CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

# Gestión de Riesgos Ciberseguridad y Privacidad

Ciclo de Workshops

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

# Agenda

- Contexto de la Gestión de Riesgos
- Conceptos bases de Riesgo
- Riesgos de Ciberseguridad
- Riesgos de Privacidad

# Profesor del Curso - Carlos Lobos de Medina

carlos.lobos@gmail.com

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

- Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado 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.

# Próximas actividades


MARTES 06 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)


MIÉRCOLES 07 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)


JUEVES 08 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)


VIERNES 09 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

https://alignment.cl/programa-de-cumplimiento-digital/

# Introducción a la Gestión de Riesgos

# ¿Dónde resulta ser exigida la gestión de riesgos?

- Los reguladores son los principales impulsores de la adopción de la Gestión de Riesgos en las organizaciones, lo cual generalmente se enfoca en sectores industriales.
  - Agencia de Ciberseguridad y Protección de Datos
  - Reguladores Sectoriales
  - Infraestructuras Criticas
  - Auditoría y Cumpimiento

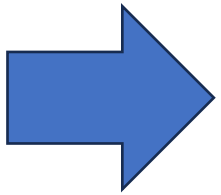
- Cuando adoptamos buenas prácticas, ya que prácticamente todos los modelos obligan para una implementación la adopción de modelos de gestión de riesgos.
  - Sistemas de Gestión de Familia ISO (Todos)
  - NIST CSF
  - COBIT
  - PCI

# Es una buena inversión especializarse en Riesgos

- Sin duda que si!!!

- Es un pilar para:
  - La implementación de un SGSI y SGIP
  - La adopción de modelos de GRC
  - Un buen gobierno corporativo
  - Adoptar leyes de ámbito transversal
  - La auditoria y cumplimiento

- Te posiciona en rol especializado:
  - Segunda línea de defensa
  - Gerencias, jefaturas, analistas y oficiales se desempeñan en esta función



**NO ES FACIL!!!**

**Requiere comprensión de los conceptos y modelos**

**Requiere comprensión del ámbito de aplicación y contexto**

**Requiere la especialización técnica en riesgos**

**Requiere la comprensión de controles especificos**

# Conociendo un poco el Rol – Riesgos de Ciberseguridad


[ENISA - Roles de Ciberseguridad]

| Profile Title | Cybersecurity Risk Manager |
|---|---|
| **Alternative Title(s)** | Information Security Risk Analyst<br>Cybersecurity Risk Assurance Consultant<br>Cybersecurity Risk Assessor<br>Cybersecurity Impact Analyst<br>Cyber Risk Manager |
| **Summary statement** | Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports. |
| **Mission** | Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls. |
| **Deliverable(s)** | • Cybersecurity Risk Assessment Report<br>• Cybersecurity Risk Remediation Action Plan |
| **Main task(s)** | • Develop an organisation's cybersecurity risk management strategy<br>• Manage an inventory of organisation's assets<br>• Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems<br>• Identification of threat landscape including attackers' profiles and estimation of attacks' potential<br>• Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy<br>• Monitor effectiveness of cybersecurity controls and risk levels<br>• Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets<br>• Develop, maintain, report and communicate complete risk management cycle |
| **Key skill(s)** | • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards<br>• Analyse and consolidate organisation's quality and risk management practices<br>• Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks<br>• Build a cybersecurity risk-aware environment<br>• Communicate, present and report to relevant stakeholders<br>• Propose and manage risk-sharing options |

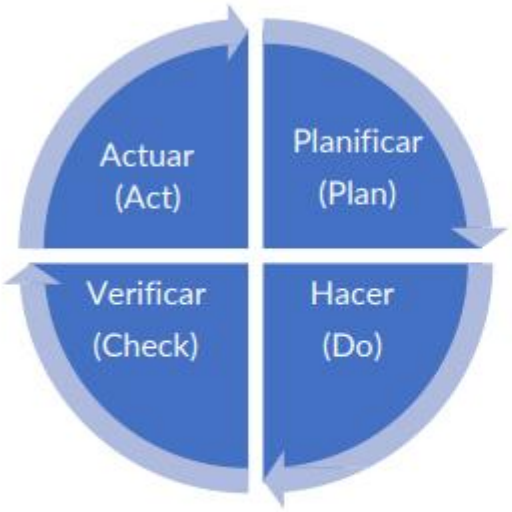
# Conociendo un poco el Rol – Riesgos de Ciberseguridad

| | |
|---|---|
| **Key skill(s)** | • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards<br>• Analyse and consolidate organisation's quality and risk management practices<br>• Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks<br>• Build a cybersecurity risk-aware environment<br>• Communicate, present and report to relevant stakeholders<br>• Propose and manage risk-sharing options |
| **Key knowledge** | • Risk management standards, methodologies and frameworks<br>• Risk management tools<br>• Risk management recommendations and best practices<br>• Cyber threats<br>• Computer systems vulnerabilities<br>• Cybersecurity controls and solutions<br>• Cybersecurity risks<br>• Monitoring, testing and evaluating cybersecurity controls' effectiveness<br>• Cybersecurity-related certifications<br>• Cybersecurity-related technologies |

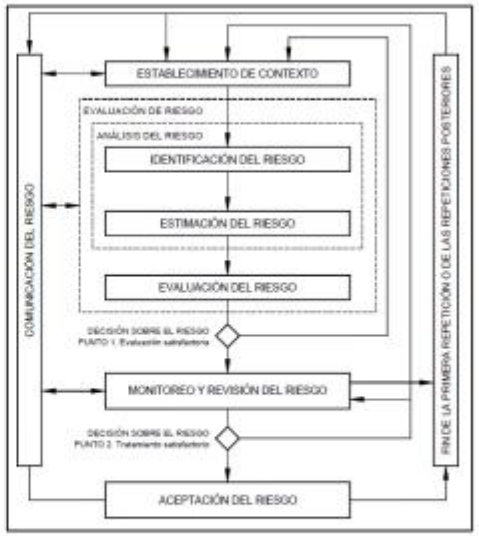
# La gestión de riesgos en estándares ISO - Caso ISO 27001

Una metodología basada en mejores prácticas que posibilita la implementación de un SGSI

**REQUISITO DE LA LEY**
**Implementar un Sistema de Gestión de Seguridad de la Información (SGSI)**




Visión de Procesos alineada al ciclo PDCA




Enfoque de Riesgos


Controles de Seguridad de la Información

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

Metodología Estandarizada

# Ley Marco de Ciberseguridad – Gestión de Riesgos

- **Implementar** un Sistema de Gestión de Seguridad de la Información (SGSI) continuo.
- **Mantener** un registro de las acciones ejecutadas del SGSI.
- **Elaborar** e implementar planes de continuidad operacional y ciberseguridad.
- **Adoptar** de forma oportuna medidas para reducir el impacto y la propagación de un incidente de ciberseguridad
- **Contar** con un programa de formación y educación continua
- **Designar** un delegado de ciberseguridad, quien actuará como contraparte de la Agencia.
- **Reportar** los incidentes de ciberseguridad en los plazos exigidos
- **Certificación** del SGSI

**El propósito de la Ley es que los riesgos de ciberseguridad sean tratados de manera oportuna y que la organización mejore continuamente su postura de riesgos**

# Para Sociedades Anónimas Abiertas

- NCG N°385 de la CMF establece directrices para el "Fortalecimiento de Estándares de Gobierno Corporativo de las Sociedades Anónimas Abiertas“

- Elemento clave de un buen gobierno corporativo:
  - El debido cuidado (due deligence)
  - Transparencia
  - Gestión de Riesgos

- Exige una Gestión Integral de Riesgos
  - Unidad de Gestión y Control de Riesgos
  - Acorde a Estándares internacionales (COSO, COBIT, ISO 31.000)
  - Riesgos directos como aquellos indirectos (empresas del grupo empresarial)
  - Impacto potencial que tendrá la materialización de los riesgos (ciberseguridad)

# Para Servicios Públicos

- Desde el 2005 a la fecha el Consejo de Auditoría Interna General de Gobierno (CAIGG) es la institución mandatada para liderar el proceso de riesgo en el Estado.

- Ha establecido las bases para la implementación del Proceso de Gestión de Riesgos en Servicios e Instituciones públicas del gobierno central

- El Documento Técnico 70 es el que define el proceso de implementación, teniendo mucha información complementaria. Todos los servicios públicos realizan la implementación del proceso basado en estas directrices.

DOCUMENTO TÉCNICO N° 70
Versión 0.3

IMPLANTACIÓN, MANTENCIÓN Y ACTUALIZACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS EN EL SECTOR PÚBLICO

Este documento tiene como principal objetivo facilitar a las organizaciones gubernamentales, la implementación y cumplimiento del Proceso de Gestión de Riesgos, así como su mantención y mejora continua. El enfoque técnico está basado principalmente en la Norma Chilena NCh-ISO 31000:2018, Gestión del Riesgo - Principios y Orientaciones, y en menor medida en el Marco de Gestión de Riesgos Corporativos ERM – COSO II.

CONSEJO DE AUDITORIA INTERNA GENERAL DE GOBIERNO
CAIGG
Ministerio Secretaría General de la Presidencia

SEPTIEMBRE 2022

[Documento Técnico 70 - CAIGG]

# Mercado Financiero (CMF) - RAN 20-10

- Desde diciembre del 2020 se establecen diversas obligaciones en materias de ciberseguridad a las instituciones reguladas por la CMF (Comisión de Mercado Financiero).

**2. Elementos generales de gestión**

En la evaluación de la gestión de la seguridad de la información y ciberseguridad que realiza este Organismo, un elemento fundamental corresponde al rol del Directorio, en lo relativo a la aprobación de la estrategia institucional en esta materia y la autorización de los recursos presupuestarios suficientes para mitigar los riesgos asociados. Es responsabilidad de esta instancia asegurar que la entidad mantenga un sistema de gestión de la seguridad de la información y ciberseguridad, que contemple la administración específica de estos riesgos en consideración a las mejores prácticas internacionales existentes, el que debe ser concordante con el volumen y complejidad de las operaciones de la entidad.

Extractos RAN 20-10

- La entidad se asegura de evaluar oportunamente los riesgos asociados a la seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades y/o definir nuevos procesos.

- La entidad realiza inversiones en tecnologías de procesamiento y seguridad de la información y ciberseguridad, que responden a una estrategia definida para estos efectos, que permiten mitigar los riesgos operacionales y tecnológicos y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

- La entidad gestiona sus alertas o amenazas e incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.

RAN 20-10 - CMF

# ¿Y que pasa con la privacidad? – Ejemplo Ley 21719 Chile

- La base de RGPD exige la gestión de riesgo y evaluación de impacto en tratamiento de datos personales.

Artículo 14 quinquies.- Deber de adoptar medidas de seguridad. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos. Asimismo, deberán evitar la alteración, destrucción, pérdida, tratamiento o acceso no autorizado.

Artículo 15 ter.- Evaluación de impacto en protección de datos personales. Cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, el responsable del tratamiento deberá realizar, previo al inicio de las operaciones del tratamiento, una evaluación del impacto en protección de datos personales.

Extractos Ley 21719


Gestión Riesgos - AEPD

# Conceptos Básicos de Riesgos

# ¿Cual es la necesidad de contar con una Gestión de Riesgos?

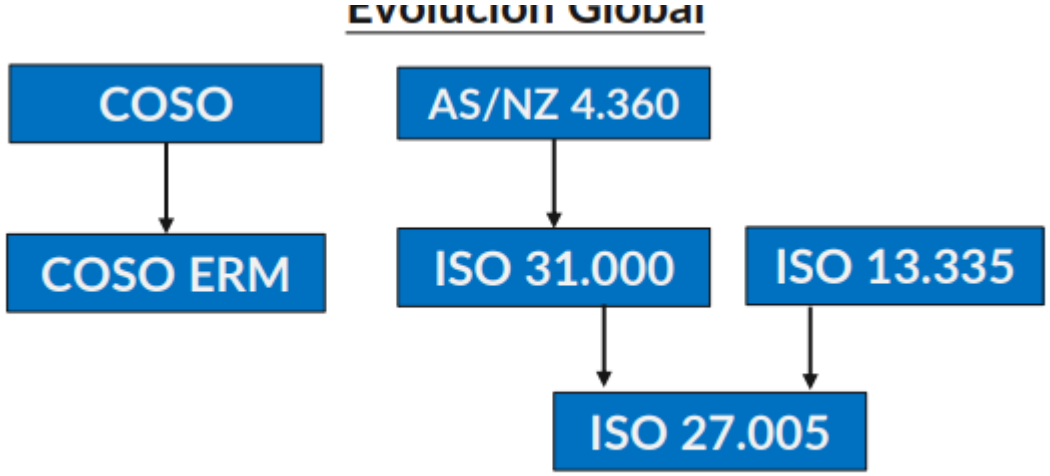

"Desarrollar una cultura que te posibilite gestionar tus objetivos y estrategia de manera efectiva para poder alcanzar tus objetivos de negocio"

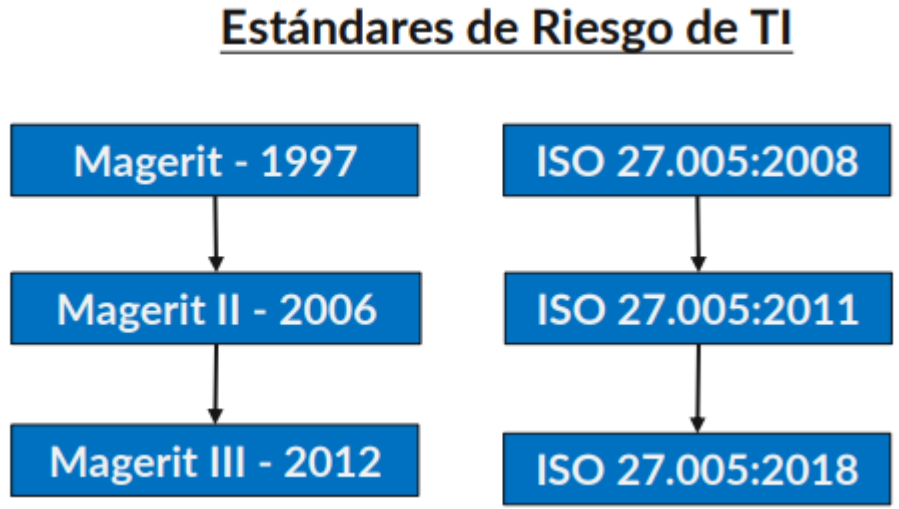
# Cumplimiento o Cumplo y Miento

- Es como usted perciba y entienda la gestión de riesgos
- Si lo articula al negocio, será siempre más fácil obtener apoyo del negocio, de la dirección y sus iniciativas, en consecuencia obtendrá mayor visibilidad y quizás también mayores recursos.
- Si crees que el problema es un malware, la fuga de información, DDoS o un Ransomware, estamos perdidos, el problema es cómo afecta esto en el negocio!!!

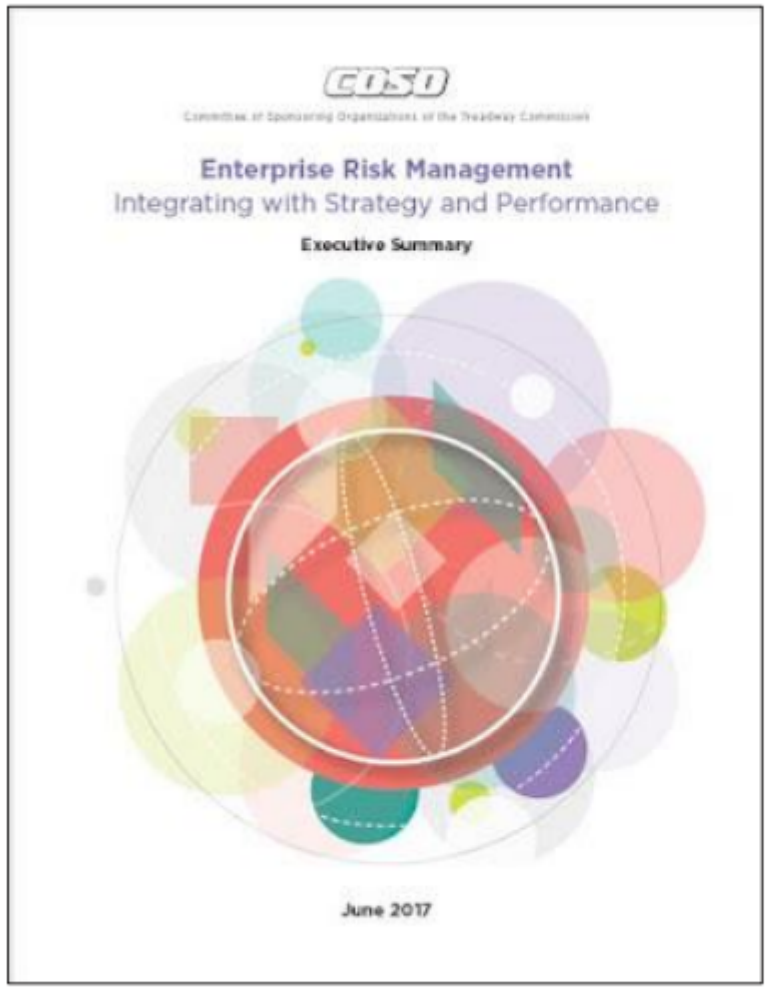
# Estándares de Referencia

- La gestión de riesgos ha evolucionado permanentemente en los últimos 30 años.
- El primer modelo que dio origen a lo que conocemos como gestión de riesgos es COSO, el cual surge como respuestas a escándalos financieros de alcance global.
- En el ámbito de la estandarización, surge la ISO 31.000:2009, la cual nace del modelo AS/NZ 4360.
- En el ámbito de las TI, la ISO 27005 surge como el modelo de gestión de riesgos para facilitar la adopción de ISO 27.001



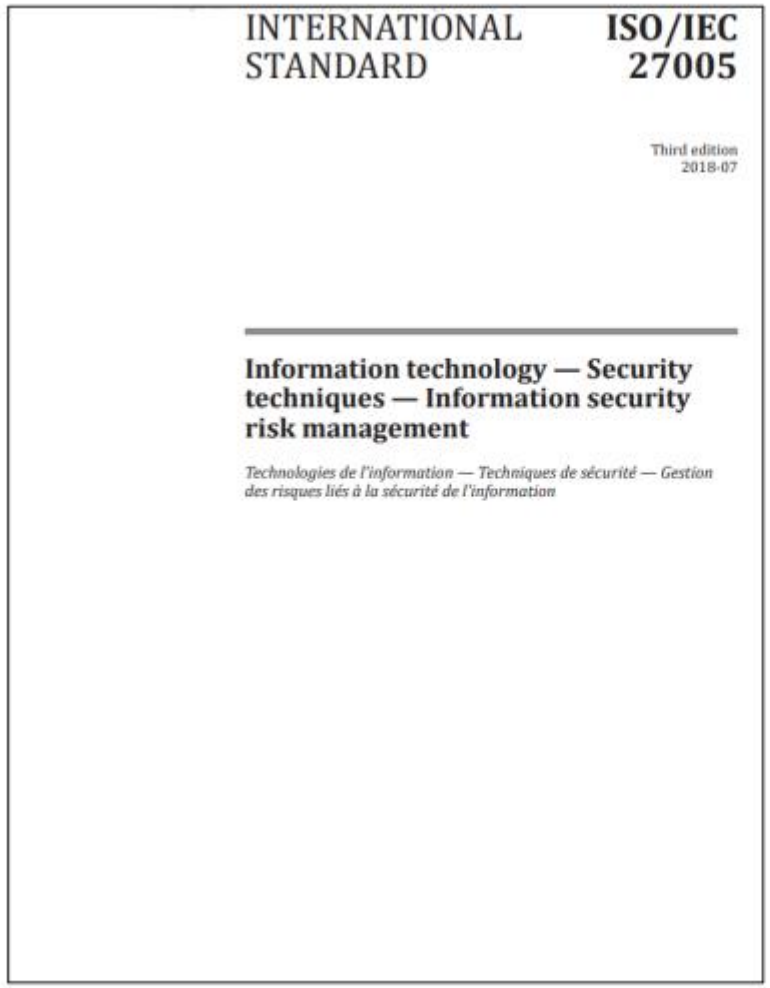
# Gobierno y Gestión de Riesgos

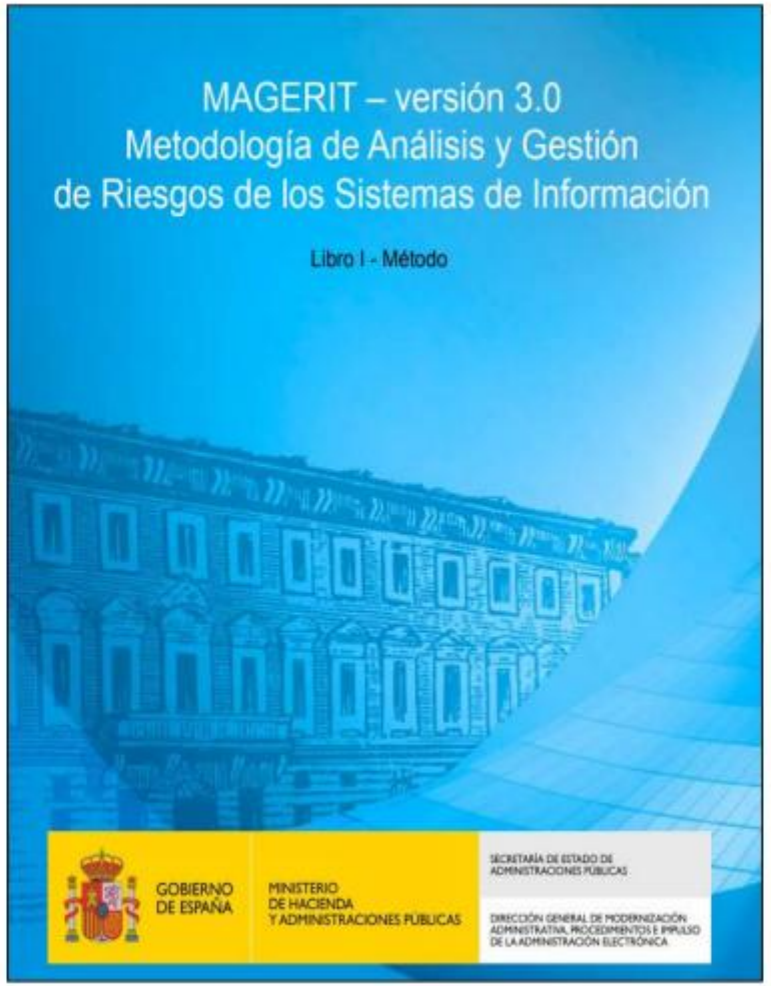




- Estándares de Gestión de Riesgos de mayor adopción.
- COSO ERM transversal al gobierno corporativo, con foco de la misión, visión y estrategia. Muy empleado en grandes organizaciones.
- ISO 31000 centrado en el proceso, más ágil y dinámico en la implementación. Muy empleado a nivel global.
- Excelentes modelos, con foco general de riesgo y alcance limitado en TI, SI y Ciber, pero altamente aplicable.

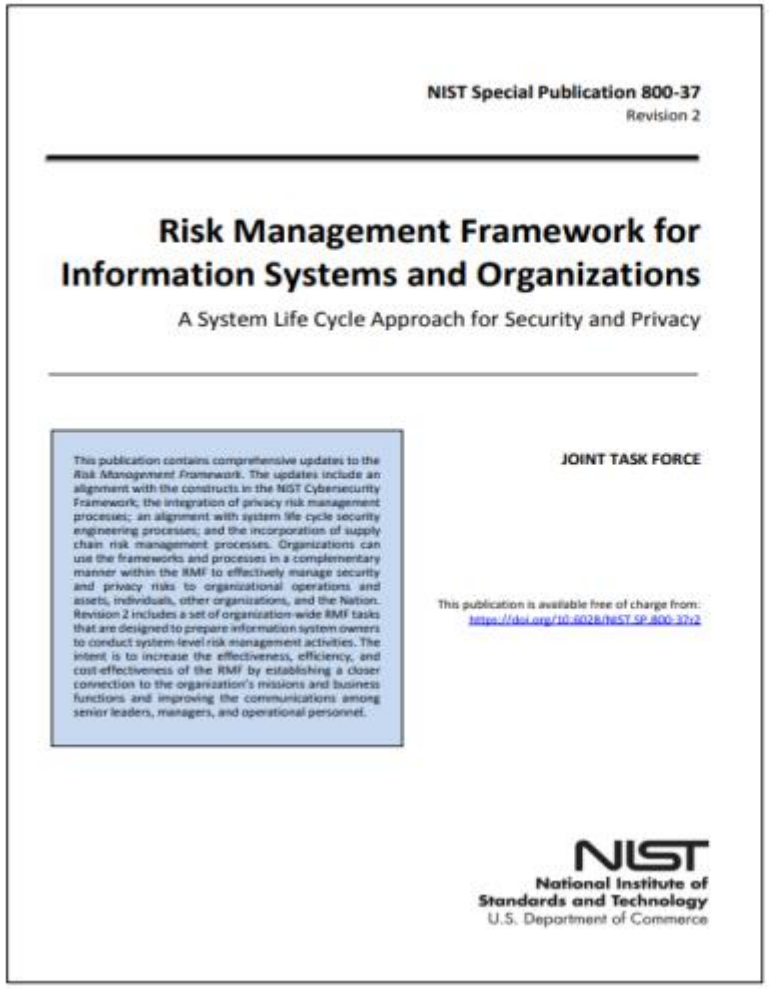
# Gestión de Riesgos de TI y Seguridad de la Información




- Estándares de Gestión de Riesgos de TI y Seguridad de la Información.
- ISO 27005 muy empleado en la adopción de ISO 27001, mecanismo de evaluación simple (amenazas y vulnerabilidades).
- Magerit modelo español, muy robusto, con definiciones precisas de activos, amenazas y salvaguardas.
- Muy recomendable en contextos de implementación inicial.

# Gestión de Riesgos de Ciberseguridad



NIST Special Publication 800-37
Revision 2

**Risk Management Framework for Information Systems and Organizations**

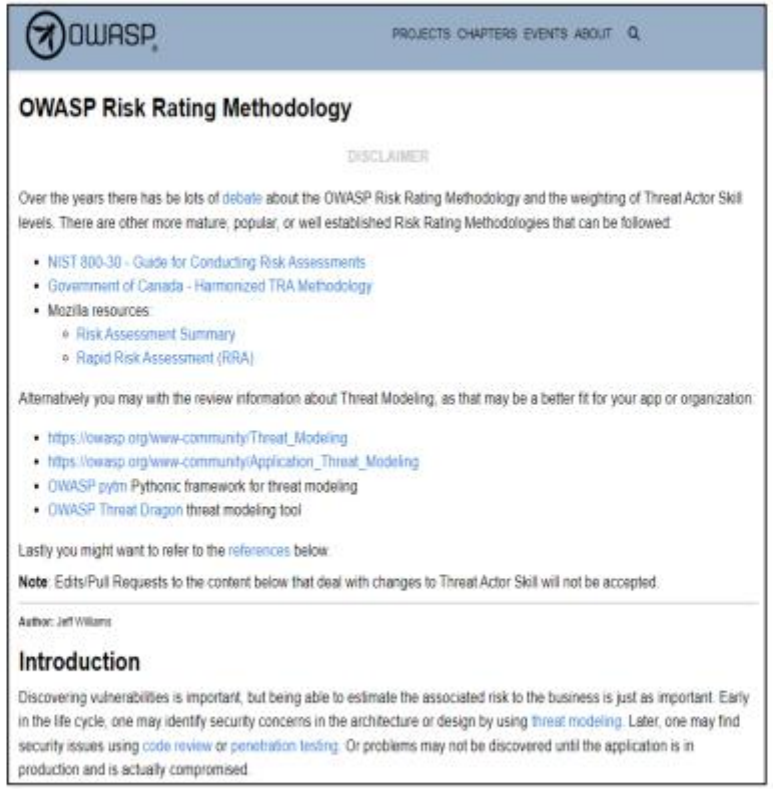
A System Life Cycle Approach for Security and Privacy

This publication contains comprehensive updates to the *Risk Management Framework*. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes. Organizations can use the frameworks and processes in a complementary manner within the RMF to effectively manage security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. Revision 2 includes a set of organization-wide RMF tasks that are designed to prepare information system owners to conduct system-level risk management activities. The intent is to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel.

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



OWASP

PROJECTS CHAPTERS EVENTS ABOUT

**OWASP Risk Rating Methodology**

DISCLAIMER

Over the years there has be lots of debate about the OWASP Risk Rating Methodology and the weighting of Threat Actor Skill levels. There are other more mature, popular, or well established Risk Rating Methodologies that can be followed:

- NIST 800-30 - Guide for Conducting Risk Assessments
- Government of Canada - Harmonized TRA Methodology
- Mozilla resources
  - Risk Assessment Summary
  - Rapid Risk Assessment (RRA)

Alternatively you may with the review information about Threat Modeling, as that may be a better fit for your app or organization:

- https://owasp.org/www-community/Threat_Modeling
- https://owasp.org/www-community/Application_Threat_Modeling
- OWASP pytm Pythonic framework for threat modeling
- OWASP Threat Dragon threat modeling tool

Lastly you might want to refer to the references below.

**Note**: Edits/Pull Requests to the content below that deal with changes to Threat Actor Skill will not be accepted.

Author: Jeff Williams

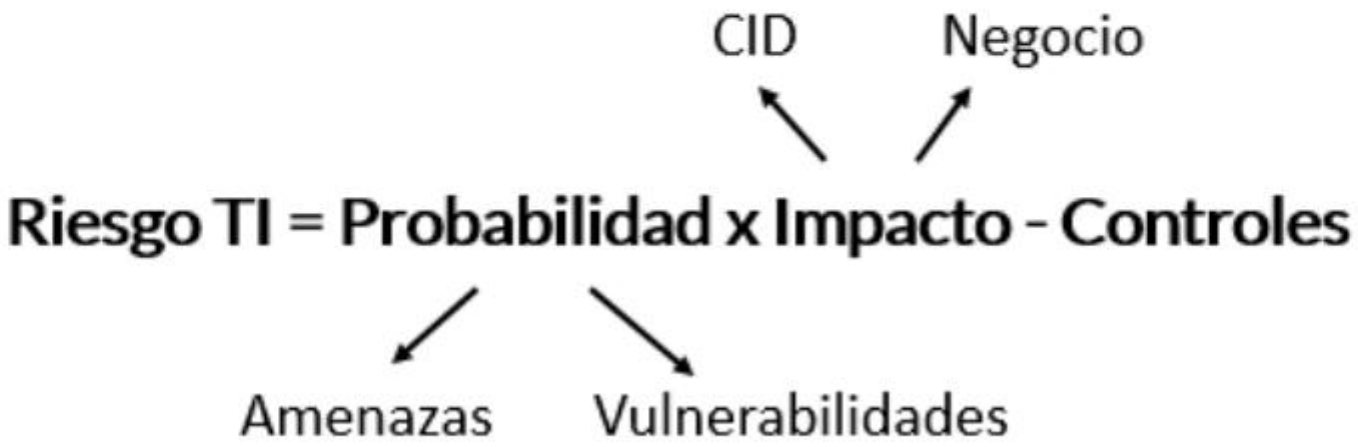
**Introduction**

Discovering vulnerabilities is important, but being able to estimate the associated risk to the business is just as important. Early in the life cycle, one may identify security concerns in the architecture or design by using threat modeling. Later, one may find security issues using code review or penetration testing. Or problems may not be discovered until the application is in production and is actually compromised.

- NIST 800-37 framework robusto e integrado, capaz de ver riesgos frente a no adversarios (operacionales o ambientales) y adversario con un nivel técnico de mucho valor
- OWAP Risk Methodology foco en riesgos de seguridad en software, ofrece un nivel técnico muy atractivo.
- Muy recomendable en contextos de implementación más maduros y de alto conocimiento en materias de ciberseguridad.

# Riesgos de Ciberseguridad

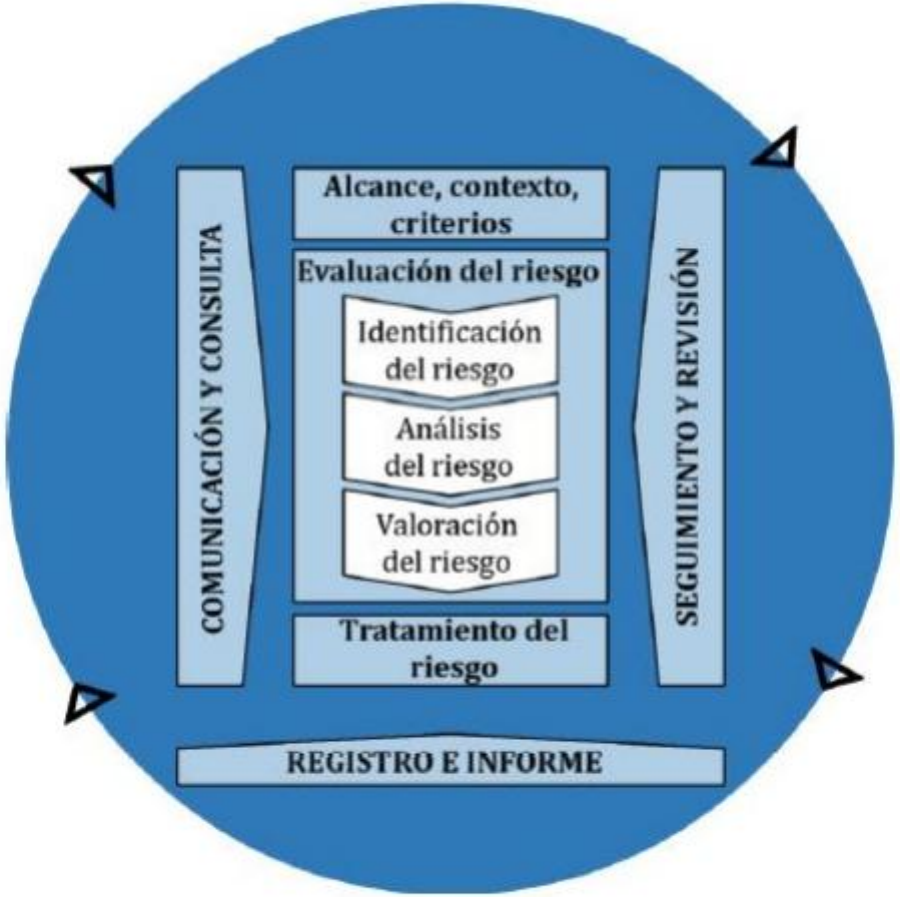
- *"Potencial de que una **amenaza** determinada explote las **vulnerabilidades** de los activos o grupos de activos causando así daño a la organización"* (ISO 27.000)



# Proceso de Gestión de Riesgos – Versión más estándar

**ISO 31000**

- Enfoque de Riesgos en proceso
- Evaluación general del Impacto
- Evaluación general de probabilidad
- Ejemplos Generales

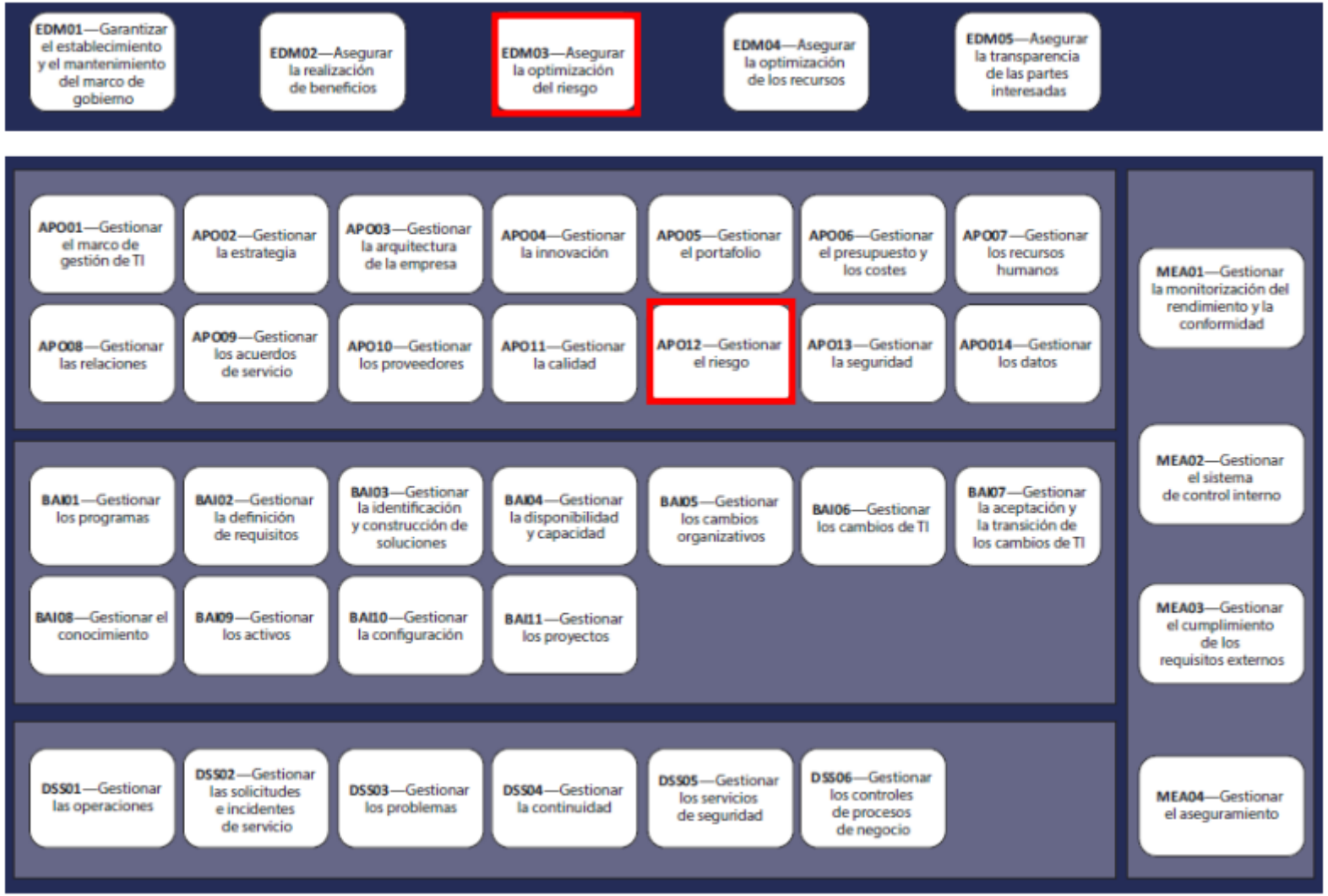



**ISO 27005**

- Enfoque de Riesgos en Activos
- Se evalúa en base a la perdida de CID
- Se evalúa con amenaza y vulnerabilidad
- Ejemplos específicos de Riesgos de TI

- La ISO 27.005 se alinea al proceso de Gestión de Riesgos establecido en ISO 31.000

# COBIT 2019 – Gestión de Riesgos



# Actividades claves del Proceso – COSO ERM

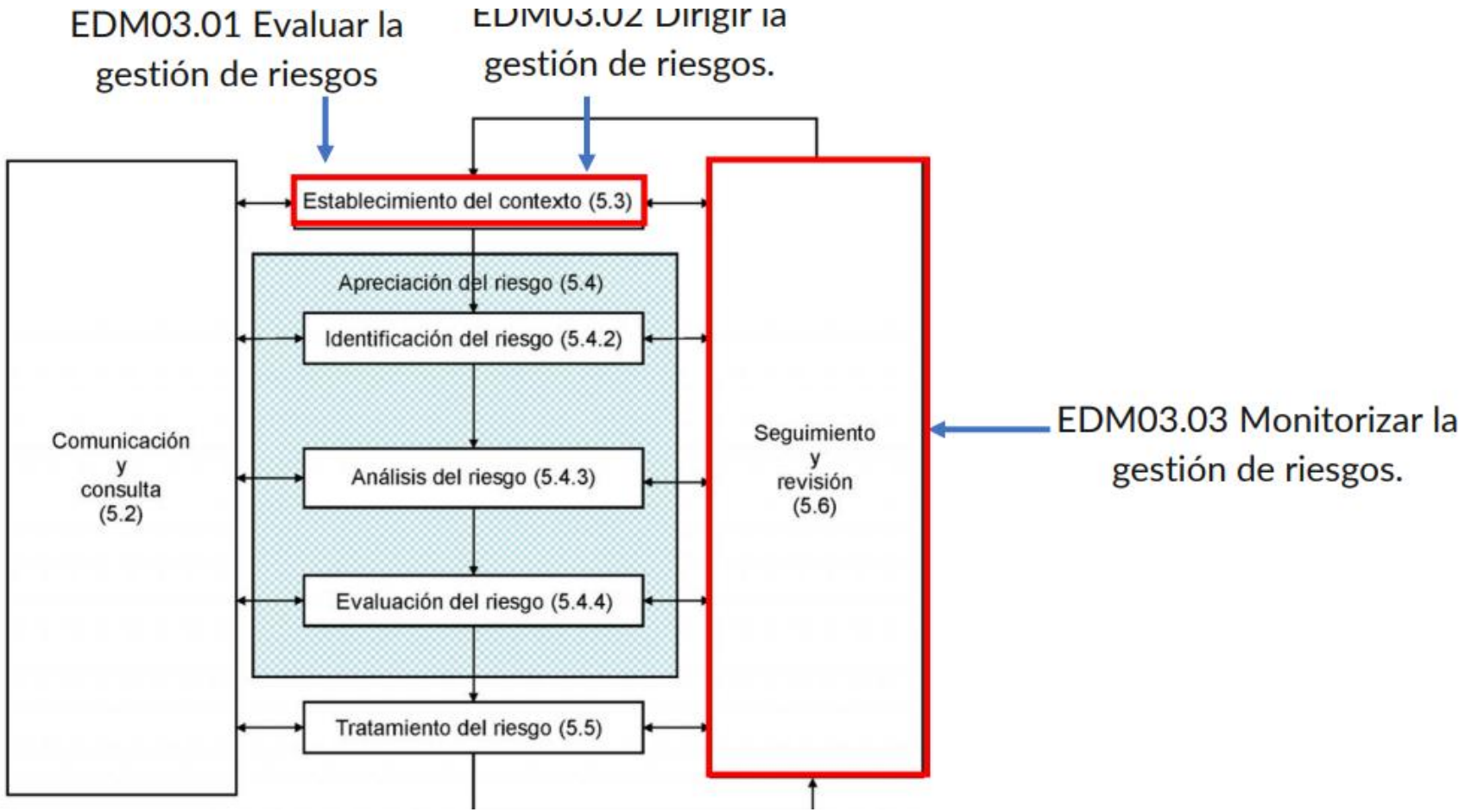
EDM03.01 Evaluar la gestión de riesgos

EDM03.03 Monitorizar la gestión de riesgos.

| Gobierno y Cultura | Estrategia y objetivos | Desempeño | Revisión | Información, comunicación y reporte |
|---|---|---|---|---|
| 1. La Junta Directiva ejerce supervisión sobre los riesgos<br>2. Establece estructuras operativas<br>3. Define la cultura deseada<br>4. Demuestra compromiso con los valores éticos<br>5. Atrae, desarrolla y retiene individuos competentes. | 6. Analiza el contexto empresarial<br>7. Define el apetito al riesgo<br>8. Evalúa estrategias alternativas<br>9. Formula los objetivos empresariales | 10. Identifica riesgos<br>11. Evalúa la severidad de los riesgos<br>12. Prioriza los riesgos<br>13. Implementas las respuestas al riesgo<br>14. Desarrollar un portafolio de riesgos | 15. Evalúa los cambios sustanciales<br>16. Revisa los riesgos y el desempeño<br>17. Propone mejoras en la gestión de riesgos empresariales | 18. Aprovecha la información y la tecnología<br>19. Comunica los riesgos de información<br>20. Informes sobre riesgos, cultura y desempeño |

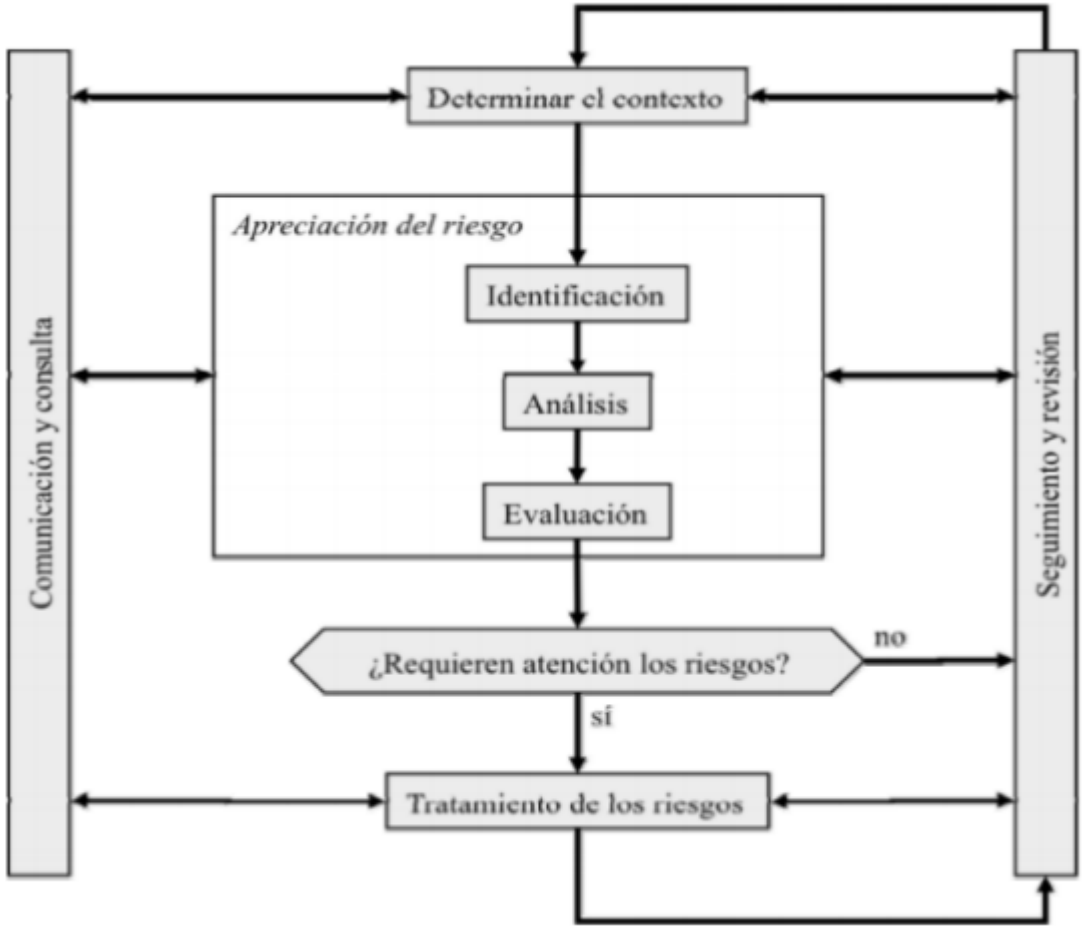
EDM03.02 Dirigir la gestión de riesgos.

# Actividades claves del Proceso – ISO 31000

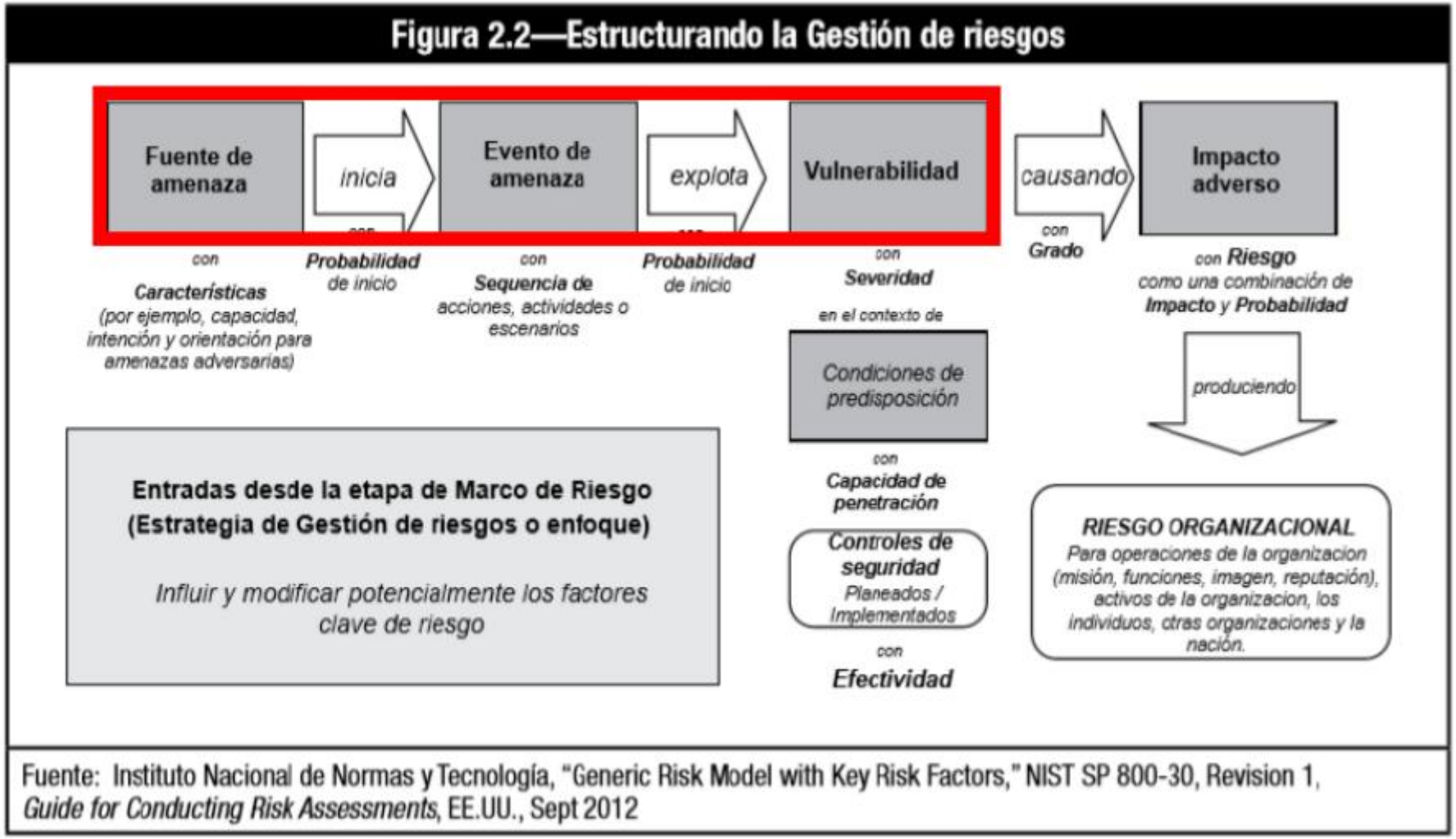


# Actividades claves del Proceso – Magerit

- Proceso similar a ISO 31.000
- Buena definición de activos
- Referencias de amenazas
- Referencias de salvaguardas



# Riesgos de Ciberseguridad




Fuente: Instituto Nacional de Normas y Tecnología, "Generic Risk Model with Key Risk Factors," NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, EE.UU., Sept 2012

# Amenazas

- "Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización" (ISO 27000:2019)

- "Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información" (INCIBE, 2019)

- Pueden ser desde un simple malware hasta sofisticados ciberataques, eventos naturales, la competencia empresarial, un empleado desvinculado, entre otros.

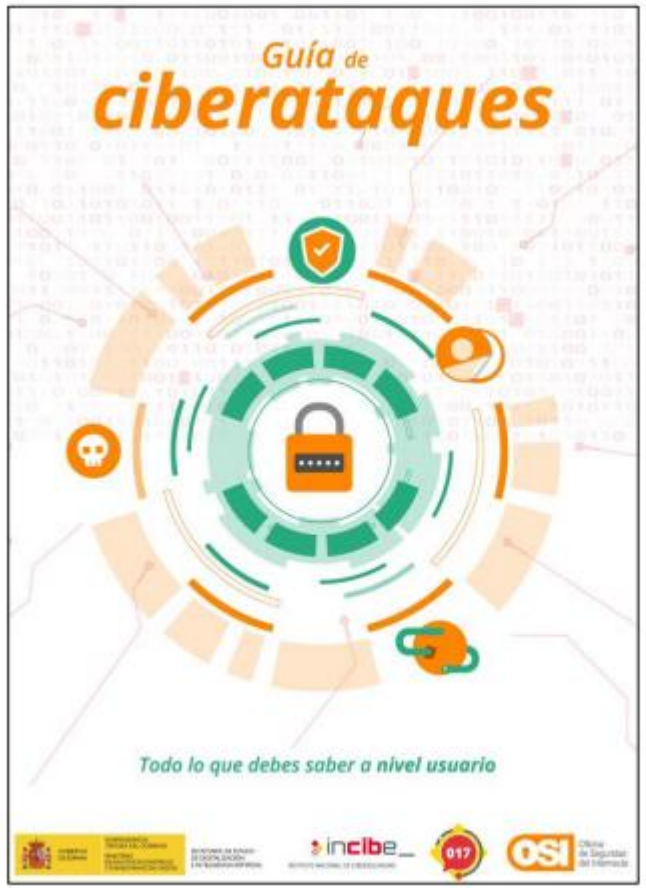
- Desde el punto de vista organizacional pueden ser tanto internas como externas.

# Amenazas – Ejemplos desde ISO 27005

| Category | No. | Threat description | Type of risk source |
|---|---|---|---|
| Physical threats | TP01 | Fire | A, D, E |
| | TP02 | Water | A, D, E |
| | TP03 | Pollution, harmful radiation | A, D, E |
| | TP04 | Major accident | A, D, E |
| | TP05 | Explosion | A, D, E |
| | TP06 | Dust, corrosion, freezing | A, D, E |
| Natural threats | TN01 | Climatic phenomenon | E |
| | TN02 | Seismic phenomenon | E |
| | TN03 | Volcanic phenomenon | E |
| | TN04 | Meteorological phenomenon | E |
| | TN05 | Flood | E |
| | TN06 | Pandemic / epidemic phenomenon | E |
| Infrastructure failures | TI01 | Failure of a supply system | A, D |
| | TI02 | Failure of cooling or ventilation | A, D |
| | TI03 | Loss of power supply | A, D, E |
| | TI04 | Failure of a telecommunications network | A, D, E |
| | TI05 | Failure of telecommunication equipment | A, D |
| | TI06 | Electromagnetic radiation | A, D, E |
| | TI07 | Thermal radiation | A, D, E |
| | TI08 | Electromagnetic pulses | A, D, E |
| Technical failures | TT01 | Failure of device or system | A |
| | TT02 | Saturation of the information system | A, D |
| | TT03 | Violation of information system maintainability | A, D |
| | TH01 | Terror. attack, sabotage | D |
| | TH02 | Social Engineering | D |

| Category | No. | Threat description | Type of risk source |
|---|---|---|---|
| Human actions | TH03 | Interception of radiation of a device | D |
| | TH04 | Remote spying | D |
| | TH05 | Eavesdropping | D |
| | TH06 | Theft of media or documents | D |
| | TH07 | Theft of equipment | D |
| | TH08 | Theft of digital identity or credentials | D |
| | TH09 | Retrieval of recycled or discarded media | D |
| | TH10 | Disclosure of information | A, D |
| | TH11 | Data input from untrustworthy sources | A, D |
| | TH12 | Tampering with hardware | D |
| | TH13 | Tampering with software | A, D |
| | TH14 | Drive-by-exploits using web-based communication | D |
| | TH15 | Replay attack, man-in-the-middle attack | D |
| | TH16 | Unauthorized processing of personal data | A, D |
| | TH17 | Unauthorized entry to facilities | D |
| | TH18 | Unauthorized use of devices | D |
| | TH19 | Incorrect use of devices | A, D |
| | TH20 | Damaging devices or media | A, D |
| | TH21 | Fraudulent copying of software | D |
| | TH22 | Use of counterfeit or copied software | A, D |
| | TH23 | Corruption of data | D |
| | TH24 | Illegal processing of data | D |
| | TH25 | Sending or distributing of malware | A, D, R |
| | TH26 | Position detection | D |
| Compromise of functions or services | TC01 | Error in use | A |
| | TC02 | Abuse of rights or permissions | A, D |
| | TC03 | Forging of rights or permissions | D |
| | TC04 | Denial of actions | D |
| Organizational threats | TO01 | Lack of staff | A, E |
| | TO02 | Lack of resources | A, E |
| | TO03 | Failure of service providers | A, E |
| | TO04 | Violation of laws or regulations | A, D |

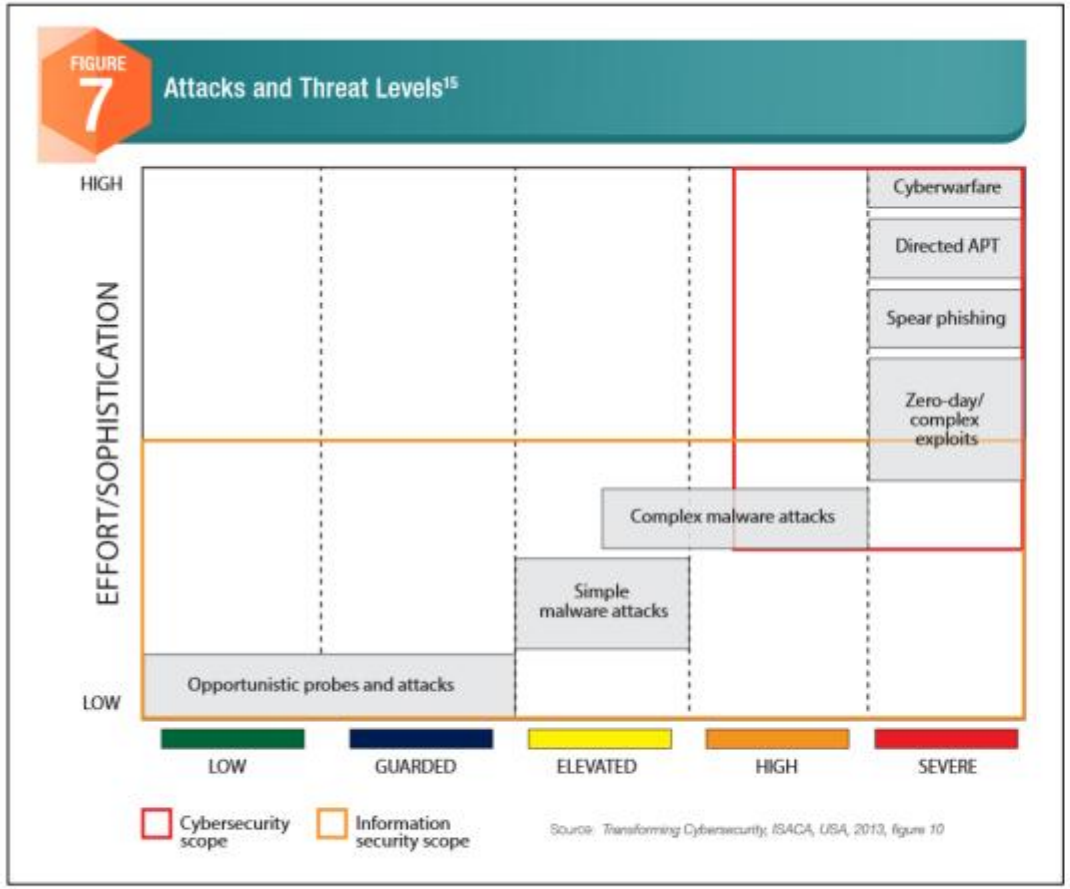
# Ciberataques – Visión Base






[Guía de Ciberataque - Enisa]

# Amenazas – Lo más prioritario




Fuente: European CybersecurityImplementation: Overview, ISACA


enisa-threat-landscape-2023

# Amenazas – hacia donde convergen


[Amenazas 2030 - ENISA]

# Ciber Kill Chain – Etapas de un ataque

# Vulnerabilidad

- "Debilidad de un activo o de un control que puede ser explotada por una o más amenazas" (ISO 27000:2019)

- "Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible." (INCIBE, 2019)

- "Debilidad de un activo o de un control que puede ser explotada por una o más amenazas"

# Ejemplos de Vulnerabilidad – ISO 27005

| Category | No. | Examples of vulnerabilities |
|---|---|---|
| Hardware | VH01 | Insufficient maintenance/faulty installation of storage media |
| | VH02 | Insufficient periodic replacement schemes for equipment |
| | VH03 | Susceptibility to humidity, dust, soiling |
| | VH04 | Sensitivity to electromagnetic radiation |
| | VH05 | Insufficient configuration change control |
| | VH06 | Susceptibility to voltage variations |
| | VH07 | Susceptibility to temperature variations |
| | VH08 | Unprotected storage |
| | VH09 | Lack of care at disposal |
| | VH10 | Uncontrolled copying |
| Software | VS01 | No or insufficient software testing |
| | VS02 | Well-known flaws in the software |
| | VS03 | No 'logout' when leaving the workstation |
| | VS04 | Disposal or reuse of storage media without proper erasure |
| | VS05 | Insufficient configuration of logs for audit trail's purposes |
| | VS06 | Wrong allocation of access rights |
| | VS07 | Widely-distributed software |
| | VS08 | Applying application programs to the wrong data in terms of time |
| | VS09 | Complicated user interface |
| | VS10 | Insufficient or lack of documentation |
| | VS11 | Incorrect parameter set up |
| | VS12 | Incorrect dates |
| | VS13 | Insufficient identification and authentication mechanisms (e.g. for user authentication) |
| | VS14 | Unprotected password tables |
| | VS15 | Poor password management |
| | VS16 | Unnecessary services enabled |
| | VS17 | Immature or new software |
| | VS18 | Unclear or incomplete specifications for developers |
| | VS19 | Ineffective change control |
| | VS20 | Uncontrolled downloading and use of software |
| | VS21 | Lack of or incomplete back-up copies |
| | VS22 | Failure to produce management reports |
| Network | VN01 | Insufficient mechanisms for the proof of sending or receiving a message |
| | VN02 | Unprotected communication lines |
| | VN03 | Unprotected sensitive traffic |
| | VN04 | Poor joint cabling |
| | VN05 | Single point of failure |
| | VN06 | Ineffective or lack of mechanisms for identification and authentication of sender and receiver |
| | VN07 | Insecure network architecture |
| | VN08 | Transfer of passwords in clear |
| | VN09 | Inadequate network management (resilience of routing) |
| | VN10 | Unprotected public network connections |

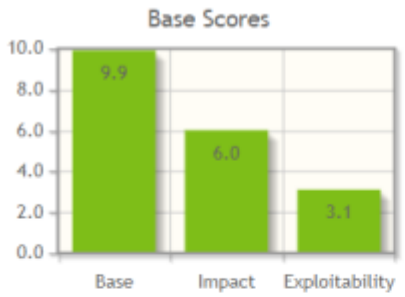
| Category | No. | Examples of vulnerabilities |
|---|---|---|
| Personnel | VP01 | Absence of personnel |
| | VP02 | Inadequate recruitment procedures |
| | VP03 | Insufficient security training |
| | VP04 | Incorrect use of software and hardware |
| | VP05 | Poor security awareness |
| | VP06 | Insufficient or lack of monitoring mechanisms |
| | VP07 | Unsupervised work by outside or cleaning staff |
| | VP08 | Ineffective or lack of policies for the correct use of telecommunications media and messaging |
| Site | VS01 | Inadequate or careless use of physical access control to buildings and rooms |
| | VS02 | Location in an area susceptible to flood |
| | VS03 | Unstable power grid |
| | VS04 | Insufficient physical protection of the building, doors and windows |
| Organization | VO01 | Formal procedure for user registration and de-registration not developed, or its implementation is ineffective |
| | VO02 | Formal process for access right review (supervision) not developed, or its implementation is ineffective |
| | VO03 | Insufficient provisions (concerning security) in contracts with customers and/or third parties |
| | VO04 | Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective |
| | VO05 | Audits (supervision) are not conducted on regular base |
| | VO06 | Procedures of risk identification and assessment not developed, or its implementation is ineffective |
| | VO07 | Insufficient or lack of fault reports recorded in administrator and operator logs |
| | VO08 | Inadequate service maintenance response |
| | VO09 | Insufficient or lack of Service Level Agreement |
| | VO10 | Change control procedure not developed, or its implementation is ineffective |
| | VO11 | Formal procedure for ISMS documentation control not developed, or its implementation is ineffective |
| | VO12 | Formal procedure for ISMS record supervision not developed, or its implementation is ineffective |
| | VO13 | Formal process for authorization of public available information not developed, or its implementation is ineffective |
| | VO14 | Improper allocation of information security responsibilities |
| | VO15 | Continuity plans do not exist, or are incomplete, or are outdated |
| | VO16 | E-mail usage policy not developed, or its implementation is ineffective |
| | VO17 | Procedures for introducing software into operational systems not developed, or their implementation is ineffective |
| | VO18 | Procedures for classified information handling not developed, or their implementation is ineffective |
| | VO19 | Information security responsibilities are not present in job descriptions |
| | VO20 | Insufficient or lack of provisions (concerning information security) in contracts with employees |
| | VO21 | Disciplinary process in case of information security incident not defined, or not functioning properly |
| | VO22 | Formal policy on mobile computer usage not developed, or their implementation is ineffective |

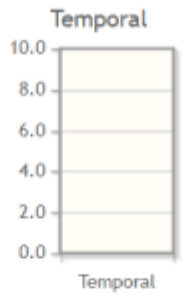
# NIST NVD: National Vulnerability Database (1 de 2)

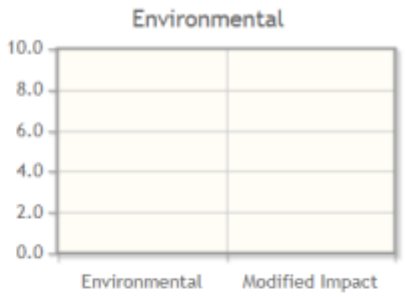
- El NVD es el repositorio de datos de vulnerabilidades oficial del gobierno de estados unidos, presentados usando el protocolo SCAP para permitir la automatización de la gestión de vulnerabilidades, cumplimiento y medidas de seguridad.

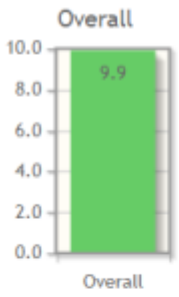
| Vuln ID | Summary | CVSS Severity |
|---|---|---|
| CVE-2024-3821 | The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions in the wdt_ajax_actions.php file in all versions up to, and including, 6.3.2. This makes it possible for unauthenticated attackers to manipulate data tables. Please note this only affects the premium version of the plugin.<br>**Published:** junio 01, 2024; 5:15:09 a. m. -0400 | *V4.0*:(not available)<br>*V3.1*: 7.3 HIGH<br>*V2.0*:(not available) |
| CVE-2024-3820 | The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to SQL Injection via the 'id_key' parameter of the wdt_delete_table_row AJAX action in all versions up to, and including, 6.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Please note this only affects the premium version of the plugin.<br>**Published:** junio 01, 2024; 5:15:09 a. m. -0400 | *V4.0*:(not available)<br>*V3.1*: 10.0 CRITICAL<br>*V2.0*:(not available) |
| CVE-2024-3200 | The wpForo Forum plugin for WordPress is vulnerable to SQL Injection via the 'slug' attribute of the 'wpforo' shortcode in all versions up to, and including, 2.3.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.<br>**Published:** junio 01, 2024; 5:15:09 a. m. -0400 | *V4.0*:(not available)<br>*V3.1*: 9.9 CRITICAL<br>*V2.0*:(not available) |
| CVE-2024-35636 | Cross-Site Request Forgery (CSRF) vulnerability in Uploadcare Uploadcare File Uploader and Adaptive Delivery (beta) uploadcare.This issue affects Uploadcare File Uploader and Adaptive Delivery (beta): from n/a through 3.0.11.<br>**Published:** junio 01, 2024; 5:15:08 a. m. -0400 | *V4.0*:(not available)<br>*V3.x*:(not available)<br>*V2.0*:(not available) |

# NIST NVD: National Vulnerability Database (2 de 2)




**CVSS Base Score:** 9.9
Impact Subscore: 6.0
Exploitability Subscore: 3.1
**CVSS Temporal Score:** NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
**Overall CVSS Score:** 9.9

Show Equations

**CVSS v3.1 Vector**
AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## Base Score Metrics

### Exploitability Metrics

**Attack Vector (AV)***
**Network (AV:N)** | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

**Attack Complexity (AC)***
**Low (AC:L)** | High (AC:H)

**Privileges Required (PR)***
None (PR:N) | **Low (PR:L)** | High (PR:H)

**User Interaction (UI)***
**None (UI:N)** | Required (UI:R)

**Scope (S)***
Unchanged (S:U) | **Changed (S:C)**

### Impact Metrics

**Confidentiality Impact (C)***
None (C:N) | Low (C:L) | **High (C:H)**

**Integrity Impact (I)***
None (I:N) | Low (I:L) | **High (I:H)**

**Availability Impact (A)***
None (A:N) | Low (A:L) | **High (A:H)**

# Probabilidad de Ocurrencia - Magerit

- Plantea elementos basados en la probabilidad de ocurrencia con foco en la amenaza.

| | | | |
|---|---|---|---|
| MA | muy alta | casi seguro | fácil |
| A | alta | muy alto | medio |
| M | media | posible | difícil |
| B | baja | poco probable | muy difícil |
| MB | muy baja | muy raro | extremadamente difícil |

*Tabla 1. Degradación del valor*

| | | | |
|---|---|---|---|
| MA | 100 | muy frecuente | a diario |
| A | 10 | frecuente | mensualmente |
| M | 1 | normal | una vez al año |
| B | 1/10 | poco frecuente | cada varios años |
| MB | 1/100 | muy poco frecuente | siglos |

*Tabla 2. Probabilidad de ocurrencia*

# Probabilidad de Ocurrencia – ISO 27005

- Incorpora elementos de medición más específicos, con foco en la probabilidad de ocurrencia de la amenaza y la clasificación de la amenaza.

- Da directrices generales, pero no posee definiciones concretas de escalas de medida.

| Descriptor de la amenaza (a) | Consecuencia (valor del activo) (b) | Probabilidad de ocurrencia de la amenaza (c) | Medida del riesgo (d) | Clasificación de la amenaza (e) |
|---|---|---|---|---|
| Amenaza A | | | | |
| Amenaza B | | | | |
| Amenaza C | | | | |
| Amenaza D | | | | |
| Amenaza E | | | | |
| Amenaza F | | | | |

# Probabilidad de Ocurrencia – NIST 800-30

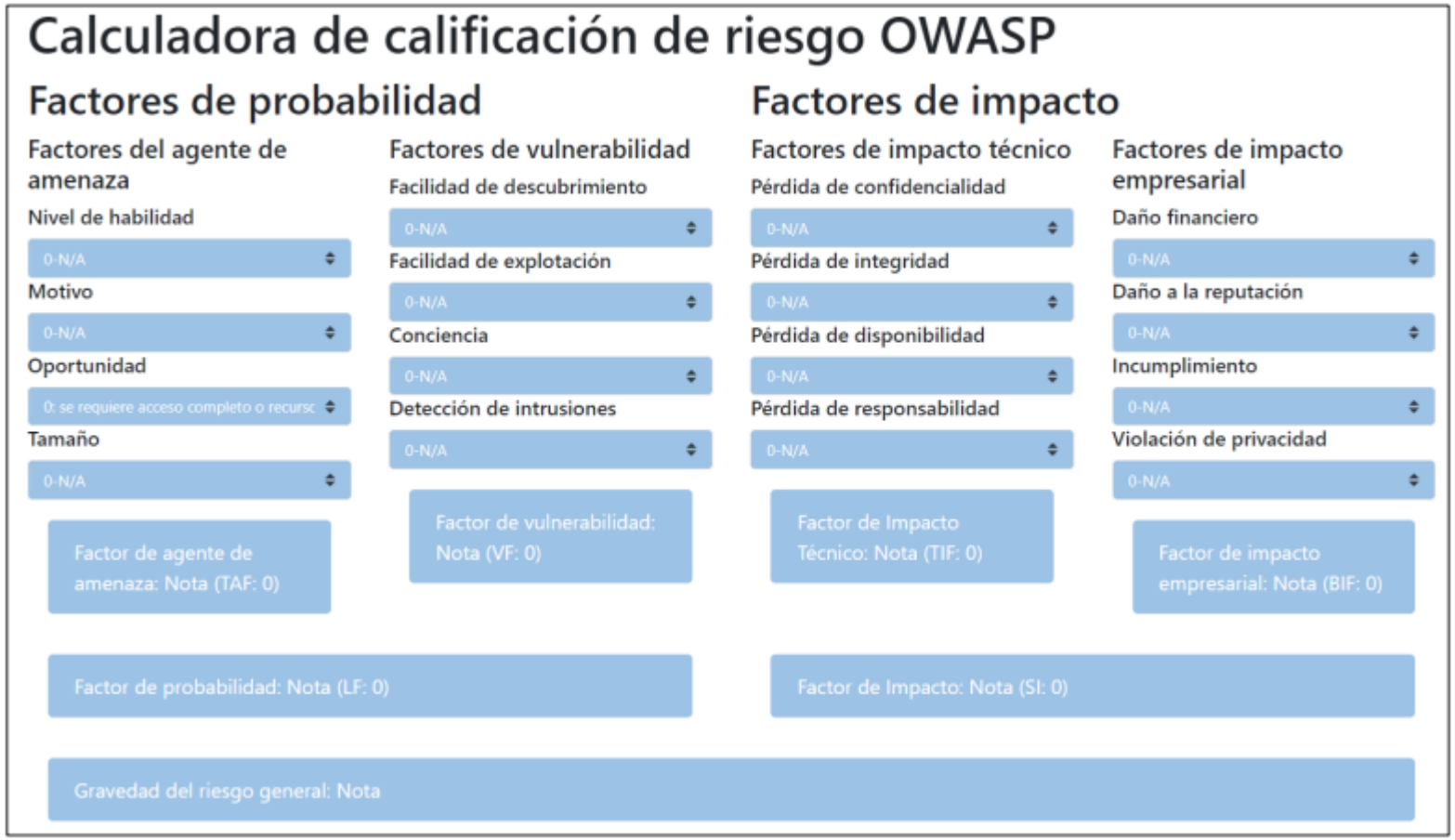
- Establece un contexto de evaluación de amenaza y vulnerabilidades basado en:
  - Capacidad del Adversario
  - Lo que intenta el Adversario
  - Objetivos del Adversario

- Para la probabilidad se establecen elementos de inicio de las amenazas, ocurrencia e impacto adverso.

- Es un muy buen nivel de definición, puesto que aborda elementos técnicos y no técnicos.

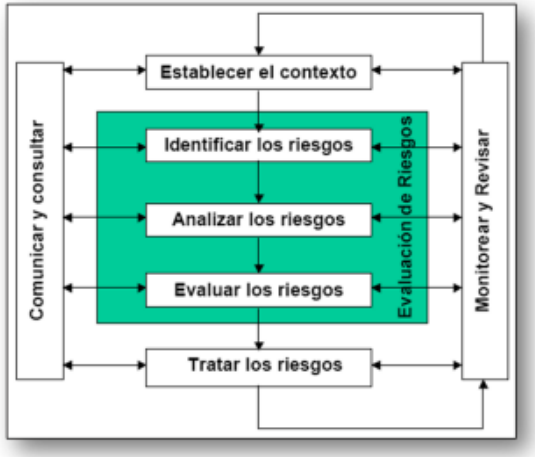
- Es quizás el más completo de los modelos y sin duda el mejor punto de referencia a considerar.

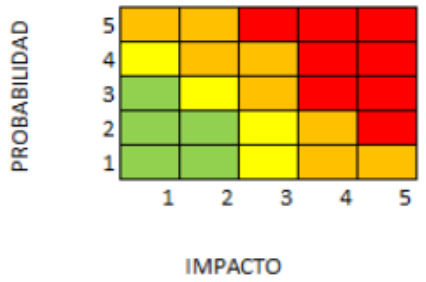
# OWASP Risk Model – Veamos un ejemplo

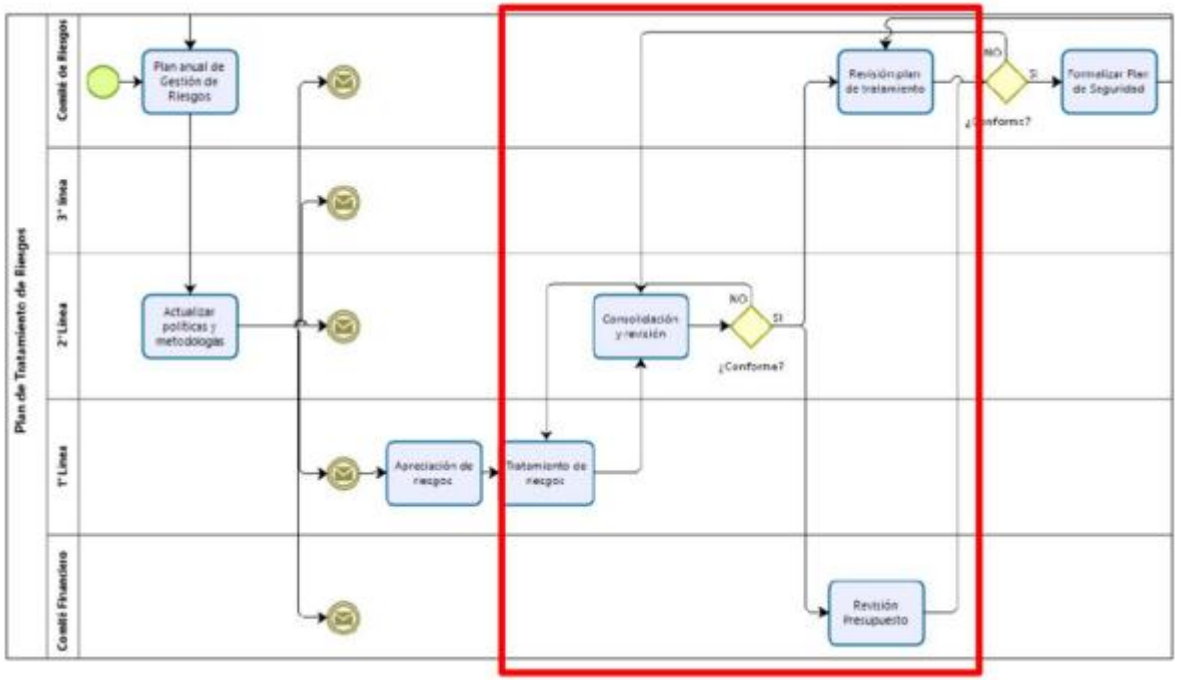



https://owasp-risk-rating.com/

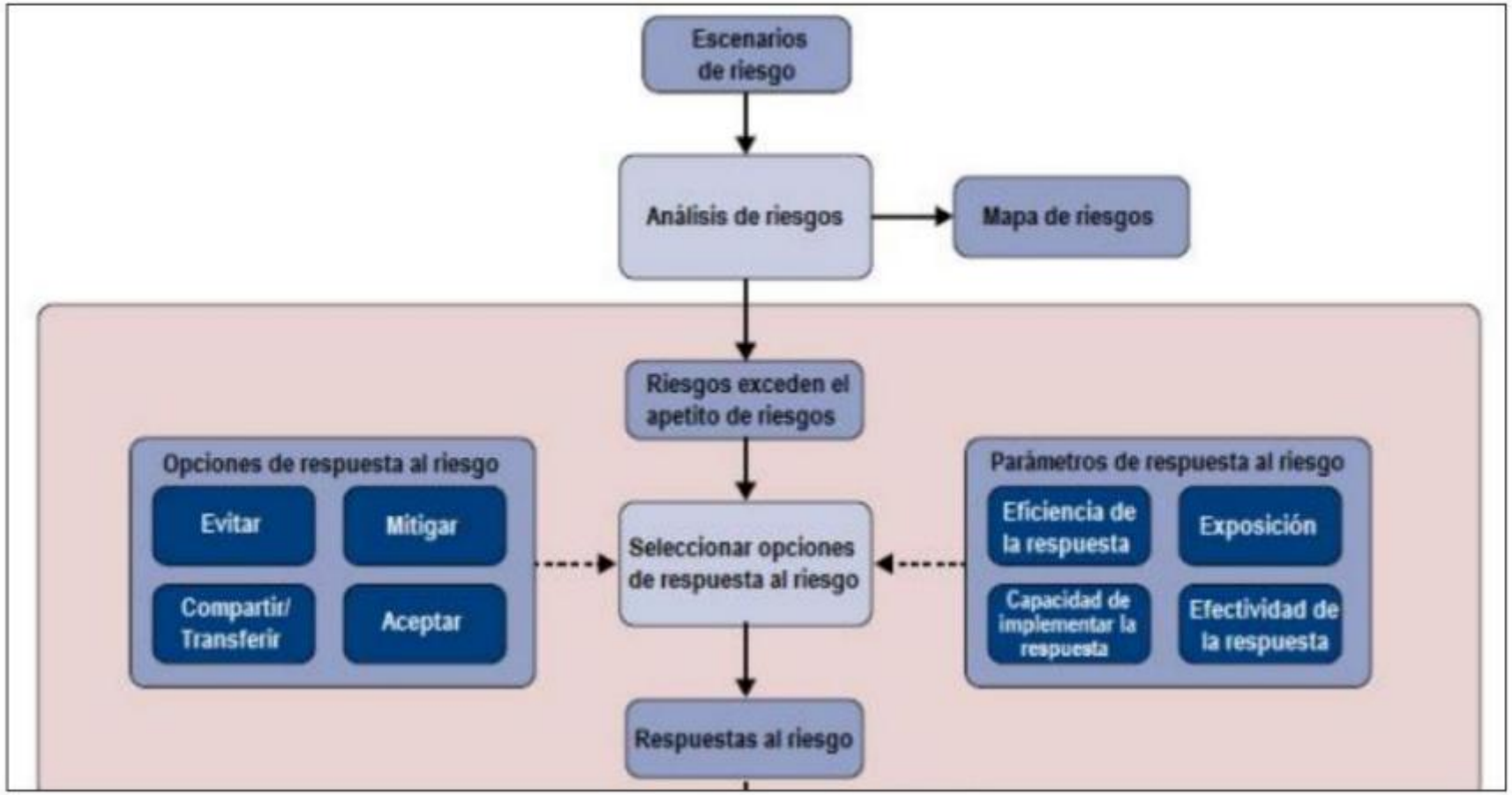
# Riesgos de Ciberseguridad

# Tratamiento de Riesgos – COBIT 5



# Medidas de Protección

International Organization for Standardization
ISO
27002

**CIS Controls**
Version 8

| | |
|---|---|
| 01 | Inventory and Control of Enterprise Assets |
| 02 | Inventory and Control of Software Assets |
| 03 | Data Protection |
| 04 | Secure Configuration of Enterprise Assets and |
| 05 | Account Management |
| 06 | Access Control Management |
| 07 | Continuous Vulnerability Management |
| 08 | Audit Log Management |
| 09 | Email and Web Browser Protections |
| 10 | Malware Defenses |
| 11 | Data Recovery |
| 12 | Network Infrastructure Management |
| 13 | Network Monitoring and Defense |
| 14 | Security Awareness and Skills Training |
| 15 | Service Provider Management |
| 16 | Application Software Security |
| 17 | Incident Response Management |
| 18 | Penetration Testing |

MITRE
ATT&CK™

# Controles de Seguridad de la Información – Visión General

**CIS Controls Version 8**

| |
|---|
| Inventario y Control de los Activos Empresariales |
| Inventario y Control de Activos de Software |
| Protección de los Datos |
| Configuración Segura de Activos y Software Empresarial |
| Administración de Cuentas |
| Gestión de Control de Accesos |
| Gestión Continua de Vulnerabilidades |
| Gestión de Registros de Auditoría |
| Protección del Correo Electrónico y Navegador Web |
| Defensas contra Malware |
| Recuperación de Datos |
| Gestión de la Infraestructura de Red |
| Monitoreo y Defensa de la red |
| Concientización en Seguridad y Formación de Habilidades |
| Gestión de Proveedores de Servicios |
| Seguridad en el Software de Aplicación |
| Gestión de Respuesta a Incidentes |
| Pruebas de Penetración |

**ISO 27002:2022 Controles de Seguridad de la Información**

| |
|---|
| Gobernanza |
| Gestión de Activos |
| Protección de Información |
| Seguridad en Recursos Humanos |
| Seguridad Fisica |
| Seguridad en Sistemas y Redes |
| Seguridad en Aplicaciones |
| Seguridad en la Configuración |
| Gestión de Identidades y Accesos |
| Gestión de Amenazas y Vulnerabilidades |
| Continuidad del Negocio |
| Seguridad en las Relaciones con Proveedores |
| Legal y Cumplimiento |
| Gestión de Eventos de Seguridad de la Información |
| Aseguramiento de la Seguridad de la Información |
| Inteligencia de Amenazas |
| Seguridad en la Nube |
| Privacidad y protección de PII |
| Gestión de Proyectos |
| Protección de Información |

**NIST SP 800-53 Revision 5**

| |
|---|
| Control de Accesos |
| Concientización y Entrenamiento |
| Auditoría y Accountability |
| Evaluación, Autorización y Monitoreo de la Seguridad |
| Gestión de la Configuración |
| Planificación de la Contigencia |
| Identificación y Autenticación |
| Respuesta a Incidentes |
| Mantención |
| Protección de Medios |
| Protección Fisica y del Entorno |
| Planificación |
| Gestión del Programa |
| Seguridad del Personal |
| Transparencia y Procesamiento de PII |
| Evaluación de Riesgos |
| Adquisición de Sistemas y Servicios |
| Protección de Sistemas y Comunicaciones |
| Integridad de la Información y Sistemas |
| Gestión de Riesgos en la Cadena de Suministros |

# La importancia de los controles - Mitre

## SOCIAL ENGINEERING

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with social engineering. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques relevant to social engineering. We do not include the techniques commonly used for follow-up activity (including for example the methods showing how malicious documents can be executed.

| Tactic | Technique | Mitigation |
|---|---|---|
| TA0043: Reconnaissance | T1595: Active Scanning<br>T1592: Gather Victim Host Information<br>T1589: Gather Victim Identity Information<br>T1590: Gather Victim Network Information<br>T1591: Gather Victim Org Information<br>T1598: Phishing for Information<br>T1597: Search Closed Sources<br>T1596: Search Open Technical Databases<br>T1593: Search Open Websites/Domains<br>T1594: Search Victim-Owned Websites | M1056: Pre-compromise<br>M1054: Software Configuration<br>M1017: User Training<br>M1013: Application Developer Guidance<br>M1047: Audit |
| TA0042: Resource Development | T1583: Acquire Infrastructure<br>T1586: Compromise Accounts<br>T1584: Compromise Infrastructure<br>T1587: Develop Capabilities<br>T1585: Establish Accounts<br>T1588: Obtain Capabilities<br>T1608: Stage Capabilities | M1056: Pre-compromise |
| TA0001: Initial Access | T1133: External Remote Services<br>T1566: Phishing<br>T1199: Trusted Relationship<br>T1078: Valid Accounts | M1035: Limit Access to Resource Over Network<br>M1032: Multi-factor Authentication<br>M1030: Network Segmentation<br>M1042: Disable or Remove Feature or Program<br>M1031: Network Intrusion Prevention<br>M1021: Restrict Web-Based Content<br>M1054: Software Configuration |

## RANSOMWARE

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with ransomware software, ransomware groups or both, according to Ransomware techniques in ATT&CK[945]. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques, starting from initial access.

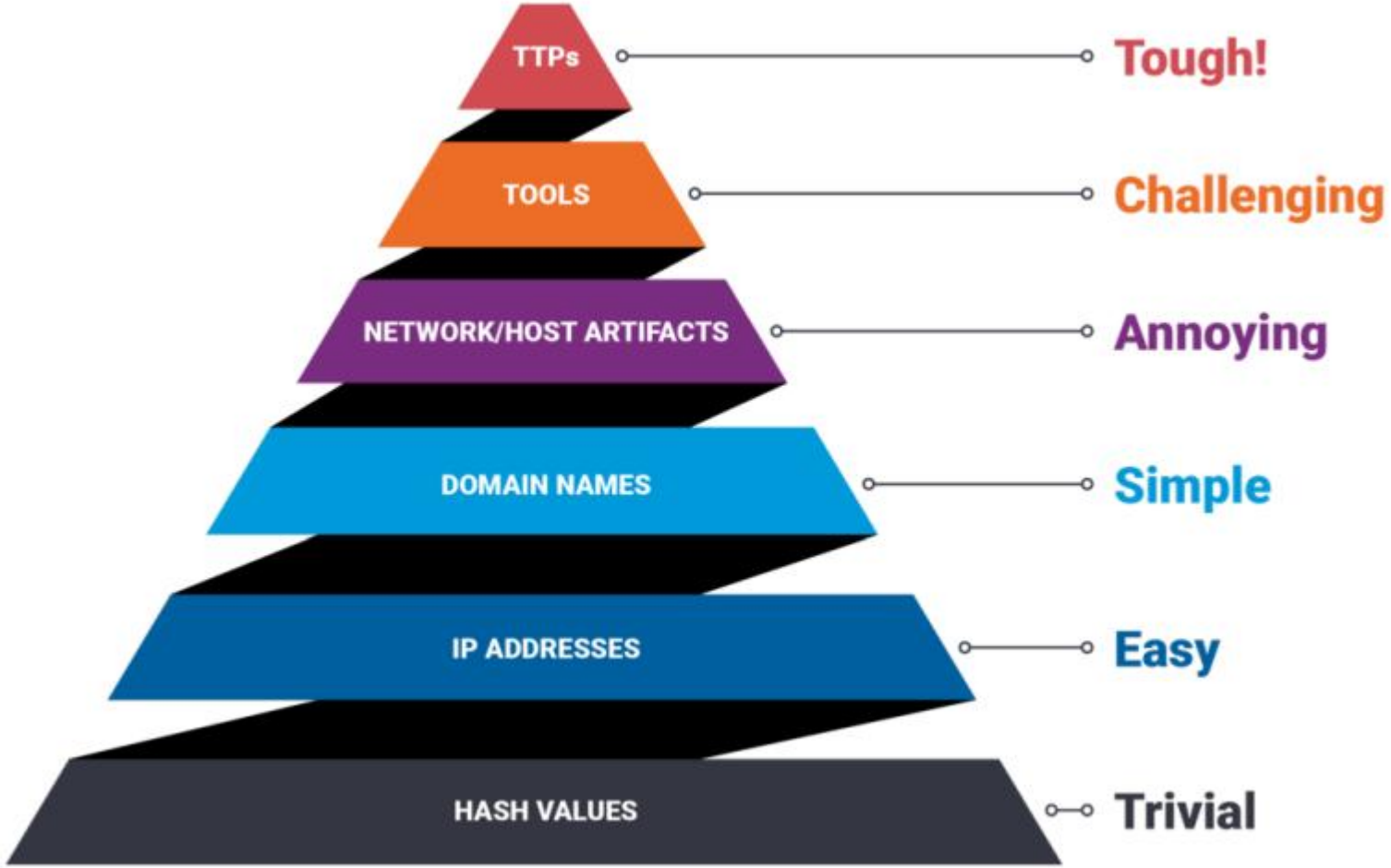
| Tactic | Technique | Mitigation |
|---|---|---|
| TA0001: Initial Access | T1190: Exploit Public-Facing Application<br>T1133: External Remote Services<br>T1566: Phishing<br>T1199: Trusted Relationship | M1048: Application Isolation and Sandboxing<br>M1050: Exploit Protection<br>M1030: Network Segmentation<br>M1026: Privileged Account Management<br>M1051: Update Software<br>M1016: Vulnerability Scanning<br>M1042: Disable or Remove Feature or Program<br>M1035: Limit Access to Resource Over Network<br>M1032: Multi-factor Authentication<br>M1049: Antivirus/Antimalware<br>M1031: Network Intrusion Prevention<br>M1021: Restrict Web-Based Content<br>M1054: Software Configuration<br>M1017: User Training<br>M1018: User Account Management |
| TA0002: Execution | T1106: Native API<br>T1047: Windows Management Instrumentation | M1040: Behaviour Prevention on Endpoint<br>M1038: Execution Prevention<br>M1026: Privileged Account Management<br>M1018: User Account Management |

# 10 técnicas mas empleadas por cibercriminales

| |
|---|
| 1. T1059 COMMAND AND SCRIPTING INTERPRETER |
| 2. T1078 VALID ACCOUNTS |
| 3. T1021.001 REMOTE DESKTOP PROTOCOL |
| 4. T1047 WINDOWS MANAGEMENT INSTRUMENTATION |
| 5. T1490 INHIBIT SYSTEM RECOVERY |
| 6. T1105 INGRESS TOOL TRANSFER |
| 7. T1083 FILE AND DIRECTORY DISCOVERY |
| 8. T1486 DATA ENCRYPTED FOR IMPACT |
| 9. T1190 EXPLOIT PUBLIC-FACING APPLICATION |
| 10. T1489 SERVICE STOP |

https://top-attack-techniques.mitre-engenuity.org/#/

# La pirámide del dolor



# Riesgos de Privacidad

# Análisis de Casos de Riesgos Privacidad - SP

- A continuación se presentan una serie de riesgos de privacidad y su aplicación en el sector publico.
- Se desarrollo en base a información de los principales estándares de riesgos de privacidad.
- Se incorporaron casos comunes de aplicación en el ámbito publico.
- El proceso fue asistida por herramientas de IA, tales como Chap GPT y Copilot.
- El resultado son riesgos generales, con elementos de clasificación que posibilitan comprender una aplicación práctica en el SP de los riesgos, así como elementos claves de auditoría.
- Este material fue desarrollo para un curso ISO 27701 para la Red de Auditores Internos Gubernamentales, en el marco de un convenio de colaboración con el CAIGG.

# Contexto General de Riesgos

🔵 **1. Filtración de datos sensibles de beneficiarios**

**Criticidad:** Alto impacto social; pérdida de confianza ciudadana; riesgo político; exposición mediática inmediata.

🔵 **2. Publicación de actos administrativos con datos personales sin anonimizar**

**Criticidad:** Incumplimiento directo de la Ley 21.719; riesgo de sumarios; observaciones de Contraloría.

🔵 **3. Acceso no autorizado en sistemas legacy**

**Criticidad:** Sistemas antiguos sin trazabilidad → brechas silenciosas y difícil detección; alta probabilidad.

🔵 **4. Procesamiento de datos sin base legal o con finalidad difusa**

**Criticidad:** Vulneración del principio de licitud; sanciones ANPD; cuestionamiento público de legitimidad institucional.

🔵 **5. Interoperabilidad sin evaluación de finalidad o proporcionalidad**

**Criticidad:** Alto riesgo de uso indebido entre organismos; falta de trazabilidad; dependencia de terceros.

🔵 **6. Manejo inadecuado de datos en Atención Ciudadana**

**Criticidad:** Errores humanos, traspaso informal de datos, impresión innecesaria; alta frecuencia de incidentes.

🔵 **7. Retención excesiva de datos por normas administrativas antiguas**

**Criticidad:** Acumulación de PII obsoleta; mayor exposición en caso de incidente; impacto masivo.

🔵 **8. Falta de procedimientos ARCO+ claros y trazables**

**Criticidad:** Reclamos ciudadanos; incumplimiento directo de la ley; pérdida de legitimidad operativa.

🔵 **9. Proveedores externos sin controles adecuados de privacidad (Encargados)**

**Criticidad:** Alto riesgo por tercerización; incidentes que afectan al organismo pero sin control directo.

🔵 **10. Riesgos en teletrabajo o trabajo híbrido**

**Criticidad:** Accesos remotos inseguros; pérdida de documentos físicos; uso indebido de dispositivos personales.

🔵 **11. Incidentes de privacidad no detectados o no reportados a tiempo**

**Criticidad:** Sanciones por notificación tardía; aumento del impacto; incremento del daño reputacional.

🔵 **12. Ausencia de DPIA en programas sociales de alto impacto**

**Criticidad:** Tratamientos de alto riesgo sin análisis previo; exposición política y regulatoria; impacto impredecible.

🔵 **13. Brechas en correos electrónicos institucionales (phishing / fuga)**

**Criticidad:** Exfiltración rápida de información; vectores comunes de incidentes; impacto transversal.

🔵 **14. Acceso privilegiado mal gestionado en bases de datos**

**Criticidad:** Riesgo interno crítico; difícil trazabilidad; posibilidad de uso indebido o extracción silenciosa.

🔵 **15. Tratamiento masivo de datos sin controles de minimización**

**Criticidad:** Procesos que recolectan más información de la necesaria; alto riesgo de exposición.

🔵 **16. Integración con sistemas externos sin garantías técnicas ni legales**

**Criticidad:** Flujos no documentados; dependencia tecnológica; vulneración de principios de transferencia y seguridad.

# Reconociendo los riesgos en el SP

## ⭐ 1. Publicación accidental de datos personales en Transparencia Activa

**Detalle:**

Este es uno de los incidentes más frecuentes en el Estado. Ocurre cuando se publican resoluciones, decretos, contratos, actas o documentos administrativos sin anonimizar nombres, RUT, direcciones, antecedentes socioeconómicos o datos sensibles. Muchas veces se suben documentos "de urgencia" sin revisión.

**Criticidad:** Muy Alta

- Exposición pública inmediata
- Difusión masiva por motores de búsqueda
- Impacto reputacional y político significativo
- Incumplimiento directo de la Ley 21.719

**TIP de Auditoría:**

Verifica si existe un **proceso formal de revisión previa** a la publicación (doble control), con **responsables designados**, y revisa **muestras reales** para confirmar que la anonimización se esté aplicando correctamente.

# Reconociendo los riesgos en el SP

## ⭐ 2. Envío de datos personales por correo a destinatarios equivocados

**Detalle:**

Planillas con PII enviadas a otro servicio, adjuntos incorrectos enviados a ciudadanos, uso de correos personales, reenvíos sin control. Es un riesgo extremadamente común por error humano y ausencia de cifrado.

**Criticidad:** Alta

- Difícil trazabilidad
- Riesgo frecuente y repetitivo
- Fácil de denunciar por terceros

**TIP de Auditoría:**
Revisa si el servicio tiene **política de uso del correo**, cifrado habilitado, y si existen **registros o reportes de incidentes** asociados a correos enviados por error.

# Reconociendo los riesgos en el SP

## ⭐ 3. Sistemas legacy sin trazabilidad ni auditoría de accesos

**Detalle:**

Muchos servicios aún operan sistemas antiguos que no registran accesos, no permiten perfilar permisos por rol, ni cuentan con control de sesiones. Esto genera brechas silenciosas difíciles de detectar.

**Criticidad:** Alta

- Alto riesgo de acceso indebido
- Imposible reconstruir incidentes
- Limitaciones técnicas para aplicar controles modernos

**TIP de Auditoría:**

Solicita **evidencia de logs**, revisa si hay **controles compensatorios**, y valida si el sistema está incluido en el **plan de modernización tecnológica** del organismo.

# Reconociendo los riesgos en el SP

## ⭐ 4. Recolección excesiva de datos personales (no minimización)

**Detalle:**

Trámites que piden datos que no son estrictamente necesarios: número de hijos, estado civil, antecedentes médicos, ingresos, etc. Muchas veces "porque siempre se ha hecho así".

**Criticidad:** Media–Alta

- Incrementa volumen de PII expuesta
- Dificulta retención y eliminación
- Riesgo regulatorio por no justificar finalidad

**TIP de Auditoría:**

Selecciona 3–5 trámites y revisa si **justifican cada dato** solicitado y si existe **análisis de proporcionalidad** documentado.

# Reconociendo los riesgos en el SP

## ⭐ 5. Interoperabilidad con otros organismos sin DPIA ni finalidad clara

**Detalle:**

Flujos de datos entre ministerios, municipios, servicios sociales, Registro Civil u otros, sin análisis formal de proporcionalidad, seguridad o riesgo.

**Criticidad:** Alta

- Uso indebido entre organismos
- Riesgo político si el uso no está bien fundamentado
- Inexistencia de trazabilidad completa del flujo

**TIP de Auditoría:**

Revisa convenios, bases legales y exige **DPIA o justificación de proporcionalidad.** Audita **trazabilidad de flujo** (qué se envía, quién recibe, con qué seguridad).

# Reconociendo los riesgos en el SP

## ⭐ 6. Proveedores externos sin control como Encargados del Tratamiento

**Detalle:**

Servicios cloud, software de RRHH, CRM ciudadanos, plataformas web o call centers sin contratos robustos, sin auditorías ni garantías reales sobre el tratamiento.

**Criticidad:** Muy Alta

- Datos del Estado en manos de terceros sin control
- Riesgo de fuga o uso indebido en subencargados
- Posible incumplimiento contractual y legal

**TIP de Auditoría:**

Revisa políticas de retención, coteja con unidades misionales, y valida si existe un **plan de depuración y eliminación segura** en marcha.

# Reconociendo los riesgos en el SP

## ⭐ 7. Retención indefinida de datos por prácticas administrativas antiguas

**Detalle:**

Expedientes físicos y digitales almacenados por décadas "por si acaso", sin análisis de necesidad o plazos de conservación.

**Criticidad:** Alta

- Acumulación masiva de datos expuestos
- Aumenta impacto en caso de brecha
- Dificulta cumplimiento de derechos ARCO+

**TIP de Auditoría:**

Revisa políticas de retención, coteja con unidades misionales, y valida si existe un **plan de depuración y eliminación segura** en marcha.

# Reconociendo los riesgos en el SP

## ⭐ 8. Procesos ARCO+ lentos, informales o sin trazabilidad

**Detalle:**

Solicitudes sin registro, demoras, respuestas incorrectas, falta de validación de identidad o inexistencia de responsable formal.

**Criticidad:** Alta

- Reclamos ciudadanos
- Incumplimiento directo de la Ley 21.719
- Riesgo reputacional por mala atención

**TIP de Auditoría:**

Solicita el **registro de solicitudes ARCO+**, revisa tiempos de respuesta y verifica si existe un **proceso formal aprobado** y difundido.

# Reconociendo los riesgos en el SP

## ⭐ 9. Exposición de datos de beneficiarios en sitios web o plataformas públicas

**Detalle:**

Listados de subsidios, transferencias, beneficiarios, puntajes socioeconómicos o resultados de programas publicados con datos personales visibles.

**Criticidad:** Muy Alta

- Alto impacto político y social
- Exposición de datos sensibles
- Difusión viral en redes y prensa

**TIP de Auditoría:**

Realiza búsquedas manuales y automatizadas (Google dorks), revisa sitios del organismo y supervisa si existe un **proceso de revisión previa** y una **matriz de riesgo para publicaciones.**

# Reconociendo los riesgos en el SP

## ⭐ 10. Carpetas compartidas o repositorios institucionales con permisos incorrectos

**Detalle:**

Carpetas en SharePoint, Google Drive, OneDrive o servidores institucionales abiertas al público o con permisos heredados que exponen historiales sociales, fichas, documentos o bases completas.

**Criticidad:** Muy Alta

- Exposición silenciosa durante meses o años
- Afecta grandes volúmenes de información
- Alto impacto en auditorías

**TIP de Auditoría:**

Solicita **evidencia de revisión periódica de permisos**, ejecuta una inspección al azar y verifica si existe una **política de control de accesos a carpetas compartidas.**

# Reconociendo los riesgos en el SP

## ⭐ 11. Accesos privilegiados mal gestionados en bases de datos institucionales

**Detalle:**

Usuarios con permisos más altos de lo necesario, cuentas compartidas, administradores sin registro de actividades o sin rotación de credenciales.

**Criticidad:** Alta

- Riesgo interno crítico
- Posibilidad de extracción masiva de datos
- Difícil detección de mal uso

**TIP de Auditoría:**

Revisa la **matriz de accesos**, los **registros de administración**, políticas de segregación de funciones y validación de **rotación de contraseñas.**

# Reconociendo los riesgos en el SP

## ⭐ 12. Incidentes de privacidad no detectados o no reportados oportunamente

**Detalle:**

No existe un proceso formal para identificar, escalar, registrar o notificar incidentes; los funcionarios no saben qué es un incidente ni cuándo reportarlo.

**Criticidad:** Muy Alta

- Incremento del impacto del incidente
- Sanción por notificación tardía ante ANPD
- Pérdida de confianza ciudadana

**TIP de Auditoría:**

Solicita el **registro de incidentes**, revisa tiempos de atención y verifica si existe un **procedimiento de respuesta**, roles asignados y simulaciones recientes.

# Próximas Actividades

# Próximas actividades


MARTES 06 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)


MIÉRCOLES 07 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)


JUEVES 08 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)


VIERNES 09 DE ENERO – 11:00 A 13:00 HRS (GMT-3 Hora Chile)

https://alignment.cl/programa-de-cumplimiento-digital/

# Próximas cursos Avanzados


CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

# Gestión de Riesgos Ciberseguridad y Privacidad

Ciclo de Workshops

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD