Switch Dell 7048 RC Switch Core	Obligación	3 Mediano
Switch Dell 7048 RS Switch Core	Obligación	3 Mediano
Servidor Power Edge R620 Hypervisor	Costo	2 Bajo
Servidor Power Edge R720 Hypervisor	Costo	1 Insig.



## Paso 3 — Valoración de Probabilidad de Amenazas

### Amenazas Humanas

Acceso no autorizado

4

Explotación errores

3

Virus

3

### Amenazas del Entorno

Fallas eléctricas

3

Incendios

2

### Naturales

Terremotos

1

### Vulnerabilidades

Copias de seguridad

4

Políticas seguridad

4



4 = Alta



3 = Mediana



2 = Baja



1 = Insignificante

## Paso 4 — Cálculo del Riesgo: $\text{Riesgo} = \text{Impacto} \times \text{Probabilidad}$

Activo	Imp.	Acceso	Explotación	Virus	Fallas	Incendios	Terremotos	Copias
Probabilidades →		4	3	3	3	2	1	4
Firewall de Borde Zentyal	4	16	12	12	12	8	4	16
Switch Dell 7048 RC Switch Core	3	12	9	9	9	6	3	12
Switch Dell 7048 RS Switch Core	3	12	9	9	9	6	3	12
Servidor Power Edge R620	4	16	12	12	12	8	4	16
Servidor Power Edge R720	4	16	12	12	12	8	4	16

## Paso 5 — Semáforo de Riesgo y Hallazgos Principales

### SEMÁFORO DE RIESGO

**ALTO**

12–16

**MEDIO**

8–9

**BAJO**

1–6

### ALTO RIESGO — Acción Inmediata

- Firewall Zentyal: Acceso no autorizado = 16 ( $\text{Imp.4} \times \text{Prob.4}$ )
- Servidores Hypervisor: Vulnerabilidades en documentación y políticas = 16
- Todos los activos críticos expuestos a Código Malicioso = 12

### MEDIO RIESGO — Vigilancia Activa

- Switches Dell: Fallas eléctricas = 9 ( $\text{Imp.3} \times \text{Prob.3}$ )
- Explotación de errores en servidores = 8–12
- Revisar configuraciones periódicamente



# Plan de Tratamiento de Riesgos

## ELIMINAR

Suprimir la actividad o el activo que genera el riesgo cuando su valor no justifica la exposición.

### Ejemplo:

*Desactivar servicios no esenciales expuestos en el Firewall.*

## TRANSFERIR

Trasladar la responsabilidad del riesgo a un tercero mediante seguros o contratos de outsourcing.

### Ejemplo:

*Contratar seguro de ciberseguridad para los Servidores Hypervisor.*

## MITIGAR

Implementar controles técnicos y administrativos que reduzcan la probabilidad o el impacto.

### Ejemplo:

*Actualizar firmware de Switches; implementar IDS/IPS en red perimetral.*

## ACEPTAR

Documentar formalmente la decisión de asumir el riesgo cuando está dentro del nivel tolerado.

### Ejemplo:

*Riesgos BAJOS documentados con justificación y revisión anual.*



## Conclusión

La gestión del riesgo informático, sustentada en una matriz robusta, permite a las organizaciones anticipar amenazas, proteger sus activos estratégicos y tomar decisiones fundamentadas para garantizar la continuidad operacional.