ANÁLISIS DE RIESGOS

Juan Delfín Peláez Álvarez
jpela@unileon.es

INDICE

- **Definiciones**
- **Metodologías internacionales**
- **Dimensiones de la seguridad de la información**
- **Caso práctico 1: RGPD-Facilita**
- **Elementos de un análisis de riesgos formal**
- **Grado de ciberseguridad**
- **Caso práctico 2: Análisis y gestión del riesgo con la herramienta PILAR**

universidad de león

DEFINICIONES

RIESGO:

Estimación del **grado** de exposición a que una **amenaza** se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

ANÁLISIS DE RIESGOS:

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

TRATAMIENTO DE RIESGOS:

Selección e implantación de las medidas o '**salvaguardas**' de seguridad adecuadas para **prevenir**, **impedir**, **reducir** o **controlar** los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. El tratamiento de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

GESTIÓN DE RIESGOS:

Es el proceso de análisis y tratamiento de riesgos.

AUDITORÍA DE SEGURIDAD: Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

METOLODOLOGÍAS INTERNACIONALES DE ANÁLISIS DE RIESGOS

METOLODOLOGÍAS INTERNACIONALES

METODOLOGÍAS DE ANÁLISIS DE RIESGOS		
Nombre	**Comentarios**	**Enlace**
MAGERIT v3	MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.	https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/
OCTAVE	OCTAVE - Operationally Critical Threat Asset and Vulnerability Evaluation. Desarrollado por el CERT en Carnegie Mellon University	http://www.cert.org/resilience/products-services/octave/
CRAMM	Desarrollada por la British CCTA (*Central Communication and Telecommunication Agency*).	http://rm-inv.enisa.europa.eu/methods/m_cramm.html
MEHARI	Diseñada por el CLUSIF (*Club de la Sécurité de l'Information Français*).	http://www.clusif.asso.fr/fr/production/mehari/
SP800-30	Desarrollada por el NIST (*National Institute of Standards and Techonogy*).	http://csrc.nist.gov/publications/PubsSPs.html

Un listado más exhaustivo puede encontrarse en:
www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/

Análisis de Riesgos

MAGERIT V.3

MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en **2012** en su versión 3

MAGERIT versión 3 se ha estructurado en **tres libros**:

- ❑ "Método"
- ❑ "Catálogo de Elementos"
- ❑ "Guía de Técnicas"

MAGERIT persigue los siguientes **objetivos**:

Directos:

1. **Concienciar** a los responsables de las organizaciones de la **existencia de riesgos y de la necesidad de gestionarlos**
2. Ofrecer un **método sistemático para analizar los riesgos** derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y **planificar el tratamiento** oportuno para mantener los riesgos bajo control

Indirectos:

1. **Preparar a la Organización** para procesos de **evaluación**, **auditoría**, **certificación** o **acreditación**, según corresponda en cada caso

Análisis de Riesgos

OCTAVE

octave®

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

OCTAVE es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en el año 2001, y su acrónimo significa "Operationally Critical Threat, Asset and Vulnerability Evaluation", estudia los riesgos en base a tres principios **Confidencialidad, Integridad y Disponibilidad**, esta metodología se emplea por distintas agencias gubernamentales tales como el Departamento de defensa de Estados Unidos.

OCTAVE dispone de tres versiones:

- ❑ OCTAVE-Original
- ❑ OCTAVE-S para pymes
- ❑ OCTAVE- ALLEGRO vers. simplificada

OCTAVE cuenta con 3 fases:

1. La primera contempla la **evaluación de la organización**, se construyen los perfiles activo-amenaza, recogiendo los principales activos, así como las amenazas y requisitos como imperativos legales que puede afectar a los activos, las medidas de seguridad implantadas en los activos y las debilidades organizativas.
2. En la segunda se **identifican las vulnerabilidades** a nivel de infraestructura de TI
3. En la última fase de desarrolla un **plan y una estrategia de seguridad**, siendo analizados los riesgos en esta fase en base al impacto que puede tener en la misión de la organización.

Análisis de Riesgos

CRAMM

CRAMM

Cabinet Office

CCTA Central Computer and Telecommunications Agency

•CRAMM es la metodología de análisis de riesgos desarrollado por la **Agencia Central de Comunicación y Telecomunicación del gobierno británico**. El significado del acrónimo proviene de **CCTA Risk Analysis and Management Method**. Su versión inicial data de 1987 y la versión vigente es la 5.2. Al igual que MAGERIT, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento.

CRAMM proporciona una librería unas **3.000 medidas de seguridad**

CRAMM cuenta con 3 etapas:

1. La primera de las etapas recoge la definición global de los **objetivos de seguridad** entre los que se encuentra la definición del **alcance**, la identificación y evaluación de los **activos** físicos y software implicados, la determinación del **valor** de los datos en cuanto a **impacto** en el negocio y la identificación.
2. En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las **amenazas** que afecta al sistema, así como las **vulnerabilidades** que explotan dichas amenazas y por último el **cálculo de los riesgos** de materialización de las mismas.
3. En la tercera etapa se identifican y seleccionan las **medidas de seguridad** aplicadas en la entidad obteniendo los riesgos residuales.

Análisis de Riesgos

MEHARI

MEHARI
www.mehari.info

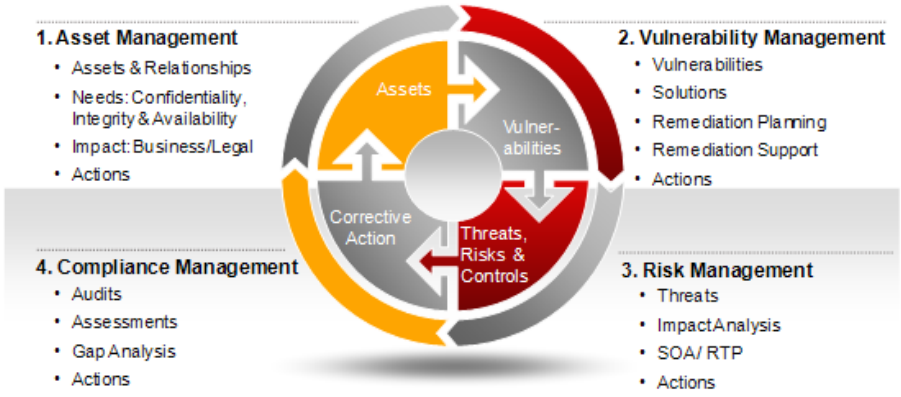
CLUSIF

MEHARI es la metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (CLUb de la Sécurité de l'Information Français) en 1995 y deriva de las metodologías previas Melissa y Marion. La metodología ha evolucionado proporcionando una **guía de implantación de la seguridad** en una entidad a lo largo del ciclo de vida. Del mismo modo, evalúa riesgos en base a los criterios de **disponibilidad, integridad y confidencialidad**.

SP800-30

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

SP800-30 es un documento de la serie SP-800 dedicada a la seguridad de la información y desarrollada por el **NIST** (National Institute of Standards and Techonogy), la cual es una agencia del Departamento de Comercio de los Estados Unidos. La publicación de esta guía data julio de 2002.



universidad de León

Legislación Española
Análisis de Riesgos

Análisis de Riesgos

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan.

https://www.aepd.es/normativa/

RD 12/2018 SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN – DIRECTIVA NIS

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

LEY 8/2011 PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

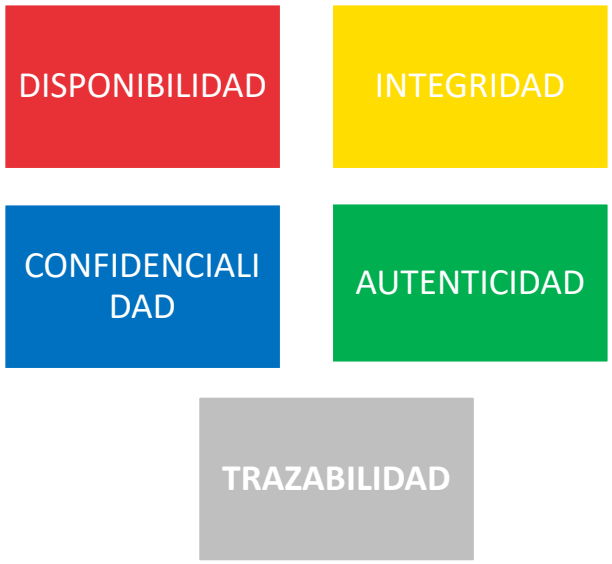
Análisis de riesgos: el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

Los **Planes de Seguridad del Operador** deberán establecer una **metodología de análisis de riesgos** que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos.

http://www.cnpic.es/Legislacion_Aplicable/Generico/index.html

Análisis de Riesgos

Dimensiones de la seguridad de la información



- **DISPONIBILIDAD:** disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
- **INTEGRIDAD:** mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.
- **CONFIDENCIALIDAD:** que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.
- **AUTENTICIDAD:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.
- **TRAZABILIDAD:** Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Análisis de Riesgos

HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO
RGPD FACILITA

https://www.aepd.es/herramientas/facilita.html

Herramienta para empresas que realicen un **tratamiento de datos personales de escaso riesgo (sin datos especialmente protegidos o a gran escala)**.
Está dividida en tres bloques:

1. Información sobre el **sector de actividad** y el **tipo de datos** que trata.
2. **Información sobre la empresa** (nombre, dirección, CIF o teléfono, entre otros).
3. Información sobre los **tratamientos que realiza** (clientes, empleados, currículums de candidatos, proveedores, videovigilancia, etc.)

La herramienta genera los **documentos mínimos indispensables para facilitar el cumplimiento de la normativa.**

MEDIDAS DE SEGURIDAD MÍNIMAS

ORGANIZATIVAS

- Confidencialidad y secreto
- Notificar violaciones de seguridad de datos de carácter personal

TÉCNICAS

- Identificación
- Actualización de ordenadores y dispositivos
- Malware
- Cortafuegos
- Cifrado de datos
- Copia de seguridad

Referencia: Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos Al RGPD: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

CASO PRÁCTICO 1 - ANALISIS DE RIESGOS CON FACILITA_RGPD

Realizar un análisis de riesgo de una "academia de formación" (escaso riesgo).
Utilizar la herramienta FACILITA de la AEPD.
Referencia:
https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

Academia de Formación Militar SL

Academia de formación militar

C\general militar

NIF: 10000000

Teléfono: 000000

Correo Electrónico: militar@militar.com

Actividad: Educación

TRATAMIENTO DE DATOS:

CLIENTES

- Datos Clientes: identificación, datos académicos, características personales, datos bancarios.
- Finalidad: Prestación de servicios, Facturación, fidelización.
- Cesión: AEAT, INSS Bancos, FCSE

EMPLEADOS

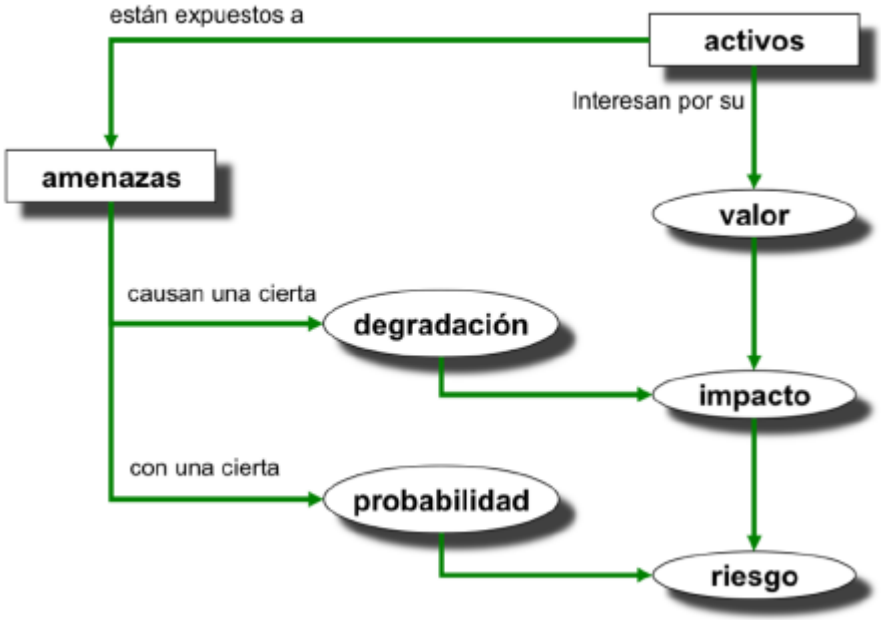
- Datos Clientes**:** identificación, datos académicos, características personales, datos bancarios, datos profesionales.
- Facilitados por ellos.
- Finalidad: Nomina, Formación y relación laboral.
- Cesión: AEAT, INSS Bancos, FCSE
- Datos Gestoría: 2, c\general militar 10000001

CÁMARAS DE VIDEOVIGILANCIA

Referencia: Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos Al RGPD:
https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

ANÁLISIS DE RIESGOS FORMAL

ELEMENTOS DE UN ANÁLISIS DE RIESGOS FORMAL



- **ACTIVOS:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la Organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), Comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
- **VALOR DE UN ACTIVO:** el valor puede ser propio o acumulado en base a las dependencias de activos.
- **AMENAZAS:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Pueden ser: De origen natural, industrial, defectos en aplicaciones, intencionadas o accidentales.
- **DEGRADACIÓN:** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

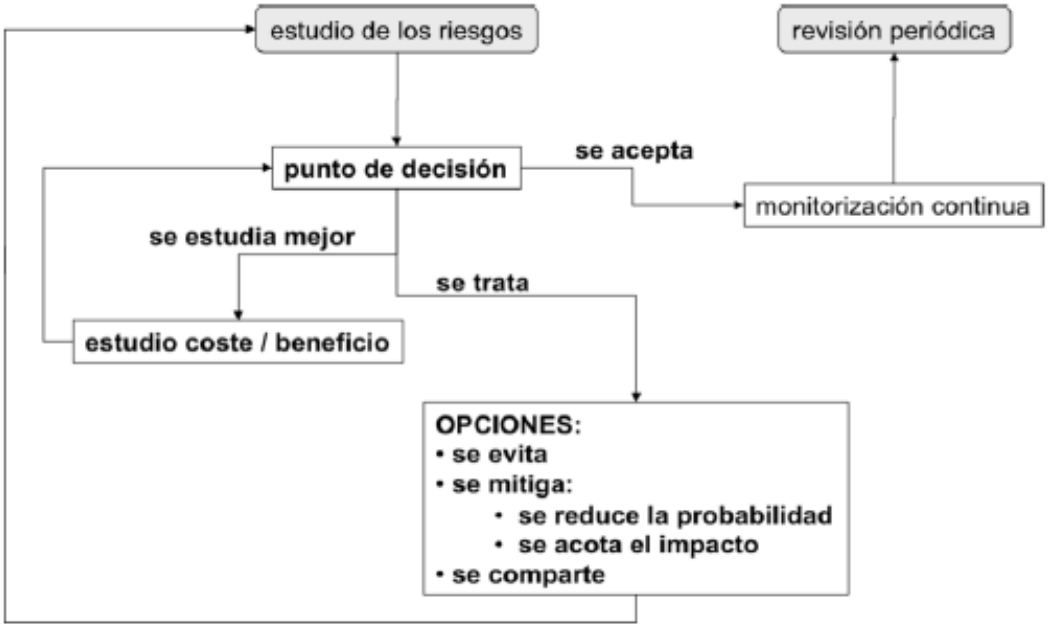
- **PROBABILIDAD:** cuán probable o improbable es que se materialice la amenaza. Por ejemplo: Muy frecuente (a diario, frecuente (mensualmente), normal (una vez al año), poco frecuente (cada varios años), muy poco frecuente (siglos).
- **IMPACTO:** la medida del daño sobre el activo derivado de la materialización de una amenaza . El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

RIESGO = PROBABILIDAD x IMPACTO

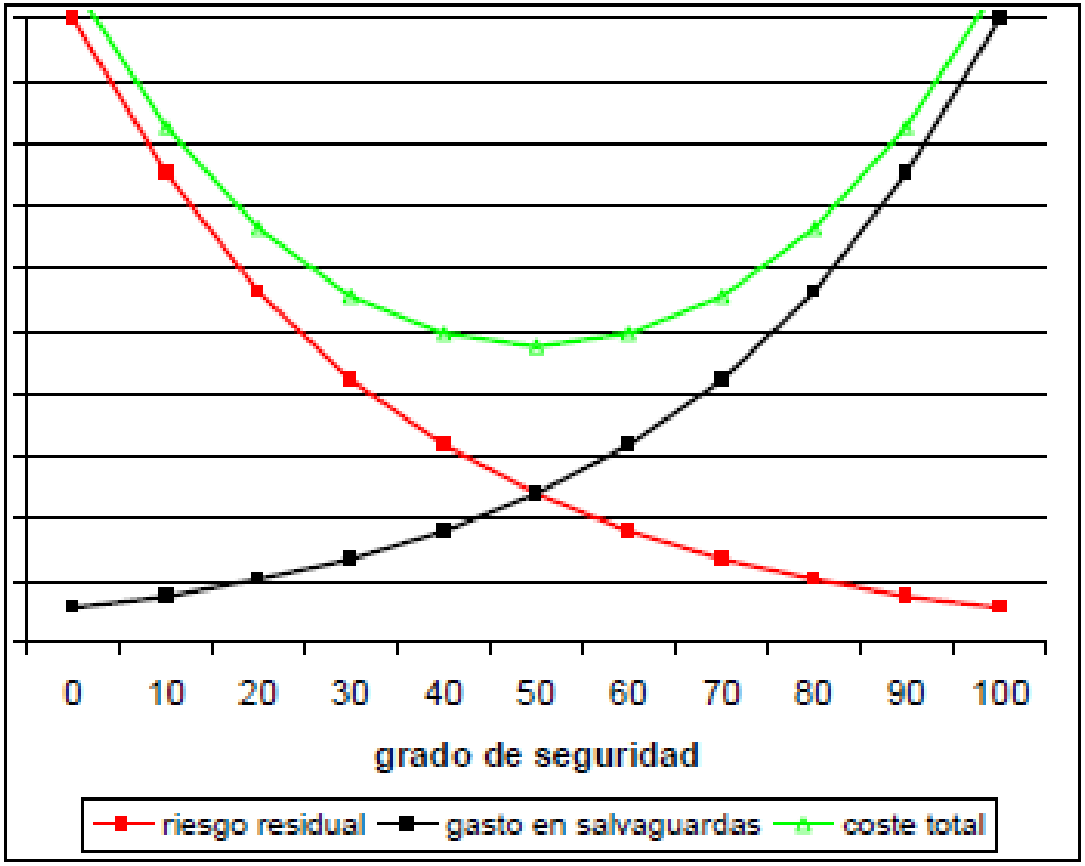
TRATAMIENTO DEL RIESGO

Posibles decisiones que se pueden tomar tras haber estudiado los riesgos



- **Se ACEPTA el riesgo**, siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno, para mantener el suministro eléctrico, puede ser demasiado alto y por tanto, la organización puede optar por asumir el riesgo.
- **SE TRATA el riesgo para :**
  - **EVITAR el riego eliminándolo.** Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. Por ejemplo, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
  - **MITIGAR el riesgo implantando medidas de seguridad.** Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.
  - **COMPARTIR el riesgo transfiriéndolo** a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.

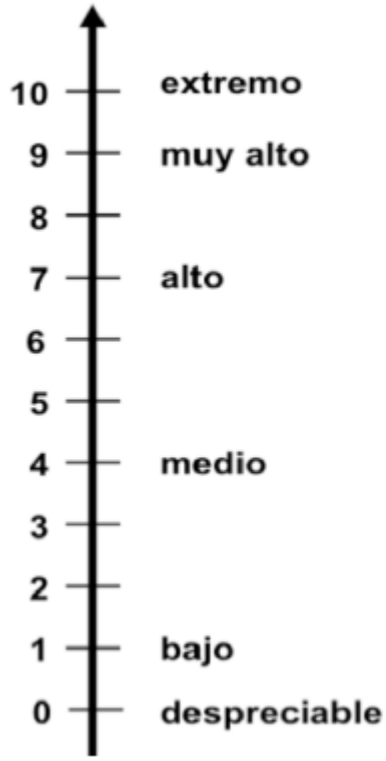
Análisis de Riesgos



Esta gráfica refleja cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. El riesgo cae fuertemente con pequeñas inversiones y el coste de las inversiones se dispara para alcanzar niveles de seguridad cercanos al 100%. Existe un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa, punto al que hay que tender si la única consideración es económica.

CRITERIOS DE VALORACIÓN DE ACTIVOS

- **CRITERIO CUANTITATIVO**: Dinero
- **CRITERIO CUALITATIVO**: Criterio subjetivo a determinar por el usuario



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

CRITERIOS DE VALORACIÓN DE ACTIVOS

- **CRITERIO CUALITATIVO**: Criterio subjetivo a determinar por el usuario
  - **[pi] Información de carácter personal**
  - **[lpo] Obligaciones legales**
  - **[si] Seguridad**
  - **[cei] Intereses comerciales o económicos**
  - **[da] Interrupción del servicio**
  - **[po] Orden público**
  - **[olm] Operaciones**
  - **[adm] Administración y gestión**
  - **[lg] Pérdida de confianza (reputación)**
  - **[crm] Persecución de delitos**
  - **[rto] Tiempo de recuperación del servicio**
  - **[lbl.nat] Información clasificada (nacional)**
  - **[lbl.ue] Información clasificada (Unión Europea)**

CRITERIOS DE VAORACIÓN DE ACTIVOS

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

CRITERIOS DE VAORACIÓN DE ACTIVOS

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

CRITERIOS DE VAORACIÓN DE ACTIVOS

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

TIPOS DE AMENAZAS

Amenazas

- 5.1. [N] Desastres naturales
  - 5.1.1. [N.1] Fuego
  - 5.1.2. [N.2] Daños por agua
  - 5.1.3. [N.*] Desastres naturales
- 5.2. [I] De origen industrial
  - 5.2.1. [I.1] Fuego
  - 5.2.2. [I.2] Daños por agua
  - 5.2.3. [I.*] Desastres industriales
  - 5.2.4. [I.3] Contaminación mecánica
  - 5.2.5. [I.4] Contaminación electromagnética
  - 5.2.6. [I.5] Avería de origen físico o lógico
  - 5.2.7. [I.6] Corte del suministro eléctrico
  - 5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad
  - 5.2.9. [I.8] Fallo de servicios de comunicaciones
  - 5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales
  - 5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información
  - 5.2.12. [I.11] Emanaciones electromagnéticas
- 5.3. [E] Errores y fallos no intencionados
  - 5.3.1. [E.1] Errores de los usuarios
  - 5.3.2. [E.2] Errores del administrador
  - 5.3.3. [E.3] Errores de monitorización *(log)*
  - 5.3.4. [E.4] Errores de configuración
  - 5.3.5. [E.7] Deficiencias en la organización
  - 5.3.6. [E.8] Difusión de software dañino
  - 5.3.7. [E.9] Errores de [re-]encaminamiento
  - 5.3.8. [E.10] Errores de secuencia
  - 5.3.9. [E.14] Escapes de información
  - 5.3.10. [E.15] Alteración accidental de la información
  - 5.3.11. [E.18] Destrucción de información
  - 5.3.12. [E.19] Fugas de información
  - 5.3.13. [E.20] Vulnerabilidades de los programas (software)
  - 5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)
  - 5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - 5.3.16. [E.24] Caída del sistema por agotamiento de recursos
  - 5.3.17. [E.25] Pérdida de equipos
  - 5.3.18. [E.28] Indisponibilidad del personal
- 5.4. [A] Ataques intencionados
  - 5.4.1. [A.3] Manipulación de los registros de actividad (log)
  - 5.4.2. [A.4] Manipulación de la configuración
  - 5.4.3. [A.5] Suplantación de la identidad del usuario
  - 5.4.4. [A.6] Abuso de privilegios de acceso
  - 5.4.5. [A.7] Uso no previsto
  - 5.4.6. [A.8] Difusión de software dañino
  - 5.4.7. [A.9] [Re-]encaminamiento de mensajes
  - 5.4.8. [A.10] Alteración de secuencia
  - 5.4.9. [A.11] Acceso no autorizado
  - 5.4.10. [A.12] Análisis de tráfico
  - 5.4.11. [A.13] Repudio
  - 5.4.12. [A.14] Interceptación de información (escucha)
  - 5.4.13. [A.15] Modificación deliberada de la información
  - 5.4.14. [A.18] Destrucción de información
  - 5.4.15. [A.19] Divulgación de información
  - 5.4.16. [A.22] Manipulación de programas
  - 5.4.17. [A.23] Manipulación de los equipos
  - 5.4.18. [A.24] Denegación de servicio
  - 5.4.19. [A.25] Robo
  - 5.4.20. [A.26] Ataque destructivo
  - 5.4.21. [A.27] Ocupación enemiga
  - 5.4.22. [A.28] Indisponibilidad del personal
  - 5.4.23. [A.29] Extorsión
  - 5.4.24. [A.30] Ingeniería social (picaresca)

TIPOS DE AMENAZAS

[I.5] Avería de origen físico o lógico

Tipos de activos:	Dimensiones:
• [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1. [D] disponibilidad

Descripción:
fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

Origen:
Entorno (accidental)
Humano (accidental o deliberado)

Ver:
EBIOS:
28 - AVERÍA DEL HARDWARE
29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

[E.3] Errores de monitorización *(log)*

Tipos de activos:	Dimensiones:
• [D.log] registros de actividad	1. [I] integridad (trazabilidad)

Descripción:
inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...

Ver:
EBIOS: no disponible

[E.19] Fugas de información

Tipos de activos:	Dimensiones:
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	1. [C] confidencialidad

Descripción:
revelación por indiscreción.

Incontinencia verbal, medios electrónicos, soporte papel, etc.

Ver:
EBIOS: no disponible

[A.12] Análisis de tráfico

Tipos de activos:	Dimensiones:
• [COM] redes de comunicaciones	1. [C] confidencialidad

Descripción:
el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.

A veces se denomina "monitorización de tráfico".

Ver:
EBIOS: no disponible

Análisis de Riesgos

https://www.youtube.com/watch?v=THnQ2FH7NtU

https://www.youtube.com/watch?v=g7EPuzN5Awg

https://www.youtube.com/watch?v=9T9X0q2y6vQ

ISO 27000

ISO/IEC 27000-series

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). la mayoría de estas normas se encuentran en preparación e incluyen:

ISO/IEC 27000 - es un vocabulario estándar para el SGSI.

ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI.

ISO/IEC 27002 Es código de buenas prácticas para la gestión de seguridad de la información.

ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001.

ISO/IEC 27004 - son métricas para la gestión de seguridad de la información.

ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información.

ISO/IEC 27006 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.

ISO/IEC 27007 - es una guía para auditar al SGSI.

Análisis de Riesgos

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

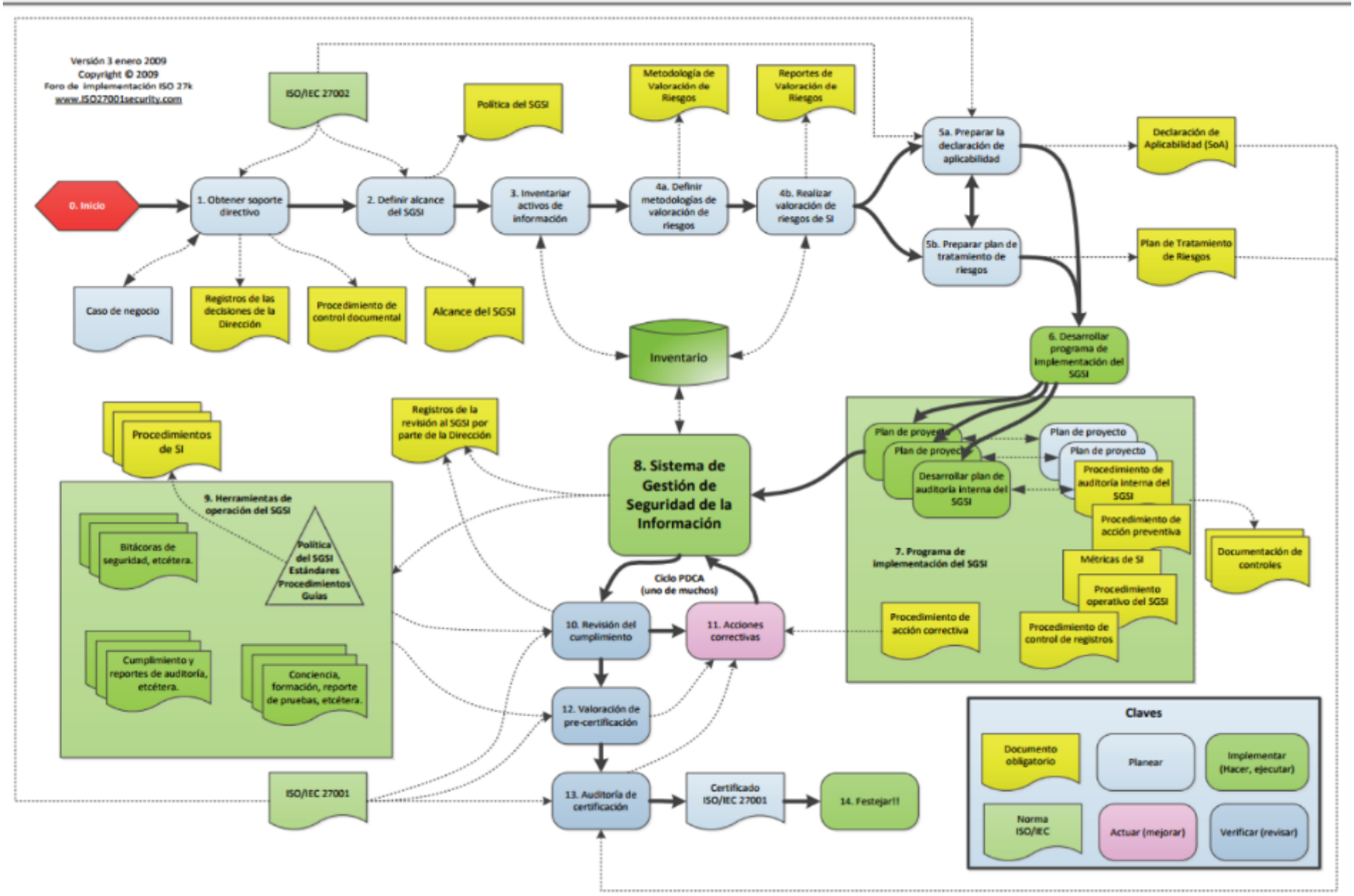
Análisis de Riesgos

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html

NIVELES DE MADUREZ

Nivel	Descripción
L0	Inexistente. Esta medida no está siendo aplicada en este momento.
L1	Inicial / ad hoc. En el nivel L1 de madurez, el proceso existe, pero no se gestiona. La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.
L2	Repetible, pero intuitivo. En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
L3	Proceso definido. Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
L4	Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5	Optimizado. El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Análisis de Riesgos



Análisis de Riesgos

CASO PRÁCTICO 2 – ANALISIS Y GESTIÓN DEL RIESGO CON LA HERRAMIENTA PILAR

En esta práctica se va a realizar un análisis, gestión y tratamiento de riesgos en un sistema de información de una organización.
La práctica se realizará utilizando la herramienta PILAR con licencia de evaluación. Para la realización de esta práctica, se recomienda leer los siguientes artículos y documentos:

- PILAR-Manual de Usuario
- PILAR – Manual Avanzado
- Metodología de Gestión de Riesgos MAGERIT

EJERCICIO 1: INSTALACION Y TOMA de CONTACTO

El alumno deberá realizar los pasos siguientes, documentando lo realizado con capturas de pantalla de las acciones seguidas.

- **Paso 1**: Instalar la herramienta de Gestión de Riesgos PILAR. Descargar e instalar la Herramienta PILAR (PILAR RM-ES /ENS) desde https://www.ar-tools.com/es/tools/download.html y solicitar la licencia de evaluación.
- **Paso 2**: Configuración Inicial. Utilizar la librería de configuración STIC_es.car. Seleccionar la licencia de evaluación. Abra el fichero de ejemplo ejemplo_es.mgr correspondiente a una unidad administrativa de una oficina de atención al ciudadano. En el menú Editar->opciones: Verifique que las amenazas están configuradas en modo automático (Es la herramienta la que incluye amenazas automáticamente según el tipo de activo registrado)
- **Paso 3:** Acceda a las siguientes pantallas de la aplicación
    - **A.1. Identificación de Activos.** Indicar en que capas están divididos los activos del ejemplo. Selecciones 5 activos de distintas capas, e identifique la clase de activo a la que está asignado.
    - **A.1. Valoración de Activos** Para cada uno de los activos del punto anterior, indique que valoración tiene para las dimensiones de seguridad confidencialidad, integridad y disponibilidad. Para cada caso, indique si la valoración se basa en un criterio o en un valor numérico. En caso de que se base en criterio, indique el criterio seleccionado. Pulse el botón “valor acumulado” y observe como cambian algunos de los valores, por ejemplo la confidencialidad de los “expedientes en curso” pasa a valor 4. El valor acumulado se obtiene de la dependencia que existen entre los activos. Para ver las dependencias configure Editar->opciones->valoración:mix y entre en la pantalla **A1. Dependencias** y observe que existe una dependencia entre “expedientes en curso” y “Tramitación presencial”, esta última con valor 4 en confidencialidad.

Análisis de Riesgos

CASO PRÁCTICO 2 – ANALISIS Y GESTIÓN DEL RIESGO CON LA HERRAMIENTA PILAR

- **A.4 Identificación de Amenazas** Para cada uno de los activos del punto anterior, indique que amenazas tiene asociadas. ¿Por qué no es posible asociar ("aplicar") nuevas amenazas a un activo?
- **A.4 Valoración de Amenazas.** Para cada uno de los activos y amenazas del punto anterior, indique que probabilidad de ocurrencia tiene la amenaza (MB-Muy Baja, B-Baja, M-Media, A-Alta, MA-Muy Alta), y que porcentaje de degradación tienen para cada uno de las dimensiones Integridad, Disponibilidad e Integridad. ¿Por qué no es posible cambiar la probabilidad y el porcentaje de valoración?
- **A.5 Valoración (fases) de Salvaguardas** Seleccione 10 salvaguardas de distintos aspectos (G-Gestión, T-Técnico, F-Seguridad Física), de distintos tdp (tipos de protección).

  PR–prevención
  DR –disuasión
  EL –eliminación
  IM –minimización del impacto
  CR–corrección
  RC–recuperación

Y observe su nivel de madurez (L0-L5) actual y objetivo.

- **A.7 riesgo repercutido** Para cada uno de los activos del punto anterior, indique que valoración de riesgo potencial, actual y objetivo tienen para las dimensiones de seguridad confidencialidad, integridad y disponibilidad.
- **E. Perfiles de Seguridad [27002:2013]. Valoración** ¿Cuántos dominios funcionales, objetivos de control y controles tiene la ISO:27002? Seleccionar 10 controles de la ISO:27002 e indicar que valoración actual y objetivo tienen.
- R. Informes. Riesgo acumulado activo. Seleccione todos los activos y obtenga el grafico araña para las fases actual y objetivo

Análisis de Riesgos

CASO PRÁCTICO 2 – ANALISIS Y GESTIÓN DEL RIESGO CON LA HERRAMIENTA PILAR

EJERCICIO 2- ANLISIS DE RIESGOS DE UN AYUNTAMIENTO

Realizar un análisis de riesgos de un servicio de una organización, por ejemplo, la Administración de la Sede Electrónica de un ayuntamiento, siguiendo los pasos vistos en el ejercicio anterior. El alumno, siendo lo más realista posible.

Puede tomar de referencia la situación actual del siguiente ayuntamiento:

https://www.ayto-castrillon.es/attachments/article/484/pliego%20tecnico%20suministro%20cpds.pdf

Deberá realizar, al menos, los pasos siguientes, documentando lo realizado, su justificación y capturas de pantalla de las acciones seguidas.

1. **Cree un nuevo proyecto.**
2. Cree una capa estándar para dar de alta al menos 5 activos de distintas capas, identificando la clase de activo a la que está asignado. Algunos ejemplos de activos para el ayuntamiento, podrían ser: Servicio de incidencias municipales, servicio de consulta del padrón municipal, servidor, sistema operativo, navegador, herramienta máquinas virtuales, conexión a internet, …
3. **Valore los activos del punto anterior,** para los dominios de seguridad confidencialidad, integridad y disponibilidad.
4. **Identifique las amenazas** asociadas a los activos, su probabilidad y porcentaje de degradación que ocasionaría.
5. **Realice la valoración de las salvaguardas actual y objetivo.** Valore al menos 10 salvaguardas de distintos aspectos (G-Gestión, T-Técnico, F-Seguridad Física) y de distintos tdp (tipos de protección).
6. **Indique cuáles son los activos que actualmente están en mayor riesgo actual** desde el punto de vista de la confidencialidad, integridad y disponibilidad, y cuáles son la amenazas que hace que esos activos tengan esos niveles de riesgo.

Obtenga el gráfico araña del riesgo acumulado para las fases potencial, actual y objetivo

Gracias por su atención