OBJETO

El presente documento desarrolla el Mapa de Riesgos como pieza clave para la identificación y la gestión de los riesgos relacionados con la Ciberseguridad OT y la protección de las Infraestructuras Críticas de FMB.

Su estructura y contenido se ha efectuado cumpliendo las recomendaciones, preceptos y obligaciones legales contenidas en la documentación siguiente: **Guías de aplicación del Esquema Nacional de Seguridad (CCN), Guías de aplicación del Método MAGERIT, Gestión de Riesgos según metodología INCIBE, Gestión de Riesgos según metodología CNPIC, Legislación Vigente de aplicación sobre: seguridad en la Información, protección de datos e Infraestructuras Críticas, cuerpo Normativo de Seguridad de TMB, Guías emitidas por la Oficina Nacional de Seguridad (CNI),** en las recomendaciones recopiladas en la Normativa**: UNE-EN IEC 62443, ISO 27000, ISO 27001, ISO 27002, UNE-CLC/TS 50701** y por último en la **Guía RAILWAY CYBERSECURITY Good practices in cyber risk management emitida por ENISA.**

TAXONOMÍA DE AMENAZAS

Desde el punto de vista de la Ciberseguridad para los sistemas OT y desde las Infraestructuras Críticas, una **AMENAZA** es una situación o una acción potencial de causar un daño.

Para la Gestión de Riesgos, las amenazas se agrupan en 5 familias o tipologías según su naturaleza de procedencia:

- **DESASTRES NATURALES**
- **ORIGEN INDUSTRIAL**
- **ERRORES Y FALLOS NO INTENCIONADOS**
- **ATAQUES INTENCIONADOS**
- **SEGURIDAD NACIONAL (Exclusivo para infraestructuras críticas)**

COD.	TIPOLOGÍA	DESCRIPCIÓN
N	**DESASTRES NATURALES**	**Sucesos que pueden ocurrir por procesos naturales sin intervención (directa o indirecta) de la acción humana que destruye o altera la funcionalidad de los activos**
REF FAMILIA	**TIPOLOGÍA**	**DETALLE**
N.1	**FUEGO**	Incendio, combustión, deflagración, temperatura extrema, ignición...
N.2	**AGUA**	Inundaciones, escapes, filtraciones, salpicaduras, humedad excesiva...
N.*	**FENÓMENO ADVERSO**	Siniestro natural mayor, contaminación, fenómeno climático, fenómeno sísmico, fenómeno de origen volcánico, fenómeno meteorológico, ...

Bases y parámetros para realizar el análisis			
TMB		**Proveedor**	
X	NO identificamos en nuestras dependencias		
X	Rieras exteriores o aguas subterráneas en estación		
X	Instalaciones en intemperie		

COD.	TIPOLOGÍA	DESCRIPCIÓN
I	**ORIGEN INDUSTRIAL**	**Sucesos que pueden ocurrir de forma accidental o deliberada derivados por la acción (activa o pasiva) humana**
REF FAMILIA	**TIPOLOGÍA**	**DETALLE**
I.1	**FUEGO**	Incendio, combustión, deflagración, temperatura extrema, ignición...
I.2	**AGUA**	Inundaciones, escapes, filtraciones, salpicaduras, humedad excesiva...
I.*	**DESASTRES INDUSTRIALES**	Explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuación eléctrica, accidentes de tráfico, accidentes aéreos...
I.3	**CONTAMINACIÓN MECÁNICA**	Vibraciones, polvo, suciedad...
I.4	**CONTAMINACIÓN ELECTROMAGNÉTICA**	Interferencias de radio, luz ultravioleta, infrarrojos, radiaciones térmicas, campos magnéticos, impulsos electromagnéticos...
I.5	**AVERÍA FÍSICA o LÓGICA**	Fallos sobrevenidos durante su funcionamiento en equipos y/o programas cuyo origen puede ser incluso un defecto de diseño, construcción o implementación...

Bases y parámetros para realizar el análisis			
TMB		**Proveedor**	
X	Evaluar entorno / ubicación	X	Su sistema
X	Evaluar entorno / ubicación		
X	Evaluar entorno / ubicación		
X	Evaluar entorno / ubicación		
X	Evaluar entorno / ubicación	X	Su sistema
		X	Su sistema

I.6	**CORTE SUMINISTRO ELÉCTRICO**	Cese de alimentación	X	Evaluar entorno / ubicación	X	Su sistema
I.7	**CLIMATIZACIÓN**	Deficiencias de humedad, temperatura, etc., en los lugares de ubicación de los activos que provocan trabajo fuera de rango recomendado	X	Evaluar entorno / ubicación		
I.8	**FALLO DE COMUNICACIONES**	Incapacidad de llevar un dato de un lugar a otro. Incapacidad de compartir datos entre equipos o sistemas cuyos datos generan dependencia funcional. Incapacidad de gestionar el tráfico de datos existente.	X	En caso de que haya una interdependencia (sistema TMB)	X	Su sistema
I.9	**INTERRUPCIÓN DE SERVICIOS O SUMINISTROS ESENCIALES**	Servicios o suministros clave para la operación de los equipos: papel, refrigerante, tóner…	X	Como impacta tras la entrega	X	Su sistema
I.10	**DEGRADACIÓN DE SOPORTE DE ALMACENAMIENTO**	Fallos imputables al paso del tiempo.			X	Su sistema
I.11	**EMANACIÓN ELECTROMAGNÉTICA**	Radiación de datos o información indirecta no voluntaria o deseada con aprovechamiento de terceros.			X	Su sistema
COD.	**TIPOLOGÍA**	**DESCRIPCIÓN**				
E	**ERRORES Y FALLOS NO INTENCIONADOS**	**Sucesos originados o como consecuencia de acciones no intencionales de origen humano**				
REF FAMILIA	**TIPOLOGÍA**	**DETALLE**				
E.1	**ERRORES DE LOS USUARIOS**	Equivocaciones de personas cuando acceden o usan los activos.				
E.2	**ERRORES DEL ADMINISTRADOR**	Equivocaciones de personas con responsabilidades en la instalación y gestión de los activos.				
E.3	**ERRORES DE MONITORIZACIÓN**	Inadecuado o deficiente registro/trazabilidad de actividades.				
E.4	**ERRORES DE CONFIGURACIÓN**	Introducción de datos de configuración erróneos en los activos.				

Bases y parámetros para realizar el análisis

TMB		Proveedor	
X	Procesos y procedimientos (formación, manuales…)	X	Su sistema
X	Procesos y procedimientos (formación, manuales…)	X	Su sistema
X	Procesos y procedimientos (formación, manuales…)	X	Su sistema
X	Procesos y procedimientos (formación, manuales…)	X	Su sistema

E.7	**DEFICIENCIAS EN LA ORGANIZACIÓN**	Acciones descoordinadas, falta de asignación de responsabilidades sobre los activos, falta de toma de decisiones, ausencia de identificación de propietarios o administradores de los activos.	X	Procesos y procedimientos (formación, manuales...)		
E.8	**DIFUSIÓN DE SW DAÑINO**	Propagación inocente o inconsciente de vulnerabilidades (virus, malware, ...)	X	Procesos y procedimientos (formación, manuales...)	X	Su sistema
E.9	**ERRORES DE RE-ENCAMINAMIENTO**	Envío de información o datos usando de forma accidental una ruta incorrecta que lleva la información por donde o donde no es debido. Error de encaminamiento que finaliza con la entrega de la información en manos inesperadas.			X	Su sistema
E.10	**ERRORES DE SECUENCIA**	Alteración accidental del orden de los mensajes transmitidos.			X	Su sistema
E.14	**ESCAPES DE INFORMACIÓN**	La información acaba en destinatarios que, por su naturaleza, no debería disponer de la misma.	X	Concienciación		
E.15	**ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN**	Alteración accidental de la información que produce una pérdida de confianza de contenido, fiabilidad o trazabilidad de la misma.			X	Su sistema
E.18	**DESTRUCCIÓN DE LA INFORMACIÓN**	Pérdida involuntaria de datos o información de forma total o parcial.	X	Concienciación	X	Su sistema
E.19	**FUGAS DE INFORMACIÓN**	Revelación (por cualquier medio) de datos o información por indiscreción, incontinencia o minusvaloración de responsabilidades de secreto o custodia.	X	Concienciación		
E.20	**FALLOS SISTEMÁTICOS / VULNERABILIDADES ALEATORIOS DE LOS PROGRAMAS o SISTEMAS**	Defectos o funcionalidad segura no contemplada en el diseño o construcción. Errores o incumplimiento de verificación durante el Ciclo de Vida. Defectos en el código que finaliza en una operación defectuosa, impacto en la integridad de los datos o en defectos en el almacenamiento de información. Fallos aleatorios de alta ocurrencia.			X	Su sistema
E.21	**ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS**	Defectos en los procedimientos de mantenibilidad o de controles de actualización de código que permiten que se utilicen programas con defectos conocidos. Errores de mantenimiento de SW que afectan a cualquier dimensión de seguridad en los activos.	X	Procesos y procedimientos (formación, manuales...)	X	Su sistema

E.23	**ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS**	Defectos en los procedimientos de mantenibilidad o de controles de actualización de los equipos que permiten que se utilicen más allá del tiempo nominal de uso o de su ciclo de vida. Errores de mantenimiento de HW que afectan a cualquier dimensión de seguridad en los activos.	X	Procesos y procedimientos (formación, manuales...)	X	Su sistema
E.24	**CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS**	Carencia de recursos suficientes que provoca el colapso del sistema por exigencias de una alta demanda. Saturación del sistema.			X	Su sistema
E.25	**PÉRDIDA DE EQUIPOS**	Pérdida de equipos que provocan: carencia de medios para la prestación de servicios, pérdida o fuga de información o pérdida de almacenamiento de datos. Fallos aleatorios de alta ocurrencia.			X	Su sistema
E.28	**INDISPONIBILIDAD DEL PERSONAL**	Ausencia no voluntaria del puesto de trabajo. Daño a la disponibilidad del personal.	X	Analizar casos		
EF19	**INDISPONIBILIDAD EDIFICIOS / INSTALACIONES**	Indisponibilidad de edificios o instalaciones por errores y fallos no autorizados. Puede separarse por edificios o instalaciones clave.	X	Evaluar entorno / ubicación		

COD.	**TIPOLOGÍA**	**DESCRIPCIÓN**
A	**ATAQUES INTENCIONADOS**	Fallos deliberados causados por acciones de origen humano

REF FAMILIA	**TIPOLOGÍA**	**DETALLE**	**Bases y parámetros para realizar el análisis**			
			TMB		**Proveedor**	
A.3	**MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD**	Alteración interesada de datos o de información que impactan en cualquier dimensión de seguridad de los activos, aunque con especial relevancia en la dimensión INTEGRIDAD. Dejación negligente de funciones.			X	Su sistema
A.4	**MANIPULACIÓN DE LA CONFIGURACIÓN**	Alteración interesada en la configuración de los activos que impactan en cualquier dimensión de los mismos. Dejación negligente de funciones.			X	Su sistema
A.5	**SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO**	Alteración interesada para la obtención ilícita de los privilegios de otro usuario. Usurpación de personalidad. Impacto en la dimensión AUTENTICIDAD.			X	Su sistema

A.6	**ABUSO DE PRIVILEGIOS DE ACCESO**	Abuso de confianza efectuando un uso de los privilegios otorgados como usuario para fines ajenos a los mismos. Abuso de derecho. Actuación ilícita de privilegios para obtención de beneficios personales.			X	Su sistema
A.7	**USO NO PREVISTO**	Abuso de confianza efectuando un uso no previsto de los activos para fines personales.			X	Su sistema
A.8	**DIFUSIÓN DE SW DAÑINO**	Propagación intencionada de SW con virus, malware, bombas lógicas, troyanos, …			X	Su sistema
A.9	**RE-ENCAMINAMIENTO DE MENSAJES**	Forzado en transmisión de datos o información por canales o caminos indebidos, con el fin de: hacer llegar la misma a destinatarios distintos de quien tiene la necesidad de conocer, hacer un uso fraudulento o incurrir en un alto riesgo de ser interceptada.			X	Su sistema
A.10	**ALTERACIÓN DE SECUENCIA**	Forzado o manipulación del orden de los mensajes o de la información con el ánimo de que el nuevo orden genere una alteración del significado de la misma.			X	Su sistema
A.11	**ACCESO NO AUTORIZADO**	Acceso indebido a un activo sin disponer de autorización para ello.			X	Su sistema
A.12	**ANÁLISIS DEL TRÁFICO**	Acceso indebido a la monitorización del tráfico de comunicaciones o del traspaso de datos, que permite obtener conclusiones a partir de los atributos: origen, destino, volumen, frecuencia, …			X	Su sistema
A.13	**REPUDIO**	Negación consciente y deliberada de: acciones, actuaciones o de compromisos asociados a la propia persona que las niega.			X	Su sistema
A.14	**INTERCEPTACIÓN DE INFORMACIÓN**	Acceso indebido a información. Escucha pasiva.			X	Su sistema
A.15	**MODIFICACIÓN DELIBERADA DE INFORMACIÓN**	Alteración intencionada de la información con el fin de obtener un beneficio o causar un perjuicio.			X	Su sistema
A.18	**DESTRUCCIÓN DE INFORMACIÓN**	Eliminar u ocasionar daños irreversibles de la información con el fin de obtener un beneficio o causar un perjuicio.			X	Su sistema
A.19	**DIVULGACIÓN DE INFORMACIÓN**	Revelación no autorizada de información. Indicar geolocalización de activos. Copias ilegales o ilícitas.			X	Su sistema
A.22	**MANIPULACIÓN DE PROGRAMAS**	Alteración intencionada de un SW para obtener un beneficio o causar un perjuicio.			X	Su sistema

A.23	**MANIPULACIÓN DE EQUIPOS**	Alteración intencionada del HW para obtener un beneficio o causar un perjuicio. Sabotaje de un activo.			X	Su sistema
A.24	**DENEGACIÓN DE SERVICIO**	Alteración intencionada de los recursos para saturar el sistema y provocar su caída.			X	Su sistema
A.25	**ROBO**	Sustracción de activos o de elementos de soporte (documentos, sistemas de almacenamiento de información, ...) que vulneran cualquier dimensión de seguridad.			X	Su sistema
A.26	**ATAQUE DESTRUCTIVO**	Destrucción de activos por vandalismo, ataque militar, terrorismo, sabotaje, ...	X	Evaluar entorno / ubicación	X	Su sistema
A.27	**OCUPACIÓN ENEMIGA**	Ocupación de lugares físicos con pérdida de control sobre ellos	X	Evaluar entorno / ubicación		
A.28	**INDISPONIBILIDAD DEL PERSONAL**	Ausencia voluntaria del puesto de trabajo. Daño a la disponibilidad del personal. Bloqueo de accesos.	X	Evaluar entorno / ubicación		
A.29	**EXTORSIÓN**	Presión realizada mediante amenazas o coacciones para obrar en un sentido determinado.	X	Nuestra organización	X	Su organización
A.30	**INGENIERÍA SOCIAL**	Abuso, por parte interesada de un tercero, de la buena fe de las personas, con el fin de obtener un beneficio mediante el robo de información personal / confidencial Manipulación colectiva o social.	X	Nuestra organización	X	Su organización
AI25	**INDISPONIBILIDAD DE PROVEEDORES**	Ausencia deliberada de uno o de más proveedores: Huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. Esta tipología de ataque afecta directamente a la cadena de suministro.	X	Nuestra organización	X	Su organización
AI26	**INDISPONIBILIDAD DE EDIFICIOS / INSTALACIONES**	Indisponibilidad de edificios / Instalaciones por ataques intencionados de origen interno o externos	X	Evaluar entorno / ubicación		

COD.	TIPOLOGÍA	DESCRIPCIÓN
SN	SEGURIDAD NACIONAL	Factores que afectan a la Seguridad Nacional * El tratamiento se tendrá en cuenta para determinar los niveles resultantes finales, pero no se establecerán salvaguardas específicas para las amenazas de esta familia dado que están fuera del alcance del ámbito de FMB ** Estos riesgos serán actualizados de forma anual, al ser dinámicos en el tiempo)

REF FAMILIA	TIPOLOGÍA	DETALLE
SN1	TENSIÓN ESTRATÉGICA Y REGIONAL	Riesgo de que se produzcan tensiones con impacto directo sobre los intereses nacionales e incluso sobre la propia soberanía, constituye una seria amenaza para la Seguridad Nacional, cuya máxima expresión podría llegar a adoptar la forma de conflicto armado.
SN2	TERRORISMO Y RADICALIZACIÓN VIOLENTA	Extremismos expresados mediante actos violentos, en ocasiones acompañados de campañas propagandísticas.
SN3	EPIDEMIAS Y PANDEMIAS	Ocasionan daños a personas y tienen importantes consecuencias sociales y económicas a países, sociedades y ciudadanos.
SN4	AMENAZAS A LAS INFRAESTRUCTURAS CRÍTICAS	Imposibilitan el normal desarrollo de la actividad socio-económica y son objetivo de amenazas, tanto físicas como digitales, que podrían llevar a una interrupción o negación de servicios.
SN5	EMERGENCIAS Y CATÁSTROFES	Distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana accidental o intencionada.
SN6	ESPIONAJE E INJERENCIAS DESDE EL EXTERIOR	Actividades de inteligencia hostiles orientadas al ciberespionaje, atentados contra la competitividad económica y la propiedad intelectual o uso de las IICC como elementos dentro de acciones o estrategias híbridas.

Bases y parámetros para realizar el análisis

Exclusivo para IICC

SN7	**VULNERABILIDAD DEL CIBERESPACIO**	Ciberataques del exterior, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización. Se incluye el uso de Inteligencia Artificial, Big Data y utilización de algoritmos para efectuar toma de decisiones automáticas.
SN8	**VULNERABILIDAD DEL ESPACIO MARÍTIMO**	El espacio marítimo es considerado uno de los espacios comunes globales, espacios de conectividad de flujos, información, personas, servicios y bienes, cuya interrupción u obstaculización puede tener un impacto económico severo.
SN9	**VULNERABILIDAD AEROESPACIAL**	Cualquier disrupción que afecte a las aeronaves, los aeropuertos o las instalaciones en tierra relacionadas con la navegación aérea. Uso ilícito de vehículos aéreos no tripulados considerados como potenciales armas o medios para sabotajes o acciones terroristas.
SN10	**INESTABILIDAD ECONÓMICA Y FINANCIERA**	Factores que pueden contribuir a la inestabilidad económica y financiera se incluyen los desequilibrios en las vías de financiación de la Hacienda Pública; la inestabilidad financiera internacional; el fraude, la evasión y la planificación fiscal; la corrupción; el blanqueo de capitales y el uso indebido de los fondos procedentes de subvenciones y contratos públicos. Estos factores socavan la seguridad económica y provocan desafección social de las instituciones oficiales.
SN11	**CRIMEN ORGANIZADO Y DELINCUENCIA GRAVE**	El crimen organizado como amenaza a la seguridad que se caracteriza por su finalidad esencialmente desestabilizadora o económica.
SN12	**FLUJOS MIGRATORIOS IRREGULARES**	Movimientos migratorios ilícitos o irregulares cuyas actividades conllevan graves vulneraciones de derechos humanos
SN13	**VULNERABILIDAD ENERGÉTICA**	Efectos técnicos o socioeconómicos relacionados con las fuentes de energía primaria con impacto en la seguridad energética.

SN14	**PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA**	Exposiciones de riesgos derivado de la precariedad de los tratados vigentes para el control de la proliferación de armas de destrucción masiva y de sus vectores de lanzamiento. Amenaza biológica, entendida como el empleo deliberado de agentes patógenos, toxinas o elementos genéticos u organismos genéticamente modificados dañinos por parte de Estados, individuos, redes criminales u organizaciones terroristas, Uso de armas químicas. Riesgos derivados del desvío y contrabando de materiales de doble uso.
SN15	**EFECTOS DEL CAMBIO CLIMÁTICO Y DE LA DEGRADACIÓN**	Riesgos -especialmente para el área mediterránea- sobre seguridad ambiental de segunda ronda (olas de calor, la reducción de los recursos hídricos, la desertificación, fenómenos meteorológicos adversos, calidad del aire, ...) derivados del cambio climático.
	DEL MEDIO NATURAL	Falta de seguridad alimentaria (desordenes sociales)

TAXONOMÍA DE ESCENARIOS DE CONSECUENCIA

Los **ESCENARIOS DE CONSECUENCIA** son escenarios finales que podrían materializarse a partir de amenazas. Cada escenario está vinculado a una o una serie de amenazas que, si no se gestionan adecuadamente, pueden derivar en consecuencias adversas, tales como:

- **EXPOSICIÓN DE DATOS SENSIBLES**
- **ACCESO NO AUTORIZADO**
- **PÉRDIDA DE DISPONIBILIDAD**
- **MALWARE Y RANSOMWARE**
- **NO CUMPLIMIENTO**
- **INSUFICIENTE CONCIENCIACIÓN EN SEGURIDAD**
- **ATAQUE A TRAVÉS DE LA CADENA DE SUMINISTRO**
- **BRECHAS EN LA IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS**
- **AFECTACIÓN A LA SEGURIDAD OPERACIONAL**
- **SABOTAJE Y ALTERACIÓN DE INTEGRIDAD INDUSTRIAL**
- **VIOLACIÓN DE SEGURIDAD FÍSICA**
- **ESPIONAJE Y PÉRDIDA DE PROPIEDAD INTELECTUAL**

PROCESO PARA ANALIZAR EL RIESGO

Previo al proceso de evaluación de riesgos, TMB determinará el contexto sobre el que podría impactar para la Organización en caso de materializarse la amenaza, según:

Criterios para establecer el contexto	Disponibilidad Operacional
	Integridad (Safety)
	Confidencialidad
	Integridad (Negocio)

El ejecutor de este proceso será:

Modificación sistema o sustitución parcial	TMB
Sistema nuevo o sustitución total	Proveedor

Siguiendo la siguiente metodología:

1. Analizando la lista de amenazas, identificar aquellas que se pueden producir e INVENTARIAR los posibles tipos de ATAQUE que podrían darse, indicando:
   a. Identificador
   b. Descripción del escenario de ataque
   c. Actor(es) de amenaza considerados
   d. Activo(s) involucrados en el escenario
   e. A través de que Amenaza(s)
   f. Otros que se consideren de interés, por ejemplo, a qué dimensión de seguridad puede afectar – **C**onfidencialidad, **D**isponibilidad, **I**ntegridad, **A**utenticidad, **T**razabilidad -

   A modo ejemplo:

Id.	Título	Descripción del escenario	Actor	Activo Involucrado	Amenaza
TA_XX	Ingeniería social	Mediante ingeniería social, un agente externo podría obtener credenciales de acceso de empleados de los que se ha ganado previamente su confianza para obtener acceso a sistemas críticos en el Centro de Control o en las estaciones, utilizando por ejemplo técnicas de phishing	Externo	Servidor, Puesto de Operación ...	Ingeniería Social

2. Proceder a realizar la EVALUACIÓN DE LA PROBABILIDAD para cada tipo de ataque identificado, determinando:
   a. El Nivel de Experiencia requerido – EXP
   b. El Equipamiento necesario – EQP
   c. La Ventana de Oportunidad - WOO
   d. El Tiempo necesario - TIM

   Para poder determinar el Índice de Probabilidad del ataque según:

Evaluación de la probabilidad TS 50701- tabla E.3

EXP	EQP	WOO	TIM	PROBABILIDAD
Grupo de expertos	A medida	Corta	Largo	**BAJA**
Experto	Especializado	Moderada	Moderado	**MEDIA**
Avanzado	COTS	Larga	Corto	**ALTA**
Aficionado	Estándar	Ilimitada	Muy corto	**MUY ALTA**

3. Realizar una EVALUACIÓN DE IMPACTO del sistema, para cada tipo de ataque, considerando la consecuencia de su materialización sobre aquellas dimensiones sobre las que se impacta, según el contexto que se haya determinado en tabla "Criterios para establecer el contexto":

Evaluación de impacto TS 50701- tabla E.5				
Cat.	**Disponibilidad Operacional**	**Integridad (Safety)**	**Confidencialidad**	**Integridad (Negocio)**
MUY ALTO	Interrupción importante de la operación que afecta a la red o a la flota o pérdida del servicio para más de 500.000 personas durante un largo tiempo.	Accidente catastrófico, típicamente afectando a un gran número de personas y conduciendo a múltiples fatalidades.	Pérdida de seguridad relacionada con la información. Ej: Credenciales, concediendo acceso directo al sistema y conduciendo a seguridad catastrófica, impacto en la disponibilidad y el negocio.	Impacto catastrófico en el negocio posiblemente conduciendo a la banca rota o la pérdida de la licencia de operación.
ALTO	Gran interrupción de operación afectando a la red o a la flota o pérdida del servicio para más de 500.000 personas durante un tiempo significativo o de una línea o estación o vehículo por un largo tiempo.	Accidente crítico, típicamente afectando a pequeño número de personas y conduciendo a una única fatalidad.	Pérdida de seguridad relacionada con la información, el acceso indirecto al sistema es posible (protección física), el atacante puede realizar comandos conduciendo al menos a disponibilidad critica, impactos en la seguridad y el negocio.	Impacto crítico en el negocio posiblemente conduciendo a un impacto severo en los ingresos o las ganancias (>10% anualmente).
MEDIO	Interrupción importante afectando a la red o la flota o más de 500.000 personas durante un corto tiempo o de una línea o estación o unos pocos vehículos durante un tiempo significativo.	Implicaciones de seguridad, típicamente conduciendo a lesiones que requieren hospitalización.	Pérdida de seguridad relacionada con la información, el acceso indirecto al sistema es posible (protección física) el atacante no puede llevar a cabo ningún comando relacionado con la seguridad critica: Ej: Sólo es posible el acceso de lectura a datos de diagnóstico; pérdida de datos que están bajo protección de la ley o que son comercialmente sensibles.	Impacto significante en el negocio posiblemente conduciendo a un impacto substancial en los ingresos o las ganancias (anualmente).
BAJO	Interrupción importante de la operación de una línea o estación o unos pocos vehículos durante un tiempo significativo.	Implicaciones de seguridad menores, típicamente conduciendo a lesiones que no requieren hospitalización.	Pérdida de datos no relevantes para la seguridad, datos que están bajo protección; el atacador puede hacer uso comercial de los datos combinándolos con otra información.	Impacto marginal en el negocio.
Insignif.	Típicamente, sin influencia	Típicamente, sin implicaciones de seguridad	Pérdida de datos relevantes inseguros, datos que no están bajo protección.	Impacto negligible en el negocio.

4. Realizar la estimación del NIVEL DE RIESGO POTENCIAL (Impacto vs Probabilidad) para cada tipo de ataque según:

Nivel de riesgo		**IMPACTO**			
		BAJO	**MEDIO**	**ALTO**	**MUY ALTO**
PROBABILIDAD	**BAJA**	**Despreciable**	**Tolerable**	**No deseable**	**Intolerable**
	MEDIA	**Tolerable**	**No deseable**	**Intolerable**	**Intolerable**
	ALTA	**No deseable**	**Intolerable**	**Intolerable**	**Intolerable**
	MUY ALTA	**Intolerable**	**Intolerable**	**Intolerable**	**Intolerable**

El criterio de aceptación del riesgo será según:

CATEGORÍA ACEPTACIÓN NIVEL DE RIESGO	
CATEGORÍA	**ACCIONES A APLICAR**
Intolerable	El riesgo debe eliminarse.
No deseable	Sólo será aceptado cuando la reducción del riesgo sea impracticable y se acuerde un control en base al criterio de aceptación del riesgo residual. La aceptación será por parte del Responsable del Servicio e Información de FMB.
Tolerable	Aceptable tras evidencia de reducción del riesgo y valoración de la magnitud del impacto en caso de ocurrencia. La aceptación será por parte del Responsable del Servicio e Información de FMB.
Despreciable	Riesgo aceptable sin acuerdo, pero con acciones de supervisión.

PROCESO PARA ANALIZAR EL ACTIVO EN FUNCIÓN DE LAS DIMENSIONES DE SEGURIDAD

Este proceso se llevará a cabo cuando se produzca un cambio en algún activo de Soporte / Secundario, según la taxonomía descrita en NTOTIC_010 TAXONOMÍA DE ACTIVOS, partiendo de la clasificación para cada dimensión de seguridad – **C**onfidencialidad, **D**isponibilidad, **I**ntegridad, **A**utenticidad, **T**razabilidad – del sistema esencial del que forma parte.

Para el cálculo del riesgo resultante, se deberá seguir la siguiente metodología:

1. Evaluar el NIVEL de DEGRADACIÓN que podría darse en caso de materializarse la amenaza según:

DEGRADACIÓN		
CUANTITATIVO	**CUALITATIVO**	**DEFINICIÓN**
BAJA	**1%**	Pequeña degradación, con pocas consecuencias
MEDIA	**10%**	Degradación de la mitad del valor (en sistemas redundados)
ALTA	**100%**	Degradación total o muy alta del valor

2. Determinar el IMPACTO que tendría sobre la dimensión de seguridad afectada según:

Impacto		**DEGRADACIÓN**		
		BAJA	**MEDIA**	**ALTA**
VALOR DE LA DIMENSIÓN DE SEGURIDAD	**BAJA**	**BAJO**	**BAJO**	**BAJO**
	MEDIA	**BAJO**	**MEDIO**	**MEDIO**
	ALTA	**BAJO**	**MEDIO**	**ALTO**

* El valor de cada dimensión vendrá dado por la clasificación efectuada por el Rble. de Información y Servicio de FMB

3. Determinar la PROBABILIDAD de ocurrencia según:

PROBABILIDAD		
CUANTITATIVO	**CUALITATIVO**	**DEFINICIÓN**
BAJA	**Improbable**	La amenaza se materializa una vez entre 5 y 10 años
MEDIA	**Posible**	La amenaza se materializa una vez entre 1 y 5 años
ALTA	**Probable**	La amenaza se materializa una vez cada año
MUY ALTA	**Muy Probable**	La amenaza se materializa varias veces al año

4. Realizar la estimación del NIVEL DE RIESGO para dicha dimensión según:

Nivel de riesgo		**IMPACTO**		
		BAJO	**MEDIO**	**ALTO**
PROBABILIDAD	**BAJA**	**Despreciable**	**Tolerable**	**No deseable**
	MEDIA	**Tolerable**	**No deseable**	**Intolerable**
	ALTA	**No deseable**	**Intolerable**	**Intolerable**
	MUY ALTA	**Intolerable**	**Intolerable**	**Intolerable**

El criterio de aceptación del riesgo será según:

CATEGORÍA ACEPTACIÓN NIVEL DE RIESGO	
CATEGORÍA	**ACCIONES A APLICAR**
Intolerable	El riesgo debe eliminarse.
No deseable	Sólo será aceptado cuando la reducción del riesgo sea impracticable y se acuerde un control en base al criterio de aceptación del riesgo residual. La aceptación será por parte del Responsable del Servicio e Información de FMB.
Tolerable	Aceptable tras evidencia de reducción del riesgo y valoración de la magnitud del impacto en caso de ocurrencia. La aceptación será por parte del Responsable del Servicio e Información de FMB.
Despreciable	Riesgo aceptable sin acuerdo, pero con acciones de supervisión.

SALVAGUARDAS

El riesgo potencial es aquel al que estará expuesto el activo sin ningún tipo de protección. Para reducir dicho riesgo se aplicarán salvaguardas hasta conseguir el nivel más bajo posible - riesgo residual -.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, ya sea reduciendo la probabilidad (preventivas) o acotando su degradación:

Efecto	Tipo	Descripción
Preventivas	**[PR]**	Preventivas [PR]
	[DR]	Disuasorias [DR]
	[EL]	Eliminatorias [EL]
Acotan la degradación	**[IM]**	Minimizadoras [IM]
	[CR]	Correctivas [CR]
	[RC]	Recuperativas [RC]
Consolidan el efecto de las demás	**[MN]**	De monitorización [MN]
	[DC]	De detección [DC]
	[AW]	De concienciación [AW]
	[AD]	Administrativas [AD]

Del catálogo de Magerit v3, las salvaguardas que se identifican como aplicables son:

Salvaguarda	Grupo	Descripción
[S.A] Aseguramiento de la disponibilidad	Protección de los servicios	Protocolos y procedimientos establecidos para garantizar la calidad de sus productos y servicios
[HW.A] Aseguramiento de la disponibilidad	Protección de los equipos (hardware)	Protocolos y procedimientos establecidos para garantizar los materiales, físicos, destinados a soportar directa o indirectamente los servicios
[COM.A] Aseguramiento de la disponibilidad	Protección de las comunicaciones	Redundancia de las comunicaciones, red interna, puntos WIFI
[MP.A] Aseguramiento de la disponibilidad	Protección de los soportes de información	Virtualización, replicación, duplicación, seguridad, compresión, análisis de tráfico, automatización de procesos, aprovisionamiento de almacenamiento y técnicas relacionadas
[AUX.A] Aseguramiento de la disponibilidad	Proteción de los elementos auxiliares	Protecciones de instalación, suministro eléctrico y climatización
[PS.A] Aseguramiento de la disponibilidad	Salvaguardas relativas al personal	Personas que tienen relación con el sistema de información
[H.tools] Herramientas de seguridad	Protecciones generales u horizontales	FIREWALL, IPS-IDS, ANTIVIRUS, EDR, AD
[S] Protección de los Servicios	Protección de los servicios	Asegurar la disponibilidad y el acceso
[S.www] Protección de servicios y aplicaciones web	Protección de los servicios	Asegurar la disponibilidad, verificar usuarios, 2FA, códigos SMS o APP
[SW] Protección de las Aplicaciones Informáticas	Protección de las applicaciones (software)	Abarca hardware, software y procedimientos que identifican o minimizan las vulnerabilidades de seguridad
[COM] Protección de las Comunicaciones	Protección de las comunicaciones	Protección de accesos no autorizados a la red

Determinando su eficacia frente al riesgo según:

Factor	Nivel	Significado
0%	**L0**	Inexistente
20%	**L1**	Inicial /ad hoc
40%	**L2**	Reproducible, pero intuitivo
60%	**L3**	proceso definido
80%	**L4**	gestionado y medible
100%	**L5**	optimizado

PROCESO PARA ANALIZAR EL RIESGO RESIDUAL

Para el sistema definitivo a entregar – arquitectura global incluyendo las salvaguardas y los mecanismos de seguridad – se deberá determinar la probabilidad residual y la degradación residual, según el tipo de salvaguarda que se haya empleado, para determinar el riesgo residual antes de ser transferido y aceptado por FMB.