POPBL6

ANÁLISIS DE RIESGOS

GRADO EN INGENIERÍA INFORMÁTICA

Autores: Unai Orive, Egoitz San Martin, Unai Mendieta, Unai Aguinaco y Daniel Luengo

17 de Mayo del 2021

Índice

1. Análisis de Riesgos

Toda la información y metodología presentada el documento se basa en la metodología de MAGERIT v.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).
Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.
El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

> **Disponibilidad:** o 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:** o 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:** o 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.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual es que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

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

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema:

> **Análisis de riesgos:** proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Sabiendo lo que podría pasar, hay que tomar decisiones:
>
> **Tratamiento de los riesgos:** proceso destinado a modificar el riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.
Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio. Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo:

> *Efecto de la incertidumbre sobre la consecución de los objetivos.*
> *[ISO Guía 73]*

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

1.1. Activos

> **Definición:** 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.

Estos son los diferentes tipos de activos relevantes:

- **Datos** que materializan la información.
- **Servicios auxiliares** que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (**software**) que permiten manejar los datos.
- Los equipos informáticos (**hardware**) y que permiten hospedar datos, aplicaciones y servicios.
- Los **soportes de información** que son dispositivos de almacenamiento de datos.
- El **equipamiento auxiliar** que complementa el material informático.
- Las **redes de comunicación** que permiten intercambiar datos.
- Las **instalaciones** que acogen equipos informáticos y de comunicaciones.
- Las **personas** que explotan u operan todos los elementos anteriormente citados.

Teniendo en cuenta los distintos tipos de activos y después de un análisis de estos dentro de la empresa, esta es la clasificación que hemos hecho:

1.1.1. Datos / Información

- [files] ficheros
- [backup] copias de seguridad
- [int] datos de gestión interna
- [auth] datos de validación de credenciales
- [source] código fuente
- [log] registro de actividad
- [exe] código ejecutable
- [test] código de prueba

1.1.2. Servicios

- [www] world wide web
- [email] correo electrónico

1.1.3. Software

- [std] estándar (off the shelf)
    - [browser] navegador web
    - [www] servidor de presentación
    - [app] servidor de aplicaciones
    - [email_client] cliente de correo electrónico
    - [dbms] sistema de gestión de bases de datos
    - [office] ofimática
    - [av] anti virus
    - [os] sistema operativo
    - [backup] sistema de backup

1.1.4. Hardware

    - [pc] informática personal
    - [mobile] informática móvil

1.1.5. Redes de comunicación

- [wifi] red inalámbrica
- [mobile] telefonía móvil
- [Internet] Internet

1.1.6. Soporte de información

- [electronic] electrónicos
    - [disk] discos
    - [san] almacenamiento en red
    - [usb] memorias USB

1.1.7. Equipamiento auxiliar

- [power] fuentes de alimentación
- [cabling] cableado
    - [wire] cable eléctrico
    - [fiber] fibra óptica

1.1.8. Instalaciones

- [local] cuarto
- [mobile] plataformas móviles
    - [car] vehículo terrestre: coche

1.1.9. Personal

- [ue] usuarios externos
- [ui] usuarios internos
- [adm] administradores de sistemas
- [com] administradores de comunicaciones
- [dba] administradores de BBDD
- [sec] administradores de seguridad
- [des] desarrolladores / programadores

1.2. Amenazas

> **Definición:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

1.2.1. Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

1.2.1.1. Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

1.2.1.2. Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA	

Debido a que los servidores son alquilados a AWS (Amazon Web Service), es decir, no han sido montados por nosotros, todos los riesgos de desastres naturales son transferidos a Amazon Web Service.

1.2.2. Errores y fallos no intencionados

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

1.2.2.1. Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. **Ver:** EBIOS: 38 - ERROR DE USO	

1.2.2.2. Errores del administrador

[E.2] Errores del administrador	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: equivocaciones de personas con responsabilidades de instalación y operación **Ver:** EBIOS: 38 - ERROR DE USO	

1.2.2.3. Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

1.2.2.4. Errores de (re-)encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. **Ver:** EBIOS: no disponible	

1.2.2.5. Escapes de información

[E.14] Escapes de información	
Tipos de activos: •	**Dimensiones:** 1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

1.2.2.6. Destrucción de información

[E.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. **Ver:** EBIOS: no disponible	

1.2.2.7. Fugas de información

[E.19] Fugas de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones • [P] personal (revelación)	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. **Ver:** EBIOS: no disponible	

1.2.2.8. Vulnerabilidades de los programas

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. **Ver:** EBIOS: no disponible	

1.2.2.9. Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

1.2.2.10. Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ... **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

1.2.3. Ataques intencionados

Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

1.2.3.1. Manipulación de registros de actividad (log)

[A.4] Manipulación de los registros de actividad (log)	
Tipos de activos: • [D.log] registros de actividad	**Dimensiones:** 1. [I] integridad (trazabilidad)
Descripción: **Ver:** EBIOS: no disponible	

1.2.3.2. Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. **Ver:** EBIOS: 40 - USURPACIÓN DE DERECHO	

1.2.3.3. Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. **Ver:** EBIOS: 39 - ABUSO DE DERECHO	

1.2.3.4. Difusión de software maligno

[A.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

1.2.3.5. (re-)Encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. **Ver:** EBIOS: no disponible	

1.2.3.6. Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dim1nsiones:** 1. [C] confidencialidad 2. [I] integridad
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. **Ver:** EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

1.2.3.7. Interceptación de información

[A.14] Interceptación de información (escucha)	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. **Ver:** EBIOS: 19 - ESCUCHA PASIVA	

1.2.3.8. Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

1.2.3.9. Destrucción de información

[A.18] Destrucción de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. **Ver:** EBIOS: no disponible	

1.2.3.10. Divulgación de información

[A.19] Revelación de información	
Tipos de activos: • [D] datos / información • [keys] claves criptográficas • [S] servicios (acceso) • [SW] aplicaciones (SW) • [COM] comunicaciones (tránsito) • [Media] soportes de información • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: revelación de información. **Ver:** EBIOS: 23 – DIVULGACIÓN 27 – GEOLOCALIZACIÓN 34 - COPIA ILEGAL DE SOFTWARE	

1.2.3.11. Manipulación de programas

[A.22] Manipulación de programas	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. **Ver:** EBIOS: 26 - ALTERACIÓN DE PROGRAMAS	

1.2.3.12. Denegación de servicios

[A.24] Denegación de servicio	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. **Ver:** EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

1.2.3.13. Indisponibilidad del personal

[A.28] Indisponibilidad del personal	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ... **Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL	

1.2.3.14. Ingeniería social

[A.30] Ingeniería social (picaresca)	
Tipos de activos: • [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. **Ver:** EBIOS: no disponible	

1.3. Salvaguardas

> **Definición:** Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Debido a que este es el primer análisis de riesgos, la empresa no dispone de ningún método de seguridad. Una vez realizado el análisis de el riesgo y probabilidad de las amenazas, se tomarán las medidas de seguridad necesarias en base a las necesidades de nuestro sistema.

1.4. Evaluación de riesgos

Una vez detectadas las distintas amenazas potenciales de nuestro sistema, se evalúa el impacto y riesgo potencial de las mismas. Para ello, utilizaremos tablas para determinar el nivel de la amenaza, clasificándolas en **muy bajo**, **bajo**, **mediano**, **alto** y **muy alto.**

1.4.1. Errores y fallos no intencionados

1.4.1.1. Errores de los usuarios

1.4.1.1.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			X
	Mediano			
	Alto			

1.4.1.2. Errores del administrador

1.4.1.2.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

1.4.1.3. Difusión de software dañino

1.4.1.3.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

1.4.1.4. Errores de (re-)encaminamiento

1.4.1.4.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

1.4.1.5. Escapes de información

1.4.1.5.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

1.4.1.6. Destrucción de información

1.4.1.6.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

1.4.1.7. Fugas de información

1.4.1.7.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

1.4.1.8. Vulnerabilidades de los programas

1.4.1.8.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

1.4.1.9. Caída del sistema por agotamiento de recursos

1.4.1.9.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			X
	Alto			

1.4.1.10. Indisponibilidad del personal

1.4.1.10.1. Personal interno

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

1.4.2. Ataques intencionados

1.4.2.1. Manipulación de registros de actividad

1.4.2.1.1. Registros de actividad

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto		X	

1.4.2.2. Suplantación de la identidad del usuario

1.4.2.2.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			X
	Alto			

1.4.2.3. Abuso de privilegios de acceso

1.4.2.3.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

1.4.2.4. Difusión de software maligno

1.4.2.4.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto		X	

1.4.2.5. (re-)Encaminamiento de mensajes

1.4.2.5.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano		X	
	Alto			

1.4.2.6. Acceso no autorizado (base de datos)

1.4.2.6.1. Base de datos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

1.4.2.6.2. Otros activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			X
	Mediano			
	Alto			

1.4.2.7. Interceptación de información (comunicaciones)

1.4.2.7.1. Comunicaciones

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

1.4.2.8. Modificación deliberada de la información

1.4.2.8.1. Base de datos y comunicaciones

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto		X	

1.4.2.8.2. Otros activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

1.4.2.9. Destrucción de información

1.4.2.9.1. Base de datos y comunicaciones

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

1.4.2.9.1. Otros activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano		X	
	Alto			

1.4.2.10. Divulgación de información

1.4.2.10.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto		X	

1.4.2.11. Manipulación de programas

1.4.2.11.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto		X	

1.4.2.12. Denegación de servicios

1.4.2.12.1. Base de datos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

1.4.2.12.2. Servidor web

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			X
	Alto			

1.4.2.13. Indisponibilidad del personal

1.4.2.13.1. Personal interno

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

1.4.2.14. Ingeniería social

1.4.2.14.1. Personal interno

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

1.5. Tratamiento de riesgos

Debido a la cantidad de riesgos, en este primer análisis se tratarán los riesgos de nivel **alto** o **muy alto.** En esta categoría caen las siguientes amenazas:

- Destrucción involuntaria de información
- Vulnerabilidades de los programas
- Caída del sistema por agotamiento de recursos
- Manipulación de registros de actividad (log)
- Suplantación de la identidad del usuario
- Acceso no autorizado
- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información
- Manipulación de programas
- Denegación de servicios

Analizados los riesgos y las posibles soluciones y medidas de seguridad a implementar para la mitigación de riesgos y de amenazas, así clasificamos las medidas escogidas y los riesgos que estas mitigan:

1.5.1. Sistemas de control de acceso

> **Definición:** El **control de acceso** consiste en la verificación de si una entidad solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

En los sistemas de ciberseguridad tenemos los siguientes tipos de sistemas de control de acceso: **DAC** (Discretionary Access Control), **RBAC** (Role-Based Access Control) y **MAC** (Mandatory Access Control).

Implementaremos estos sistemas en todos los servidores tanto públicos como internos de nuestra empresa, reduciendo así los siguientes riesgos:

- Destrucción involuntaria de información
- Acceso no autorizado
- Destrucción de información
- Divulgación de información
- Modificación deliberada de la información
- Manipulación de registros de actividad (log)
- Manipulación de programas

1.5.2. Firewall

> **Definición:** En informática, un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Debido a que poseemos servidores como bases de datos con datos internos y otros públicos como una página web, se plantea instalar un firewall en cada sistema con reglas específicas dependiendo de las necesidades de este. Riesgos mitigados:

- Denegación de servicios
- Acceso no autorizado
- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información
- Manipulación de programas
- Manipulación de registros de actividad (log)

1.5.3. Lenguajes / funciones seguras

Muchas funciones en lenguajes de programación como C, corren el riesgo de que un atacante las aproveche para sobreescribir zonas de la memoria manipulando así el funcionamiento del programa a su beneficio. Para evitar estas funciones existen alternativas seguras, las cuales utilizaremos para evitar posibles ataques.

Por otra parte, se utilizarán lenguajes de programación seguros como Java, que corren sobre una máquina virtual lo que imposibilita la manipulación de la memoria.

Con estas medidas mitigamos los siguientes peligros:

- Vulnerabilidades de los programas
- Manipulación de programas

1.5.4. Multi-threading

Aunque esta no sea directamente una medida de seguridad, si no una medida para agilizar los procesos de, por ejemplo, el servidor, podemos evitar problemas como la caída del servidor por saturación de recursos. Se pretende implementar multi-threading en todos los servidores de cara al público, ya que estos serán los que reciban mayor carga. Riesgos mitigados:

- Caída del sistema por agotamiento de recursos

1.5.5. Contraseñas seguras

> **Definición:** Una contraseña segura es una contraseña que otras personas no pueden determinar fácilmente adivinándola o utilizando programas automáticos.

Las contraseñas pueden ser más o menos seguras, a través de caracteres especiales, la alternancia entre mayúsculas y minúsculas… Por eso, seguiremos una política para que los usuarios utilicen contraseñas seguras, evitando así problemas de robos de cuentas.

- Suplantación de la identidad del usuario

1.5.6. Protocolo seguro de transferencia (HTTPS)

> **Definición:** HTTPS (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web.

Cualquier conexión exterior a nuestros servicios web debe mantener indispensablemente la integridad y la confidencialidad para poder cumplir con nuestra política de privacidad. Por este motivo, todo servicio web en nuestro sistema utilizará este protocolo de transferencia. Riesgos mitigados:

- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información

1.5.7. JSON Web Token

> **Definición:** JSON Web Token es un estándar abierto basado en JSON propuesto por IETF para la creación de tokens de acceso que permiten la propagación de identidad y privilegios o claims en inglés.

Los sistemas como bases de datos deben asegurar la accesibilidad correcta de los mismos, ya que no se puede permitir la extracción de información confidencial a usuarios no autorizados. Por este motivo, se utilizará tokens de identificación para asegurar que la información en estos sistemas se proporciona al usuario adecuado. Riesgos mitigados:

- Suplantación de la identidad del usuario
- Acceso no autorizado
- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información

1.5.8. JSON Schema Validator

> **Definición:** JSON Schema is a vocabulary that allows you to annotate and validate JSON documents.

Todos los objetos JSON serán validados mediante esquemas antes de ser utilizados en nuestros servicios, asegurando así que toda información que llega a nuestro sistema cumpla con los estándares previamente definidos. Riesgos mitigados:

- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información

1.5.9. Hash de contraseñas (BCrypt)

> **Definición:** Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Utilizaremos BCrypt para generar hashes con salt de las contraseñas de los usuarios. Además, utilizaremos un slow hashing adaptativo para aumentar la seguridad si algún atacante intenta acceder a una cuenta que no es suya. Riesgos mitigados:

- Suplantación de la identidad del usuario
- Acceso no autorizado
- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información

1.5.10. Spring Security

> **Definición:** Spring Security es un marco Java / Java EE que proporciona autenticación, autorización y otras características de seguridad para aplicaciones empresariales.

Spring Security proporcionará a nuestra página web, nuestro servicio principal de cara al público, de un sistema de roles para evitar que usuarios no autorizados accedan a apartados para los que no tengan permisos, como por ejemplo, que un usuario no logeado no pueda acceder a ningún apartado de la página que no sea el registro o el log-in. Riesgos mitigados:

- Suplantación de la identidad del usuario
- Acceso no autorizado

1.5.11. TLS/SSL (Transport Layer Security)

> **Definición:** Seguridad de la capa de transporte (en inglés: Transport Layer Security o TLS) y su antecesor Secure Sockets Layer (SSL; en español capa de puertos seguros) son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Utilizaremos TLS para securizar la transmisión de datos, cifrando de extremo a extremo las comunicaciones y utilizando un sistema de claves para la autenticación. Riesgos mitigados:

- Suplantación de la identidad del usuario
- Acceso no autorizado
- Interceptación de información
- Modificación deliberada de la información
- Destrucción de información
- Divulgación de información

1.5.12. Copias de Seguridad

> **Definición:** Una copia de seguridad, respaldo, copia de respaldo o copia de reserva (en inglés backup y data backup) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Haremos copias de seguridad en la nube y locales para que en el caso de perder nuestros servidores podamos recuperarlos rápidamente asegurando así la disponibilidad de nuestros servicios. Riesgos mitigados:

- Destrucción involuntaria de información

2. Análisis de riesgos residuales

Una vez definidas las medidas de seguridad propuestas en el análisis de riesgo, y teniendo en cuenta los recursos del grupo, estos son los distintos salvaguardas de nuestro sistema:

- Firewall
- Lenguajes / funciones seguras
- Multi-threading
- Contraseñas seguras
- Protocolo seguro de transferencia (HTTPS)
- JSON Schema Validator
- Hasheo de contraseñas (BCrypt)
- Spring Security
- TLS/SSL (Transport Layer Security)
- Copias de Seguridad

Teniendo en cuenta estas medidas es necesario hacer un segundo análisis para determinar qué nuevos riesgos afronta nuestro sistema y que medidas adicionales podrían solventar estas amenazas.

2.1. Segunda evaluación de riesgos

Una vez detectadas las distintas amenazas potenciales de nuestro sistema, se evalúa el impacto y riesgo potencial de las mismas. Para ello, utilizaremos tablas para determinar el nivel de la amenaza, clasificándolas en **muy bajo**, **bajo**, **mediano**, **alto** y **muy alto.**

Teniendo en cuenta que una vez instaladas las medidas de seguridad este sistema debería ser seguro, las amenazas que antes eran de menor riesgo pasan a ser de mayor riesgo.

2.1.1. Errores y fallos no intencionados

2.1.1.1. Errores de los usuarios

2.1.1.1.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

2.1.1.2. Errores del administrador

2.1.1.2.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			X
	Alto			

2.1.1.3. Difusión de software dañino

2.1.1.3.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.1.1.4. Errores de (re-)encaminamiento

2.1.1.4.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

2.1.1.5. Escapes de información

2.1.1.5.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.1.6. Destrucción de información

2.1.1.6.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

2.1.1.7. Fugas de información

2.1.1.7.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			X
	Alto			

2.1.1.8. Vulnerabilidades de los programas

2.1.1.8.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.1.9. Caída del sistema por agotamiento de recursos

2.1.1.9.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.1.1.10. Indisponibilidad del personal

2.1.1.10.1. Personal interno

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

2.1.2. Ataques intencionados

2.1.2.1. Manipulación de registros de actividad

2.1.2.1.1. Registros de actividad

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.2. Suplantación de la identidad del usuario

2.1.2.2.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			X
	Alto			

2.1.2.3. Abuso de privilegios de acceso

2.1.2.3.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto		X	

2.1.2.4. Difusión de software maligno

2.1.2.4.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.5. (re-)Encaminamiento de mensajes

2.1.2.5.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.1.2.6. Acceso no autorizado (base de datos)

2.1.2.6.1. Base de datos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.6.2. Otros activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo		X	
	Mediano			
	Alto			

2.1.2.7. Interceptación de información (comunicaciones)

2.1.2.7.1. Comunicaciones

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.8. Modificación deliberada de la información

2.1.2.8.1. Base de datos y comunicaciones

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.8.2. Otros activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.1.2.9. Destrucción de información

2.1.2.9.1. Base de datos y comunicaciones

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.9.1. Otros activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.1.2.10. Divulgación de información

2.1.2.10.1. Todos los activos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.11. Manipulación de programas

2.1.2.11.1. Software

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto	X		

2.1.2.12. Denegación de servicios

2.1.2.12.1. Base de datos

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano			
	Alto			X

2.1.2.12.2. Servidor web

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.1.2.13. Indisponibilidad del personal

2.1.2.13.1. Personal interno

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo	X		
	Mediano			
	Alto			

2.1.2.14. Ingeniería social

2.1.2.14.1. Personal interno

		Probabilidad		
		Bajo	Mediano	Alto
Impacto	Bajo			
	Mediano	X		
	Alto			

2.2. Tratamiento de riesgos

Debido a la cantidad de riesgos, en este primer análisis se tratarán los riesgos de nivel **alto** o **muy alto.** En esta categoría caen las siguientes amenazas:

- Errores del administrador
- Destrucción de información
- Fugas de información
- Suplantación de la identidad del usuario
- Acceso no autorizado

Analizados los riesgos y las posibles soluciones y medidas de seguridad a implementar para la mitigación de riesgos y de amenazas, así clasificamos las medidas escogidas y los riesgos que estas mitigan:

2.2.1. Sistemas de control de acceso

> **Definición:** El **control de acceso** consiste en la verificación de si una entidad solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

En los sistemas de ciberseguridad tenemos los siguientes tipos de sistemas de control de acceso: **DAC** (Discretionary Access Control), **RBAC** (Role-Based Access Control) y **MAC** (Mandatory Access Control).

Implementaremos estos sistemas en todos los servidores tanto públicos como internos de nuestra empresa, reduciendo así los siguientes riesgos:

- Errores del administrador
- Destrucción de información
- Fugas de información

2.2.2. JSON Web Token

> **Definición:** JSON Web Token es un estándar abierto basado en JSON propuesto por IETF para la creación de tokens de acceso que permiten la propagación de identidad y privilegios o claims en inglés.

Los sistemas como bases de datos deben asegurar la accesibilidad correcta de los mismos, ya que no se puede permitir la extracción de información confidencial a usuarios no autorizados. Por este motivo, se utilizará tokens de identificación para asegurar que la información en estos sistemas se proporciona al usuario adecuado. Riesgos mitigados:

- Suplantación de la identidad del usuario
- Acceso no autorizado

2.2.3. CSRF tokens

> **Definición:** Un token CSRF es un valor único, secreto e impredecible que genera la aplicación del lado del servidor y se transmite al cliente de tal manera que se incluye en una solicitud HTTP posterior realizada por el cliente.

Utilizaremos esta medida para evitar ataques de CSRF (Cross-Site Request Forgery). Riesgos mitigados:

- Suplantación de la identidad del usuario

2.2.4. “Connection Keep Alive” y colas y exchanges “durables”

Tanto Node-RED como RabbitMQ poseen herramientas para almacenar en disco la información, asegurando así que, en caso de que el servidor falle, no se pierda la información. Riesgos mitigados:

- Destrucción de información
- Fugas de información