CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Gestión de Riesgos de Ciberseguridad

Master Class

Carlos Lobos de Medina

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Contexto
- Estándares de Referencia
- Visión de Procesos
- Estructuras, Roles y Perfil
- Apreciación del Riesgo
- Tratamiento de Riesgos

Profesor

Carlos Lobos de Medina

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

carlos.lobos@usach.cl

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

Contexto

¿Cuál 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"

¿Se pueden alinear los objetivos del negocio con ciberseguridad?

Referencia	Dimensión del BSC	Meta empresarial	Métricas de ejemplo
EG01	Financiera	Portafolio de productos y servicios competitivos	• Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado • Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente • Porcentaje de productos y servicios que proporcionan una ventaja competitiva • Plazo de comercialización para nuevos productos y servicios
EG02	Financiera	Gestión de riesgo de negocio	• Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos • Tasa (ratio) de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes • Frecuencia adecuada de la actualización del perfil de riesgo
EG03	Financiera	Cumplimiento de leyes y regulaciones externas	• Coste de incumplimiento regulatorio, incluyendo liquidacionesy multas • Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa • Número de problemas de incumplimiento señalados por los reguladores o autoridades supervisoras • Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios empresariales
EG04	Financiera	Calidad de la información financiera	• Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa • Coste de incumplimiento regulatorio con respecto a regulaciones financieras
EG05	Cliente	Cultura de servicio orientada al cliente	• Número de interrupciones del servicio al cliente • Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios al cliente cumpla con los niveles de servicio acordados • Número de quejas de los clientes • Tendencia de los resultados de la encuesta de satisfacción al cliente
EG06	Cliente	Continuidad y disponibilidad del servicio del negocio	• Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos • Coste empresarial causado por los incidentes • Número de horas de procesamiento perdidas por el negocio debido a interrupciones inesperadas del servicio • Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados
EG07	Cliente	Calidad de la información de gestión	• Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones • Número de incidentes causados por decisiones erróneas de negocio basadas en información incorrecta • Tiempo que se tarda en proporcionar la información de soporte para permitir la toma de decisiones empresariales eficaces • Puntualidad en la entrega de la información de gestión

Referencia	Dimensión del BSC	Meta empresarial	Métricas de ejemplo
EG08	Interna	Optimización de la funcionalidad de procesos internos del negocio	• Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso del negocio • Niveles de satisfacción de los clientes con las capacidades de prestación de servicios • Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro
EG09	Interna	Optimización de costes de los procesos del negocio	• Relación entre el coste y los niveles de servicio conseguidos • Niveles de satisfacción del consejo de administración y la dirección ejecutiva con los costes de proceso del negocio
EG10	Interna	Habilidades, motivación y productividad del personal	• Productividad del personal comparada con benchmarks • Nivel de satisfacción de las partes interesadas con los niveles de experiencia y habilidades del personal • Porcentaje de personal cuyas habilidades son insuficientes con respecto a la competencia requerida para sus funciones • Porcentaje de personal satisfecho
EG11	Interna	Cumplimiento con las políticas internas	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de las partes interesadas que entienden las políticas • Porcentaje de políticas respaldadas por estándares y prácticas de trabajo eficaces
EG12	Crecimiento	Gestión de programas de transformación digital	• Número de programas ejecutados a tiempo y dentro del presupuesto • Porcentaje de partes interesadas satisfechas con la ejecución del programa • Porcentaje de programas de transformación del negocio suspendidos • Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas periódicamente
EG13	Crecimiento	Innovación de producto y negocio	• Nivel de conciencia y comprensión de las oportunidades de innovación del negocio • Satisfacción de las partes interesadas con los niveles de experiencia e ideas sobre innovación y productos • Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras

¿Se pueden alinear los objetivos del negocio con ciberseguridad?

Referencia	Dimensión del BSC	Meta empresarial	Métricas de ejemplo
EG01	Financiera	Portafolio de productos y servicios competitivos	• Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado • Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente • Porcentaje de productos y servicios que proporcionan una ventaja competitiva • Plazo de comercialización para nuevos productos y servicios
EG02	Financiera	Gestión de riesgo de negocio	• Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos • Tasa (ratio) de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes • Frecuencia adecuada de la actualización del perfil de riesgo
EG03	Financiera	Cumplimiento de leyes y regulaciones externas	• Coste de incumplimiento regulatorio, incluyendo liquidacionesy multas • Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa • Número de problemas de incumplimiento señalados por los reguladores o autoridades supervisoras • Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios empresariales

¿Se pueden alinear los objetivos del negocio con ciberseguridad?

EG04	Financiera	Calidad de la información financiera	• Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa • Coste de incumplimiento regulatorio con respecto a regulaciones financieras
EG05	Cliente	Cultura de servicio orientada al cliente	• Número de interrupciones del servicio al cliente • Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios al cliente cumpla con los niveles de servicio acordados • Número de quejas de los clientes • Tendencia de los resultados de la encuesta de satisfacción al cliente
EG06	Cliente	Continuidad y disponibilidad del servicio del negocio	• Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos • Coste empresarial causado por los incidentes • Número de horas de procesamiento perdidas por el negocio debido a interrupciones inesperadas del servicio • Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados
EG07	Cliente	Calidad de la información de gestión	• Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones • Número de incidentes causados por decisiones erróneas de negocio basadas en información incorrecta • Tiempo que se tarda en proporcionar la información de soporte para permitir la toma de decisiones empresariales eficaces • Puntualidad en la entrega de la información de gestión

¿Se pueden alinear los objetivos del negocio con ciberseguridad?

EG08	Interna	Optimización de la funcionalidad de procesos internos del negocio	• Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso del negocio • Niveles de satisfacción de los clientes con las capacidades de prestación de servicios • Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro
EG09	Interna	Optimización de costes de los procesos del negocio	• Relación entre el coste y los niveles de servicio conseguidos • Niveles de satisfacción del consejo de administración y la dirección ejecutiva con los costes de proceso del negocio
EG10	Interna	Habilidades, motivación y productividad del personal	• Productividad del personal comparada con benchmarks • Nivel de satisfacción de las partes interesadas con los niveles de experiencia y habilidades del personal • Porcentaje de personal cuyas habilidades son insuficientes con respecto a la competencia requerida para sus funciones • Porcentaje de personal satisfecho
EG11	Interna	Cumplimiento con las políticas internas	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de las partes interesadas que entienden las políticas • Porcentaje de políticas respaldadas por estándares y prácticas de trabajo eficaces
EG12	Crecimiento	Gestión de programas de transformación digital	• Número de programas ejecutados a tiempo y dentro del presupuesto • Porcentaje de partes interesadas satisfechas con la ejecución del programa • Porcentaje de programas de transformación del negocio suspendidos • Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas periódicamente
EG13	Crecimiento	Innovación de producto y negocio	• Nivel de conciencia y comprensión de las oportunidades de innovación del negocio • Satisfacción de las partes interesadas con los niveles de experiencia e ideas sobre innovación y productos • Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras

Es una Necesidad de Cumplimiento Normativo?

- Totalmente
- En prácticamente cualquier marco de referencia actual la gestión de riesgos es necesaria.
- A modo de ejemplo, a nivel internacional, que lo exige:
  - Nist CSF 2.0
  - HIPPA
  - ISO 27001 (y en toda ISO que defina un Sistema de Gestión)
  - GDPR
  - DORA
- A modo de ejemplo, en Chile, que lo exige:
  - Ley de Gobiernos Corporativos
  - Ley Marco de Ciberseguridad
  - RAN 20-10 - CMF
  - Estándar de Ciberseguridad SEN – Coordinador Eléctrico

Cumplimiento o Cumplo y Miento

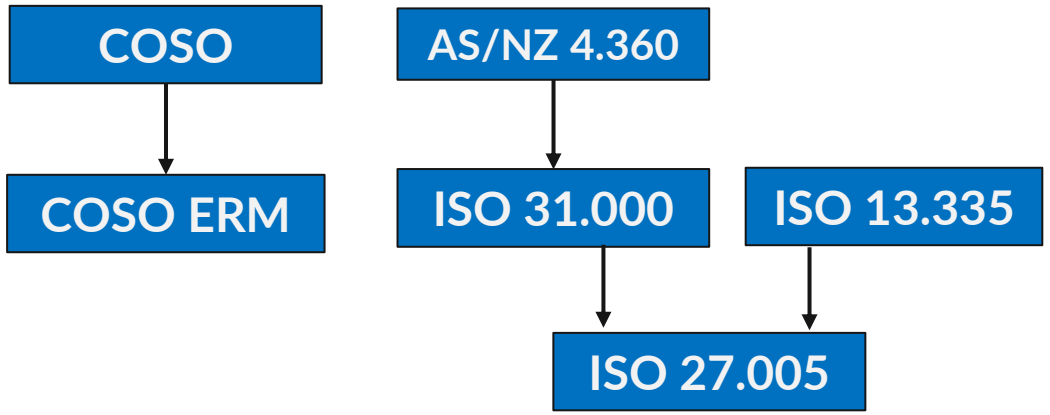
- Es como usted perciba y entienda la gestión de riesgos
- Si lo articula al negocio, será siempre más fácil obtener apoyo del negocio, de la dirección y sus iniciativas, en consecuencia obtendrá mayor visibilidad y quizás también mayores recursos.
- Si crees que el problema es un malware, la fuga de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

Estándares de Referencia

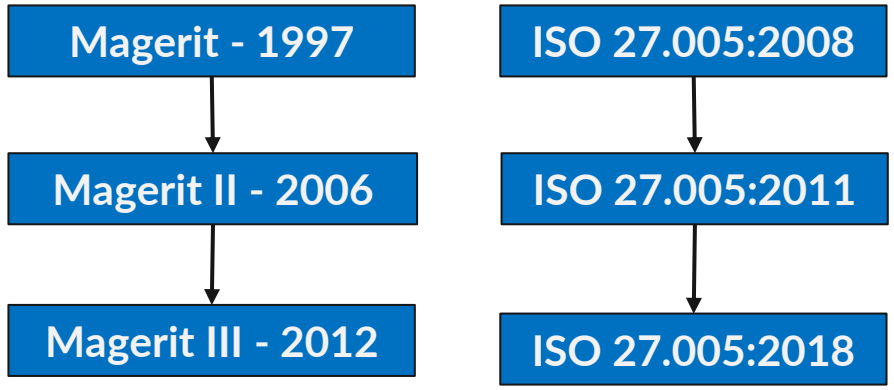
Estandares de Referencia

- 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

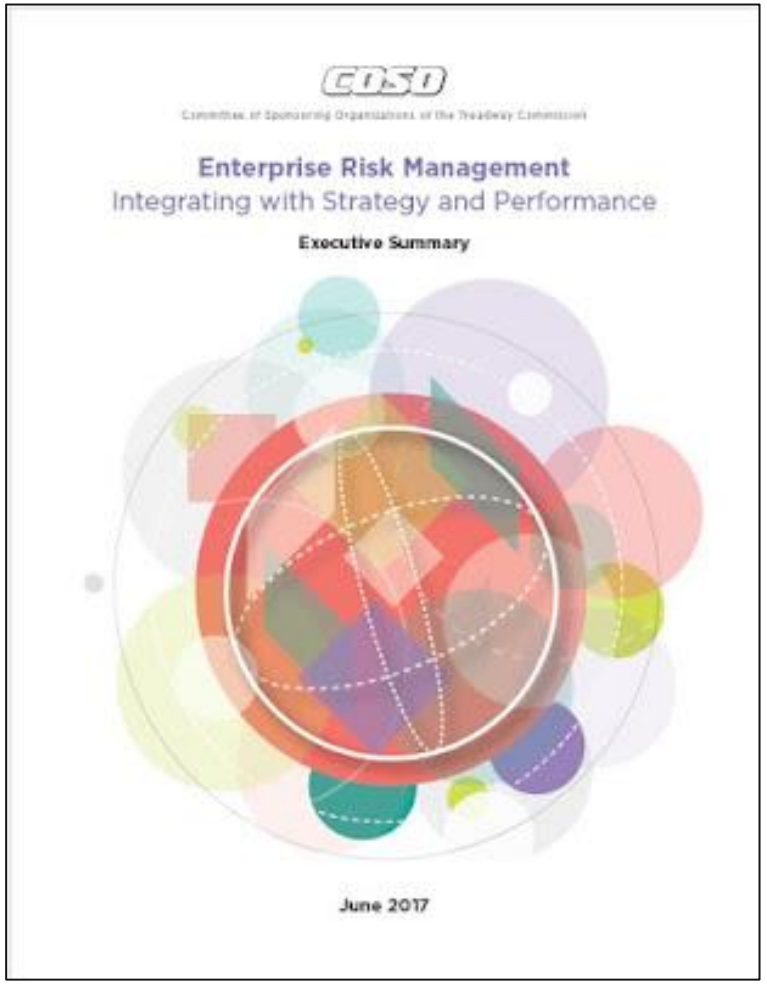
Evolución Global

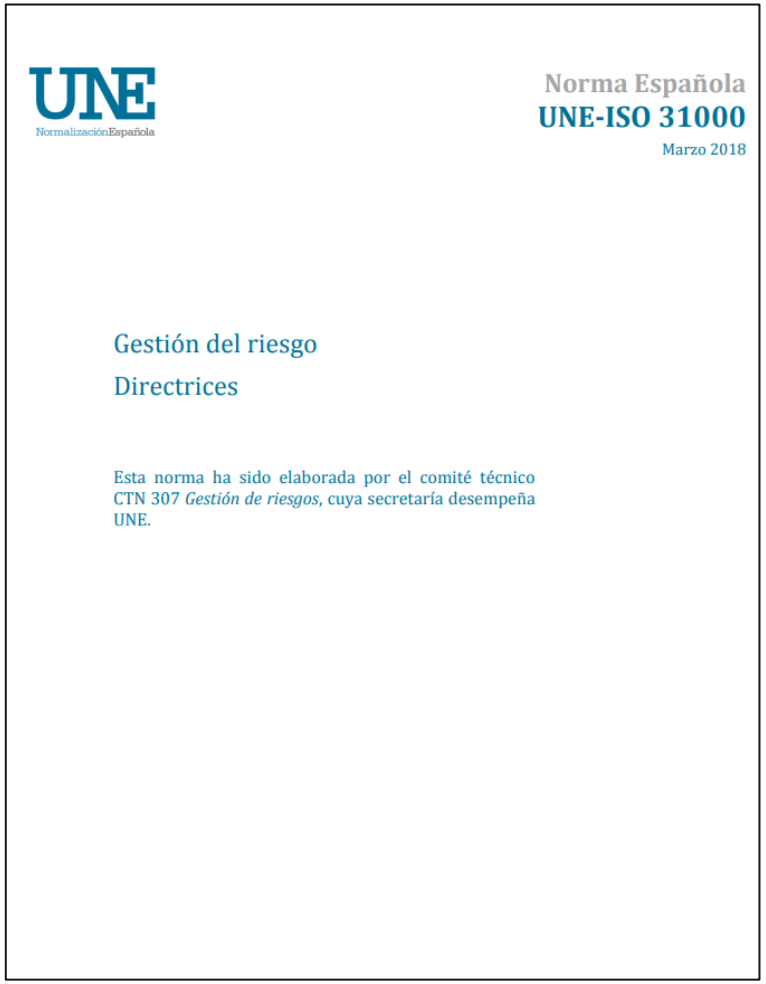


Estándares de Riesgo de TI



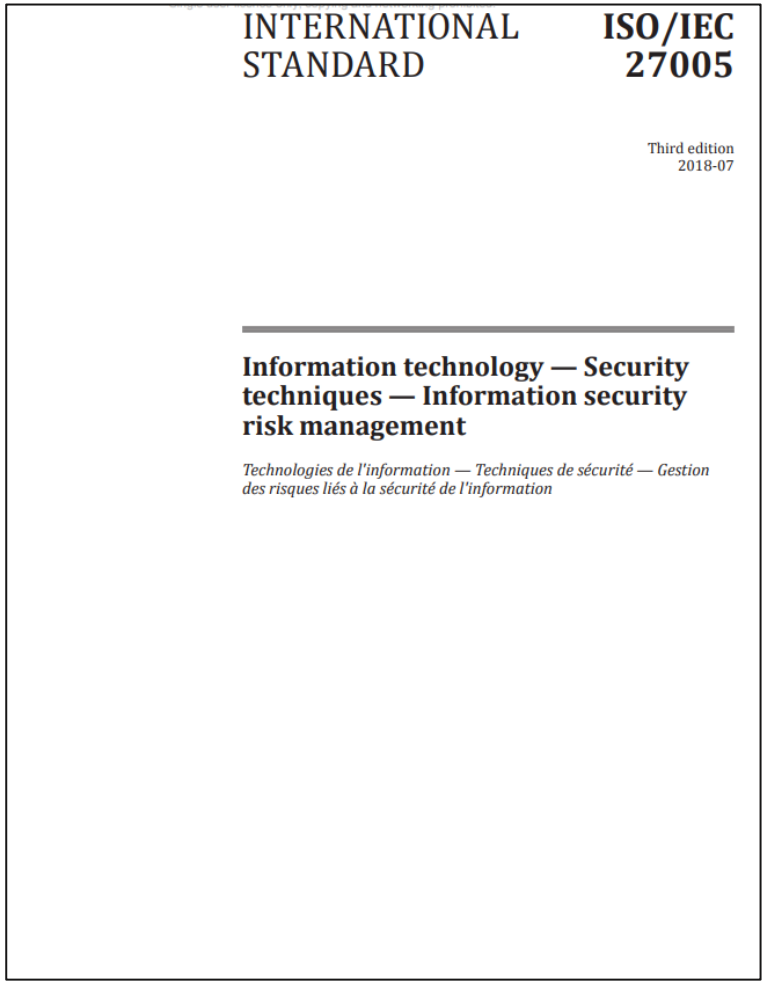
Gobierno y Gestión de Riesgo

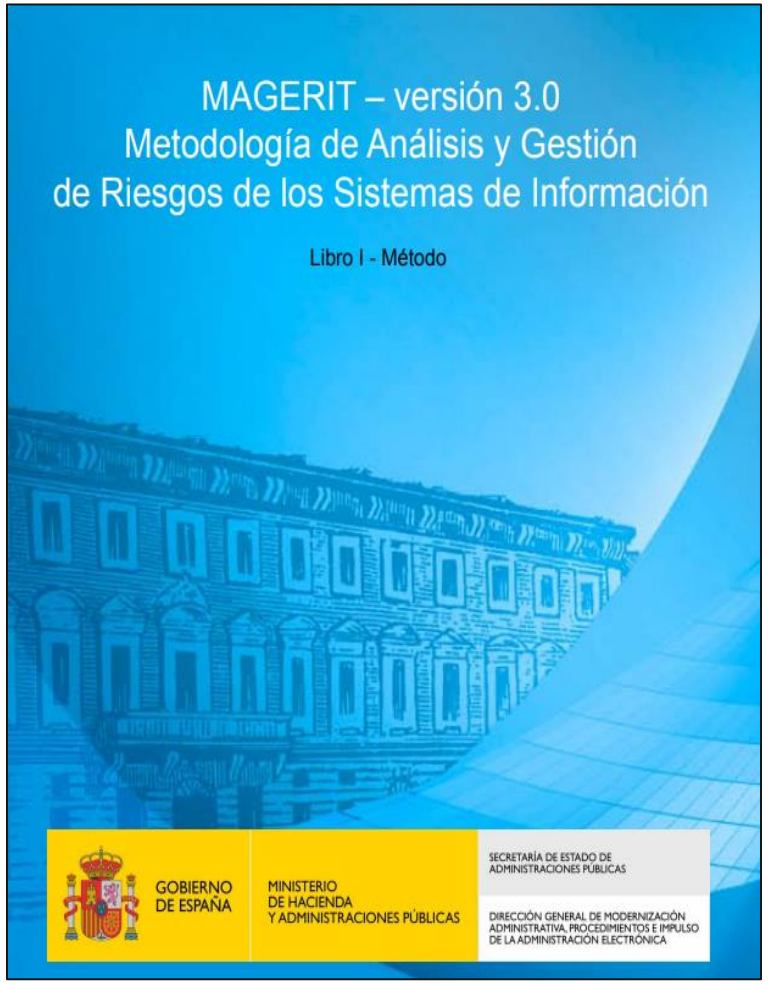




- Estándares de Gestión de Riesgos de mayor adopción.
- COSO ERM transversal al gobierno corporativo, con foco de la misión, visión y estrategia. Muy empleado en grandes organizaciones.
- ISO 31000 centrado en el proceso, más ágil y dinámico en la implementación. Muy empleado a nivel global.
- Excelentes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

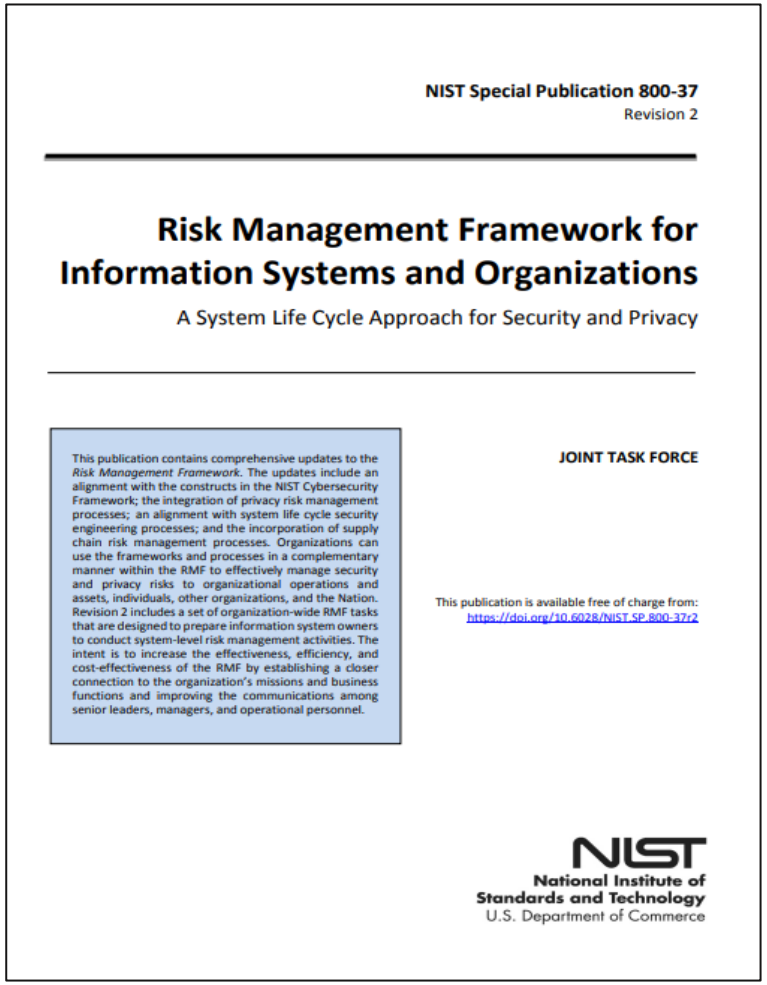
Gestión de Riesgo de TI y Seguridad de la Información





- 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 Riesgo de Ciberseguridad



NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

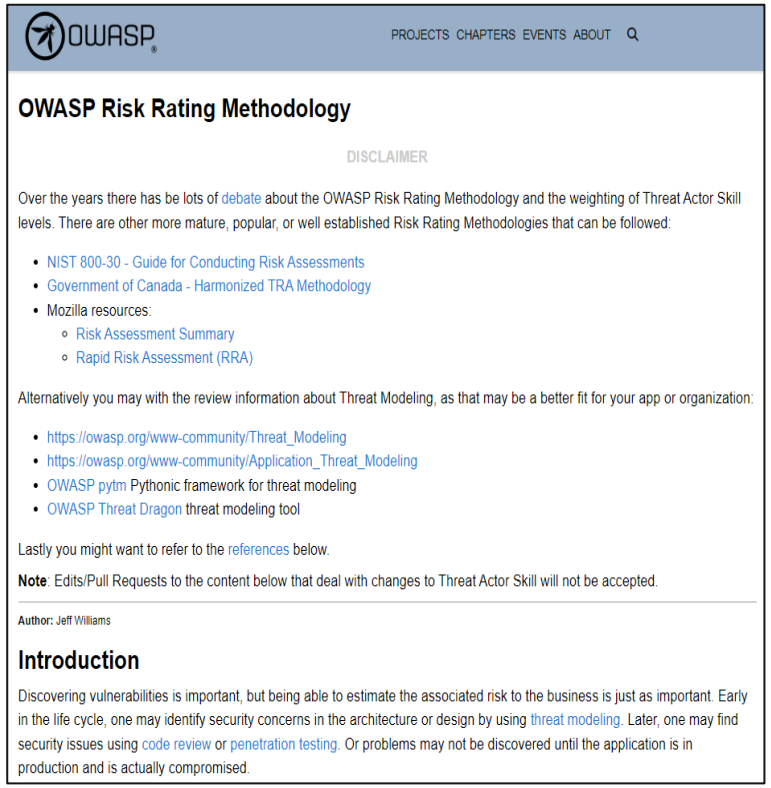
A System Life Cycle Approach for Security and Privacy

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.

Estandares de Referencia

- Veremos más de los modelos de referencia a continuación, para entender sus potenciales ámbitos de aplicación, no obstante ellos son muy integrables.

- La comprensión de las buenas prácticas no solo pasa en conocerlas, sino como uno puede sacar lo mejor de estas, cuando y como poder aplicarlas.

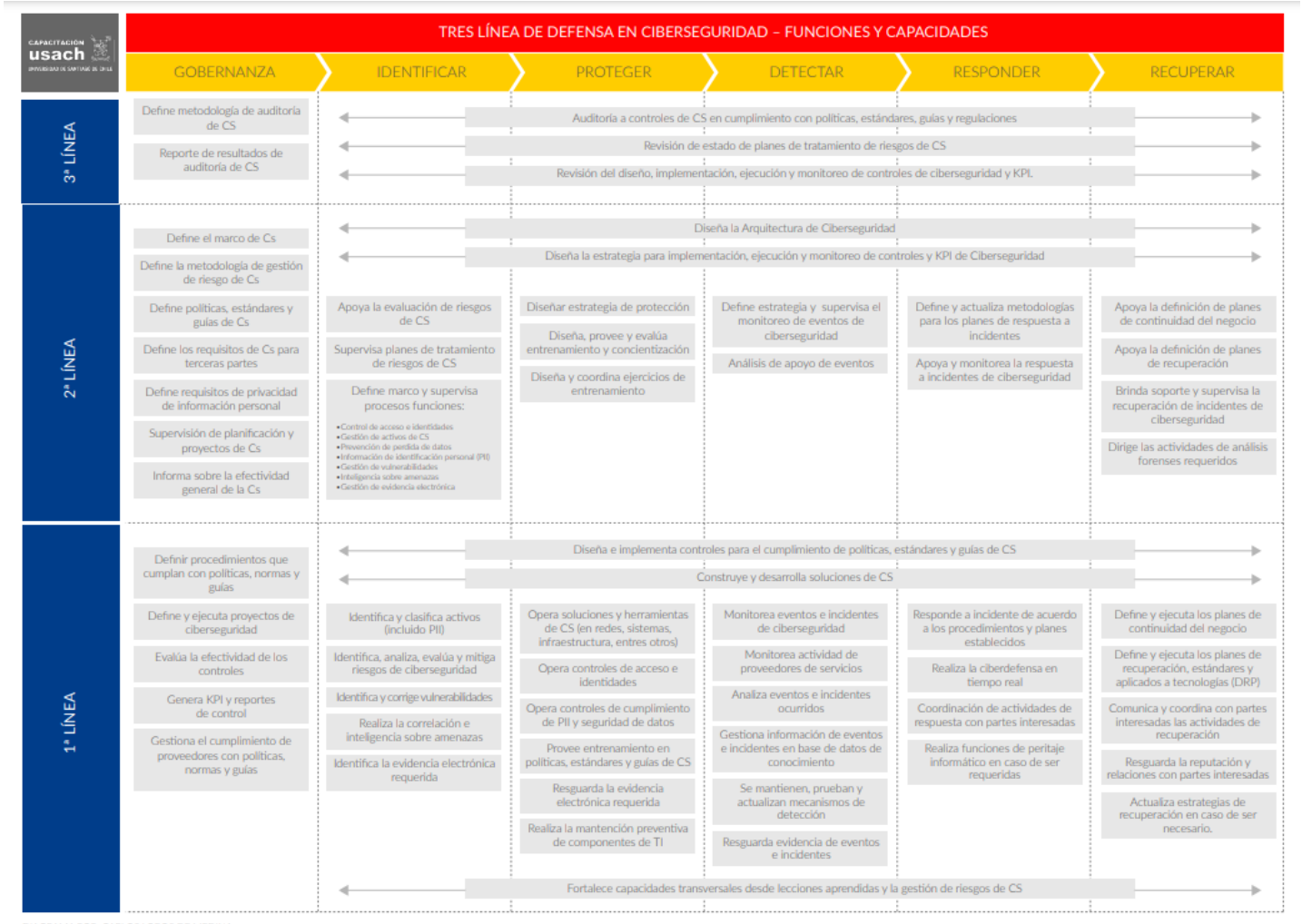
- A priori, no hay ningún modelo optimo de riesgos que uno pueda recomendar a una organización, hay muchos elementos que conocer:

  - Cultura Organizacional
  - Objetivos de Negocio
  - Cumplimiento Normativo
  - Contexto de Riesgos
  - Madurez de Procesos Tecnológicos
  - Madurez de la Ciberseguridad
  - Estructura Organizacional
  - Capacidades en Ciberseguridad

Estructuras, Roles y Perfil

Tres líneas de Defensa

Tres líneas de Defensa



Visión de Procesos

COSO ERM – Principios de ERM

- COSO ERM establece 20 principio para la gestión de riesgos, organizados en 5 componentes.

Gobierno y Cultura

1. Ejerce la Supervisión de Riesgos a través del Consejo de Administración
2. Establece Estructuras Operativas
3. Define la Cultura Deseada
4. Demuestra Compromiso con los Valores Clave
5. Atrae, Desarrolla y Retiene a Profesionales Capacitados

Estrategia y Establecimiento de Objetivos

6. Analiza el Contexto Empresarial
7. Define el Apetito al Riesgo
8. Evalúa Estrategias Alternativas
9. Formula Objetivos de Negocio

Desempeño

10. Identifica el Riesgo
11. Evalúa la Gravedad del Riesgo
12. Prioriza Riesgos
13. Implementa Respuestas ante los Riesgos
14. Desarrolla una Visión a nivel de Cartera

Revisión y Monitorización

15. Evalúa los Cambios Significativos
16. Revisa el Riesgo y el Desempeño
17. Persigue la Mejora de la Gestión del Riesgo Empresarial

Información, Comunicación y Reporte

18. Aprovecha la Información y la Tecnología
19. Comunica Información sobre Riesgos
20. Informa sobre el Riesgo, la Cultura y el Desempeño

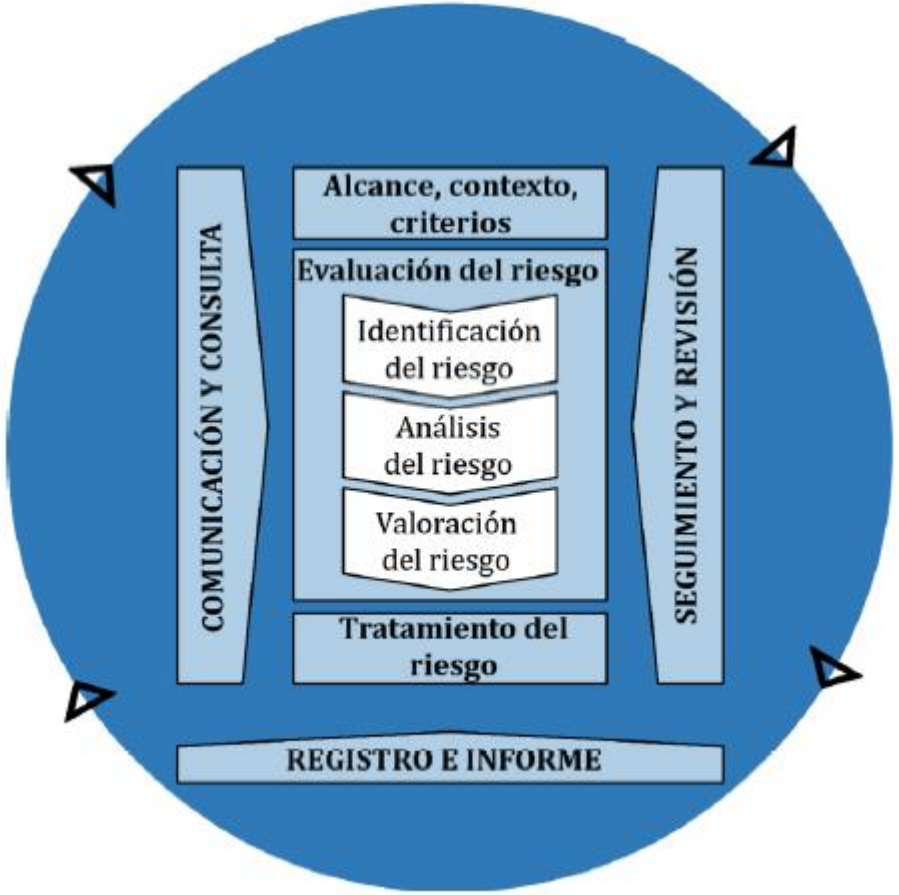
ISO 31.000 e ISO 27.005

- ISO 31.000 es el modelo de mayor adopción a nivel global, principalmente fuera de Norteamérica y muy de la mano con las necesidades de otros estándares ISO.
- Establece cada una de las etapas del proceso completamente, con menor integración al Gobierno Corporativos con respecto a COSO, razón por la cual es más fácil de implementar.
- La ISO 27.005 se basa en el proceso establecido en la ISO 31.000, siendo el marco de referencia que mejor se adapta a ISO 27.001, su contra que es más complejo de implementar.
- A continuación se presentan similitudes y diferencias.

Proceso de Gestión de Riesgos – ISO 31.000 → ISO.27.005

ISO 31000

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



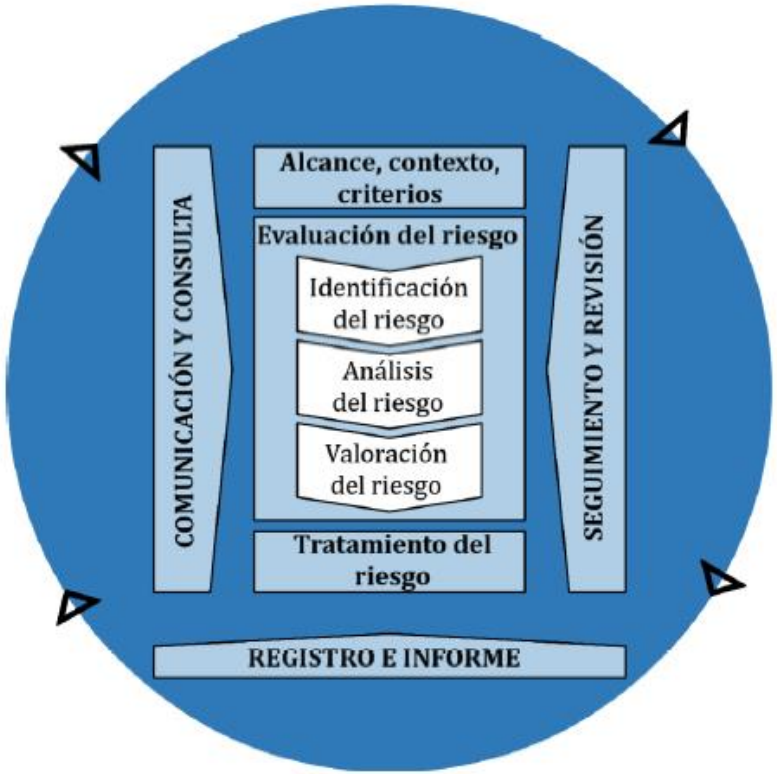
ISO 27005

- 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

Revisión del Proceso desde 31.000 e ISO 27.001

- ISO 31.000:2018

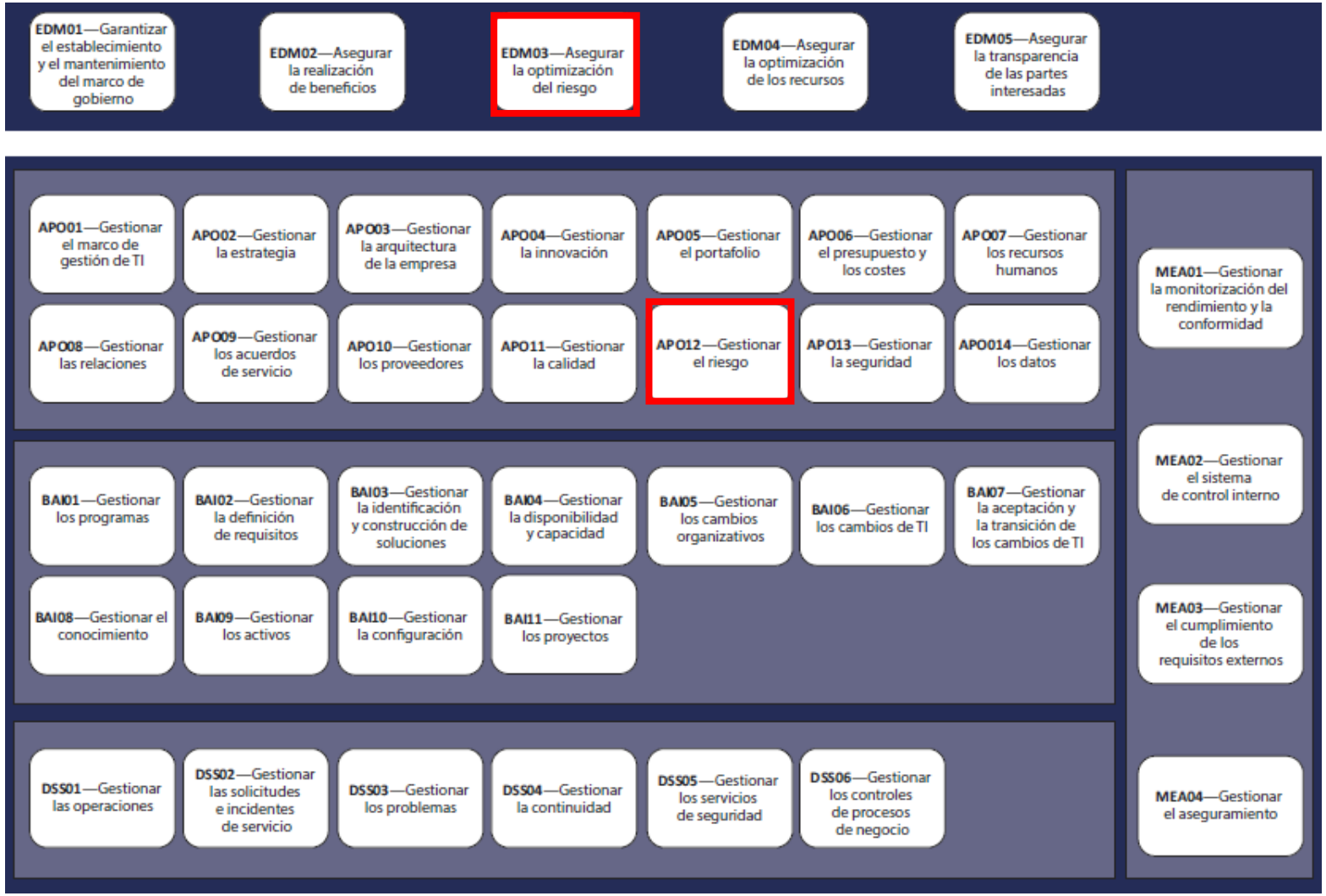


- ISO 27.001:2017

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

- Revisaremos los requisitos y prácticas relacionadas desde ambas normas y la integraremos con ejemplos.

COBIT 2019 - Objetivos de Gobierno y Gestión



Actividades claves del Proceso – COSO ERM

EDM03.01 Evaluar la gestión de riesgos

EDM03.03 Monitorizar la gestión de riesgos.

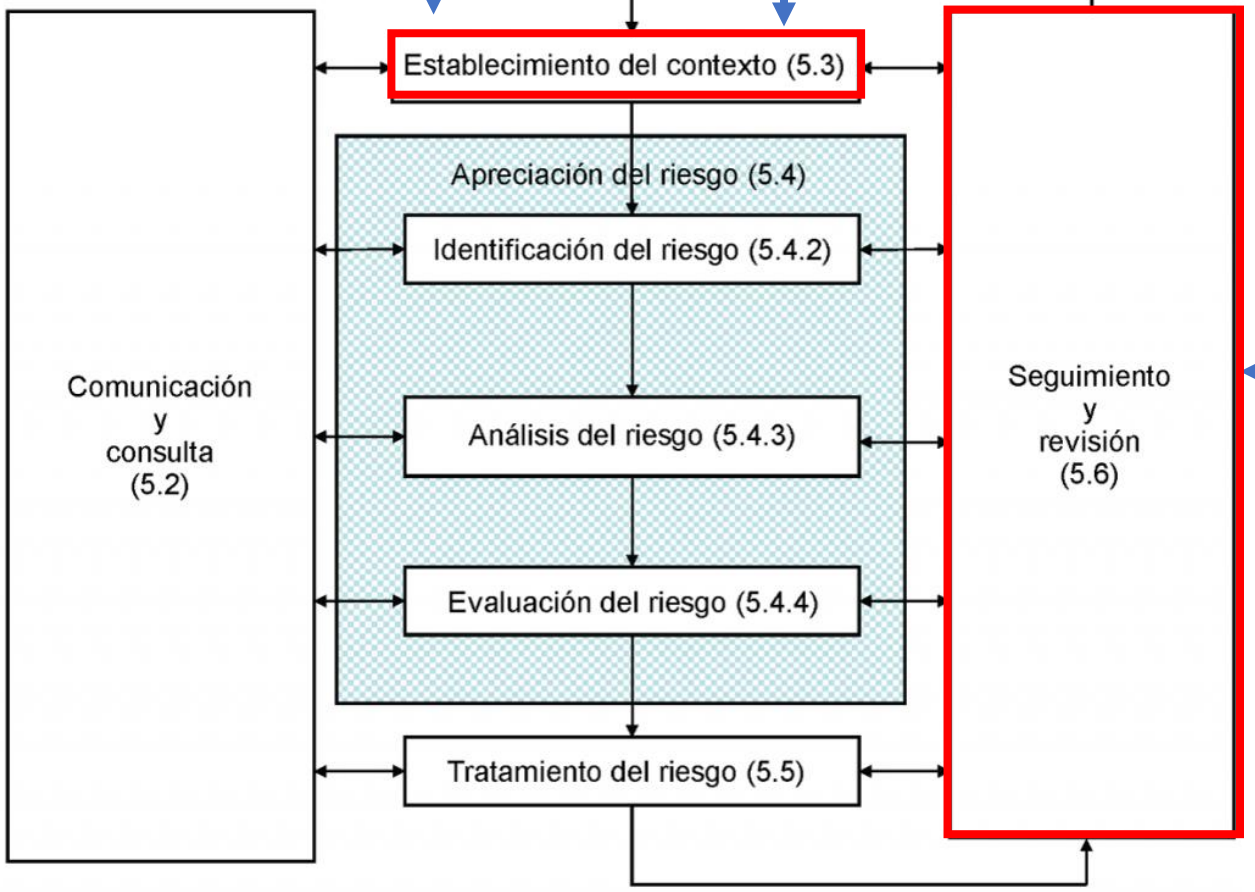
Gobierno y Cultura	Estrategia y objetivos	Desempeño	Revisión	Información, comunicación y reporte
1. La Junta Directiva ejerce supervisión sobre los riesgos 2. Establece estructuras operativas 3. Define la cultura deseada 4. Demuestra compromiso con los valores éticos 5. Atrae, desarrolla y retiene individuos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

EDM03.02 Dirigir la gestión de riesgos.

Actividades claves del Proceso – ISO 31.000

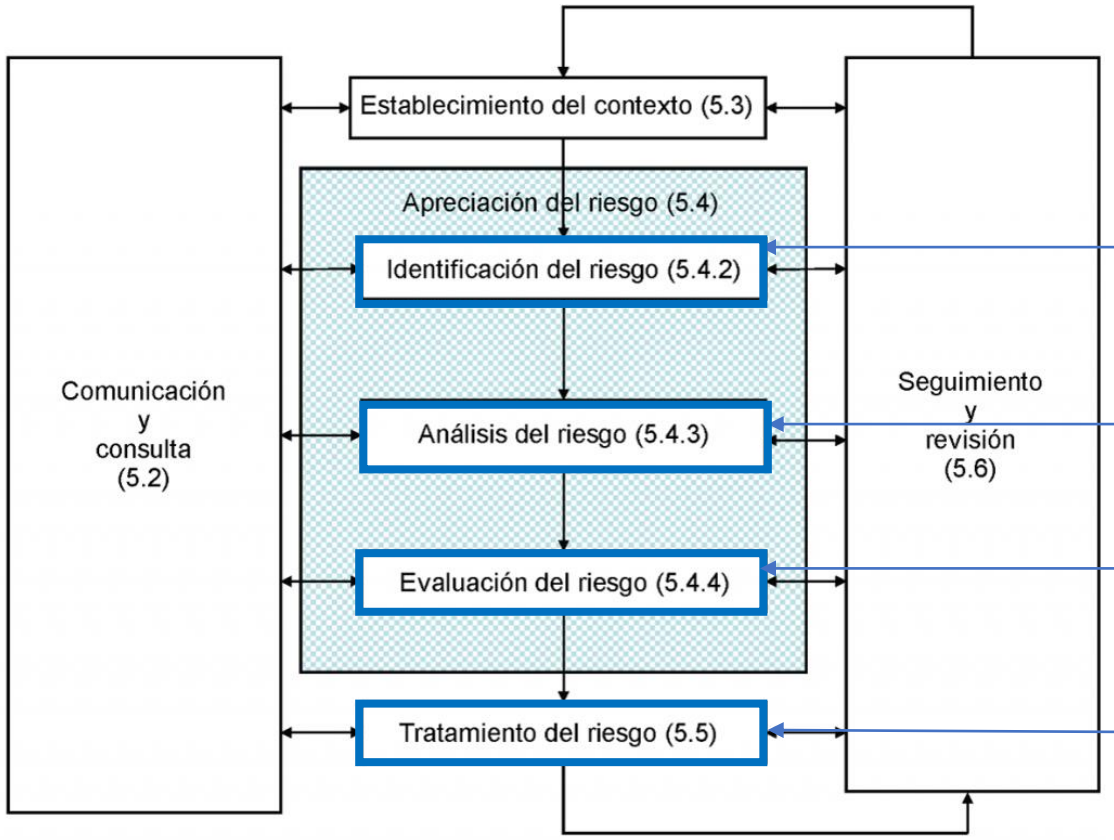
EDM03.01 Evaluar la gestión de riesgos

EDM03.02 Dirigir la gestión de riesgos.



EDM03.03 Monitorizar la gestión de riesgos.

APO12 - Gestionar los Riesgos (ISO 31.000)



APO12.01 Recopilar datos
APO12.03 Mantener un perfil de riesgo

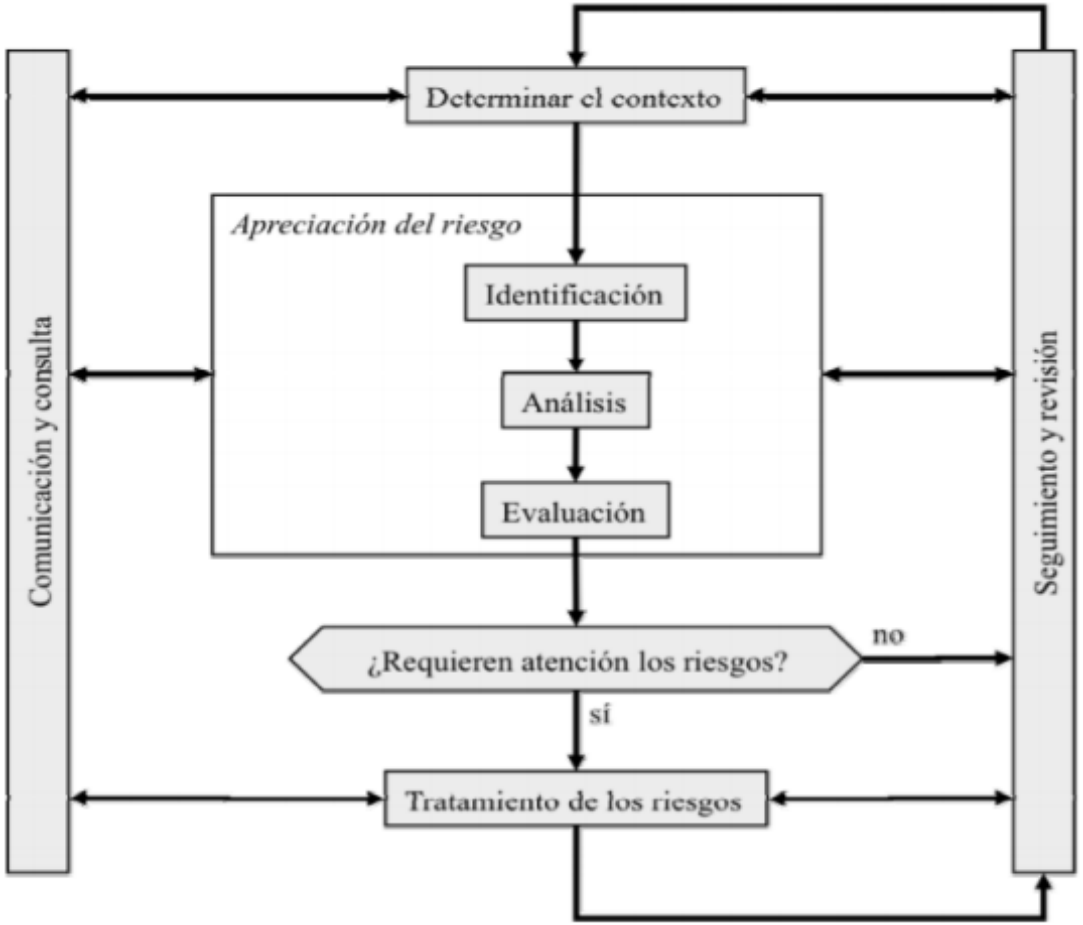
APO12.02 Analizar el riesgo

APO12.04 Expresar el riesgo

APO12.05 Definir un portafolio de acciones
APO12.06 Responder al riesgo

Magerit – Método de Análisis de Riesgos

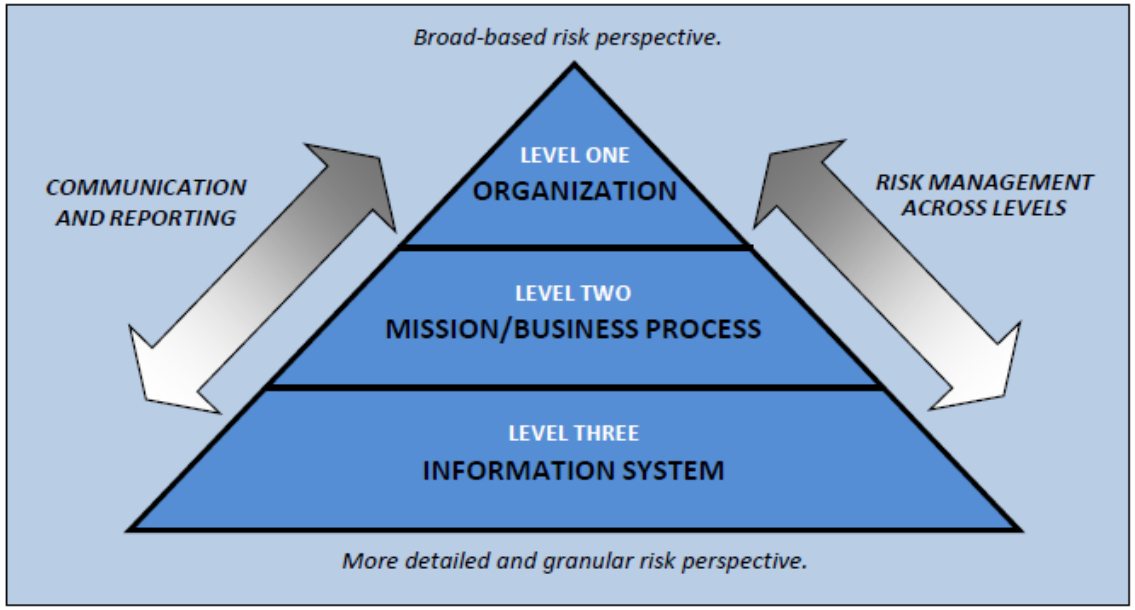
- Proceso similar a ISO 31.000
- Buena definición de activos
- Referencias de amenazas
- Referencias de salvaguardas



NIST 800-37

- El más distintos de los modelos vistos.
- Provee una visión centrada solo en lo tecnológico con una buena integración en la misión, visión y objetivos organizacionales.
- Es un completo framework, el cual viene relacionado con un enfoque de controles muy potente NIST 800-53.
- Provee variados aspectos de interés:
  - Clasificación de activos
  - Tablas de evaluación simples
  - Caracterización de amenazas y vulnerabilidades
  - Ponderación de vulnerabilidades
- Ofrece mecanismos un poco disruptivos al momento de gestionar riesgos.

Enfoque de Riesgos NIST 800-37



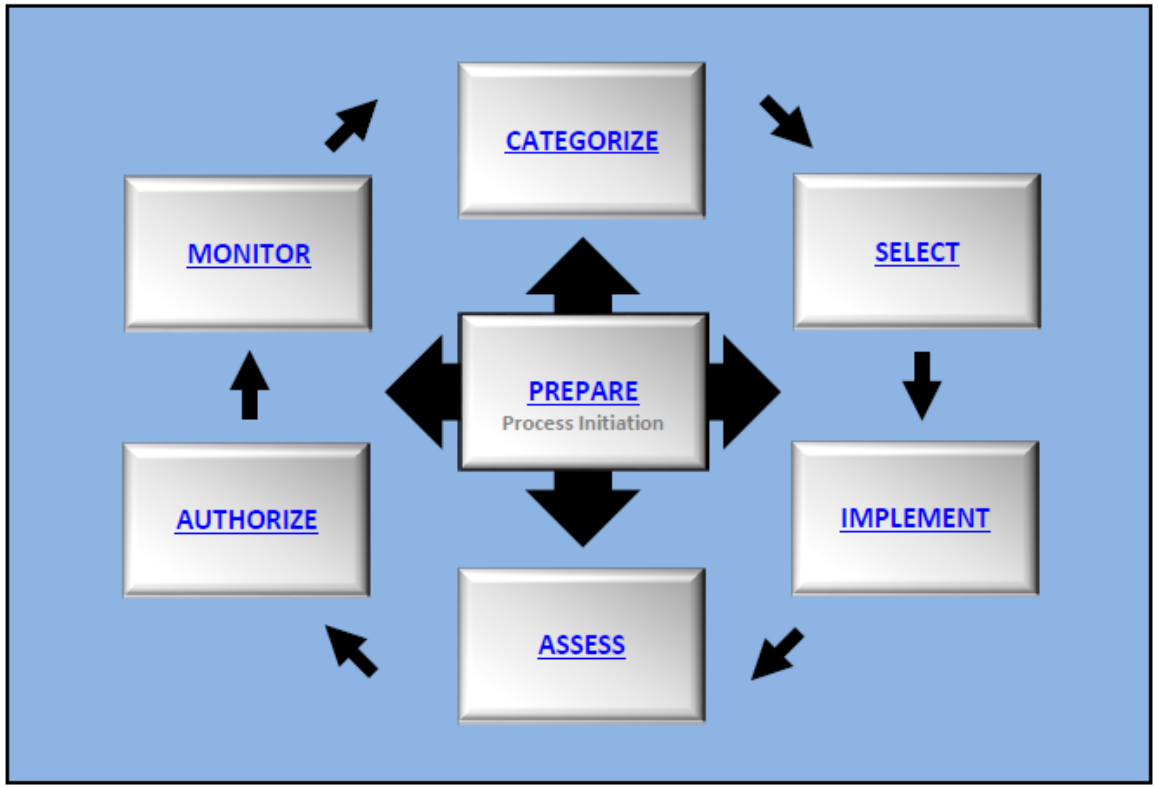
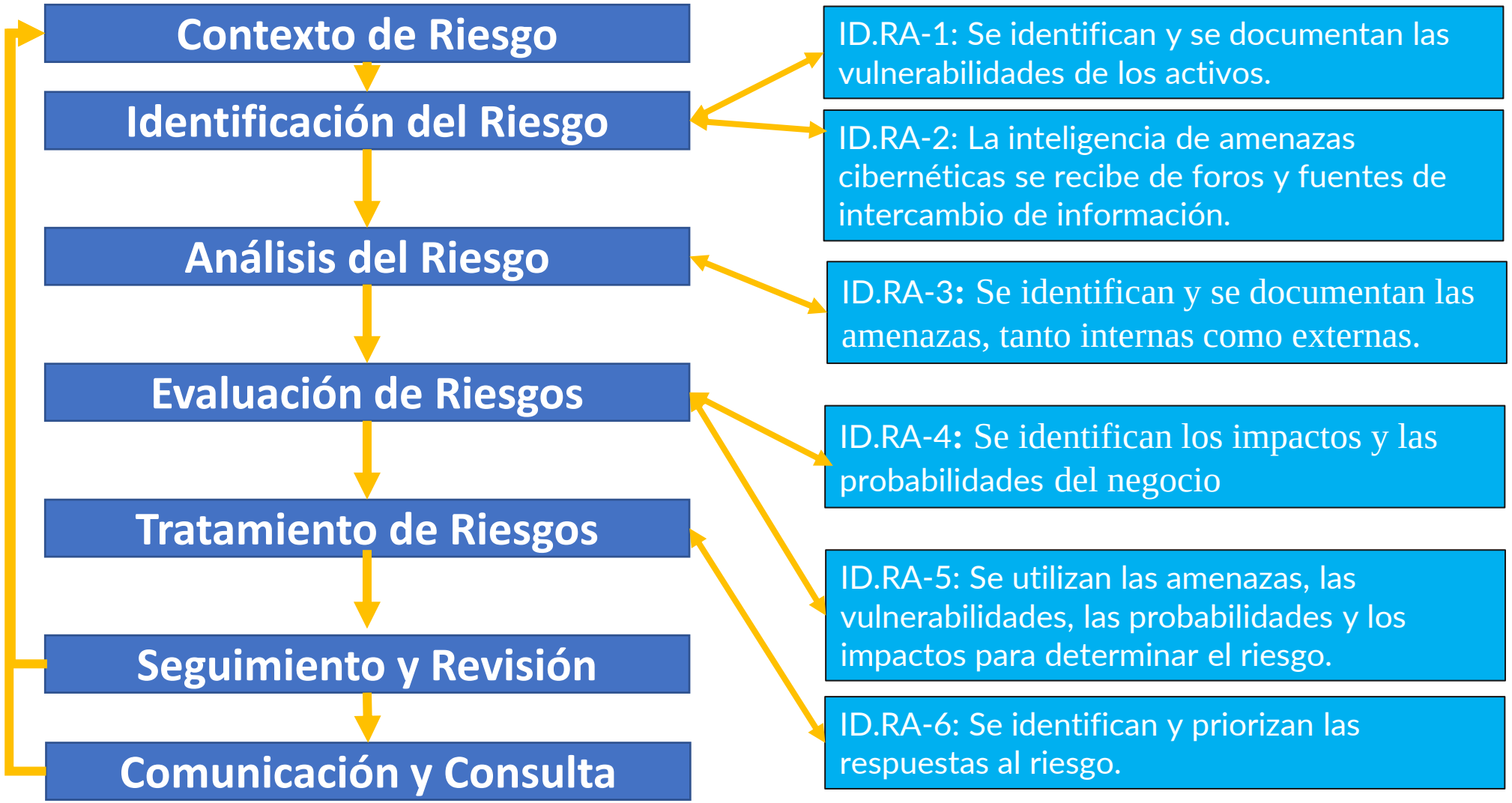
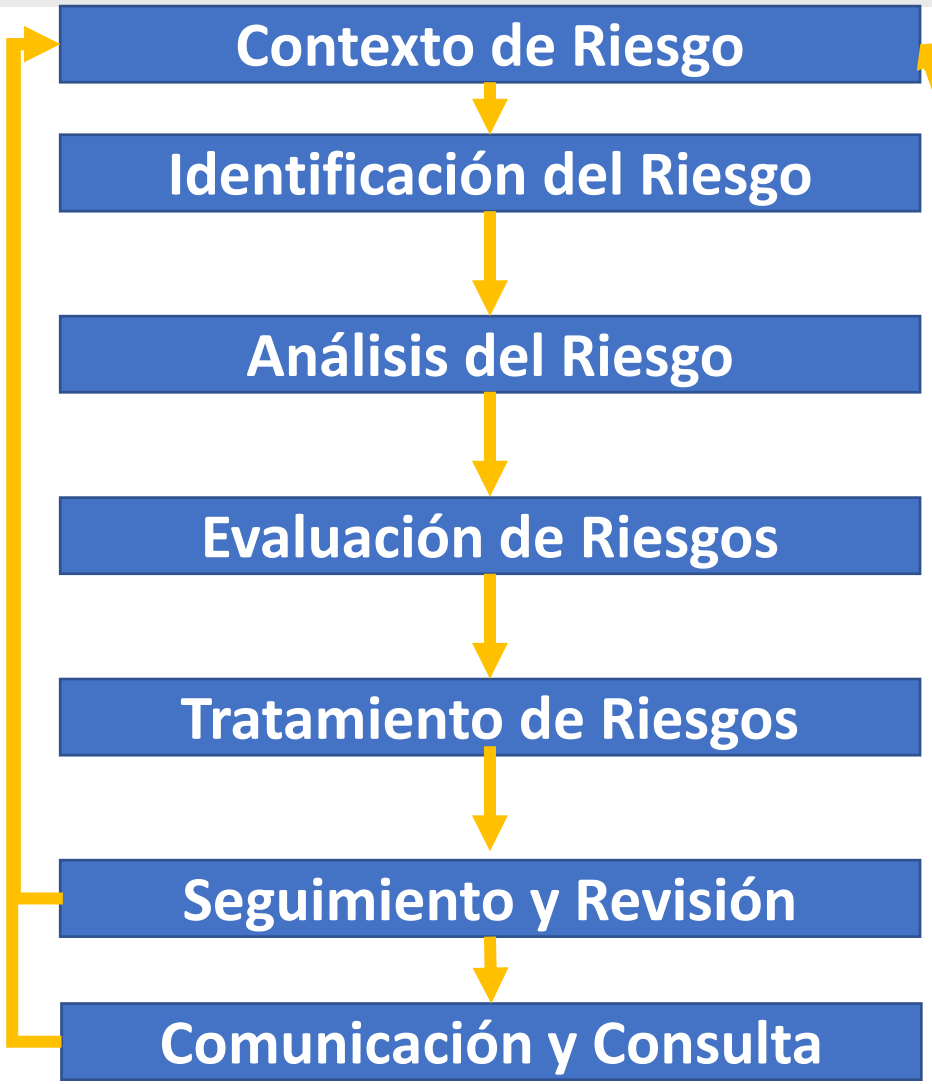


FIGURE 2: RISK MANAGEMENT FRAMEWORK

Mapeo con las etapas claves del proceso de Riesgos – ID-RA



Mapeo con las etapas claves del proceso de Riesgos – ID-RM



ID.RM-1: Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.

ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente

ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.

Apreciación del Riesgo

Identificación de Activos

- **ISO 31.000:2018**

- 6.4.2 Identificación del Riesgo
- El propósito es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos.

- Se deben considerar diversos factores:
  - ....
  - Causas y eventos
  - Amenazas y oportunidades
  - Vulnerabilidades y capacidades
  - .....

- **ISO 27.001:2017**

c) identifique los riesgos de seguridad de la información:

1) llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,

2) identificando a los dueños de los riesgos;

- Implica gestionar los activos de información tal como se describió en el modulo de Activos de Información

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN									
Nombre Activo	Id. o código	Tipo	Ubicación	Responsable / dueño	Soporte	Persona Autorizada para Manipular	Persona autorizada para Copiar	Medio de almacenamiento	Tiempo de retención
Base de Datos de Postulantes	ID-0001	Base de Datos	Google.com	Director Comercial	Digital	Coordinadora Ejecutiv	No aplica	Nube Proveedor	1 año
Plataforma Moodle	ID-0002	SW	Amazon.com	Director Academico	Digital	Profesores	Soporte Técnico	Nube Proveedor	1 año
Plataforma Vimeo	ID-0003	SW	Vimeo.com	Jefe Comunicaciones	Digital	Soporte Técnico	No aplica	Nube Proveedor	1 año
Plataforma Webex	ID-0004	SW	Servidor Webex	Jefe Comunicaciones	Digital	Soporte Técnico	No aplica	Nube Proveedor	3 meses
Profesores	ID-0005	Persona	Ubicación Personal	Director Academico	No Aplica	No aplica	No aplica	No aplica	No Aplica
Material del Curso	ID-0006	Documento	Dropbox.com	Director Academico	Digital	Profesores	Soporte Técnico	Servidor de Directorio	3 años
Soporte Técnico	ID-0007	Persona	Ubicación Personal	Director de TI	No Aplica	No aplica	No aplica	No aplica	No Aplica

- Nótese que la norma no establece que sea por activos de información.

Ejemplos - Incibe

- ***Nombre:*** Puede incluir modelo, marca, nombre descriptivo, etc.
- ***Descripción:*** No es necesario que sea demasiado extensa, pero sí debe contener información sobre el uso del activo.
- ***Identificador:*** Código único para el activo. Debe seguir un patrón elegido por la empresa
- ***Tipo:*** Recoge el grupo al que pertenece el activo.
- ***Propietario:*** Todo activo debe tener un propietario. Este será el encargado de tomar decisiones como el reemplazo del mismo.
- ***Responsable:*** El responsable es la persona encargada de que el activo se encuentre operativo, así como de gestionar los accesos al mismo. En muchas ocasiones podrá coincidir con el propietario.
- ***Ubicación:*** Lugar donde se encuentra físicamente el activo. Si se trata de un activo físico la ubicación será un lugar, si se trata de un activo lógico la ubicación será un activo físico.
- ***Valoración del activo:*** Valor a asignar al activo que permita evaluar su impacto en el sistema. Para ello pueden tenerse en cuenta diversos parámetros como por ejemplo:
  - ***Disponibilidad:*** Valor cualitativo o cuantitativo que determine la importancia que tiene la ausencia del activo.
  - ***Integridad:*** Valor cualitativo o cuantitativo que determine las repercusiones para el negocio que tendría la modificación del activo sin autorización.
  - ***Confidencialidad:*** Valor cualitativo o cuantitativo que determine el grado de confidencialidad que requiere el activo.
  - ***Criticidad:*** Valor que determina la dependencia del proceso con el activo. A mayor valor de criticidad mayores consecuencias para el negocio supone la pérdida del activo.
  - ***Coste:*** Valor económico del activo.

- Instituto de Ciberseguridad de España - https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

Ejemplos – MINTIC - Colombia

Información básica

La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente[13]

Identificador: Número consecutivo único que identifica al activo en el inventario.
Proceso: Nombre del proceso al que pertenece el activo.
Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.
Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
Tipo: Define el tipo al cual pertenece el activo.

Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

Propiedad

Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

Acceso

Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Gestión

Fecha ingreso del Activo: Fecha de ingreso del activo de información en el inventario

Fecha salida del Activo: Fecha de exclusión del activo de información del inventario.

- Guía para la Gestión y Clasificación de Activos de Información – MINTIC- Gob de Colombia
- https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Ejemplos Prácticos

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Ejemplo de Incibe

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN						ANÁLISIS DE CRITICIDAD			
Nombre Activo	Tipo	Ubicación	Responsable / dueño	Soporte	Persona Autorizada para Manipular	Confidencialidad	Integridad	Disponibilidad	Criticidad

Ejemplo del PMG Seguridad

Atributos de los activos de información

- **Nombre del Activo**
- **Identificador**
- **Tipo**
- **Ubicación**
- **Responsable**
- Soporte
- Persona Aut. Manipular
- Persona Aut. Copiar
- Medio de almacenamiento
- Tiempo de Retención
- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- **Criticidad**

- **Identificador**
- **Proceso**
- **Nombre**
- Descripción
- **Tipo**
- **Ubicación**
- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- **Criticidad**
- **Propietario**
- Custodio
- Usuarios
- Fecha Ingreso
- Fecha de Salida

- **Nombre**
- **Descripción**
- **Identificador**
- **Tipo**
- **Propietario**
- **Responsable**
- **Ubicación**
- **Valoración**
- **Confidencialidad**
- **Criticidad**
- Costo

Ejemplos de Tipo de Activos – Cada Gobierno

- Base de Datos
- Documento
- Equipo
- Expediente
- Formulario
- Infraestructura Física
- Persona
- Sistema
- Software

- Información
- Software
- Recurso Humano
- Servicio
- Hardware
- Otros

- Servicios
- Datos/Información
- Aplicaciones
- Hardware
- Redes de comunicación
- Soporte de Información
- Equipamiento Auxiliar
- Instalaciones
- Personal

- **Procesos**
- **Información**
- *Hardware*
- *Software*
- *Red*
- *Personal*
- *Sitio*
- *Organización*

- http://www.dipres.gob.cl/598/articles-51683_intro_Guia_Metodologica04_2015.pdf - Chile
- https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf - Colombia
- https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf - España

Ejemplos de Sub categoría de Activos – España (PILAR)

- Servicios

```
[anon] anónimo (sin requerir identificación del usuario)
[pub] al público en general (sin relación contractual)
[ext] a usuarios externos (bajo una relación contractual)
[int] interno (usuarios y medios de la propia organización)
[cont] contratado a terceros (se presta con medios ajenos)

[www] world wide web
[telnet] acceso remoto a cuenta local
[email] correo electrónico
[file] almacenamiento de ficheros
[ftp] transferencia de ficheros
[edi] intercambio electrónico de datos

[dir] servicio de directorio (1)
[idm] gestión de identidades (2)
[ipm] gestión de privilegios
[pki] PKI - infraestructura de clave pública (3)
```

- Datos/Información

```
[vr] datos vitales (vital records) (1)
[com] datos de interés comercial (2)
[adm] datos de interés para la administración pública
[int] datos de gestión interna

[voice] voz
[multimedia] multimedia
[source] código fuente
[exe] código ejecutable
[conf] datos de configuración
[log] registro de actividad (log)
[test] datos de prueba

[per] datos de carácter personal (3)
  [A] de nivel alto
  [M] de nivel medio
  [B] de nivel básico

[label] datos clasificados (4)
  [S] secreto
  [R] reservado
  [C] confidencial
  [DL] difusión limitada
  [SC] sin clasificar
```

- https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf - España

Ejemplos de Evaluación de Criticidad – Magerit (España)

- Para los activo se evalúa:
  - Disponibilidad
  - Integridad
  - Confidencialidad
  - Autenticidad usuario
  - Autenticidad del origen de datos
  - Trazabilidad del servicio
  - Trazabilidad de Datos

valor		*criterio*
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a efectos prácticos

[D] disponibilidad
Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
¿Qué importancia tendría que el activo no estuviera disponible?

[I] integridad de los datos
Garantía de la exactitud y completitud de la información y los métodos de su procesamien-to.
¿Qué importancia tendría que los datos fueran modificados fuera de control?

[C] confidencialidad de los datos
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

[A_S] autenticidad de los usuarios del servicio
Aseguramiento de la identidad u origen.
¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

[A_D] autenticidad del origen de los datos
Aseguramiento de la identidad u origen.

[T_S] trazabilidad del servicio
Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

[T_D] trazabilidad de los datos
Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
¿Qué importancia tendría que no quedara constancia del acceso a los datos?

- https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf - España

Ejemplos de Evaluación de Criticidad – PMG Seguridad Inf. Chile

Para cada activo se evalúa

Tabla 1: Valores para Cálculo de Criticidad

Variables asociadas a la criticidad	Grado	Significado
CONFIDENCIALIDAD	Pública	El activo no tiene restricciones de acceso.
	Reservada	Activo de información cuyo acceso no autorizado tiene impacto para la institución o terceros.
INTEGRIDAD	Baja	Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
	Media	Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
	Alta	Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros
DISPONIBILIDAD	Baja	Activo de Información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.
	Media	Activo de Información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.
	Alta	Activo de Información cuya inaccesibilidad, tiene impacto grave para la institución o terceros.

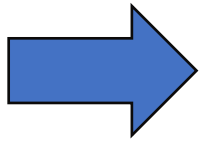
Estima Criticidad

- "Baja" : Ninguno de los valores asignados a la triada supera el valor "público" o "bajo".
- "Media": Alguno de los valores asignados a la triada es "medio".
- "Alta" : Alguno de los valores asignados a la triada es "Reservado" o "Alto".

- http://www.dipres.gob.cl/598/articles-51683_intro_Guia_Metodologica04_2015.pdf - Chile

Ejemplos de Evaluación de Criticidad – NIST 800-60

Para cada activo se evalúa



Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[7] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf - NIST 800-60

Consideraciones

- La confidencialidad esta muy arraigada a definiciones del negocio, es clave una definición con respecto los datos personales.

- La integridad es compleja de tratar, generalmente es algo intrazable ¿Qué información queremos que no posea integridad? Buscar un equilibrio es la clave.

- La disponibilidad es la más fácil de emplear con criterios cuantitativos, producto de su relación con el tiempo, niveles de servicio y/o tiempos objetivos de recuperación (RTO).

- Veamos un ejemplo más detallado.

Análisis y valoración del Riesgo

- **ISO 31.000:2018**
  - 6.4.3 Análisis del Riesgo
  - Se deben considerar
  - diversos factores:
    - .....
    - CID
    - Probabilidad
    - Consecuencia
    - Eficacia de controles
    - ....
  - 6.4.4 Valoración del Riesgo
  - Comparar los resultados del análisis con los criterios del riesgo establecidos para determinar cuando se requiere una acción adicional.

- **ISO 27.001:2017**

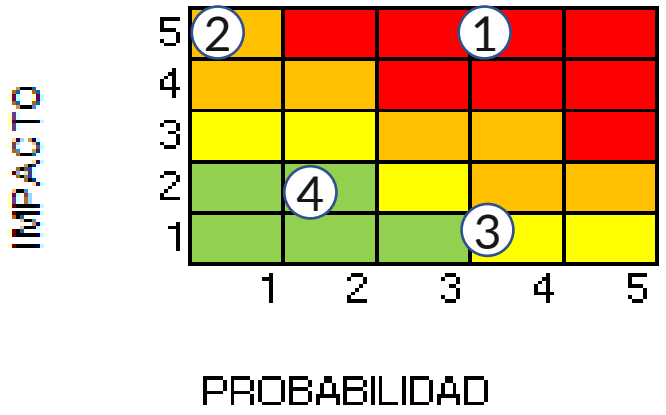
d) analiza los riesgos de la seguridad de la información:

1) evalúa las posibles consecuencias que podrían resultar si los riesgos identificados en 6.1.2 c) 1) se hicieran realidad;

2) evalúa la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y

3) determina los niveles de riesgo;

- Comparar con el apetito de riesgo
- Priorizar aquellos riesgos de mayor criticidad



Probabilidades

Documento Técnico 70 - CAIGG

Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

MAGERIT

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

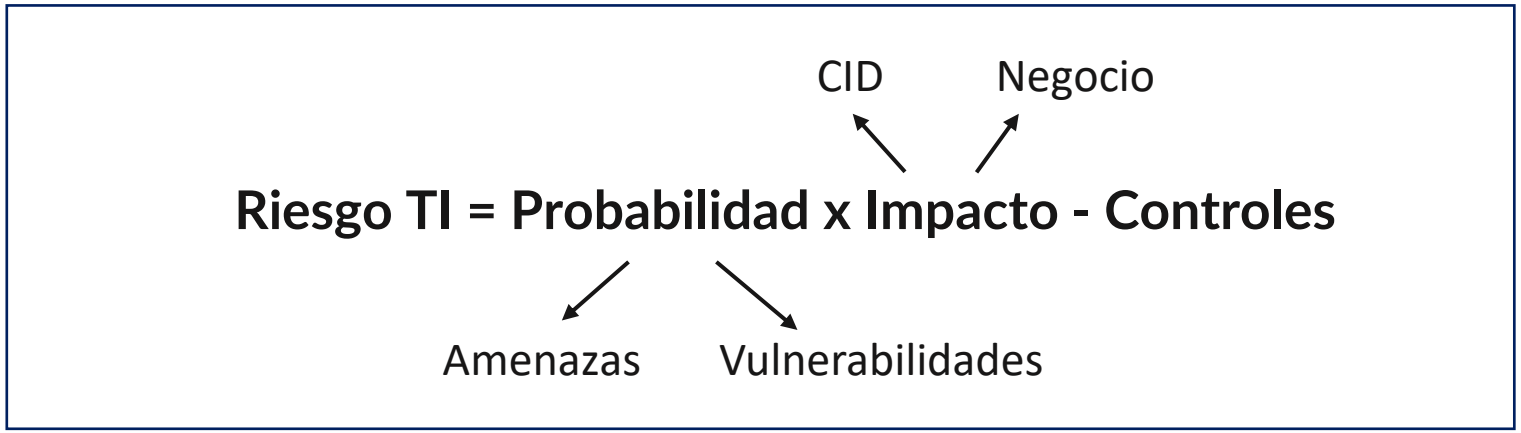
MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 2. Probabilidad de ocurrencia

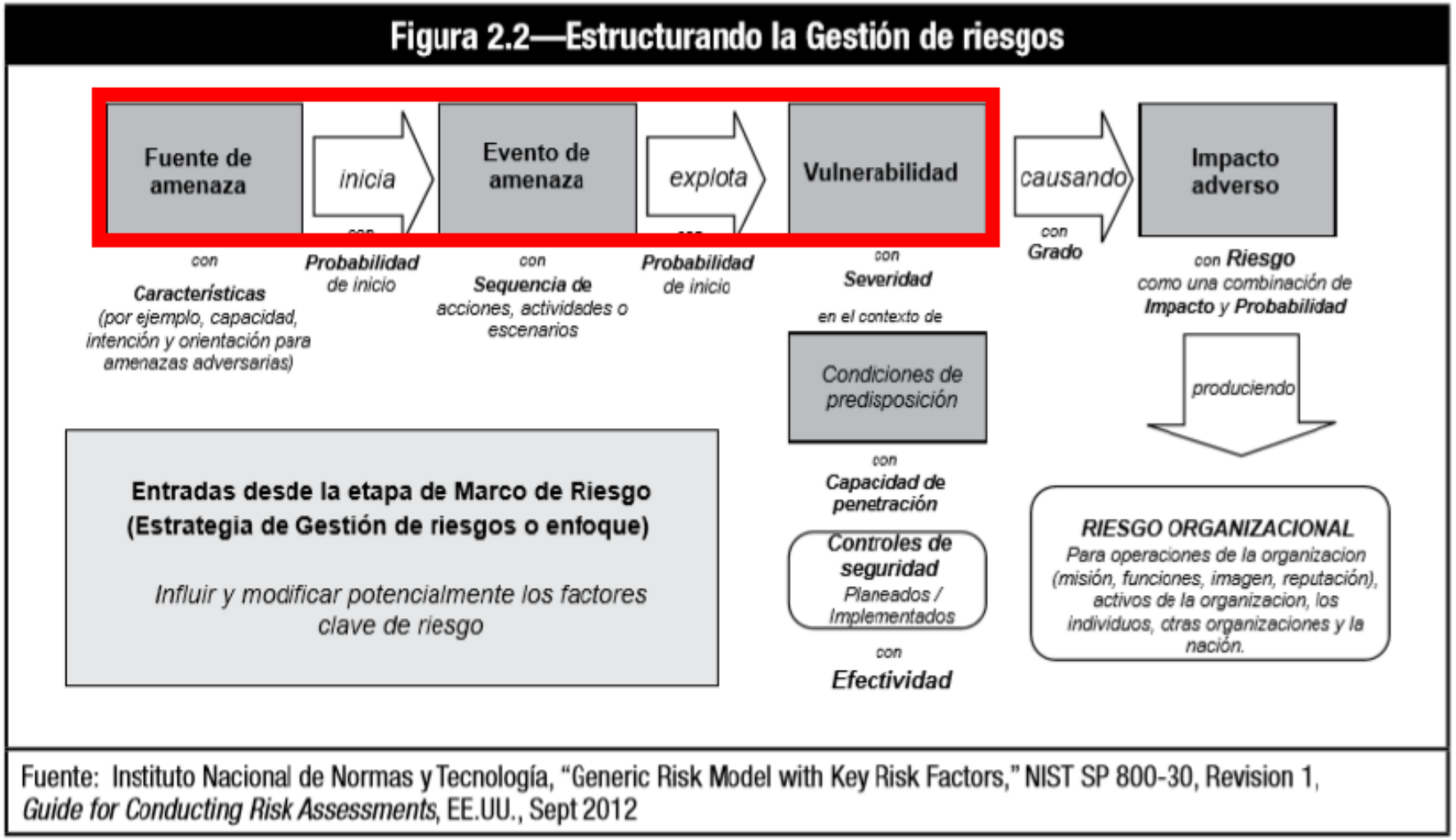
Recordemos

Riesgo

- Efecto de la incertidumbre en la consecución de los objetivos.



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

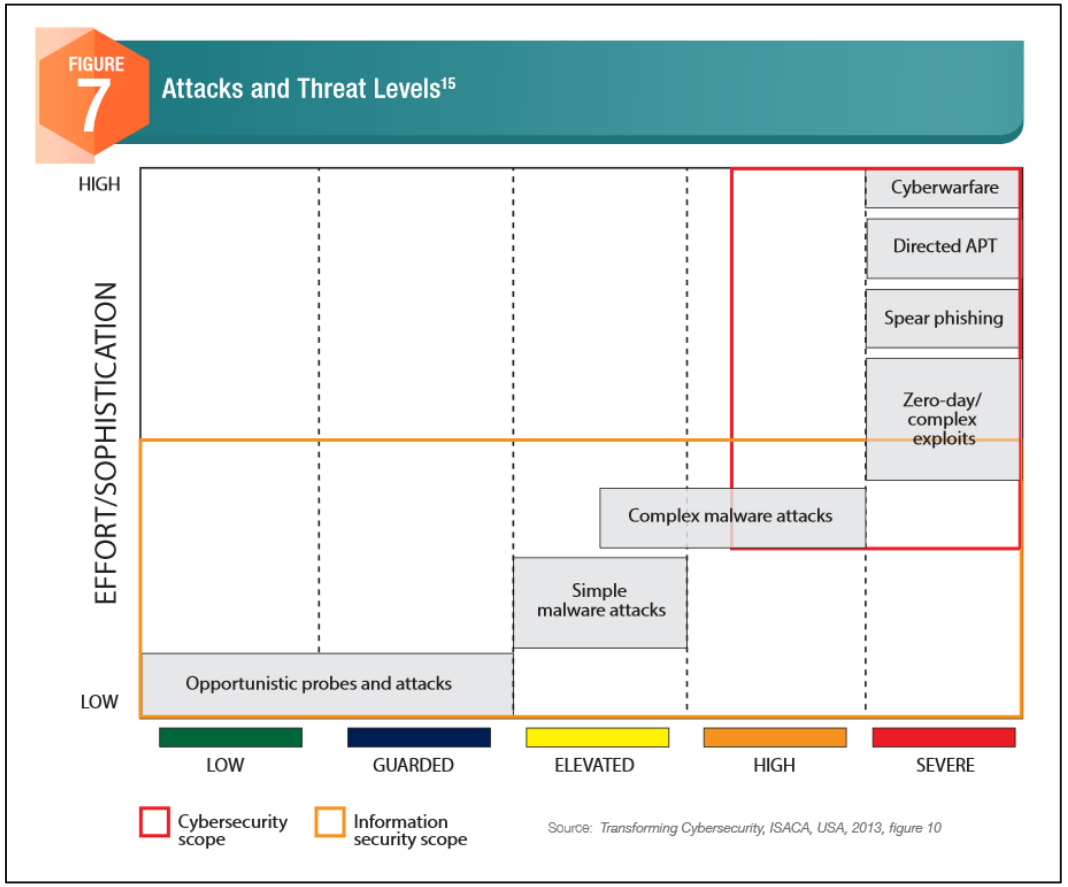
- “Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización” (ISO 27000:2019)

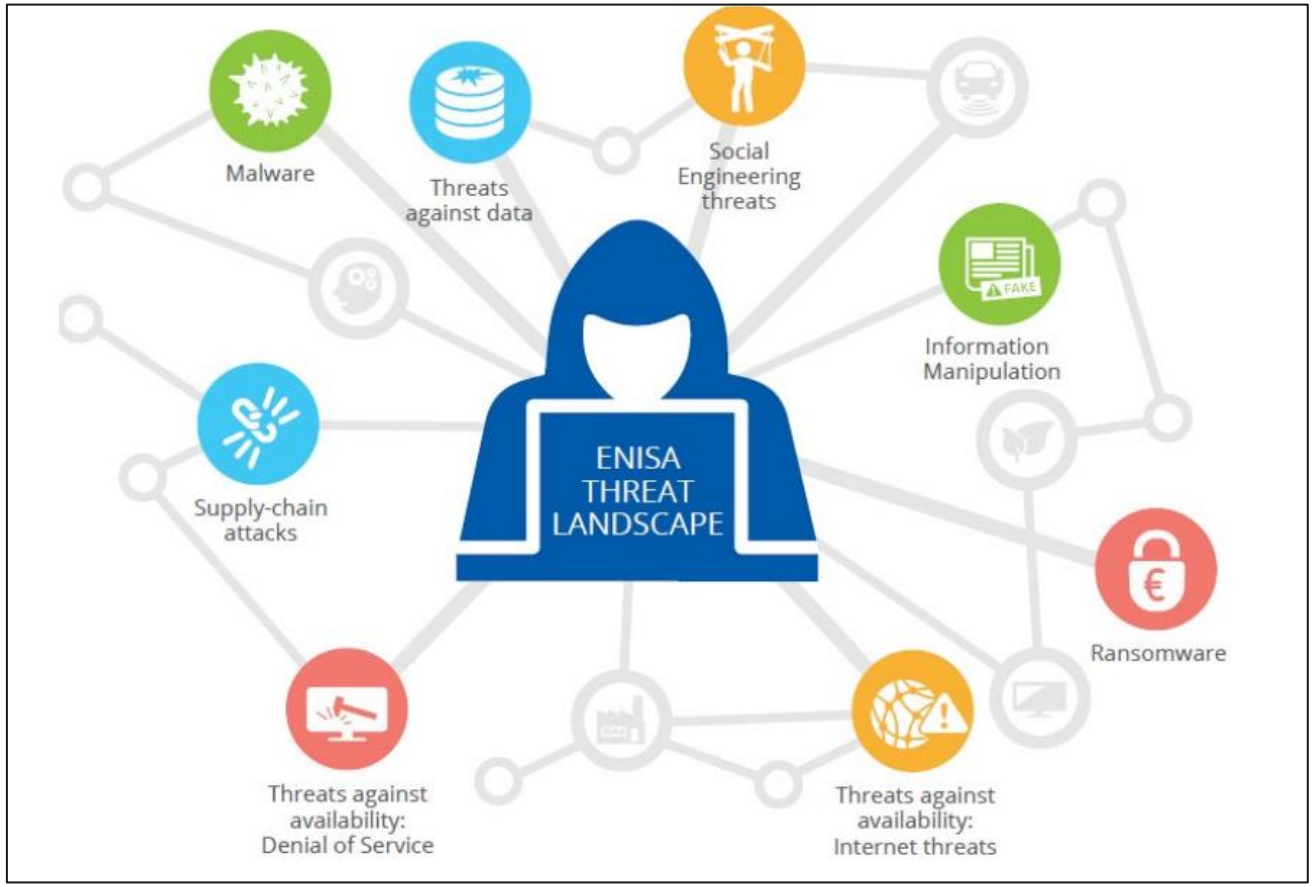
- “Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información” (INCIBE, 2019)

- 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 – Lo más prioritario





Fuente: European CybersecurityImplementation: Overview, ISACA

enisa-threat-landscape-2023

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)

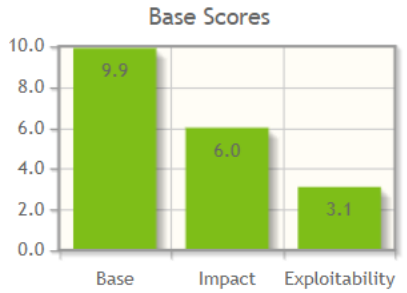
- "Debilidad de un activo o de un control que puede ser explotada por una o más amenazas"

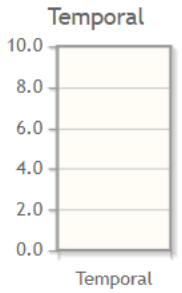
NIST NVD: National Vulnerability Database (1 de 2)

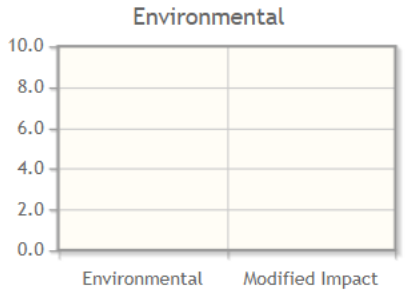
- El NVD es el repositorio de datos de vulnerabilidades oficial del gobierno de estados unidos, presentados usando el protocolo SCAP para permitir la automatización de la gestión de vulnerabilidades, cumplimiento y medidas de seguridad.

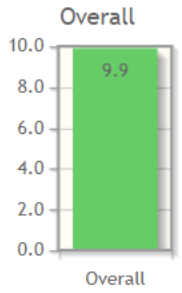
Vuln ID	Summary	CVSS Severity
CVE-2024-3821	The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions in the wdt_ajax_actions.php file in all versions up to, and including, 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. **Published:** junio 01, 2024; 5:15:09 a. m. -0400	*V4.0:*(not available) *V3.1:* 7.3 HIGH *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. **Published:** junio 01, 2024; 5:15:09 a. m. -0400	*V4.0:*(not available) *V3.1:* 10.0 CRITICAL *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. **Published:** junio 01, 2024; 5:15:09 a. m. -0400	*V4.0:*(not available) *V3.1:* 9.9 CRITICAL *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. **Published:** junio 01, 2024; 5:15:08 a. m. -0400	*V4.0:*(not available) *V3.x:*(not available) *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)**

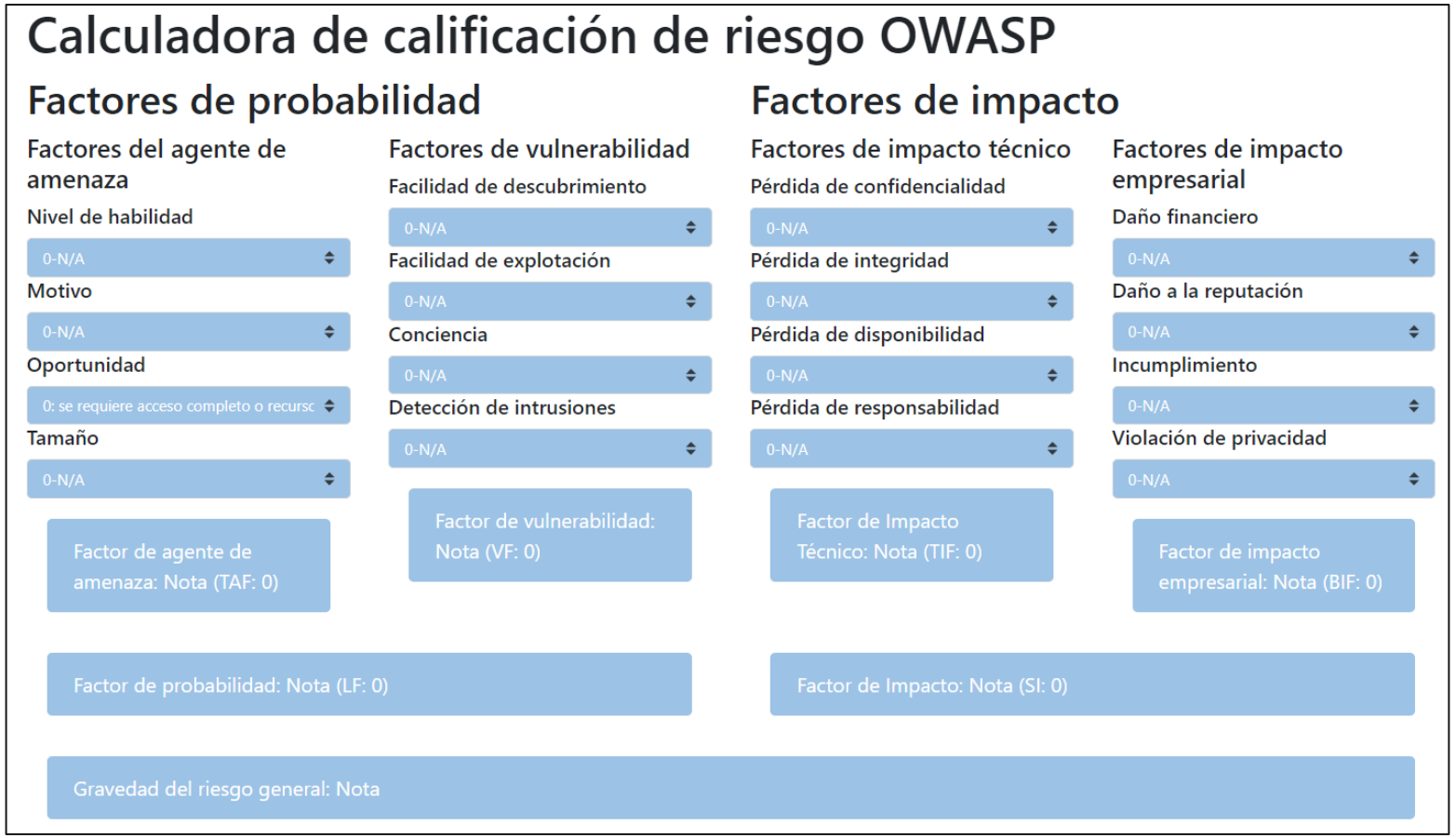
Impact Metrics

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)**

OWASP Risk Model



https://owasp-risk-rating.com

Impacto - CAIGG

Categoría	Valor	Descripción
Catastróficas	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización y del Gobierno. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal en el año en curso.
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización y del Gobierno. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

Severidad del Riesgo

Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

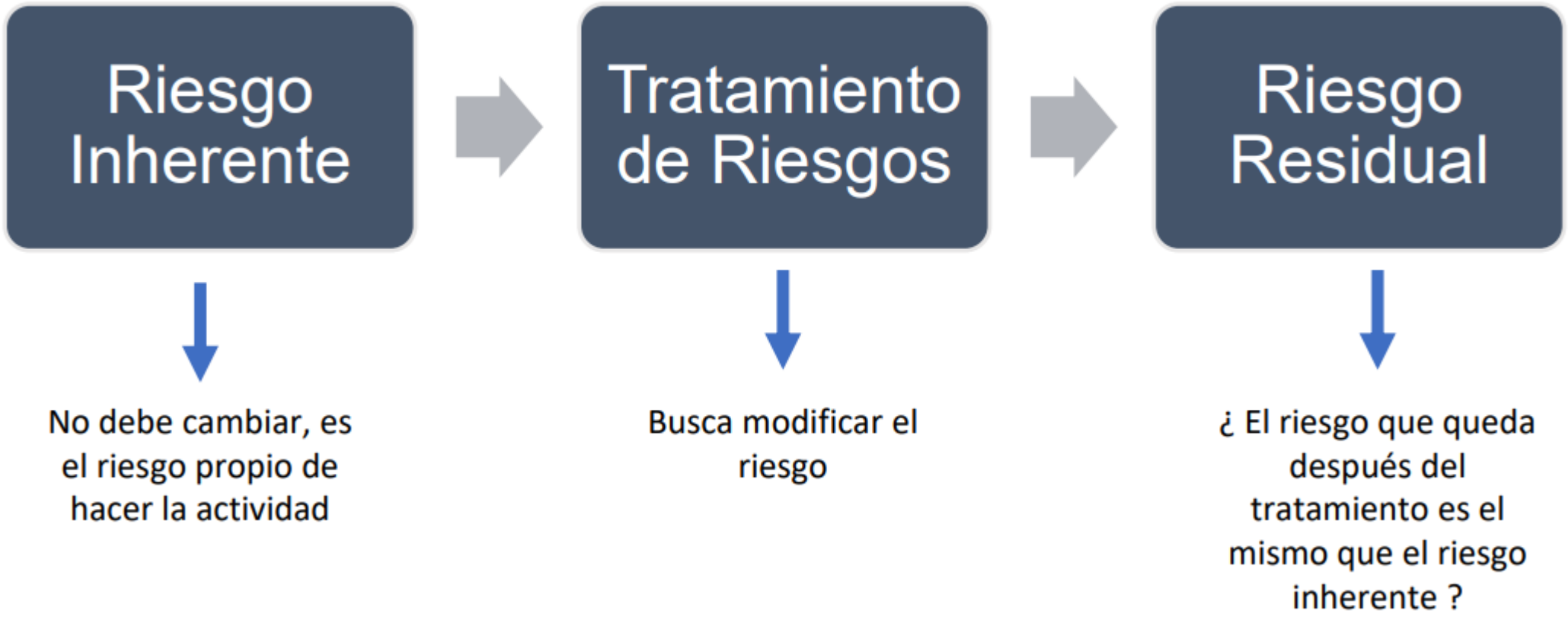
1.2.- **Cuadro N° 2: Categorías de Impacto:**

Categoría	Valor	Descripción
Catastróficas	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización y del Gobierno. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal en el año en curso.
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización y del Gobierno. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

NIVEL PROBABILIDAD (P)		NIVEL IMPACTO (I)		SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza	(5)	Catastróficas	(5)	EXTREMO (25)
Casi Certeza	(5)	Mayores	(4)	EXTREMO (20)
Casi Certeza	(5)	Moderadas	(3)	EXTREMO (15)
Casi Certeza	(5)	Menores	(2)	ALTO (10)
Casi Certeza	(5)	Insignificantes	(1)	ALTO (5)
Probable	(4)	Catastróficas	(5)	EXTREMO (20)
Probable	(4)	Mayores	(4)	EXTREMO (16)
Probable	(4)	Moderadas	(3)	ALTO (12)
Probable	(4)	Menores	(2)	ALTO (8)
Probable	(4)	Insignificantes	(1)	MODERADO (4)
Moderado	(3)	Catastróficas	(5)	EXTREMO (15)
Moderado	(3)	Mayores	(4)	EXTREMO (12)
Moderado	(3)	Moderadas	(3)	ALTO (9)
Moderado	(3)	Menores	(2)	MODERADO (6)
Moderado	(3)	Insignificantes	(1)	BAJO (3)
Improbable	(2)	Catastróficas	(5)	EXTREMO (10)
Improbable	(2)	Mayores	(4)	ALTO (8)
Improbable	(2)	Moderadas	(3)	MODERADO (6)
Improbable	(2)	Menores	(2)	BAJO (4)
Improbable	(2)	Insignificantes	(1)	BAJO (2)
muy improbable	(1)	Catastróficas	(5)	ALTO (5)
muy improbable	(1)	Mayores	(4)	ALTO (4)
muy improbable	(1)	Moderadas	(3)	MODERADO (3)
muy improbable	(1)	Menores	(2)	BAJO (2)
muy improbable	(1)	Insignificantes	(1)	BAJO (1)

Tratamiento de Riesgos

Ciclo Base


Riesgo Inherente
Tratamiento de Riesgos
Riesgo Residual
No debe cambiar, es el riesgo propio de hacer la actividad
Busca modificar el riesgo
¿ El riesgo que queda después del tratamiento es el mismo que el riesgo inherente ?

Plan de tratamiento del Riesgo

- 6.5.1 Tratamiento del Riesgo
- El propósito es seleccionar e implementar opciones para abordar el riesgo.

- 6.5.2 Opciones de Tratamiento
- Evitar el riesgo
- Mitigar el riesgo
- Aceptar el riesgo
- Compartir el riesgo

- Modificar la probabilidad
- Modificar la consecuencia

6.1.3 Tratamiento de los riesgos de seguridad de la información

La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:

a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;

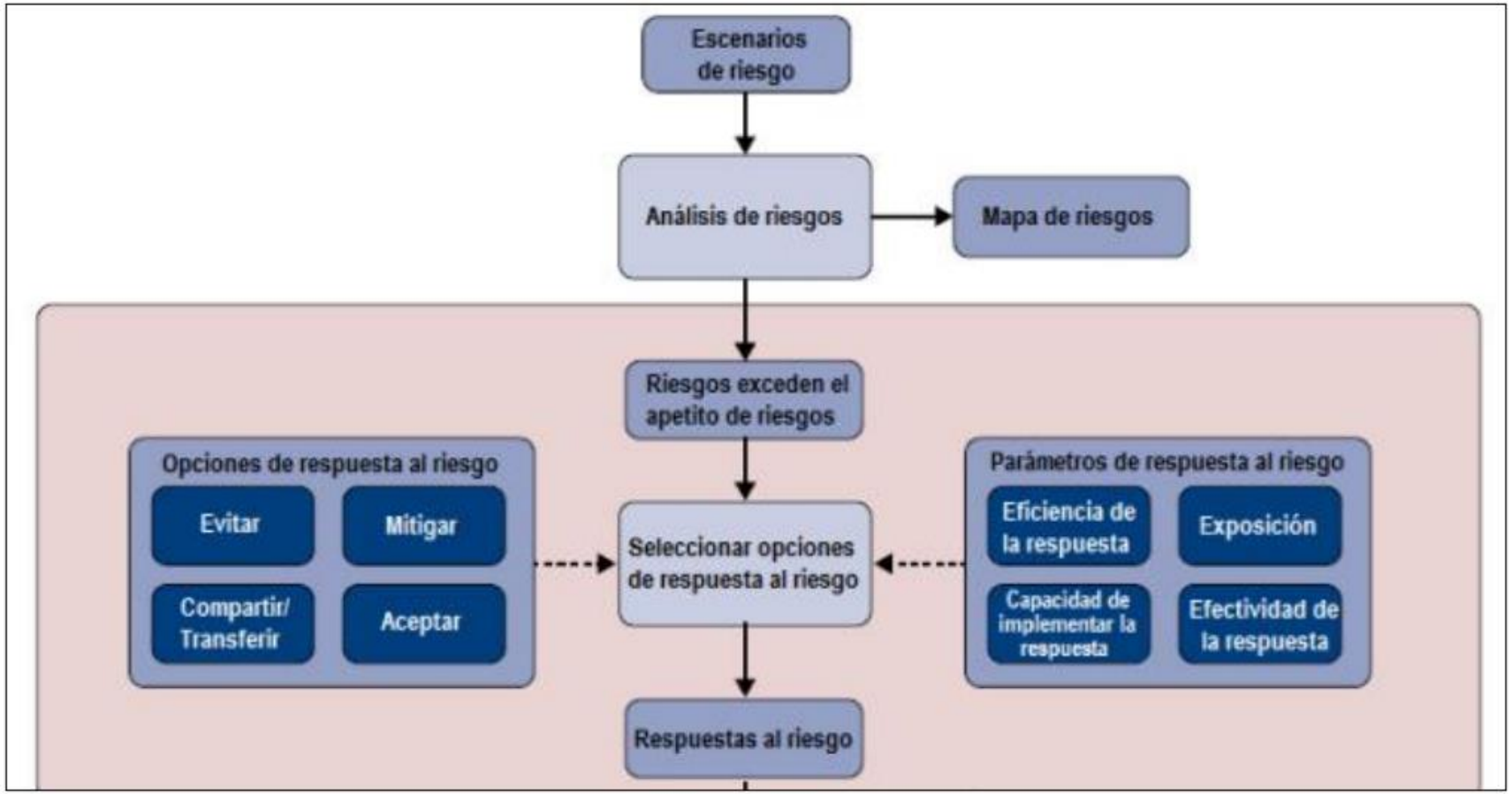
b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

- No establece las opciones de tratamiento la ISO 27.001:2017

- Evitar el Riesgo, no hacer la actividad que motiva el riesgo
- Mitigar el Riesgo, usando controles
- Compartir el Riesgo, distribuir el riesgo con terceras partes
- Aceptar el Riesgo, aceptar los beneficios o perdidas potenciales motivadas por un riesgo

- Siempre que externalizo un riesgo asumo otro.

Plan de Tratamiento de Riesgos – COBIT 5



El SoA (Declaración de Aplicabilidad de Controles)

c) comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios;

NOTA 1 El anexo A contiene una amplia lista de objetivos de control y controles. Se indica a los usuarios de esta norma internacional que se dirijan al anexo A para asegurar que no se pasan por alto controles necesarios.

NOTA 2 Los objetivos de control se incluyen implícitamente en los controles seleccionados. Los objetivos de control y los controles enumerados en el anexo A no son exhaustivos, por lo que pueden ser necesarios objetivos de control y controles adicionales.

d) elaborar una "Declaración de Aplicabilidad" que contenga:

- los controles necesarios [véase 6.1.3 b) y c)];
- la justificación de las inclusiones;
- si los controles necesarios están implementados o no; y
- la justificación de las exclusiones de cualquiera de los controles del anexo A.

e) formular un plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.

El SoA (Declaración de Aplicabilidad de Controles)

Control	Descripción	Adoptado	Origen	Justificación	Evidencia
A.05.01.01	Políticas de seguridad de la información	Si	Requisito Norma	Complementario a la clasula 5.2	- Politica de Seguridad
A.05.01.02	Revisión de las políticas de seguridad de la información	Si	Requisito Norma	Complementario a la clasula 5.2	- Plan de Concientización
A.06.01.01	Roles y responsabilidades de la seguridad de la informacion.	Si	Requisito Norma	Complementario a la clasula 5.3	- Organigrama - Roles y Funciones del SGSI - Perfiles de Cargo
A.06.01.02	Segregación de funciones	Si	Matriz de Riesgos	Control implementado para mitigar riesgos del negocio.	- Procedimiento de Creación de Perfiles
A.06.01.03	Contacto con autoridades	Si	Buena Práctica	Se implementa control para gestionar incidentes de alta criticidad y planes de continuidad del negocio	- Procedimiento de Gestión de Incidencias
A.06.01.04	Contacto con grupos especiales de interés.	Si	Buena Práctica	Se implementa control para gestionar incidentes de alta criticidad y planes de continuidad del negocio	- Procedimiento de Gestión de Incidencias
A.06.01.05	Seguridad de la información en la gestión de proyecto.	Si	Matriz de Riesgos	Control implementado para mitigar riesgos del negocio.	- Procedimiento de Desarrollo de Proyectos - Procedimiento de Gestión de Proveedores
A.06.02.01	Política de dispositivos móviles.	Si	Matriz de Riesgos	Control implementado para mitigar riesgos del negocio.	- Politica de Dispositivos Moviles
A.06.02.02	Trabajo Remoto.	No	Exclusión	No esta considerado el trabajo remoto en la organización	
A.07.01.01	Selección.	Si	Buena Práctica	Se implementa para fortalecer el proceso de contratación	- Procedimiento de Gestión de Personas

Opciones generales de tratamiento de Riesgo

Opción	ISO 31.000	UNE 62.198	ISO 27.005
Evitar el riesgo	▪ Evitar no iniciando o continuando con la actividad. ▪ Eliminar la fuente	▪ Evitar eliminando la fuente o no iniciando la actividad o no continuar con la actividad	▪ Evitar eliminando la fuente o no iniciando la actividad o no continuar con la actividad
Aceptar el Riesgo	▪ Aceptar o aumentar en busca de una oportunidad ▪ Retener el riesgo con base a una decisión informada	▪ Consecuencias positivas ▪ Asumir de manera informada	▪ Retención, siempre y cuando este bajo el apetito. ▪ Se hace después del riesgo residual, no es una opción en si.
Mitigar el Riesgo	▪ Modificar la probabilidad ▪ Modificar consecuencias	▪ Modificar la probabilidad ▪ Modificar consecuencias ▪ Foco en las positivas y negativas	▪ Reducción en base a controles
Compartir el Riesgo	▪ Compartir el riesgo	▪ Compartir el riesgo	▪ Transferencia

Medidas de Protección

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™

Se pueden Mapear

CIS Controls v8 Mappings

Download individual mappings below or visit our **CIS Controls Navigator** for all mappings to CIS Controls v8.

- AICPA Trust Services Criteria (SOC2)
- ASD's Essential Eight
- CIS Controls v8 to Enterprise ATTCK v82 Master Mapping
- CISA's Cross-Sector CPGs
- CMMC Cybersecurity Maturity Model Certification v2.0
- CRI Profile v1.2
- Criminal Justice Information Services
- CSA CCM Cloud Security Alliance Cloud Control Matrix
- Cyber Essentials v2.2
- FFEIC-CAT
- GSMA FS.31 Baseline Security Controls
- HIPAA Health Insurance Portability and Accountability Act of 1996
- ISACA COBIT 19
- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Microsoft Cloud Security Benchmark
- MITRE Enterprise ATT&CK v8.2

https://www.cisecurity.org/controls/v8

Vamos a ver el valor de analizar ejemplos conjuntos

Mapeo ISO 27002:2022 con CIS Control v8

https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec2-27002-2022

Consideraciones de la Implementación – Visión de Controles

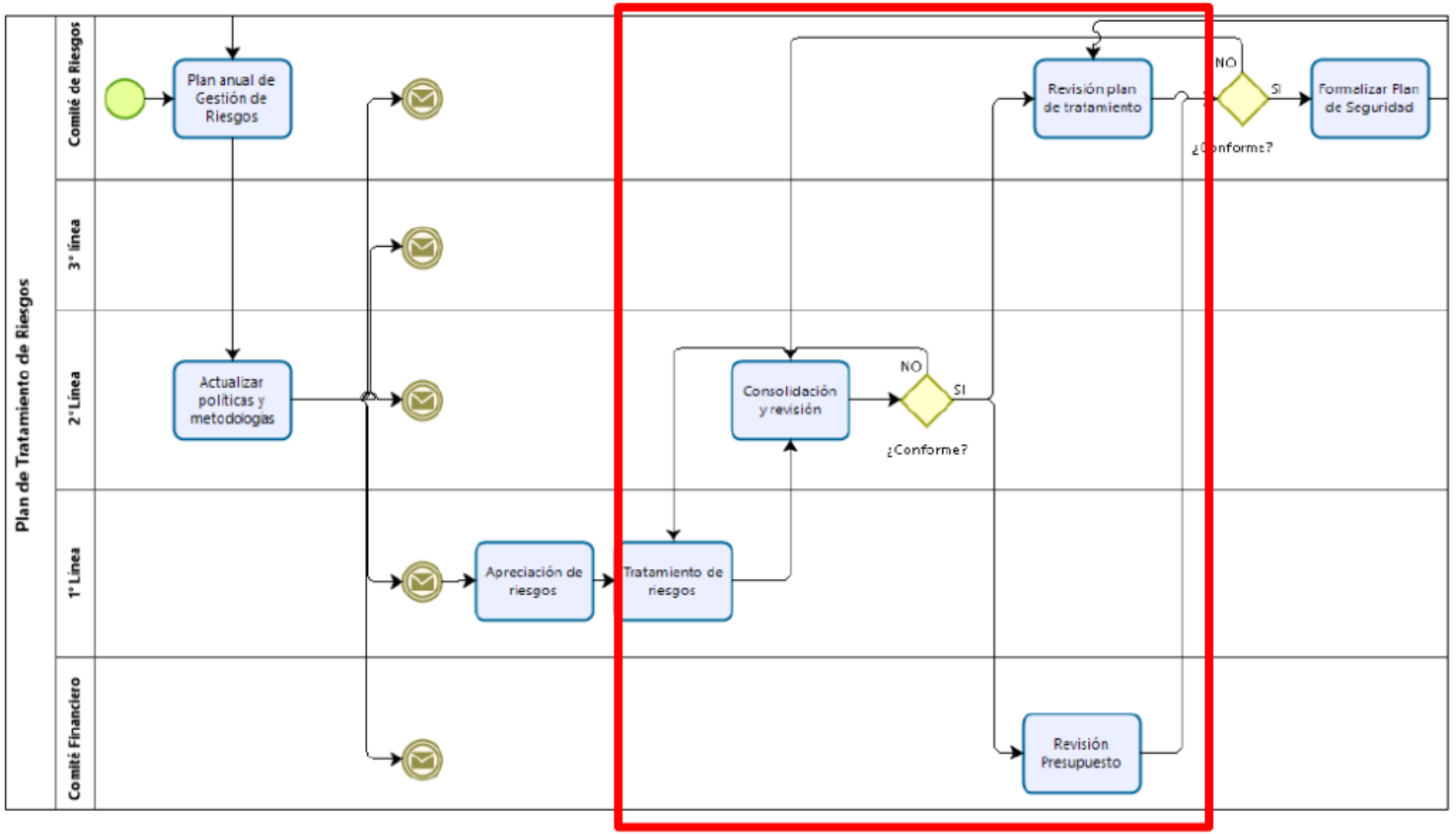
Gobernanza	Gestión de Proyectos	Gestión de Activos	Control de Accesos	Seguridad en RRHH	Capacitación y Concientización	Protección de Información y Medios	Seguridad Física
Seguridad en la Configuración	Seguridad Operaciones	Gestión de Vulnerabilidades	Seguridad en Redes	Seguridad en Software	Seguridad con Proveedores	Gestión de la Continuidad	Gestión de Incidentes
Ciberinteligencia	Riesgos en Cadena de Suministro	Privacidad y Cumplimiento	Pentesting	Monitoreo Red y Servicios	Seguridad en la Nube	Auditoría y Aseguramiento	Gestión de Logs y Evidencia

Controles Administrativos

Controles en TI

Controles Ciber

Complejidad del Proceso



Referencias

Información de referencia

- COSO ERM
  - https://www.coso.org/guidance-erm
- Magerit
  - https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- NIST 800-37
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- OWASP Risk Methodology
  - https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
- Tres líneas de defensa
  - https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-spanish.pdf
- Modelos de Riesgos
  - Chile CAIGG - https://biblioteca.digital.gob.cl/items/4dc92b73-c337-48ea-b2a2-a647515b563e
  - Chile SSI - https://www.dipres.gob.cl/598/articles-51683_intro_Guia_Metodologica04_2015.pdf
  - Colombia - https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf
  - España Incibe - https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Gestión de Riesgos de Ciberseguridad

Master Class

Carlos Lobos de Medina

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD