OBJECTE

El present document desenvolupa el mapa de riscos com a peça clau per a la identificació i la gestió dels riscos relacionats amb la ciberseguretat OT i la protecció de les infraestructures crítiques d'FMB.

L'estructura i el contingut s'han efectuat complint les recomanacions, els preceptes i les obligacions legals contingudes en la documentació següent: **guies d'aplicació de l'Esquema Nacional de Seguretat (CCN), guies d'aplicació del mètode MAGERIT, gestió de riscos segons la metodologia INCIBE, gestió de riscos segons la metodologia CNPIC, legislació vigent aplicable sobre: seguretat en la informació, protecció de dades i infraestructures crítiques, cos normatiu de seguretat de TMB, guies emeses per l'Oficina Nacional de Seguretat (CNI),** en les recomanacions recopilades en la normativa**: UNE-EN IEC 62443, ISO 27000, ISO 27001, ISO 27002, UNEIX-CLC/TS 50701** i, finalment, en la **guia RAILWAY CYBERSECURITY Good practices in cyber risk management emesa per ENISA.**

TAXONOMIA D'AMENACES

Des del punt de vista de la ciberseguretat per als sistemes OT i des de les infraestructures crítiques, una **AMENAÇA** és una situació o una acció potencial de causar un dany.

Per a la gestió de riscos, les amenaces s'agrupen en 5 famílies o tipologies segons la naturalesa de procedència:

- **DESASTRES NATURALS**
- **ORIGEN INDUSTRIAL**
- **ERRORS I FALLADES NO INTENCIONATS**
- **ATACS INTENCIONATS**
- **SEGURETAT NACIONAL (Exclusiu per a infraestructures crítiques)**

CODI	TIPOLOGIA	DESCRIPCIÓ
N	**DESASTRES NATURALS**	**Successos que poden ocórrer per processos naturals, sense intervenció (directa o indirecta) de l'acció humana, que destrueixen o alteren la funcionalitat dels actius**
REF. FAMÍLIA	**TIPOLOGIA**	**DETALL**
N.1	**FOC**	Incendi, combustió, deflagració, temperatura extrema, ignició...
N.2	**AIGUA**	Inundacions, fuites, filtracions, esquitxades, humitat excessiva...
N.*	**FENOMEN ADVERS**	Sinistre natural major, contaminació, fenomen climàtic, fenomen sísmic, fenomen d'origen volcànic, fenomen meteorològic...
CODI	**TIPOLOGIA**	**DESCRIPCIÓ**
I	**ORIGEN INDUSTRIAL**	**Successos que poden ocórrer de forma accidental o deliberada derivats per l'acció (activa o passiva) humana**
REF. FAMÍLIA	**TIPOLOGIA**	**DETALL**
I.1	**FOC**	Incendi, combustió, deflagració, temperatura extrema, ignició...
I.2	**AIGUA**	Inundacions, fuites, filtracions, esquitxades, humitat excessiva...
I.*	**DESASTRES INDUSTRIALS**	Explosions, ensulsiades, contaminació química, sobrecàrrega elèctrica, fluctuació elèctrica, accidents de trànsit, accidents aeris...
I.3	**CONTAMINACIÓ MECÀNICA**	Vibracions, pols, brutícia...
I.4	**CONTAMINACIÓ ELECTROMAGNÈTICA**	Interferències de ràdio, llum ultraviolada, infrarojos, radiacions tèrmiques, camps magnètics, impulsos electromagnètics...
I.5	**AVARIA FÍSICA o LÒGICA**	Fallades sobrevingudes durant el funcionament en equips i/o programes l'origen de les quals pot ser, fins i tot, un defecte de disseny, construcció o implementació...

Bases i paràmetres per fer l'anàlisi

TMB		Proveïdor	
X	NO identifiquem a les nostres dependències		
X	Rieres exteriors o aigües subterrànies en estació		
X	Instal·lacions en intempèrie		

Bases i paràmetres per fer l'anàlisi

TMB		Proveïdor	
X	Avaluar entorn/ubicació	X	El seu sistema
X	Avaluar entorn/ubicació		
X	Avaluar entorn/ubicació		
X	Avaluar entorn/ubicació		
X	Avaluar entorn/ubicació	X	El seu sistema
		X	El seu sistema

I.6	**TALL SUBMINISTRAMENT**	Cessament d'alimentació	X	Avaluar entorn/ubicació	X	El seu sistema
I.7	**CLIMATITZACIÓ**	Deficiències d'humitat, temperatura, etc., als llocs d'ubicació dels actius que provoquen treball fora de rang recomanat	X	Avaluar entorn/ubicació		
I.8	**FALLADA DE COMUNICACIONS**	Incapacitat de portar una dada d'un lloc a un altre. Incapacitat de compartir dades entre equips o sistemes les dades dels quals generen dependència funcional. Incapacitat de gestionar el trànsit de dades existent.	X	En cas que hi hagi una interdependència (sistema TMB)	X	El seu sistema
I.9	**INTERRUPCIÓ DE SERVEIS O SUBMINISTRAMENTS ESSENCIALS**	Serveis o subministraments clau per a l'operació dels equips: paper, refrigerant, tòner...	X	Com impacta després del lliurament	X	El seu sistema
I.10	**DEGRADACIÓ DE SUPORT D'EMMAGATZEMATGE**	Fallades imputables al pas del temps.			X	El seu sistema
I.11	**EMANACIÓ ELECTROMAGNÈTICA**	Radiació de dades o informació indirecta no voluntària o desitjada amb aprofitament de tercers.			X	El seu sistema
CODI	**TIPOLOGIA**	**DESCRIPCIÓ**				
E	**ERRORS I FALLADES NO INTENCIONATS**	**Successos originats per accions no intencionals d'origen humà o a conseqüència d'aquestes**				
REF. FAMÍLIA	**TIPOLOGIA**	**DETALL**	**Bases i paràmetres per fer l'anàlisi**			
E.1	**ERRORS DELS USUARIS**	Equivocacions de persones quan accedeixen als actius o ells usen.	**TMB**		**Proveïdor**	
E.2	**ERRORS DE L'ADMINISTRADOR**	Equivocacions de persones amb responsabilitats en la instal·lació i gestió dels actius.	X	Processos i procediments (formació, manuals...)	X	El seu sistema
E.3	**ERRORS DE MONITORATGE**	Registre/traçabilitat inadequat o deficient d'activitats.	X	Processos i procediments (formació, manuals...)	X	El seu sistema
E.4	**ERRORS DE CONFIGURACIÓ**	Introducció de dades de configuració errònies en els actius.	X	Processos i procediments (formació, manuals...)	X	El seu sistema
			X	Processos i procediments (formació, manuals...)	X	El seu sistema

E.7	**DEFICIÈNCIES EN L'ORGANITZACIÓ**	Accions descoordinades, falta d'assignació de responsabilitats sobre els actius, falta de presa de decisions, absència d'identificació de propietaris o administradors dels actius.	X	Processos i procediments (formació, manuals...)		
E.8	**DIFUSIÓ DE SW NOCIU**	Propagació innocent o inconscient de vulnerabilitats (virus, programari maliciós...).	X	Processos i procediments (formació, manuals...)	X	El seu sistema
E.9	**ERRORS DE REENCAMINAMENT**	Enviament d'informació o dades usant de forma accidental una ruta incorrecta que porta la informació per on no es deuria o on no es deuria. Error d'encaminament que finalitza amb el lliurament de la informació en mans inesperades.			X	El seu sistema
E.10	**ERRORS DE SEQÜÈNCIA**	Alteració accidental de l'ordre dels missatges transmesos.			X	El seu sistema
E.14	**FUITES D'INFORMACIÓ**	La informació acaba en destinataris que, per la seva naturalesa, no haurien de disposar d'aquesta.	X	Conscienciació		
E.15	**ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ**	Alteració accidental de la informació que produeix una pèrdua de confiança de contingut, fiabilitat o traçabilitat d'aquesta.			X	El seu sistema
E.18	**DESTRUCCIÓ DE LA INFORMACIÓ**	Pèrdua involuntària de dades o informació de forma total o parcial.	X	Conscienciació	X	El seu sistema
E.19	**FUITES D'INFORMACIÓ**	Revelació (per qualsevol mitjà) de dades o informació per indiscreció, incontinència o menysvaloració de responsabilitats de secret o custòdia.	X	Conscienciació		
E.20	**FALLADES SISTEMÀTIQUES / VULNERABILITATS ALEATORIS DELS PROGRAMES o SISTEMES**	Defectes o funcionalitat segura no contemplada en el disseny o la construcció. Errors o incompliment de verificació durant el cicle de vida. Defectes en el codi, que finalitza en una operació defectuosa, en l'impacte en la integritat de les dades o en defectes en l'emmagatzematge d'informació. Fallades aleatòries d'alta ocurrència.			X	El seu sistema
E.21	**ERRORS DE MANTENIMENT/ACTUALITZACIÓ DE PROGRAMES**	Defectes en els procediments de mantenibilitat o de controls d'actualització de codi que permeten que s'utilitzin programes amb defectes coneguts. Errors de manteniment de programari que afecten qualsevol dimensió de seguretat als actius.	X	Processos i procediments (formació, manuals...)	X	El seu sistema

E.23	**ERRORS DE MANTENIMENT/ACTUALITZACIÓ D'EQUIPS**	Defectes en els procediments de mantenibilitat o de controls d'actualització dels equips que permeten que s'utilitzin més enllà del temps nominal d'ús o del seu cicle de vida. Errors de manteniment de maquinari que afecten qualsevol dimensió de seguretat als actius.	X	Processos i procediments (formació, manuals...)	X	El seu sistema
E.24	**CAIGUDA DEL SISTEMA PER ESGOTAMENT DE RECURSOS**	Manca de prou recursos que provoca el col·lapse del sistema per exigències d'una alta demanda. Saturació del sistema.			X	El seu sistema
E.25	**PÈRDUA D'EQUIPS**	Pèrdua d'equips que provoca: manca de mitjans per a la prestació de serveis, pèrdua o fuita d'informació o pèrdua d'emmagatzematge de dades. Fallades aleatòries d'alta ocurrència.			X	El seu sistema
E.28	**INDISPONIBILITAT DEL PERSONAL**	Absència no voluntària del lloc de treball. Dany a la disponibilitat del personal.	X	Analitzar casos		
EF19	**INDISPONIBILITAT EDIFICIS/INSTAL·LACIONS**	Indisponibilitat d'edificis o instal·lacions per errors i fallades no autoritzats. Pot separar-se per edificis o instal·lacions clau.	X	Avaluar entorn/ubicació		

CODI	**TIPOLOGIA**	**DESCRIPCIÓ**
A	**ATACS INTENCIONATS**	Fallades deliberades causades per accions d'origen humà

Bases i paràmetres per fer l'anàlisi			
TMB		**Proveïdor**	
		X	El seu sistema
		X	El seu sistema
		X	El seu sistema

REF. FAMÍLIA	**TIPOLOGIA**	**DETALL**
A.3	**MANIPULACIÓ DELS REGISTRES D'ACTIVITAT**	Alteració interessada de dades o d'informació que impacta en qualsevol dimensió de seguretat dels actius, encara que amb especial rellevància en la dimensió INTEGRITAT.
A.4	**MANIPULACIÓ DE LA CONFIGURACIÓ**	Alteració interessada en la configuració dels actius que impacta en qualsevol dimensió d'aquests. Desistiment negligent de funcions.
A.5	**SUPLANTACIÓ DE LA IDENTITAT DE L'USUARI**	Alteració interessada per a l'obtenció il·lícita dels privilegis d'un altre usuari. Usurpació de personalitat. Impacte en la dimensió AUTENTICITAT

A.6	**ABÚS DE PRIVILEGIS D'ACCÉS**	Abús de confiança, en què s'efectua un ús dels privilegis atorgats com a usuari per a finalitats alienes a aquests. Abús de dret. Actuació il·lícita de privilegis per a obtenció de beneficis			X	El seu sistema
A.7	**ÚS NO PREVIST**	Abús de confiança, en què s'efectua un ús no previst dels actius per a finalitats personals.			X	El seu sistema
A.8	**DIFUSIÓ DE SW NOCIU**	Propagació intencionada de programari amb virus, programari maliciós, bombes lògiques, troians...			X	El seu sistema
A.9	**REENCAMINAMENT DE MISSATGES**	Forçament en transmissió de dades o informació per canals o camins indeguts, amb la finalitat de: fer-la arribar a destinataris diferents de qui té la necessitat de conèixer-la, fer-ne un ús fraudulent o incórrer en un alt risc de ser			X	El seu sistema
A.10	**ALTERACIÓ DE SEQÜÈNCIA**	Forçament o manipulació de l'ordre dels missatges o de la informació amb l'ànim que el nou ordre generi una alteració del significat d'aquesta.			X	El seu sistema
A.11	**ACCÉS NO AUTORITZAT**	Accés indegut a un actiu sense disposar d'autorització per a això.			X	El seu sistema
A.12	**ANÀLISI DEL TRÀNSIT**	Accés indegut al monitoratge del trànsit de comunicacions o del traspàs de dades, que permet obtenir conclusions a partir dels atributs: origen, destinació, volum, freqüència...			X	El seu sistema
A.13	**REPUDI**	Negació conscient i deliberada de: accions, actuacions o compromisos associats a la mateixa			X	El seu sistema
A.14	**INTERCEPCIÓ D'INFORMACIÓ**	Accés indegut a informació. Escolta passiva.			X	El seu sistema
A.15	**MODIFICACIÓ DELIBERADA D'INFORMACIÓ**	Alteració intencionada de la informació amb la finalitat d'obtenir un benefici o causar un perjudici.			X	El seu sistema
A.18	**DESTRUCCIÓ D'INFORMACIÓ**	Eliminar o ocasionar danys irreversibles de la informació amb la finalitat d'obtenir un benefici o causar un			X	El seu sistema
A.19	**DIVULGACIÓ D'INFORMACIÓ**	Revelació no autoritzada d'informació. Indicar geolocalització d'actius. Còpies il·legals o il·lícites.			X	El seu sistema
A.22	**MANIPULACIÓ DE PROGRAMES**	Alteració intencionada d'un programa per obtenir un benefici o causar un perjudici.			X	El seu sistema

A.23	**MANIPULACIÓ D'EQUIPS**	Alteració intencionada de maquinari per obtenir un benefici o causar un perjudici. Sabotatge d'un actiu.			X	El seu sistema
A.24	**DENEGACIÓ DE SERVEI**	Alteració intencionada dels recursos per saturar el sistema i provocar-ne la caiguda.			X	El seu sistema
A.25	**ROBATORI**	Sostracció d'actius o d'elements de suport (documents, sistemes d'emmagatzematge d'informació...) que vulneren qualsevol dimensió de seguretat.			X	El seu sistema
A.26	**ATAC DESTRUCTIU**	Destrucció d'actius per vandalisme, atac militar, terrorisme, sabotatge...	X	Avaluar entorn/ubicació	X	El seu sistema
A.27	**OCUPACIÓ ENEMIGA**	Ocupació de llocs físics amb pèrdua de control sobre aquests.	X	Avaluar entorn/ubicació		
A.28	**INDISPONIBILITAT DEL PERSONAL**	Absència voluntària del lloc de treball. Dany a la disponibilitat del personal. Bloqueig d'accessos.	X	Avaluar entorn/ubicació		
A.29	**EXTORSIÓ**	Pressió realitzada mitjançant amenaces o coaccions per obrar en un sentit determinat.	X	La nostra organització	X	La seva organització
A.30	**ENGINYERIA SOCIAL**	Abús, per part interessada d'un tercer, de la bona fe de les persones, amb la finalitat d'obtenir un benefici mitjançant el robatori d'informació personal/confidencial. Manipulació col·lectiva o social.	X	La nostra organització	X	La seva organització
AI25	**INDISPONIBILITAT DE PROVEÏDORS**	Absència deliberada d'un o de més proveïdors: vagues, absentisme laboral, baixes no justificades, bloqueig dels accessos, etc. Aquesta tipologia d'atac afecta directament	X	La nostra organització	X	La seva organització
AI26	**INDISPONIBILITAT D'EDIFICIS/INSTAL·LACIONS**	Indisponibilitat d'edificis/instal·lacions per atacs intencionats d'origen intern o extern.	X	Avaluar entorn/ubicació		

CODI	TIPOLOGIA	DESCRIPCIÓ
SN	**SEGURETAT NACIONAL**	Factors que afecten la seguretat nacional * El tractament es tindrà en compte per determinar els nivells resultants finals, però no s'establiran salvaguardes específiques per a les amenaces d'aquesta família, atès que són fora de l'abast de l'àmbit de FMB. ** Aquests riscos s'actualitzaran de forma anual, ja que són dinàmics en el temps.

Bases i paràmetres per fer l'anàlisi

exclusiva per a IC

REF. FAMÍLIA	TIPOLOGIA	DETALL
SN1	**TENSIÓ ESTRATÈGICA I REGIONAL**	Risc que es produeixin tensions amb impacte directe sobre els interessos nacionals i, fins i tot, sobre la mateixa sobirania. Constitueix una amenaça seriosa per a la seguretat nacional, la màxima expressió de la qual podria arribar a adoptar la forma de conflicte armat.
SN2	**TERRORISME I RADICALITZACIÓ VIOLENTA**	Extremismes expressats mitjançant actes violents, a vegades acompanyats de campanyes propagandístiques.
SN3	**EPIDÈMIES I PANDÈMIES**	Ocasionen danys a persones i tenen importants conseqüències socials i econòmiques en països, societats i ciutadans.
SN4	**AMENACES A LES INFRAESTRUCTURES CRÍTIQUES**	Impossibiliten el desenvolupament normal de l'activitat socioeconòmica i són amenaces, tant físiques com digitals, que podrien portar a una interrupció o negació de serveis.
SN5	**EMERGÈNCIES I CATÀSTROFES**	Diferents tipus d'emergències i catàstrofes originades per causes naturals o derivades de l'acció humana accidental o intencionada.
SN6	**ESPIONATGE I INGERÈNCIES DES DE L'EXTERIOR**	Activitats d'intel·ligència hostils orientades al ciberespionatge, atemptats contra la competitivitat econòmica i la propietat intel·lectual o ús de les IC com a elements dins d'accions o estratègies híbrides.

SN7	**VULNERABILITAT DEL CIBERESPAI**	Ciberatacs de l'exterior, entesos com a accions disruptives que actuen contra sistemes i elements tecnològics. Ús del ciberespai per dur a terme activitats il·lícites, com el cibercrim, el ciberespionatge, el finançament del terrorisme o el foment de la radicalització. S'hi inclou l'ús d'intel·ligència artificial, big data i algorismes per efectuar presa de decisions automàtiques.
SN8	**VULNERABILITAT DE L'ESPAI MARÍTIM**	L'espai marítim és considerat un dels espais comuns globals, espais de connectivitat de fluxos, informació, persones, serveis i béns, la interrupció o obstaculització dels quals pot tenir un impacte econòmic greu.
SN9	**VULNERABILITAT AEROESPACIAL**	Qualsevol disrupció que afecti les aeronaus, els aeroports o les instal·lacions en terra relacionades amb la navegació aèria. Ús il·lícit de vehicles aeris no tripulats considerats com a potencials armes o mitjans per a sabotatges o accions terroristes.
SN10	**INESTABILITAT ECONÒMICA I FINANCERA**	Factors que poden contribuir a la inestabilitat econòmica i financera. S'hi inclouen els desequilibris en les vies de finançament de la hisenda pública; la inestabilitat financera internacional; el frau, l'evasió i la planificació fiscal; la corrupció; el blanqueig de capitals i l'ús indegut dels fons procedents de subvencions i contractes públics. Aquests factors soscaven la seguretat econòmica i provoquen desafecció social de les institucions oficials.
SN11	**CRIM ORGANITZAT I DELINQÜÈNCIA GREU**	El crim organitzat com a amenaça a la seguretat que es caracteritza per la seva finalitat essencialment desestabilitzadora o econòmica.
SN12	**FLUXOS MIGRATORIS IRREGULARS**	Moviments migratoris il·lícits o irregulars les activitats dels quals comporten greus vulneracions de drets humans
SN13	**VULNERABILITAT ENERGÈTICA**	Efectes tècnics o socioeconòmics relacionats amb les fonts d'energia primària amb impacte en la seguretat energètica.

SN14	**PROLIFERACIÓ D'ARMES DE DESTRUCCIÓ MASSIVA**	Exposicions de riscos derivats de la precarietat dels tractats vigents per al control de la proliferació d'armes de destrucció massiva i dels seus vectors de llançament. Amenaça biològica, entesa com l'ús deliberat d'agents patògens, toxines o elements genètics o organismes genèticament modificats nocius per part d'estats, individus, xarxes criminals o organitzacions terroristes. Ús d'armes químiques. Riscos derivats del desviament i contraban de materials de doble ús.
SN15	**EFECTES DEL CANVI CLIMÀTIC I DE LA DEGRADACIÓ**	Riscos —especialment per a l'àrea mediterrània— sobre seguretat ambiental de segona ronda (ones de calor, reducció dels recursos hídrics, desertificació, fenòmens meteorològics adversos, qualitat de l'aire...) derivats del canvi climàtic.
	DEL MEDI NATURAL	Falta de seguretat alimentària (desordres socials)

TAXONOMIA D'ESCENARIS DE CONSEQÜÈNCIA

Els **ESCENARIS DE CONSEQÜÈNCIA** són escenaris finals que podrien materialitzar-se a partir d'amenaces. Cada escenari es vincula a una o una sèrie d'amenaces que, si no es gestionen adequadament, poden derivar en conseqüències adverses, tals com:

- **EXPOSICIÓ DE DADES SENSIBLES**
- **ACCÉS NO AUTORITZAT**
- **PÈRDUA DE DISPONIBILITAT**
- **MALWARE I RANSOMWARE**
- **NO COMPLIMENT**
- **INSUFICIENT CONSCIENCIACIÓ EN SEGURETAT**
- **ATAC A TRAVÉS DE LA CADENA DE SUBMINISTRAMENT**
- **BRETXES EN LA IMPLEMENTACIÓ DE NOVES TECNOLOGIES**
- **AFECTACIÓ A LA SEGURETAT OPERACIONAL**
- **SABOTATGE I ALTERACIÓ D'INTEGRITAT INDUSTRIAL**
- **VIOLACIÓ DE SEGURETAT FÍSICA**
- **ESPIONATGE I PÈRDUA DE PROPIETAT INTEL·LECTUAL**

PROCÉS PER ANALITZAR EL RISC

Prèviament al procés d'avaluació de riscos, TMB determinarà el context sobre el qual podria impactar l'amenaça per a l'organització en cas de materialitzar-se, segons:

Criteris per establir el context	Disponibilitat operacional
	Integritat (Safety)
	Confidencialitat
	Integritat (Negoci)

L'executor d'aquest procés serà:

Modificació sistema o substitució parcial	TMB
Sistema nou o substitució total	Proveïdor

Seguint la metodologia següent:

1. Analitzant la llista d'amenaces, identificar aquelles que es poden produir i INVENTARIAR els possibles tipus d'ATAC que podrien donar-se, tot indicant:
   a. Identificador
   b. Descripció de l'escenari d'atac
   c. Actor(s) d'amenaça considerat(s)
   d. Actiu(s) involucrat(s) en l'escenari
   e. A través de quina/es amenaça/ces
   f. Altres que es considerin d'interès, per exemple, a quina dimensió de seguretat pot afectar – **c**onfidencialitat, **d**isponibilitat, **i**ntegritat, **a**utenticitat, **t**raçabilitat-

   A tall d'exemple:

Id.	Títol	Descripció de l'escenari	Actor	Actiu involucrat	Amenaça
TA_XX	Enginyeria social	Mitjançant enginyeria social, un agent extern podria obtenir credencials d'accés d'empleats dels quals s'ha guanyat prèviament la confiança per obtenir accés a sistemes crítics al centre de control o a les estacions, utilitzant, per exemple, tècniques de phishing	Extern	Servidor, Lloc d'operació...	Enginyeria social

2. AVALUAR LA PROBABILITAT de cada tipus d'atac identificat, determinant:
   a. El nivell d'experiència requerit – EXP
   b. L'equipament necessari – EQP
   c. La finestra d'oportunitat - WOO
   d. El temps necessari - TIM

   Per poder determinar l'índex de probabilitat de l'atac segons:

Avaluació de la probabilitat TS 50701 - taula E.3

EXP	EQP	WOO	TIM	PROBABILITAT
Grup d'experts	A mida	Curta	Llarg	**BAIXA**
Expert	Especialitzat	Moderada	Moderat	**MITJANA**
Avançat	COTS	Llarga	Curt	**ALTA**
Aficionat	Estàndard	Il·limitada	Molt curt	**MOLT ALTA**

3. AVALUAR L'IMPACTE sobre el sistema, per a cada tipus d'atac, considerant la conseqüència de la seva materialització en aquelles dimensions sobre les quals s'impacta, segons el context que s'hagi determinat en taula "Criteris per establir el context":

Avaluació d'impacte TS 50701 - taula E.5				
Cat.	**Disponibilitat operacional**	**Integritat (Safety)**	**Confidencialitat**	**Integritat (Negoci)**
MOLT ALT	Interrupció important de l'operació que afecta la xarxa o la flota o pèrdua del servei per més de 500.000 persones durant un llarg temps.	Accident catastròfic, típicament que afecta un gran nombre de persones i condueix a múltiples fatalitats.	Pèrdua de seguretat relacionada amb la informació. Ex.: credencials, de manera que es concedeix accés directe al sistema i això condueix a seguretat catastròfica, impacte en la disponibilitat i el negoci.	Impacte catastròfic en el negoci que possiblement condueix a la fallida o la pèrdua de la llicència d'operació.
ALT	Gran interrupció d'operació que afecta la xarxa o la flota, o pèrdua del servei per més de 500.000 persones durant un temps significatiu o d'una línia o estació o vehicle per un llarg temps.	Accident crític, típicament que afecta un petit nombre de persones i condueix a una única fatalitat.	Pèrdua de seguretat relacionada amb la informació: l'accés indirecte al sistema és possible (protecció física), l'atacant pot donar ordres que condueixen almenys a disponibilitat crítica, impactes en la seguretat i el negoci.	Impacte crític en el negoci que possiblement condueix a un impacte greu en els ingressos o els guanys (>10 % anualment).
MITJÀ	Interrupció important que afecta la xarxa o la flota o més de 500.000 persones durant un temps curt, o una línia o estació o uns pocs vehicles durant un temps significatiu.	Implicacions de seguretat, que típicament condueixen a lesions que requereixen hospitalització.	Pèrdua de seguretat relacionada amb la informació; l'accés indirecte al sistema és possible (protecció física); l'atacant no pot dur a terme cap ordre relacionada amb la seguretat crítica. Ex.: només és possible l'accés de lectura a dades de diagnòstic; pèrdua de dades que estan sota protecció de la llei o que són comercialment sensibles.	Impacte significant en el negoci que possiblement condueix a un impacte substancial en els ingressos o els guanys (anualment).
BAIX	Interrupció important de l'operació d'una línia o estació o uns pocs vehicles durant un temps significatiu.	Implicacions de seguretat menors, que típicament condueixen a lesions que no requereixen hospitalització.	Pèrdua de dades no rellevants per a la seguretat, dades que estan sota protecció; l'atacant pot fer ús comercial de les dades combinant-les amb una altra informació.	Impacte marginal en el negoci.
Insignif.	Típicament, sense influència.	Típicament, sense implicacions de seguretat.	Pèrdua de dades rellevants insegures, dades que no estan sota protecció.	Impacte negligible en el negoci.

4. Estimar el NIVELL DE RISC POTENCIAL (impacte vs. probabilitat) per a cada tipus d'atac segons:

Nivell de risc		**IMPACTE**			
		BAIX	**MITJÀ**	**ALT**	**MOLT ALT**
PROBABILITAT	**BAIXA**	**Negligible**	**Tolerable**	**No desitjable**	**Intolerable**
	MITJANA	**Tolerable**	**No desitjable**	**Intolerable**	**Intolerable**
	ALTA	**No desitjable**	**Intolerable**	**Intolerable**	**Intolerable**
	MOLT ALTA	**Intolerable**	**Intolerable**	**Intolerable**	**Intolerable**

El criteri d'acceptació del risc és segons:

CATEGORIA ACCEPTACIÓ NIVELL DE RISC	
CATEGORIA	**ACCIONS A APLICAR**
Intolerable	El risc ha d'eliminar-se.
No desitjable	Només s'accepta quan la reducció del risc sigui impracticable i s'acordi un control sobre la base del criteri d'acceptació del risc residual. L'acceptació és per part del responsable del Servei i Informació de FMB.
Tolerable	Acceptable després d'evidència de reducció del risc i valoració de la magnitud de l'impacte en cas d'ocurrència. L'acceptació és per part del responsable del Servei i Informació de FMB.
Negligible	Risc acceptable sense acord, però amb accions de supervisió.

PROCÉS PER ANALITZAR L'ACTIU EN FUNCIÓ DE LES DIMENSIONS DE SEGURETAT

Aquest procés s'ha de dur a terme quan es produeixi un canvi en algun actiu de Suport/Secundari, segons la taxonomia descrita en NTOTIC_010 TAXONOMIA D'ACTIUS, partint de la classificació per a cada dimensió de seguretat –**c**onfidencialitat, **d**isponibilitat, **i**ntegritat, **a**utenticitat, **t**raçabilitat– del sistema essencial del qual forma part.

Per al càlcul del risc resultant, cal seguir la metodologia següent:

1. Avaluar el NIVELL de DEGRADACIÓ que podria donar-se en cas de materialitzar-se l'amenaça, segons:

DEGRADACIÓ		
QUANTITATIU	**QUALITATIU**	**DEFINICIÓ**
BAIXA	**1**	Petita degradació, amb poques conseqüències
MITJANA	**10**	Degradació de la meitat del valor (en sistemes redundats)
ALTA	**100**	Degradació total o molt alta del valor

2. Determinar l'IMPACTE que tindria sobre la dimensió de seguretat afectada, segons:

Impacte		**DEGRADACIÓ**		
		BAIXA	**MITJANA**	**ALTA**
VALOR DE LA DIMENSIÓ DE SEGURETAT	**BAIXA**	**BAIX**	**BAIX**	**BAIX**
	MITJANA	**BAIX**	**MITJÀ**	**MITJÀ**
	ALTA	**BAIX**	**MITJÀ**	**ALT**

* El valor de cada dimensió el donarà la classificació efectuada pel resp. d'Informació i Servei d'FMB

3. Determinar la PROBABILITAT d'ocurrència segons:

PROBABILITAT		
QUANTITATIU	**QUALITATIU**	**DEFINICIÓ**
BAIXA	**Improbable**	L'amenaça es materialitza una vegada entre 5 i 10 anys
MITJANA	**Possible**	L'amenaça es materialitza una vegada entre 1 i 5 anys
ALTA	**Probable**	L'amenaça es materialitza una vegada cada any
MOLT ALTA	**Molt probable**	L'amenaça es materialitza diverses vegades a l'any

4. Estimar el NIVELL DE RISC per a aquesta dimensió segons:

Nivell de risc		**IMPACTE**		
		BAIX	**MITJÀ**	**ALT**
PROBABILITAT	**BAIXA**	**Negligible**	**Tolerable**	**No desitjable**
	MITJANA	**Tolerable**	**No desitjable**	**Intolerable**
	ALTA	**No desitjable**	**Intolerable**	**Intolerable**
	MOLT ALTA	**Intolerable**	**Intolerable**	**Intolerable**

El criteri d'acceptació del risc és segons:

CATEGORIA ACCEPTACIÓ NIVELL DE RISC	
CATEGORIA	**ACCIONS A APLICAR**
Intolerable	El risc ha d'eliminar-se.
No desitjable	Només s'accepta quan la reducció del risc sigui impracticable i s'acordi un control sobre la base del criteri d'acceptació del risc residual. L'acceptació és per part del responsable del Servei i Informació de FMB.
Tolerable	Acceptable després d'evidència de reducció del risc i valoració de la magnitud de l'impacte en cas d'ocurrència. L'acceptació és per part del responsable del Servei i Informació de FMB.
Negligible	Risc acceptable sense acord, però amb accions de supervisió.

SALVAGUARDES

El risc potencial és aquell al qual estarà exposat l'actiu sense cap mena de protecció. Per reduir aquest risc s'han d'aplicar salvaguardes fins a aconseguir el nivell més baix possible —risc residual—.

Es defineixen les salvaguardes o contramesures com aquells procediments o mecanismes tecnològics que redueixen el risc, sigui reduint-ne la probabilitat (preventives) o fitant-ne la degradació:

Efecte	Tipus	Descripció
Preventives	**[PR]**	Preventives [PR]
	[DR]	Dissuasives [DR]
	[EL]	Eliminatòries [EL]
Fiten la degradació	**[IM]**	Minimitzadores
	[CR]	Correctives [CR]
	[RC]	Recuperatives [RC]
Consoliden l'efecte de les altres	**[MN]**	De monitoratge [MN]
	[DC]	De detecció [DC]
	[AW]	De conscienciació [AW]
	[AD]	Administratives [AD]

Del catàleg de Magerit v3, les salvaguardes que s'identifiquen com a aplicables són:

Salvaguarda	Grup	Descripció
[SA] **Assegurament de la disponibilitat**	Protecció dels serveis	Protocols i procediments establerts per garantir la qualitat dels seus productes i serveis
[HW.A] **Assegurament de la disponibilitat**	Protecció dels equips (maquinari)	Protocols i procediments establerts per garantir els materials, físics, destinats a suportar directament o indirectament els serveis
[COM.A] **Assegurament de la disponibilitat**	Protecció de les comunicacions	Redundància de les comunicacions, xarxa interna, punts wifi
[MP.A] **Assegurament de la disponibilitat**	Protecció dels suports d'informació	Virtualització, replicació, duplicació, seguretat, compressió, anàlisi de trànsit, automatització de processos, aprovisionament d'emmagatzematge i tècniques relacionades
[AUX.A] **Assegurament de la disponibilitat**	Protecció dels elements auxiliars	Proteccions d'instal·lació, subministrament elèctric i climatització
[PS.A] **Assegurament de la disponibilitat**	Salvaguardes relatives al personal	Persones que tenen relació amb el sistema d'informació
[H.tools] **Eines de seguretat**	Proteccions generals o horitzontals	FIREWALL, IPS-IDS, ANTIVIRUS, EDR, AD
[S] **Protecció dels serveis**	Protecció dels serveis	Assegurar la disponibilitat i l'accés
[S.www] **Protecció de serveis i aplicacions web**	Protecció dels serveis	Assegurar la disponibilitat, verificar usuaris, 2FA, codis SMS o APP
[SW] **Protecció de les aplicacions informàtiques**	Protecció de les aplicacions (programari)	Abasta maquinari, programari i procediments que identifiquen o minimitzen les vulnerabilitats de seguretat
[COM] **Protecció de les comunicacions**	Protecció de les comunicacions	Protecció d'accessos no autoritzats a la xarxa

Determinant-ne l'eficàcia enfront del risc segons:

Factor	Nivell	Significat
0 %	**L0**	Inexistent
20 %	**L1**	Inicial / ad hoc
40 %	**L2**	Reproduïble, però intuïtiu
60 %	**L3**	procés definit
80 %	**L4**	gestionat i mesurable
100 %	**L5**	optimitzat

PROCÉS PER ANALITZAR EL RISC RESIDUAL

Per al sistema definitiu que s'ha de lliurar —arquitectura global que inclogui les salvaguardes i els mecanismes de seguretat— s'haurà de determinar la probabilitat residual i la degradació residual, segons el tipus de salvaguarda que s'hi hagi emprat, per determinar el risc residual abans de ser transferit i acceptat per FMB.