Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

GESTIÓN DE RIESGOS – ACADEMIA FORMACON

1. Introducción

Trabajo como CONSULTORA DE SEGURIDAD para la academia **FormaCon S.A.** Antes de poner en funcionamiento la academia se debe hacer una Gestión del Riesgo. Para ello se han considerado los siguientes activos:

- Activos esenciales:
  - Información: expediente académico del alumno
  - Servicios:
    - Gestión de Captación del alumno: servicio de búsqueda y contacto con futuros nuevos alumnos
    - Gestión de clases: visualización en tiempo real y/o diferido de las clases.
    - Gestión de expedientes: Servicio de valoración de notas y creación del certificado de superación.
    - Gestión del Correo electrónico de alumnos y profesores (Se le asignará a cada alumno, profesor y trabajador un correo electrónico @formacon.es).
- Activos que dan soporte:
  - Plataforma Web: medio por el cual se imparten las clases.
  - Plataforma Youtuve: medio donde se almacenan las clases impartidas
  - Plataforma FormaCon S.A.: plataforma interna para la gestión de la información de los nuevos alumnos y personal contratado (profesores, coordinadores, recursos humanos, etc.)
  - Página web: medio por el que se publicitan los servicios de la academia.
  - Datos:
    - Identificativos.
      - Nombre, Apellidos, DNI, correo electrónico, etc
    - Curriculum Vitae.
      - Estudios, formación.
    - Resultado de las notas.
      - Asignaturas, notas.
    - Registro de asistencia a clase.
      - Correo del alumno, clases visualizadas.
    - Videos y Audios grabados de las clases impartidas.
  - Toda la información será almacenada en dos servidores de datos:
    - Servidor youtuve: donde se almacenaran todos los videos
    - Servidor interno: donde se almacenarán todos los datos.

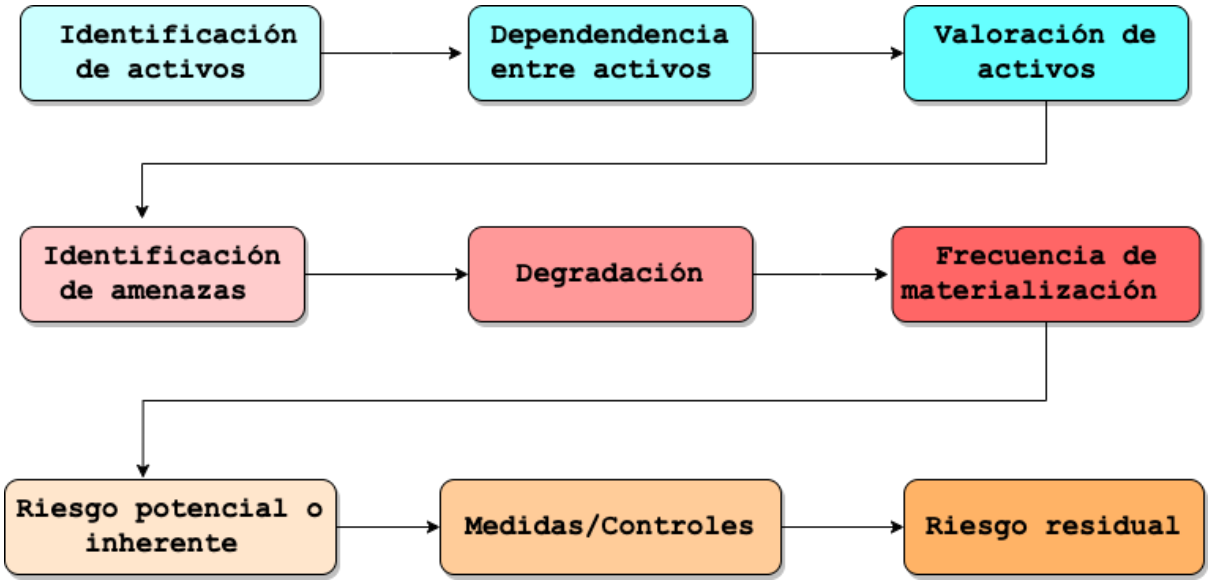
La gestión de riesgos debe de enfocarse desde los activos intangibles, que básicamente son los procesos de la empresa, ello permite entender mejor los objetivos globales de negocio.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

En el primer Nivel estarían los procesos, los cuales tienen toda la información y servicios, denominados activos intangibles de gran valor.

En el segundo nivel se localizarían los activos que soportan la información y servicios como son el hardware, software que procesa los datos –la información materializada en entidades concretas–, infraestructuras, personal de operaciones, etc.

A título ilustrativo la gestión de riesgo se distribuye en las siguientes fases:



Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

2. PREGUNTAS

¿Qué es un activo esencial?

Definimos “activo” como algo de valor para la empresa, sea tangible o no, dado que se considera valioso, debe ser protegido.

Un activo esencial es un recurso o propiedad que es fundamental para el éxito de los objetivos de negocio de una empresa. Hace referencia a aquellos activos que son críticos para la operación y generación de valor de una organización, normalmente son identificados con la información y los servicios. Por ejemplo, marcas como Apple, Microsoft o Inditex son activos esenciales que hay que proteger frente a amenazas como la falsificación o el uso no autorizado de la marca. Otro ejemplo es el servicio de respuesta a incidentes de FireEye, un servicio esencial de la compañía FireEye, actualmente adquirida por Google, FireEye prestaba servicios de respuesta a incidente/forense especializados para incidentes de grandes corporaciones y gobiernos, incidentes que pueden suponer un costo de millones de dólares, Google adquirió la empresa para la seguridad interna de sus servicios de Google Cloud. Otro activo esencial es, por ejemplo, el servicio AWS de Amazon, pionero en ofrecer infraestructura como servicio en la nube, hoy en día la migración a entornos nube –o cloud, en jerga inglesa– se da en la mayoría de grandes empresas.

Se dice que son esenciales dado este tipo de recursos son difíciles de sustituir y su pérdida puede tener un impacto negativo significativo en el desempeño y la continuidad del negocio.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

¿Cuántos tipos de activos existen o se mencionan en el enunciado?

Básicamente existen dos tipos, por un lado, activos esenciales, habitualmente identificados como información y servicios, por otro lado, activos de soporte, subordinados y dependientes de los activos esenciales y cuyo objetivo es dar soporte a los procesos que conforman la información y servicios.

Conforme enunciado podemos distribuirlos de la siguiente forma:

Activos esenciales:

- Información (expediente académico de los alumnos).
- Servicios, a saber:
    - Gestión de Captación del alumno.
    - Gestión de clases.
    - Gestión de expedientes.
    - Gestión del Correo electrónico.

Activos que dan soporte:

- Plataformas Web, Youtuve y FormaCon S.A. (interna) respectivamente.
- Página web.
- Datos, muchos de ellos de carácter personal.
- Servidores –youtuve e interno– que alojan los datos o información materializada.
- Otros activos identificados, no mencionados específicamente como activos en el enunciado, pero se puede deducir:
    - Personal (profesores, administrativo, comerciales, etc.)
    - Infraestructura de comunicaciones.
    - Instalaciones.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

3. PRÁCTICA

3.1 Análisis y Gestión de Riesgos

Se debe realizar un análisis de riesgos de la organización. Para ello se debe llevar a cabo:

- **Gestión de Activos.**

1. Inventario de activos

Activos esenciales	Activo de soporte
Expediente académico de los alumnos	Plataforma Web
Gestión de Captación del alumno	Plataforma YouTuve
Gestión de Clases	Plataforma FormaCon S. A.
Gestión de Expedientes	Página web
Gestión del Correo Electrónico	Datos
	Servidores
	Infraestructura comunicaciones
	Instalaciones
	Personal

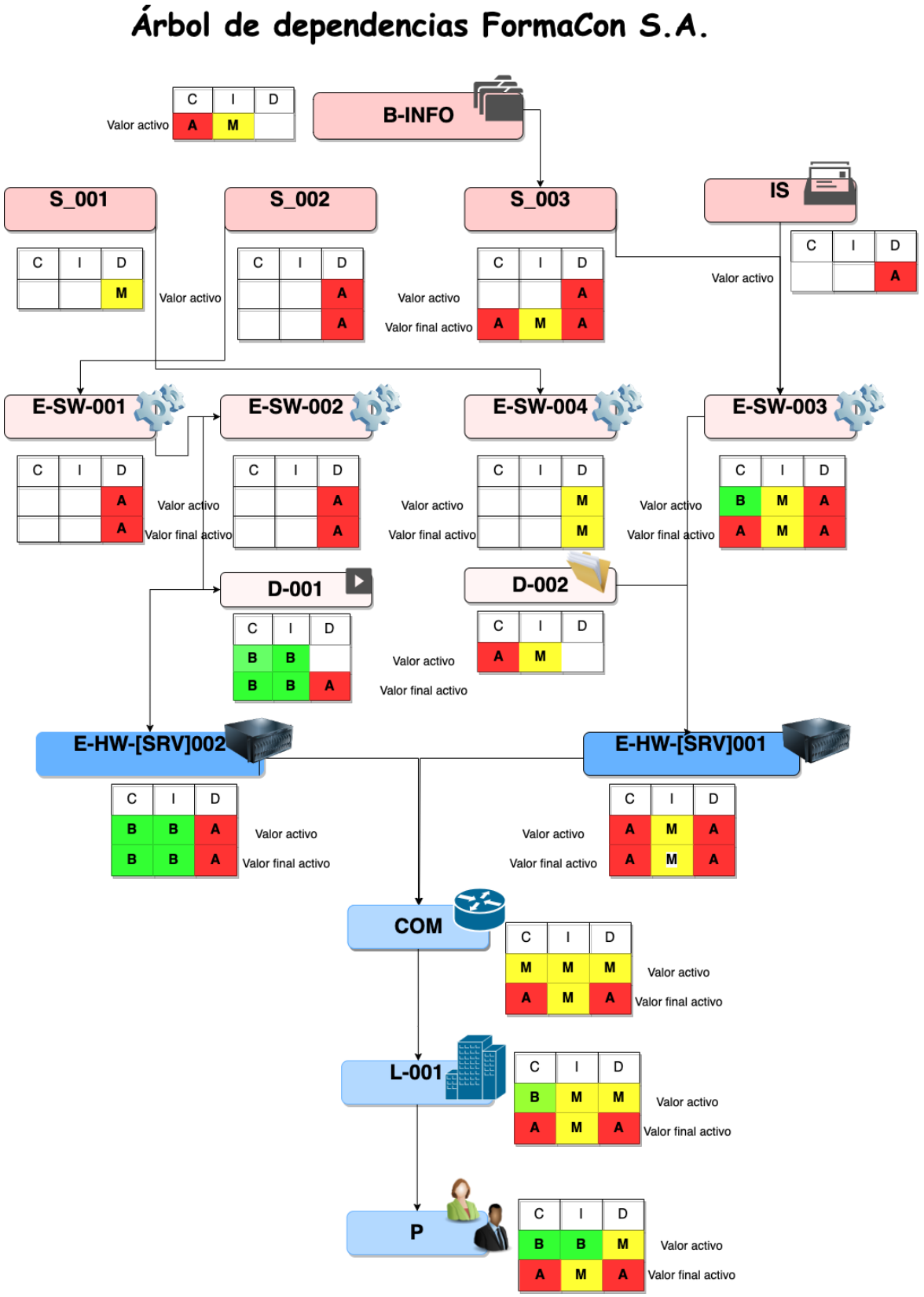
Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

2. Caracterización de los activos.

Código	Activo	Caracterización
B-INFO	Expediente académico	Información
S_001	Gestión de Captación del alumno	Servicio
S_002	Gestión de Clases	Servicio
S_003	Gestión de Expedientes	Servicio
IS	Gestión del Correo Electrónico	Servicio
E-SW-001	Plataforma Web	Software (Aplicación en línea)
E-SW-002	Plataforma YouTuve	Software (PaaS in situ)
E-SW-003	Plataforma FormaCon S.A.	Software (Aplicación interna de gestión)
E-SW-004	Página web	Software (Sitio web)
D-001	Datos	De audio y vídeo
D-002	Datos	Información
E-HW-001	Servidor Interno	Hardware (Servidor de datos)
E-HW-002	Servidor YouTuve	Hardware
COM	Comunicaciones/Red corporativa	Infraestructura
L-001	Istalaciones/Edificio	Infraestructura
P	Usuarios	Personas

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

3. Gestión de dependencias.



Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

En árbol de dependencias se pueden identificar diferentes tipos de activos, incluidos los esenciales en la parte superior y conforme descendemos por el árbol otros activos de soporte. Notar que, además de la información identificada como esencial y los datos, que vamos a considerar como un tipo de información, hay servicios, software, hardware, e infraestructura (redes, instalaciones), incluso personas (usuarios). Es esencial reconocer estos tipos de activos para poder gestionar adecuadamente su seguridad y protección en la academia FormaCon S.A. Cada tipo de activo puede requerir diferentes medidas de seguridad y estrategias para garantizar la confidencialidad, integridad, disponibilidad y protección del dato si ha lugar.

La información (expediente académico) es la base de todos los servicios proporcionados por la academia, y los servicios dependen de las plataformas web y YouTuve para impartir o almacenar las clases que se puedan ver en diferido.

La plataforma interna, Plataforma FormaCon S.A., es el núcleo para la gestión de la información relacionada con los nuevos alumnos y el personal contratado, y la página web se utiliza para la publicidad de los servicios de la academia.

Es en esa plataforma interna en la que se alojan los datos que pueden tener relevancia en cuanto a las dimensiones de la confidencialidad o incluso por ser datos protegidos, esto incluye datos como los identificativos, curriculum vitae, notas, correos… por otro lado, datos como los vídeos de las clases impartidas, se almacenan en el servidor YouTuve y su importancia radica en la disponibilidad, principalmente, ya que los vídeos no contienen, a priori, nada confidencial, pero sí deben estar disponibles para los alumnos del servicio o simplemente no se puede cumplir el objetivo principal por el que pagan estos alumnos, la formación.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

4. Valoración de los Activos

Tipo A.	Código	Descripción de activos	[C]	[I]	[D]	[DP]	Valor
Esencial	B-INFO	Expediente académico	[5]	[3]		[DP]	1.300.000 €
	S_001	Gestión de Captación del alumno			[3]		300.000 €
	S_002	Gestión de Clases			[5]		500.000 €
	S_003	Gestión de Expedientes	[5]	[3]	[5]	[DP]	1.800.000 €
	IS	Gestión del Correo Electrónico			[5]		500.000 €
Soporte	E-SW-001	Plataforma Web			[5]		500.000 €
	E-SW-002	Plataforma Youtuve			[5]		500.000 €
	E-SW-003	Plataforma FormaCon S.A.	[5]	[3]	[5]	[DP]	1.800.000 €
	E-SW-004	Página web			[3]		300.000 €
	D-001	Datos relativos a Youtuve (vídeo)	[1]	[1]			200.000 €
	D-002	Resto de datos	[5]	[3]		[DP]	1.300.000 €
	E-HW-001	Servidor Interno	[5]	[3]	[5]	[DP]	1.800.000 €
	E-HW-002	Servidor Youtuve	[1]	[1]	[5]		700.000 €
	COM	Comunicaciones/Red corporativa	[5]	[3]	[5]	[DP]	1.800.000 €
	L-001	Instalaciones/Edificio	[5]	[3]	[5]	[DP]	1.800.000 €
	P	Usuarios	[5]	[3]	[5]		1.300.000 €

Nota1: en aras de la simplicidad se ha utilizado una escala del 1 al 5, siendo 1 el valor más bajo y 5 el más alto para cada dimensión analizada.

Nota2: estimamos un valor en euros para cada activo esto facilita un análisis cuantitativo con datos financieros, que se entienden muy bien por la alta dirección. La tabla Excel con todo el detalle se encuentra en el documento `GESTION DE RIESGOS.xlsx`.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

Se han tomado en cuenta las siguientes consideraciones a la hora de valorar los activos:

- El servicio de captación del alumno (S_001) y la página web (E-SW-004) se han considerado únicamente en la dimensión de disponibilidad con un nivel medio debido a que básicamente tienen una función de marketing, publicitaria, comercial, y la falta de disponibilidad puntual no supone un problema grave, no tienen dependencias con otros activos que puedan afectar a otras dimensiones. En pocas palabras: unas horas de indisponibilidad no provocarán quejas ni bajas de alumnos, como sí puede ocurrir con otros servicios o activos.

- El resto de los servicios tienen un requisito de alta disponibilidad ya que la imposibilidad de acceso incluso momentánea o circunstancial podría derivar en un daño importante (suspensión de clases si no se puede acceder a la web S_002, devolución de matrículas (bajas de alumnos insatisfechos), fallos en las comunicaciones en el caso del servidor de correo, etc.). El servicio S_003, además, hereda las dimensiones C e I del activo esencial de información B-INFO –expedientes–, afectando y propagando hacia estructura subyacente y nodos hoja del árbol de dependencias ese peso sobre el resto de los activos subordinados, provocando que la infraestructura, software, hardware, comunicaciones e incluso instalaciones, hereden esos niveles críticos en las dimensiones correspondientes.

- El servidor Youtuve, E-HW-[SRV]002 –y activos asociados–, se ha considerado de importancia Alta en cuanto a la dimensión de la disponibilidad, ya que un alumno que no pueda acceder a las clases en vídeo es algo que puede derivar en reclamaciones y otras consecuencias, si bien, por las dependencias entre activos y el tipo de información que contiene, no se consideran el resto de dimensiones como relevantes, al fin y al cabo la información que gestiona, aunque de propiedad privada, no es de carácter confidencial ni secreta.

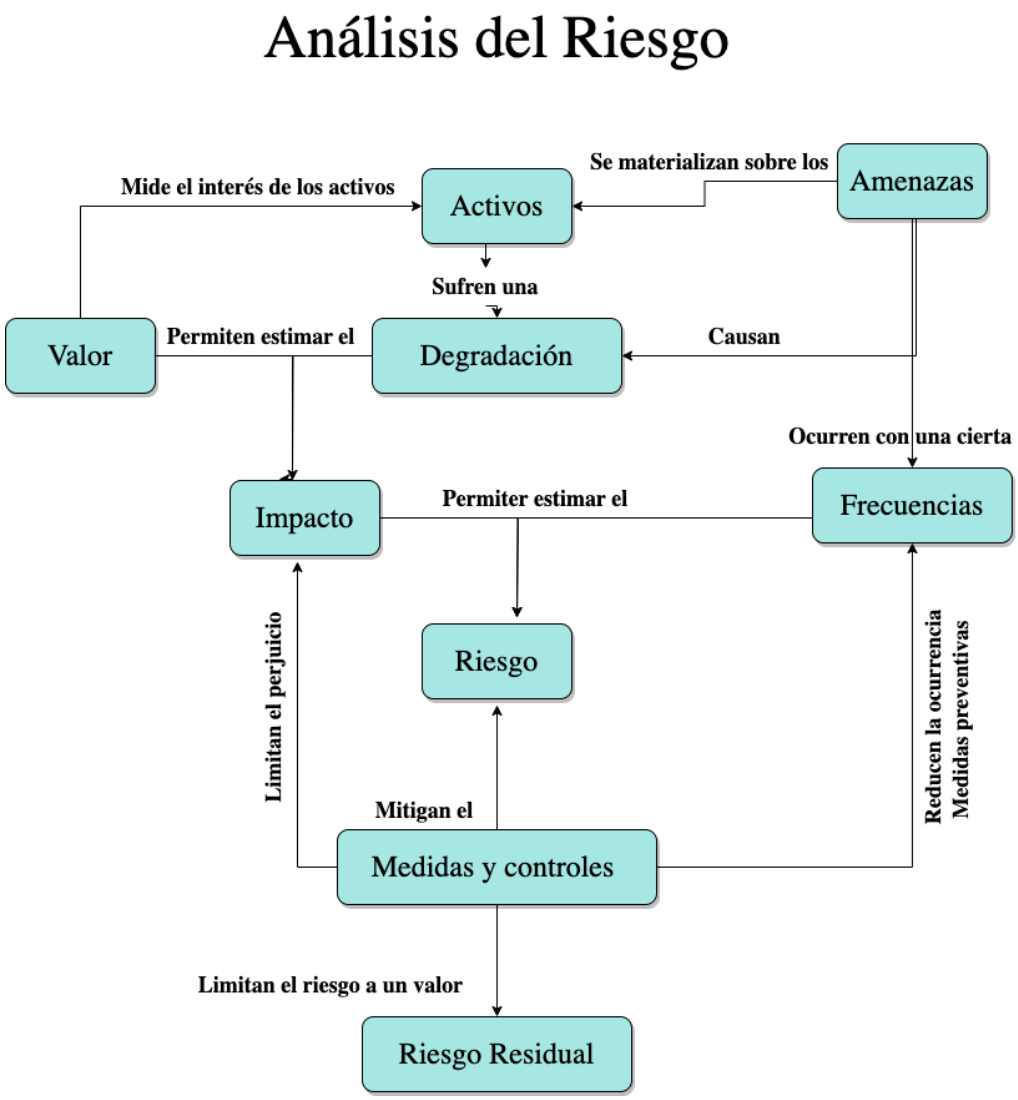
- Los datos se han considerado como una extensión de la información, la materialización de esta en entes o artefactos concretos –ficheros, tablas, bb. dd. etc.–, si bien los propios de Youtuve se valoran conforme al punto previo, el resto de los datos sí contienen incluso datos protegidos que requieren ser protegidos convenientemente. Esto aplica, por dependencias, a la infraestructura subyacente, servidor, comunicaciones –probablemente por ello la segmentación de redes es una buena práctica común– e incluso instalaciones y personal.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

5. Gestión de amenazas.

1. Inventario de amenazas.
    - Únicamente se tendrán en cuenta las amenazas que afecten a la privacidad y protección de datos.
2. Caracterización de las amenazas.
    - Se deben explicar /definir todas las amenazas que apliquen.
3. Valoración de las amenazas

    Se realizará conforme al siguiente esquema.



Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

1. Inventario de amenazas que afectan a la privacidad y PD.

Las amenazas pueden, potencialmente, materializarse con una frecuencia a estimar sobre los activos produciendo la degradación de estos, a esa combinación de probabilidad y degradación –o impacto– se le denomina riesgo potencial o inherente. Aplicando las medidas/controles adecuados es posible mitigar el riesgo inherente, si bien suele quedar un riesgo residual que también habrá que valorar para la toma de decisiones final, si bien no se pide en este ejercicio. Notar que, por formulación del enunciado, nos ceñimos a amenazas **acotadas a privacidad y protección de datos**, que básicamente estimamos que podrían agruparse conforme Magerit v 3.0 tal que:

- [E] Errores y fallos no intencionados
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador
  - [E.4] Errores de configuración
  - [E.8] Difusión de software dañino
  - [E.19] Fugas de información
  - [E.20] Vulnerabilidades de los programas
  - [E.21] Errores de mantenimiento/actualización de programas (software)
  - [E.23] Errores de mantenimiento/actualización de equipos (hardware)

- [A] Ataques intencionados
  - [A.5] Suplantación de la identidad del usuario
  - [A.6] Abuso de privilegios de acceso
  - [A.8] Difusión de software dañino
  - [A.11] Acceso no autorizado
  - [A.14] Interceptación de comunicación (escucha)
  - [A.19] Divulgación de información
  - [A.25] Robo
  - [A.29] Extorsión
  - [A.30] Ingeniería social (picaresca)

Nota: aunque puede parecer que algunas de las amenazas escogidas pueden no tener una relación directa con la privacidad y protección de datos, hay que contemplar que se mira el largo plazo y que muchos incidentes son multifase. Por ejemplo, la difusión de malware puede derivar en compromiso de la infraestructura corporativa por ransomware y, por ende, derivar en indisponibilidad de los sistemas –que se encuentran secuestrados por cifrado fuerte– pero también es habitual un segundo componente de exfiltración de la información que deriva, en fases posteriores, en chantaje y extorsión amenazando con hacer pública la información si no se realiza el pago exigido por el agente amenaza.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

2. Caracterización de las amenazas. Explicar y definir amenazas.

Código	Amenaza	Descripción
E.1	Errores de los usuarios	El factor humano en cuanto a errores no intencionados aplica a la totalidad de la tríada CIA –o CID para Magerit– para casi cualquier tipo de activo.
E.2	Errores del administrador	Ídem previo pero aumentado por el mayor nivel de acceso y privilegios de los administradores.
E.4	Errores de configuración	Conforme Magerit solo afectaría a la dimensión I, pero no coincido ya que es habitual errores de configuración que exponen BB. DD. Completas, por ejemplo, con MongoDB configurados por defecto o errores configuración entornos cloud o repositorios (por ejemplo, un Github público cuando debería ser privado puede exponer el código fuente de tu producto estrella).
E.8	Difusión de malware	Aplica a la tríada CIA completa, propagación inocente, por error, sin pretenderlo –el habitual USB encontrado en el baño–. Puede derivar en incidentes ransomwware, stealers de contraseñas de navegadores y otros que afecten a la privacidad ya sea por exfiltración de información o incidentes derivados.
E.19	Fugas de información	Aplica a [C]. Se conoce como filtración [(1)], a veces por simple indiscreción o falta de concienciación.
E.20	Vulnerabilidades software	[CID]. Operación defectuosa de consecuencias imprevisibles, por ejemplo, emisión de mensajes confidenciales a destinatarios no autorizados.
E.21	No actualización software	[ID] Conforme Magerit, [CIA] en mi opinión, ya que no actualizar software habilita el aprovechamiento de las vulnerabilidades por agentes amenaza y ello aplica a la tríada CIA completo.
E.23	No actualización hardware	[D] conforme Magerit, aunque opino que la instalación de firmware puede corregir vulnerabilidades graves sobre hardware, habitual en routers, IoT, etc.
A.5	Suplantación identidad	[CID] ataque de ingeniería social que suplanta un tercero para simular un contexto verisímil que le permita obtener información de la víctima, por ejemplo, credenciales, con las que podrá realizar otros ataques en fases posteriores.
A.6	Abuso privilegios	[CID]. Normalmente es un ataque de "insider" o empleado malicioso descontento, habitual en entornos de ERE –propensos a sabotaje–, personal que no promociona como él considera, finalización de contratos o personal que se considera maltratado (habitual en subcontratas), en España hay precedente de casos de subcontratas que exponen información de su cliente por venganza, caso "Naturgy y hacker mileurista".
A.8	Difusión de malware	[CID]. En el panorama actual de amenazas probablemente derive en robo de credenciales y exfiltración de información, además de otros –ransomware, etc.–.
A.11	Acceso no autorizado	[CI] Ocurre habitualmente por contrabando de credenciales en foros clandestinos, ataques de diccionario, etc.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

A.14	Interceptación comunicaciones	[C] Puede ocurrir si el atacante logra una posición en la red ventajosa que permita un MiTM, o simplemente si no existen controles como puede ser no usar una VPN en lugares públicos –congresos, hoteles– o cifrado de comunicaciones, por ejemplo, permitir http en lugar de https.
A.19	Divulgación información	[C] De nuevo la causa puede ser un insider o un agente amenaza externo que logra exfiltrar información tras una fase previa de ataque, por ejemplo, un ransomware. También podría darse el caso de soborno, se conoce que un empleado de Tesla recibió una oferta de 1M$ por sus credenciales de acceso por la mafia rusa.
A.25	Robo	[CD] Muy habitual el robo o pérdida de equipos informáticos, incluso por descuido… caso portátil de Hunter Biden en EE. UU. que olvidó en la tienda de reparaciones y contenía información "delicada" (más que sensible). En UK se perdió un USB con información de las cámaras de vigilancia e incluso la ruta de la reina cuando accede al aeropuerto de Heathrow.
A.29	Extorsión	[CID] Se conoce precedente, por ejemplo, tras aparecer empleados en fugas de sitios de citas –aventuras– se les chantajeó para que facilitaran información a cambio de no revelar la infidelidad a su pareja. Hubo incluso suicidios. Vía extorsión o amenazas se puede lograr que un empleado haga cualquier cosa, desconectar una alarma, facilitar acceso, etc. Normalmente suelen utilizar para el registro en los sitios de citas el correo corporativo que no es conocido por los familiares, esto permite la identificación fácil del objetivo por el agente amenaza.
A.30	Ingeniería social	[CID] Se trata de convencer a la víctima para que facilite información que no haría si supiera que está participando de un engaño. Notar que este mismo mes falleció Kevin Mitnick, apodado "El Cóndor", un pionero en este tipo de técnica. Puede derivar acciones como habilitar accesos, facilitar contraseñas, etc.

(1) Filtración: diferencio entre *filtración* –fuga de información con origen interno, muchas veces mera indiscreción– de *exfiltración*, que es el término utilizado habitualmente cuando se saca un activo de un "territorio hostil", por ejemplo, los militares suelen hablar de exfiltración como operaciones de rescate en territorio enemigo u hostil. Una exfiltración ocurriría cuando un intruso trata de extraer furtivamente información hacia infraestructura exógena a la organización, ya que si le descubren podría perder el acceso a la información objetivo.

Nota: se va a respetar el criterio de Magerit, de forma que si Magerit dice que que **E.4, errores de configuración** afecta a la dimensión de la Integridad, así se va a contemplar, si bien, en opinión del analista, un error de configuración como puede ocurrir con un repositorio o una BB. DD. en línea puede exponer información privada y afectar a otras dimensiones como la Confidencialidad.

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

3. Valoración de las amenazas.

C. Activo	C. Amenaza	Descripción	[C]	[I]	[D]	[PD]
B-INFO		Expediente académico	80%	50%		100%
S_001		Captación del alumno			80%	
S_002		Gestión de Clases			80%	
S_003		Expedientes	80%	50%	80%	
IS		Correo Electrónico	80%		80%	100%
E-SW-001		Plataforma Web			80%	
E-SW-002		Plataforma Youtuve			80%	
E-SW-003		Plataforma FormaCon	80%	50%	80%	100%
E-SW-004		Página web			80%	
	E.21	**No actualización sw**		**25%**	**80%**	
	E.4	**Error configuración**		**50%**		
	E.20	**Vulnerabilidades sw**	**80%**	**50%**	**80%**	**100%**
	A.11	**Acceso no autorizado**	**50%**		**50%**	**100%**
D-001		Youtuve (vídeo)	80%		50%	
D-002		Resto de datos	80%		50%	100%
	E.19	**Fuga información**	**25%**			
	A.25	**Robo**	**80%**		**50%**	**100%**
E-HW-001		Servidor Interno	80%	80%	80%	
E-HW-002		Servidor Youtuve	80%	80%	80%	
COM		Red corporativa	80%	80%	80%	
	E.23	**No actualización hw**			**50%**	
	A.8	**Difusión malware**	**80%**	**80%**	**80%**	
L-001		Instalaciones	80%	80%	80%	
P		Usuarios	80%	80%	80%	80%
	A.5	**Suplantación id**	**80%**	**10%**	**10%**	**80%**
	A.30	**Ingeniería social**	**80%**	**10%**	**10%**	**80%**
	A.6	**Abuso privilegios**	**80%**	**80%**	**80%**	**80%**
	A.29	**Extorsión**	**50%**	**50%**	**50%**	**50%**
	E.1	**Error usuarios**	**10%**	**10%**	**10%**	**10%**
	E.2	**Error admin**	**20%**	**20%**	**20%**	**20%**
	E.8	**Difusión malware**	**50%**	**50%**	**50%**	**50%**
	E.19	**Fuga información**	**25%**			

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

6. Riesgo potencial.

A partir de la valoración en euros de los activos, la probabilidad de materialización de cada amenaza y el impacto –en aras de la simplificación se ha elegido como impacto el mayor valor del total de dimensiones analizadas– se ha calculado el riesgo potencial para cada activo y amenaza asociada. Dado el tamaño de la tabla, se puede observar con mejor calidad en la pestaña "Riesgo Potencial" el Excel `GESTION DE RIESGOS.xlsx`.

A continuación, se muestra una captura de la tabla de cálculo de riesgo potencial por activo y amenaza.

Código Activo	Valor	Activo	Amenaza	E.21	E.4	E.20	A.11	E.19	A.25	E.23	A.8	A.5	A.30	A.6	A.29	E.1	E.2	E.8	TOTAL
			Probabilidad	0,25	0,125	0,25	0,125	0,125	0,05	0,125	0,5	0,5	0,5	0,05	0,05	1	0,125	0,125	
			Impacto	80	50	80	50	25	80	50	80	80	80	80	50	10	20	25	
B-INFO	1.300.000 €	Expediente académico		260.000 €	81.250 €	260.000 €	81.250 €												682.500 €
S_001	300.000 €	Captación del alumno		60.000 €	18.750 €	60.000 €	18.750 €												157.500 €
S_002	500.000 €	Gestión de Clases		100.000 €	31.250 €	100.000 €	31.250 €												262.500 €
S_003	1.800.000 €	Expedientes		360.000 €	112.500 €	360.000 €	112.500 €												945.000 €
IS	500.000 €	Correo Electrónico		100.000 €	31.250 €	100.000 €	31.250 €												262.500 €
E-SW-001	500.000 €	Plataforma Web		100.000 €	31.250 €	100.000 €	31.250 €												262.500 €
E-SW-002	500.000 €	Plataforma Youtuve		100.000 €	31.250 €	100.000 €	31.250 €												262.500 €
E-SW-003	1.800.000 €	Plataforma FormaCon		360.000 €	112.500 €	360.000 €	112.500 €												945.000 €
E-SW-004	300.000 €	Página web		60.000 €	18.750 €	60.000 €	18.750 €												157.500 €
D-001	200.000 €	Youtuve (vídeo)						6.250 €	8.000 €										14.250 €
D-002	1.300.000 €	Resto de datos						40.625 €	52.000 €										92.625 €
E-HW-001	1.800.000 €	Servidor Interno								112.500 €	720.000 €								832.500 €
E-HW-002	700.000 €	Servidor Youtuve								43.750 €	280.000 €								323.750 €
COM	1.800.000 €	Red corporativa								112.500 €	720.000 €								832.500 €
L-001	1.800.000 €	Instalaciones																	0 €
P	1.300.000 €	Usuarios						40.625 €				520.000 €	520.000 €	52.000 €	32.500 €	130.000 €	32.500 €	40.625 €	1.368.250 €
																			7.401.375 €

Probabilidad	
Ext. Frecuente	1
MF	0,5
F	0,25
Poco frecuente	0,125
Ext. Raro	0,05

Notar que, para estimar la frecuencia o probabilidad de materialización de la amenaza se ha utilizado la siguiente tabla:

Probabilidad	
Ext. Frecuente	1
MF	0,5
F	0,25
Poco frecuente	0,125
Ext. Raro	0,05

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

7. Gestión de medidas de seguridad.

1. Inventariar las medidas de seguridad que necesitamos para mitigar el riesgo

    - Se deben explicar cómo llevar a cabo cada medida de seguridad.
    - No es necesario valorarlas medidas de seguridad, simplemente hacer una propuesta.

Cod.	Amenaza	Cod.	Control
E.1	Errores de los usuarios	PS.AT	Concienciación y entrenamiento.
E.2	Errores del administrador	H.ST	Segregación de tareas.
E.4	Errores de configuración	H.tools.CC	Herramientas de chequeo de configuración.
E.8	Difusión de malware	H.Tools.AV H.Tools.IDS	Herramientas contra código dañito (perimetrales y en puesto de trabajo). IDS/IPS. Herramientas de detección/prevención en base análisis de tráfico de red y reglas/firmas de amenazas.
E.19	Fugas de información	H.Tools.DLP	Herramientas de monitorización de contenidos. Un servicio de inteligencia que rastree foros públicos y clandestinos también se puede contemplar.
E.20	Vulnerabilidades software	H.VM	Gestión de vulnerabilidades. Aplicar un correcto ciclo de identificación de vulnerabilidades y seguimiento hasta corrección.
E.21	No actualización software	SW.CM	Cambios (actualizaciones y mantenimiento)
E.23	No actualización hardware	HW.CM	Cambios (actualizaciones y mantenimiento)
A.5	Suplantación identidad	H.IA	Identificación y autenticación. Vía llaves hardware compatibles FIDO2, el ROI es muy bueno.
A.6	Abuso privilegios	H.ST H.AU	Segregación de tareas. Aplicación principio menos privilegio necesario. Registro y auditoría, como disuasorio y cumplimiento.
A.8	Difusión de malware	PS.AT H.tools.AV	Formación y concienciación. Herramienta contra código dañino, por ejemplo, un EDR, etc.
A.11	Acceso no autorizado	H.AC H.IA H.Tools.HP	Control de acceso lógico. Identificación y autenticación. De nuevo con llaves hardware FIDO2 o al menos MFA (por ejemplo, con apps como Authy).

Mª del Carmen Llorente Benedicto (carmenllorenteb@gmail.com | mcllorente@eiposgrados.edu.es)

			Honey net/honey pot para detección de actividad extraña.
A.14	Interceptación comunicaciones	D.C S.www S.email COM.C	Cifrado de información. Protección de servicios y aplicaciones web. Protección email. Protección criptográfica
A.19	Divulgación información	H.tools.DLP	Herramientas de monitorización de fugas de información sensible.
A.25	Robo	D.C D.A	Cifrado de la información, así, aunque exista robo no será accesible a terceros. Copias de seguridad (aunque realmente no se pide nada más que contemplar privacidad).
A.29	Extorsión	PS.AT	Formación y concienciación. Por ejemplo, no hacer uso de recursos corporativos (email) en servicios de terceros, de forma que se pueda identificar empresa y empleado por el agente amenaza.
A.30	Ingeniería social	PS.AT	Formación y concienciación.

Nota: de la aplicación de estas medidas o controles se obtendría un riesgo residual, a partir de ese riesgo residual puede decidirse si se acepta o asume el riesgo, si se evita, si se aplican nuevas medidas mitigantes o si se traslada a un tercero (seguro, externalización…). Si bien el ejercicio no solicita nada más.