Unidad 3: Metodologías, estándares y marcos de trabajo
BLOQUE I – Introducción al ciberriesgo

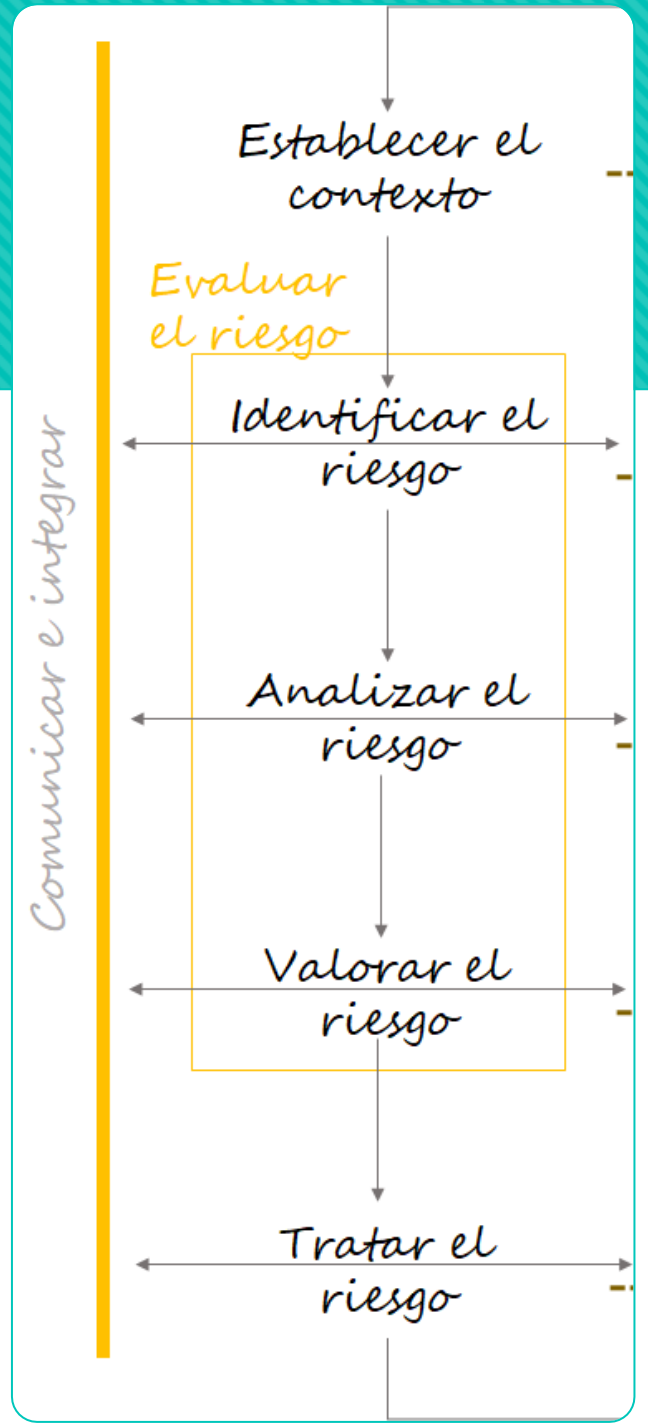
Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Fases en la gestión del ciberriesgo.
2. Metodologías, estándares y marcos de trabajo nacionales e internacionales.
3. Criterios de selección.

1. Fases en la gestión del ciberriesgo

- De momento vamos a quedarnos con las fases que ya estudiamos en la unidad 1:



1. Fases en la gestión del ciberriesgo

- En todas las organizaciones se utiliza algún estándar, marco de trabajo o metodología que ayude a llevar a cabo estas fases.
  - U otras similares o equivalentes.
- El problema es que hay muchas alternativas disponibles.
  - Algunas son redundantes, otras complementarias.
  - No usan la misma nomenclatura ni estructura.

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Ciberriesgo IT – Generalidades, taxonomías, nomenclatura, mejores prácticas

ISO 27005 (2014): Information technology - Security techniques - Information security management risk management

NIST SP 800-30 (2012): Guide for Conducting Risk Assessments

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Ciberriesgo IT – Nivel de madurez, procesos completos de gestión

ISO 27001 (2014): Information technology - Security techniques - Information security management systems - Requirements

ISO 27002 (2013): Information technology -Security techniques - Code of practice for information security controls

ISO 27032 (2012): Information technology - Security techniques - Guidelines for cybersecurity

ISO 27017 (2015): Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO 27018 (2014): Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

NIST Cybersecurity Framework v1.1 (2018) - Framework for Improving Critical Infrastructure Cybersecurity

NIST SP 800-53 & 800-53A: Security and Privacy Controls for Information Systems and Organizations

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Ciberriesgo OT – Generalidades, taxonomías, nomenclatura, mejores prácticas

IEC 62443 (3-1, 3-2, 3-3): Standard to Secure Control Systems	ISO 27019 (2017): Information technology - Security techniques - Information security controls for the energy utility industry	NIST SP 800-82Rev2 - Guide to Industrial Control Systems (ICS) Security

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Ciberriesgo OT – Nivel de madurez, procesos completos de gestión

IEC 62443 (1-1, 2-1, 2-2): Standard to Secure Control Systems

ISO 27019 (2017): Information technology - Security techniques - Information security controls for the energy utility industry

NIST SP 800-82Rev2 - Guide to Industrial Control Systems (ICS) Security

C2M2 (2014) : Cybersecurity Capability Maturity Model

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Riesgos para la privacidad y la protección de datos personales – Generalidades, taxonomías, nomenclatura, mejores prácticas

ISO 29134 (2017): Information technology - Security techniques - Guidelines for privacy impact assessment	ISO 29151 (2017) : Information technology — Security techniques — Code of practice for personally identifiable information protection	NIST SP 800-53 & 800-53A: Security and Privacy Controls for Information Systems and Organizations

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Riesgos para la privacidad y la protección de datos personales – Nivel de madurez, procesos completos de gestión

ISO 27701 (2019): Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (inicialmente conocida como ISO 27552)

ISO 29100 (2011): Information technology — Security techniques — Privacy framework

ISO 29101 (2018): Information technology — Security techniques — Privacy architecture framework

NIST Privacy Framework (2019): A Tool for Improving Privacy through Enterprise Risk Management (Preliminary Draft)

SP 800-53 & 800-53A: Security and Privacy Controls for Information Systems and Organizations

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Metodologías europeas para la gestión operativa del ciberriesgo (IT, algunas pueden adaptarse a OT), casi todas permiten cumplimiento de la ISO 27001

Magerit (España)	CORAS (Noruega)	EBIOS (Francia)	MEHARI (Francia)
CRAMM (Reino Unido)	BSI Standars (Alemania)	MIGRA (Italia)	

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Metodologías no europeas para la gestión operativa del ciberriesgo (IT, algunas pueden adaptarse a OT

TARA (Estados Unidos)	OCTAVE Allegro (Estados Unidos)	RISK IT Framework (Estados Unidos)
FAIR (Estados Unidos y Canadá)	Canadian TRA (Canadá)	

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Otras metodologías no específicas (casi todas a bajo nivel)

FMEA (Failure Modes and Effects Analysis) y su extensión FMECA	FMECA (Failure Mode, Effects, and Criticality Analysis)	DRBFM (Design Review by Failure Mode)	FTA (Fault Tree Analysis) y su extensión ETA (Event Tree Analysis)

HAZOP (Hazard & Operability Studies)	HACCP (Hazard Analysis and Critical Control Points)	Structured What-If Technique (SWIFT)

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Conviene realizar algunas aclaraciones sobre todo esto.
- Un estándar es un conjunto de modelos o patrones que son definidos por quienes poseen autoridad técnica, teórica o científica.
- Es público y se desarrolla para solventar una problemática específica
- El estándar incorpora un importante componente normativo, es decir obliga a realizar ciertas acciones con el objetivo de "cumplir" con el estándar.
- En muchas ocasiones, las organizaciones llevan a cabo procesos de auditoría externa que les permiten obtener la certificación de cumplimiento (o compliance) de dicho estándar.

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Un marco de trabajo es un conjunto de mejores prácticas y procesos que se han mostrado como exitosos frente a otros y que han sido adoptadas de forma amplia por la mayoría de la industria.
- Persigue que las organizaciones desplieguen sus procesos sin caer en los posibles errores cometidos en el pasado, al contrario, tomando como modelo los casos de éxito.
- También suelen ser públicos.
- No tienen carácter normativo aunque como los estándares, pueden ser utilizados para medir el grado de cumplimiento o alineamiento de una organización con respecto a él.
- Los marcos de trabajo, de hecho, evolucionan en muchos casos para terminar convirtiéndose en un estándar.

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Por último, una metodología es el conjunto de mecanismos o procedimientos racionales, empleados para el logro de un objetivo, o serie de objetivos que dirige una investigación científica.
- Mediante las metodologías se intenta dotar de un formalismo a los procesos de gestión del ciberriesgo, haciendo que sigan un método repetible, fiable, portable, etc.

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- En cuanto al concepto de nivel de madurez, la evaluación de este nivel suele realizarse antes de un proceso de gestión del ciberriesgo (para conocer el punto de partida) o en paralelo (para obtener datos de entrada adicionales) ya que puede ayudar mucho en sus diferentes fases o etapas.
- Las organizaciones llevan a cabo programas de seguridad en los que se incorporan diferentes controles:
  - Contramedidas y mitigaciones técnicas.
  - Políticas y procedimientos para lidiar con el factor humano.
  - Formación, concienciación y sensibilización.

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Una evaluación del nivel de madurez, permite conocer la extensión o profundidad con la que se están llevando a cabo estos programas.
  - Cuáles y cuántos controles de diferentes tipos han sido desplegados en la organización.
  - Y "como de bien" se ha hecho.
- Los estándares y mejores prácticas proponen una serie de dominios, o áreas de análisis que a su vez llevan asociadas una serie de actividades o acciones que deben realizarse.
- Para cada actividad se propone una escala que permite medir el grado de desarrollo de dicha actividad

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Por ejemplo, una actividad puede encontrarse en alguno de estos estados y en un ejercicio de evaluación (casi siempre auditoría externa para los estándares y auto-evaluación para los marcos de trabajo) ponderaría de la siguiente manera:

1. No realizada: La actividad no se ha llevado a cabo, aunque esté diseñada o planificada.
2. Realizada parcialmente, informalmente y/o en despliegue. La actividad se ha llevado a cabo de forma esporádica o puntual en alguna empresa, filial, sección sin ser considerada como iniciativa corporativa o y se encuentra actualmente desplegándose.
3. Realizada y en mejora continua. La actividad se lleva a cabo regularmente, de manera global, pero es necesario seguir trabajando en ella para estandarizarla, formalizarla, automatizarla y que todos los involucrados estén formados y concienciados.
4. Realizada y optimizada. La actividad se lleva a cabo, de manera estándar, formal, global, automática, medible y repetible con formación y concienciación asociada, etc.

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Una organización tendrá un mayor nivel de madurez cuantos más dominios y actividades haya realizado (es decir cuantos más controles haya desplegado) y cuanto más haya profundizado en la realización de cada una de las actividades (es decir cuanto mejor se esté trabajando con el control analizado).

2. Metodologías, estándares y marcos de trabajo nacionales e internacionales

- Una vez realizado un proceso de estas características:
  - Será más sencillo identificar los ciberriesgos que afectan a la organización.
  - Tendremos más información para analizar y valorar estos riesgos (sus probabilidades e impactos).
  - Sabremos hasta qué punto los ciberriesgos se están tratando de la manera adecuada y en qué dominios o actividades hay un mayor margen de mejora.

3. Criterios de selección

- Ya hemos visto que existen diferentes estándares, marcos y metodologías que pueden ser utilizados dependiendo de diferentes criterios.
- No existe una alternativa mejor que las demás, cada organización, dependiendo de los objetivos y del alcance del proyecto (ESTABLECER EL CONTEXTO) de gestión del ciberriesgo, deberá seleccionar la más adecuada en cada caso.

3. Criterios de selección

- Algunos criterios para la toma de decisiones:
  1. ¿Objetivos y alcance del proceso?
  2. ¿Tipo de entregable y resultado esperado o requerido?
  3. ¿IT, OT, privacidad y protección de datos?
  4. ¿Necesidad de cumplimiento por marco regulatorio o imposición de un agente externo/interno?

Para leer e investigar…

1. “INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK - Methodology for and assessment of interoperability among risk management frameworks and methodologies “. ENISA (2022).

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/