Protocolo de Seguridad y GDPR

1. Historia de Versiones

HISTÓRICO DE VERSIONES			
VERSIÓN	**RESPONSABLE**	**FECHA**	**CAMBIOS INTRODUCIDOS**
1.0	Primera versión	18/11/2024	Publicación al Ecosistema CIMA
1.1	TIREA	08/04/2025	Aprobación de los integrantes del comité de crisis
1.2	TIREA	07/10/2025	Actualización Mejora Continua – Excel Registro de incidentes

2. Índice

3. Introducción

3.1. Objetivo del Protocolo

Este documento establece el Protocolo de Ciberseguridad para el Ecosistema CIMA (Conectividad e Intercambio de Información Actualizada entre Entidades Aseguradoras y Corredores de Seguros), en la que su plataforma es gestionada por TIREA. El objetivo de este protocolo es definir procedimientos y directrices a seguir en caso de ciberataque que afecte la integridad, confidencialidad o disponibilidad de los datos y servicios. Este protocolo busca garantizar una respuesta rápida y coordinada ante incidentes de ciberseguridad, minimizando el impacto en las operaciones de los intervinientes que dependen de este Ecosistema.

Los intervinientes serán descritos en el apartado Intervinientes del Ecosistema CIMA

4. Alcance del Protocolo

Este protocolo de ciberseguridad se aplica a todos los procesos asociados con el Ecosistema CIMA. El protocolo abarca la gestión integral de incidentes de ciberseguridad que puedan afectar la confidencialidad, integridad, y disponibilidad de la información y servicios de la plataforma para todos los intervinientes. Incluye los procedimientos para la detección, notificación, diagnostico, recuperación, vuelta a la normalidad y mejora continua ante cualquier ciberataque.

El alcance se centra en abordar tanto amenazas internas como externas y cubre los siguientes escenarios específicos:

1. **Robo de Información**

Incidentes que impliquen la obtención, alteración o utilización de datos, en perjuicio del titular o de un tercero, u otra información que se halle registrada en ficheros o soportes informáticos, electrónicos o telemáticos, gestionados en la Plataforma CIMA. Estos incidentes pueden ocurrir por acceso legítimo o no legítimo, a través de diferentes métodos como la filtración de información, el espionaje industrial o la manipulación de datos dentro del ecosistema.

2. **Indisponibilidad del Ecosistema CIMA**

Incidentes que comprometan la accesibilidad de los servicios proporcionados por la plataforma, tales como ataques de Denegación de Servicio Distribuido (DDoS), infecciones de ransomware, fallos en la infraestructura tecnológica (hardware/software), o cualquier otro evento que resulte en la interrupción masiva del servicio a cualquiera de los intervinientes.

Este protocolo es aplicable a todos los intervinientes asociados que interactúan con la Plataforma CIMA y deben seguirse los procedimientos aquí establecidos para asegurar una respuesta eficaz ante cualquier incidente de ciberseguridad.

4.1. Definiciones y Terminología

Para una mejor comprensión del protocolo, se definen a continuación algunos términos clave utilizados en el documento:

- Ciberseguridad: Conjunto de prácticas, tecnologías, procesos y políticas diseñados para proteger redes, dispositivos, programas y datos de ataques, daños o acceso no autorizado. La ciberseguridad abarca todas las medidas necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de la información digital.

- Incidente: suceso inesperado o no deseado, con consecuencias reales o potenciales, en detrimento de la confidencialidad, integridad o disponibilidad de un sistema de información, o la información que el sistema procesa, almacena o transmite, o que constituye una violación o amenaza inminente de violación de las políticas, normas o procedimientos de seguridad de la organización.

- Incidente de Ciberseguridad: Evento que potencialmente compromete la confidencialidad, integridad o disponibilidad de la información, la seguridad de las redes, sistemas de información y servicios presentes en el ciberespacio o alcanzables a través de éste.

- Datos personales: toda información sobre una persona física identificada o identificable, se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- Datos personales especialmente protegidos por RGPD: tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual u orientaciones sexuales de una persona física.

- Ransomware: Tipo de software malicioso (malware) que cifra los datos de un sistema y exige un rescate a la víctima a cambio de la clave de descifrado. Este ataque afecta principalmente a la disponibilidad y, en algunos casos, a la integridad de la información.

- Ataque de Denegación de Servicio (DoS/DDoS): Ataque cibernético que busca hacer que un servicio o recurso sea inaccesible a sus usuarios legítimos al colapsar el sistema con una sobrecarga de tráfico o solicitudes. Un DDoS (Distributed Denial of Service) es una versión más avanzada que utiliza múltiples sistemas comprometidos para lanzar el ataque.

- Filtración de Datos: Proceso por el cual un atacante consigue transferir información desde la red interna de una organización hacia una ubicación controlada por el atacante en la cual no está prevista o autorizada compartir dicha información. Suele ser el objetivo final de un ataque avanzado que ha logrado penetrar las defensas de seguridad.

- Gestión de Crisis: todos los procedimientos seguidos para detectar, analizar, limitar un incidente, coordinación de todas las acciones y comunicaciones necesarias durante un incidente para minimizar su impacto y restaurar la confianza de las partes interesadas.

- Plan de respuesta a ciber incidentes: Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un ciber incidente.

- Equipo de Recuperación: Equipo especializado encargado de gestionar y coordinar la respuesta ante un incidente de ciberseguridad.

- Partes Interesadas: Entidades aseguradoras, corredores de seguros, empresas tecnológicas, proveedores de firma, autoridades regulatorias y organismos de seguridad del Estado que interactúan con el Ecosistema CIMA.

- Actores Internos: Aquellos usuarios del ecosistema o cualquier personal con acceso a los sistemas y datos de la organización que, intencionalmente o por negligencia, pueden provocar incidentes de seguridad.

- Actores Externos: Atacantes o entidades externas que intentan acceder sin autorización a los sistemas de la organización para robar, manipular o destruir información.

- Ecosistema CIMA: se refiere al conjunto de todos los actores, que interactúan dentro de la Plataforma CIMA para facilitar el intercambio de información.

- Plataforma CIMA: es la infraestructura tecnológica gestionada por TIREA que permite la conectividad y el intercambio de información.

4.2. Contexto Legal y Normativo

El protocolo está alineado con la legislación vigente en España en materia de ciberseguridad y protección de datos, incluyendo, pero no limitado a:

- Reglamento General de Protección de Datos (GDPR): Establece las obligaciones para la protección de datos personales y las responsabilidades en caso de violaciones de datos.

- Ley de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD): Refuerza las normas del GDPR en el contexto español.

- Directiva NIS2 (Seguridad de Redes y Sistemas de Información): Define las medidas que deben tomar los operadores de servicios esenciales y los proveedores de servicios digitales para gestionar los riesgos de ciberseguridad.

- Reglamento DORA (Digital Operational Resilience Act): Establece un marco de resiliencia operativa digital para las entidades financieras, incluidas las aseguradoras y sus proveedores de servicios críticos. DORA impone requisitos específicos en cuanto a la preparación, gestión de incidentes, comunicaciones y continuidad del negocio.

La gestión de un posible ciberincidente conforme a este marco regulador, es fundamental para proteger la información sensible de las entidades aseguradoras, corredores de seguros y clientes finales, y para garantizar el cumplimiento de las normativas de ciberseguridad aplicables.

Sin perjuicio de lo regulado en este procedimiento, el Responsable del Tratamiento del Dato en función del escenario, tendrá que evaluar y realizar las gestiones de notificación o comunicación a los afectados que considere y que quedarían fuera del ámbito de este protocolo.

5. Contexto

En un entorno digital cada vez más interconectado, la ciberseguridad y la resiliencia operativa se han convertido en elementos críticos para las organizaciones, especialmente en sectores altamente regulados como el sector asegurador. La Plataforma CIMA trata datos especialmente protegidos y procesos críticos que, ante diversos tipos de ciberataques, pueden hacerla vulnerable. Este protocolo de ciberseguridad está diseñado para mitigar los riesgos y fortalecer la respuesta ante incidentes de ciberseguridad.

Además, es importante destacar el impacto de la nueva normativa europea DORA (Digital Operational Resilience Act) en el contexto del protocolo. DORA establece un marco normativo que refuerza la resiliencia operativa digital de las entidades financieras, incluidas las aseguradoras, exigiendo que implementen medidas específicas de ciberseguridad, gestión de incidencias y continuidad de negocio.

5.1. Ámbito de Aplicación

Está definido por la necesidad de cumplir con una serie de normativas y estándares que rigen la seguridad de la información, la protección de datos personales, y la resiliencia operativa digital en el sector asegurador en España y la Unión Europea.

Este protocolo se aplica específicamente a los servicios prestados al Ecosistema CIMA y está diseñado para abordar dos escenarios críticos de ciberseguridad: *Robo de información* y la *Indisponibilidad del Ecosistema CIMA*. Las consecuencias potenciales de estos ataques incluyen:

- Compromiso de Datos Personales y Financieros: robo de datos personales de los clientes, como nombres, direcciones, números de identificación, información financiera, e historial de seguros.

- Interrupción de Operaciones Comerciales: es crucial para que las entidades aseguradoras y corredores intercambio de información relativa a la gestión de pólizas y siniestros. Cualquier interrupción puede afectar gravemente las operaciones diarias.

- Cumplimiento Normativo y Sanciones: incidente de robo de datos o de indisponibilidad en los que haya riesgo en el Ecosistema CIMA debe notificarse a las autoridades competentes. La falta de notificación o la gestión inadecuada del incidente puede conllevar la imposición de multas y/o sanciones.

- Daños a la Reputación y Confianza del Cliente: una brecha de seguridad en la que se pudieran ver comprometidos los datos afectaría la reputación de los intervinientes, generando una pérdida de confianza significativa.

- Responsabilidad Legal: sanciones bajo el RGPD y DORA, así como demandas judiciales por cualquiera de las partes afectadas, son riesgos claros que deben gestionarse mediante un protocolo robusto de ciberseguridad.

- Responsabilidad Financiera: ser tenidas en cuenta tanto una posible pérdida directa de ingresos por interrupciones prolongadas como por la falta de preparación ya que puede suponer la imposición de sanciones.

6. Roles y Responsabilidades

Este apartado define los roles y responsabilidades de todos los actores relevantes involucrados en la implementación y gestión del protocolo de ciberseguridad. La definición clara de responsabilidades asegura una respuesta coordinada y eficaz ante los incidentes de ciberseguridad, garantizando el cumplimiento de los requisitos normativos y la rápida recuperación ante incidentes.

6.1. Intervinientes del Ecosistema CIMA

Los intervinientes del Ecosistema CIMA son aquellos actores que interactúan directa o indirectamente con la plataforma y pueden verse afectados o ser necesarios para la gestión de un incidente de ciberseguridad. Estos intervinientes incluyen:

- Entidades Aseguradoras: Persona jurídica que, autorizada para ejercer la actividad aseguradora, celebra contratos de seguro privado. Respecto del Ecosistema CIMA, con Responsables del Tratamiento del Dato y deben estar preparadas para responder ante incidentes de seguridad que puedan comprometer los datos de pólizas y transacciones. Las entidades aseguradoras utilizan la plataforma CIMA para el intercambio de información con los corredores de seguros y para la firma digital de documentos.

- Corredores de Seguros: Persona física o jurídica que actúa como mediador de seguros entre el cliente y varias entidades aseguradoras de forma independiente, ofreciendo asesoramiento profesional e imparcial para la cobertura de riesgos. Utilizan la Plataforma CIMA, para el intercambio de información con las entidades aseguradoras y para participar en el proceso de firma digital de pólizas que la entidad envía a sus clientes. Los corredores son Responsables del Tratamiento del Dato, intermediarios que manejan información de sus clientes a través de CIMA, siendo críticos en la comunicación y gestión de incidentes.

- Agente/OBSV: Representante o distribuidor de seguros que facilita la venta y administración de pólizas. La responsabilidad seria de Encargado del Tratamiento del Dato, y deben cumplir con los requisitos de ciberseguridad y normativas que correspondan.

- TIREA (Tecnologías de la Información y Redes para las Entidades Aseguradoras): Proveedor de servicios tecnológicos que, como Encargado del Tratamiento del Dato, es quién comercializa, gestiona, mantiene e implanta los requerimientos de seguridad de la Plataforma CIMA.

- Empresa Tecnológica: Proveedor estratégico del software de mediación de la Plataforma CIMA para Agentes y Corredores que lo contraten. Como responsables de componentes específicos del sistema y sus datos son Encargado del Tratamiento del Dato, y deben cumplir con los requisitos de ciberseguridad y normativas.

- Proveedor de Firma: Proveedor de servicios de firma digital para la autenticación de documentos y transacciones realizadas en la Plataforma CIMA. La

responsabilidad seria de Subencargado del Tratamiento del Dato, y deben cumplir con los requisitos de ciberseguridad y normativas que correspondan.

Otros posibles intervinientes:

- Tomador: Persona física o jurídica que contrata una póliza de seguro.

A continuación, se muestra el flujo de comunicación entre los intervinientes del ecosistema CIMA y su rol con el tratamiento del dato:

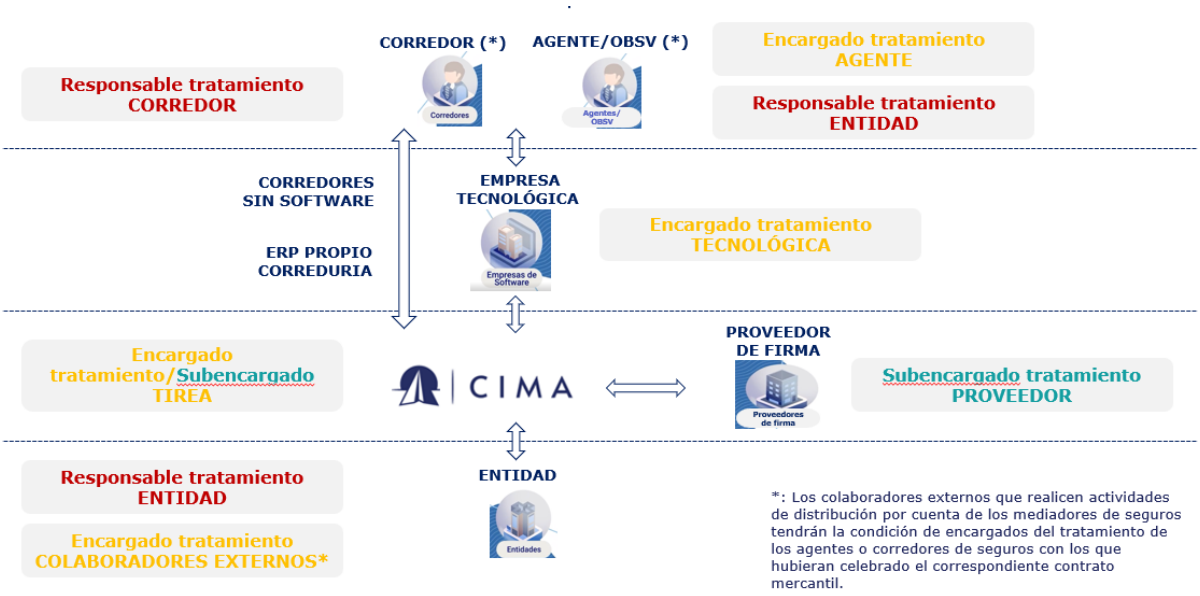


Ilustración 1 Intervinientes del Ecosistema CIMA

6.2. Equipos Involucrados

Para una gestión eficaz de incidentes de ciberseguridad en el Ecosistema CIMA, se dividen los recursos humanos en tres equipos clave: el Equipo de Evaluación Inicial, el Comité de Crisis y el Equipo de Recuperación. Esta estructuración permite una respuesta rápida, coordinada y eficiente, garantizando tanto la contención del incidente como la restauración de servicios y sistemas críticos.

6.2.1. Equipo de Evaluación Inicial:

El Equipo de Evaluación Inicial es el grupo encargado de realizar la valoración primera del incidente. Su función principal es determinar el alcance y la gravedad del incidente, y decidir si es necesario activar el Comité de Crisis. Este equipo actúa como el primer nivel de respuesta, evaluando los indicadores de compromiso (direcciones de IP sospechosas, patrones de tráfico inusuales, cambios en los registros o en los archivos de programa…) y valorando el impacto potencial del incidente en la operativa y en la seguridad de la información.

A continuación, se describen los involucrados:

- Representantes de TIREA: Como proveedor de la Plataforma CIMA, TIREA tiene un papel fundamental en la identificación, análisis y evaluación del incidente. Los representantes de TIREA, especialistas en tecnología y sistemas, son responsables de:
  - Recopilar y analizar información técnica del incidente.
  - Evaluar la infraestructura afectada y determinar si hay vulnerabilidades en los sistemas tecnológicos de CIMA.
  - Coordinar las primeras respuestas técnicas y evaluar el alcance técnico de la amenaza.

- Responsable de Comunicación interno y externo de TIREA: será el encargado de ser el nexo de unión de las comunicaciones entre el Equipo de Evaluación inicial y el Responsable del Comité de Crisis durante la gestión de la crisis. Además, consensuará con el Responsable del Comité de Crisis la activación o no del Comité de Crisis.
- Representante(s) del Interviniente Afectado: El interviniente del Ecosistema CIMA directamente afectado debe disponer de un/os representante/s con conocimiento de sus operaciones internas. Por ejemplo, roles como CISO, DPO, Responsable de Seguridad, entre otros, deberán:
  - Proporcionar información sobre el impacto operativo y potenciales daños que el incidente podría estar causando.
  - Colaborar con TIREA para entender cómo el incidente afecta los procesos y asegurar que la respuesta sea alineada a las necesidades del ecosistema.
  - Gestionar y coordinar la respuesta interna de la empresa y mantener una línea de comunicación directa con el resto de los integrantes del Equipo de Evaluación Inicial.
  - Comunicar e involucrar a la figura de Responsable del Tratamiento de Datos, en el caso de que la incidencia se produjese en un interviniente con figura de Encargado del Tratamiento de Datos.

- Responsable del Comité de Crisis: Actúa como colaborador de este equipo en la fase de evaluación, dará apoyo en:
  - Evaluar criterios para determinar el alcance del incidente.
  - Determinar, junto con el Responsable de Comunicación interno y externo de Tirea, si el incidente requiere la activación del Comité de Crisis.

6.2.2. Comité de Crisis:

El Comité de Crisis es el equipo establecido y consensuado con la Comisión CIMA, encargados de la gestión estratégica durante un incidente de ciberseguridad. Este equipo se activa ante la materialización de un incidente grave que impacta en la confidencialidad, integridad, o disponibilidad de la información y servicios de CIMA. Sus responsabilidades incluyen la toma de decisiones críticas, la coordinación general de la respuesta, y la comunicación tanto interna como externa.

A continuación, se describen los miembros permanentes:

- Representantes de las Entidades Aseguradoras: Como Responsables del Tratamiento de Datos e implicación directa en la operación del Ecosistema CIMA.

  Tomar en consideración: La entidad que ostenta la figura de Responsable del Comité de Crisis es la misma que la entidad que preside la Comisión CIMA. Las entidades que conforman este Comité serán las entidades que constituyen la Comisión CIMA.

- Organizaciones de Corredores: Como Responsables del Tratamiento de Datos e implicación directa en la operación del Ecosistema CIMA.

  Tomar en consideración: Los 2 representantes de Corredores de este Comité son las organizaciones que ostentan las vicepresidencias de la Comisión CIMA.

- Tecnologías de la Información y Redes para las Entidades Aseguradoras TIREA: Como Encargado del Tratamiento de Datos e implicación directa en la operación de la Plataforma y Ecosistema CIMA.

- Empresa Tecnológica: Como Encargado del Tratamiento de Datos e implicación directa en la operación del Ecosistema CIMA.

  Tomar en consideración: El representante de las Empresas Tecnológicas se elegirá entre las empresas del Comité Técnico CIMA.

La renovación de los representantes del Comité de Crisis será cada 2 años, coincidiendo con la renovación en la Comisión CIMA.

A continuación, se describen los miembros invitados:

- Interlocutores del Ecosistema CIMA: Cualquier interviniente, como Responsables del Tratamiento de Datos o Encargado del Tratamiento de Datos e implicación directa en la operación en función del origen y afectación de la crisis.

6.2.3. Equipo de Recuperación:

El Equipo de Recuperación es responsable de la restauración de sistemas y servicios, así como de la aplicación de medidas correctivas y de mejora tras un incidente de ciberseguridad. Este equipo tomará en consideración las propuestas establecidas por el Comité de Crisis.

Las personas involucradas serán en función del origen del incidente y el interviniente del Ecosistema CIMA afectado.

6.3. Funciones por Fase del Protocolo

1. Detección y Notificación:
   - Determinación del alcance del incidente.
   - Valoración inicial del impacto.
   - Decisión de activación del Comité de Crisis.
   - Coordinación de la notificación inicial.

2. Diagnóstico y Gestión de la Crisis:
   - Análisis detallado del incidente
   - Toma de decisiones críticas
   - Coordinación de la respuesta
   - Gestión de la comunicación

3. Recuperación y Vuelta a la Normalidad:
   - Implementación de medidas de recuperación
   - Reintegración de los sistemas

- Pruebas y validaciones
- Restauración

4. Mejora Continua:
   - Análisis post-incidente
   - Redacción Informe del incidente
   - Revisión del protocolo
   - Establecer ejercicios de pruebas/simulacros
   - Difusión de lecciones aprendidas

7. Evaluación de Amenazas y Análisis de Riesgos

7.1. Identificación de Amenazas

El alcance del presente documento se centra en los escenarios de robo de información e indisponibilidad del Ecosistema CIMA, estos eventos adversos pueden afectar a los activos de las partes interesadas.

A continuación, se aborda una descripción para cada escenario.

7.1.1. Robo de Información

Incidentes que impliquen la obtención, alteración o utilización de datos, en perjuicio del titular o de un tercero, u otra información que se halle registrada en ficheros o soportes informáticos, electrónicos o telemáticos, gestionados en la Plataforma CIMA. Estos incidentes pueden ocurrir por acceso legítimo o no legítimo, a través de diferentes métodos como la filtración de información, el espionaje industrial o la manipulación de datos dentro del ecosistema.

Esto puede ser causado por actores internos, empleados con accesos legítimos a los datos, o externos (hackers, competidores, entre otros). Los activos afectados pueden ser bases de datos, sistemas de información e infraestructura, redes y comunicaciones electrónicas, aplicaciones y software.

El alcance de este escenario incluye aquellas amenazas originadas por un ciber incidente que tienen implícita la intencionalidad de un ataque, se dejan para desarrollo posterior aquellas amenazas relacionadas con fallos internos de los sistemas o errores involuntarios. Las amenazas analizadas pueden utilizar diferentes métodos para acceder a la información como:

- Filtración de datos a través de malware: Uso de software malicioso para capturar información, puede comprometer información personal de asegurados, pólizas, transacciones entre aseguradoras, corredores, agentes, proveedores, mediadores y otros involucrados en las pólizas.
- Phishing y suplantación de identidad: Acceso no autorizado a sistemas de información mediante engaños a empleados para obtener credenciales de accesos.
- Vulnerabilidad de software y explotación de fallos de seguridad: robo de datos mediante canales o aplicaciones maliciosas, extracción de datos especialmente protegidos debido a vulnerabilidades no parcheadas.
- Ataques de fuerza bruta y credential stuffing: Acceso no autorizado a cuentas críticas mediante extracción sistemática y repetitiva de contraseñas y claves de usuarios.
- Ataques de insiders maliciosos: Acceso legítimo a los sistemas de información para cometer acciones perjudiciales a la organización con posibles consecuencias legales y regulatorias.
- Ataques a la cadena de suministro: Acceso a la infraestructura de la organización mediante la afectación de seguridad de proveedores, dificultando la detección y respuesta del servicio.

- Ingeniería social: Manipulación de personas para obtener acceso no autorizado a la información.
- Ataques Man in the Middle: Interceptación y alteración de la comunicación entre dos partes para capturar y manipular la información sin que las partes involucradas lo sepan, comprometiendo la confidencialidad de la información intercambiada.
- Acceso físico no autorizado: Acceso directo a servidores, estaciones de trabajo o dispositivos de almacenamiento

7.1.2. Indisponibilidad del Ecosistema CIMA

Incidentes que comprometan la interrupción o inaccesibilidad de los servicios críticos para la organización, esta amenaza puede ser causada por ataques de Denegación de Servicio Distribuido (DDoS), infecciones de ransomware, fallos en la infraestructura tecnológica (hardware/software), que resulten en la interrupción masiva del servicio.

Los activos afectados pueden ser datos, transacciones generadas durante las operaciones diarias, datos de backup y de recuperación, copias de seguridad que se utilizan en caso de fallo en los servicios, sistemas de información y equipos de red que proporcionan acceso a aplicaciones y datos críticos, infraestructura de comunicaciones que permiten la conexión a redes locales y externas, programas que gestionan software crítico para las operaciones de la organización como ERP, CRM o plataformas en la nube y virtualización.

Las amenazas que pueden afectar a la indisponibilidad del Ecosistema pueden ser:

Amenazas técnicas: Se refiere a aquellas amenazas que afectan directamente el equipamiento propio o su implementación, con consecuencias potencialmente negativas sobre los sistemas de información.

- Ataques de Denegación de Servicio (DDoS): Ataques que buscan el envío de peticiones a las aplicaciones web y recursos de red que provocan la interrupción o ralentización en la prestación del servicio.
- Ataques ransomware: Utilización de software malicioso para secuestrar datos e impedir el acceso a los sistemas de información, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado.
- Fallos en la infraestructura de red: Desconexión del servicio CIMA, afectando su disponibilidad para los usuarios finales, errores en equipos de servidores, almacenamiento, red o aplicaciones críticas.
- Vulnerabilidad de software y explotación de fallos de seguridad: Interrupción del servicio debido a la explotación de vulnerabilidades que interfieren con la operación normal de la plataforma.
- Fallos en los sistemas de backup o recuperación: Extensión del tiempo de inactividad e incapacidad para acceder, restaurar o utilizar copias de seguridad de la información, afectando la continuidad del servicio.
- Errores en la configuración: Indisponibilidad temporal o prolongada del servicio debido a errores en la configuración de sistemas o redes.

Amenazas Externas: Se refieren a amenazas del entorno en las cuales el origen del incidente es externo pero los sistemas de información se ven afectados de manera pasiva

- Problemas en la cadena de suministro tecnológico: Dependencia de servicios externos que pueden fallar y se pueda presentar interrupción de servicios críticos para la operatividad.
- Ataques a la infraestructura de suministro de energía: Interrupción de servicios eléctricos críticos.

Es importante destacar que el alcance de este protocolo se aplicará únicamente en caso de ciber incidentes asociados a los dos escenarios descritos. Esto se debe a que los ciber incidentes afectan principalmente a la infraestructura tecnológica y componentes de seguridad de la información que requieren un enfoque especializado en la gestión de datos y la protección de sistemas de información.

Cualquier otro tipo de amenazas, como desastres naturales o errores humanos involuntarios, que puedan impactar en la disponibilidad del Ecosistema CIMA o en la obtención ilegítima de información, se incluyen en el anexo Lista de riesgos a valorar y se dejan para desarrollo posterior al presente documento, esto se debe a que estas amenazas tienen características, impactos y respuestas diferentes, implicando que su respectiva gestión involucre a entornos e infraestructuras físicas, la seguridad del personal, además de la afectación de los sistemas tecnológicos.

7.2. Análisis de Riesgos

La evaluación del riesgo se basa en dos dimensiones principales: la probabilidad de ocurrencia del riesgo y el impacto que este tendría si se materializa.

La probabilidad de ocurrencia dependerá del entorno de las amenazas, nivel de exposición a actores internos o externos, la eficacia de las medidas de protección y la criticidad de los datos manejados.

La probabilidad puede ser alta, media o baja:

- es alta si la organización maneja grandes volúmenes de datos especialmente protegidos, tiene una alta exposición a servicios web, y carece de medidas de seguridad adecuadas,
- es de nivel medio cuando existen medidas básicas de seguridad, pero hay áreas de mejora (como autenticación débil o insuficiente monitoreo)
- es baja, si existen controles robustos y bien implementados, con auditorías y monitoreo continuos.

Para medir el impacto potencial, se tienen en cuenta las dimensiones de seguridad afectadas:

- la confidencialidad presenta alto impacto si la información comprometida es sensible (datos personales, financieros, propiedad intelectual),
- la integridad puede ser moderada o alta si los datos son alterados o manipulados de manera maliciosa, y
- la disponibilidad puede tener alto impacto si el ataque incluye una denegación de servicio que afecta el acceso a la información.

7.2.1. Matriz de Probabilidad e Impacto

Para evaluar las amenazas de seguridad, se utiliza una matriz de probabilidad e impacto que permite clasificar los riesgos de acuerdo con su gravedad y priorizarlos en función de las acciones necesarias para mitigarlos.

- Probabilidad (P): La posibilidad de que una amenaza se materialice, esta puede ser clasificada en una escala cualitativa y luego se asigna un valor cuantitativo a la matriz.
- Impacto (I): La consecuencia o daño que causaría la materialización de una amenaza.

El nivel de riesgo (NR) se calcula multiplicando la probabilidad (P) de que ocurra la amenaza por el impacto (I) que tendría para la organización. En la matriz se presenta en cada cuadrante el nivel de riesgo asignado con la escala numérica.

- Muy Alto Riesgo (15-25): Riesgo inaceptable que requiere medidas de mitigación inmediatas. Implica amenazas de gran probabilidad y alto impacto.
- Alto Riesgo (10-14): Riesgo significativo que requiere acciones de mitigación en el corto plazo.
- Riesgo Medio (5-9): Riesgo moderado que debe ser gestionado con medidas preventivas, pero no necesariamente de forma urgente.
- Riesgo Bajo (3-4): Riesgo aceptable, pero que se debe seguir monitoreando y gestionar si las circunstancias cambian.
- Muy Bajo Riesgo (1-2): Riesgo mínimo o despreciable, que puede ser asumido sin medidas adicionales de mitigación.

Tabla 1 Matriz de probabilidad e impacto

	PROBABILIDAD		
IMPACTO	**BAJO**	**MEDIO**	**ALTO**
ALTO	Medio (5-9)	Alto (10-14) **6-RIESGOS**	Muy alto (15-20) 9-RIESGOS
MEDIO	Bajo (3-4)	Medio (5-9) **5-RIESGOS**	Alto (10-14) **1-RIESGO**
BAJO	**Muy Bajo (1-2)**	Bajo (3-4)	Medio (5-9)

7.2.2. Riesgos Prioritarios

Se deben priorizar las acciones de mitigación de las amenazas que representan un nivel de riesgo Muy Alto para cada escenario.

Para ilustrar a manera de ejemplo se han seleccionado aquellos riesgos que tuvieron una calificación de 20 en la evaluación de riesgo, ya que representan mayor impacto potencial en términos de probabilidad e impacto sobre la Plataforma CIMA. Estos riesgos se consideran de alta prioridad debido a su capacidad de afectar de manera significativa la operatividad, la seguridad o la continuidad de los servicios y, por lo tanto, requieren una atención inmediata y directa para su gestión.

Las amenazas identificadas y evaluadas en cada escenario que obtuvieron una calificación inferior a 20 se documentan en el anexo Lista de riesgos a valorar. Cualquier amenaza detectada puede resultar en una notificación de incidente, sin embargo, la evaluación de la frecuencia de ocurrencia puede ser menor y por lo tanto todos los riesgos deben contemplar y seguir siendo monitoreados y gestionados de acuerdo con su nivel de importancia. Esta estrategia permite enfocar los recursos y esfuerzos en la gestión de los riesgos críticos, mientras que los riesgos de menor frecuencia y calificación se dejan en el anexo mencionado.

Escenario	Amenazas	Probabilidad	Impacto	Riesgo Inherente	Nivel de riesgo
Robo de información	Filtración de datos a través de malware	4	5	20	Muy Alto
	Phishing y suplantación de identidad	5	4	20	Muy Alto

Las acciones de mitigación de las amenazas relacionadas con robo de información se deben centrar en la implementación de soluciones de seguridad que permitan detectar y prevenir intrusiones, acciones de formación de los usuarios para reforzar el uso correcto de la información, aplicar técnicas de autenticación multifactorial, política de cambio de contraseñas periódicamente, mantener actualizaciones de software vigentes, realizar pruebas de pen testing, auditorías regulares y buenas prácticas de medidas de seguridad y control de accesos.

Escenario	Amenazas	Probabilidad	Impacto	Riesgo Inherente	Nivel de riesgo
Indisponibilidad del Ecosistema CIMA	Ataques de denegación de servicio distribuido (DDoS)	5	4	20	Muy Alto
	Ataques ransomware	4	5	20	Muy Alto
	Fallos en la infraestructura de red	4	5	20	Muy Alto

Para mitigar los riesgos priorizados de indisponibilidad de servicio, es importante implementar un conjunto de acciones y controles específicos que reduzcan tanto la probabilidad de ocurrencia como el impacto de estos incidentes. Establecer reglas en firewalls y sistemas de prevención de intrusos, implementar herramientas de monitoreo en tiempo real que puedan detectar patrones de tráfico anómalos y activar alertas tempranas de posibles amenazas, realizar copias de seguridad periódicas y almacenarlas de forma segura, preferentemente fuera de línea y en un lugar alternativo al centro de operaciones, utilizar herramientas de monitoreo de red para detectar y alertar sobre problemas potenciales antes de que resulten en fallos críticos, mantener un inventario actualizado de la infraestructura de red y documentar todas las configuraciones, etc.

8. Fases del Protocolo

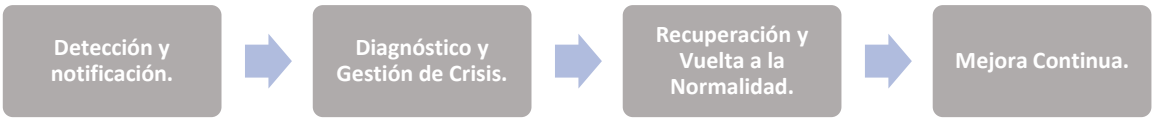
El objetivo del Protocolo es establecer el procedimiento de actuación general ante incidentes de Ciberseguridad que hayan afectado o puedan afectar a la operativa de la Plataforma CIMA.

Actualmente, dentro del alcance del protocolo se contemplan dos escenarios:

- **Robo de Información.**
- **Indisponibilidad del Ecosistema CIMA.**

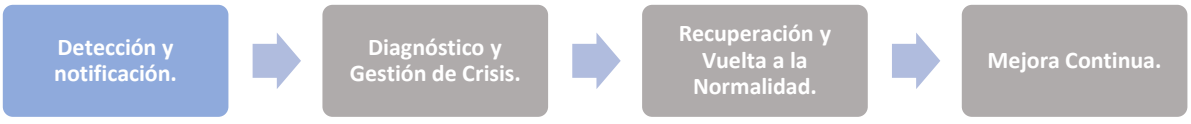
El detalle de los escenarios se encuentra explicado en el apartado "Identificación de amenazas" de este documento.

Las fases para la gestión de un incidente de Ciberseguridad son las siguientes:



1. **Detección y notificación**: inicio y escalado de la alerta, primera valoración del incidente.
2. **Diagnóstico y Gestión de Crisis**: valoración del impacto del incidente, implementación de primeras medidas y activación del Comité de Crisis.
3. **Recuperación y Vuelta a la Normalidad:** toma de decisiones para la recuperación del servicio (si aplica) y la vuelta a la normalidad.
4. **Mejora Continua**: acciones encaminadas a la implementación de planes de acción según las lecciones aprendidas del incidente.

8.1. Detección y Notificación



Objetivo	Detectar un incidente de ciberseguridad (Robo de datos y/o Indisponibilidad del Ecosistema CIMA) que afecta a la operativa de CIMA y notificar a los equipos correspondientes el detalle de la alerta. Además de tomar la decisión de activar o solo notificar el incidente al Comité de Crisis.

Involucrados	• Responsable del Comité de Crisis. • Responsable de Comunicación interna y externa de Tirea. • Representantes del interviniente afectado • Equipo de evaluación inicial.

Los pasos a seguir durante la fase de Detección y Notificación se identifican a continuación:

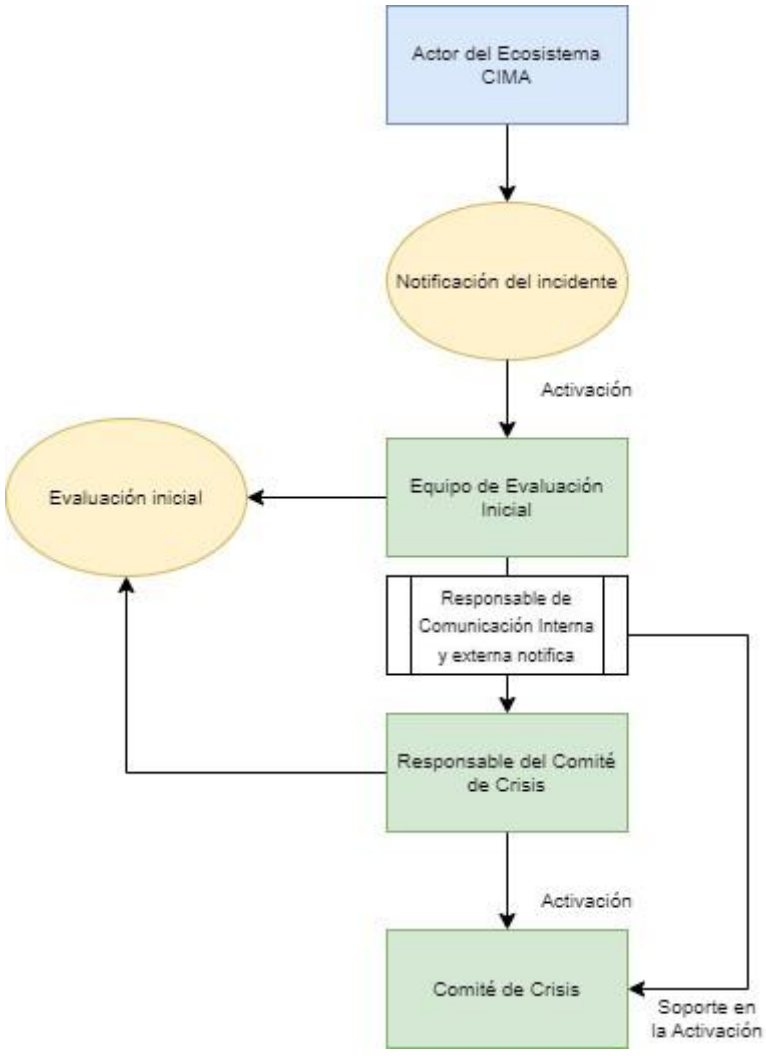


Ilustración 2 - Diagrama Fase 1

FASE I – DETECCIÓN Y NOTIFICACIÓN

PASO	Descripción
1	Un interviniente de ecosistema CIMA notifica un incidente de seguridad mediante el buzón destinado para este fin.
2	Una vez llega la alerta al buzón, se activa el Equipo de Evaluación Inicial, el Responsable de Comunicación interna y externa de Tirea notifica el suceso al Responsable del Comité de Crisis.
3	Se realiza el análisis inicial del incidente.
4	El Responsable del Comité de Crisis junto con el Responsable de Comunicación interna y externa de Tirea toman la decisión de convocar o no al Comité de Crisis.
5	Ejecución de acciones iniciales: comunicaciones, implementación de medidas de seguridad, etc.

En el momento en el que algún interviniente del Ecosistema CIMA sufra un ciberataque o tenga indicios suficientes para creer que está siendo víctima de uno, deberá notificar el suceso a TIREA, así se activará el Protocolo del Ecosistema CIMA.

El incidente se notificará mediante el envío de un correo electrónico al buzón **incidentescima@tirea.es** De manera alternativa se podrá comunicar el incidente mediante el grupo de Whatsapp destinado para este fin. Es necesario notificar el incidente durante las primeras **2 horas** de la identificación del incidente para cumplir con el tiempo que marca DORA en la notificación inicial.

- Cada interviniente debe identificar un representante que tendrá la capacidad de poder notificar los incidentes (por ejemplo, roles como CISO, DPO, Responsable de Seguridad por defecto u otra figura sugerida por la entidad).

Para notificar el incidente se deberán tener en cuenta los siguientes aspectos:

- Este **buzón solo sirve para notificar incidentes de seguridad** que afecten al ecosistema CIMA.
- Los afectados que notifican el incidente deberán realizar un **análisis previo y completar la plantilla "Notificación del Incidente"** que será enviada junto con la notificación inicial.

Una vez se ha notificado el incidente, el Responsable de Comunicación interna y externa de Tirea, que forma parte del Equipo de evaluación inicial, será el encargado de:

- Ser el **nexo** entre la persona que ha notificado el incidente y el Equipo de evaluación inicial.

- **Responsable de notificar el incidente al Responsable del Comité de Crisis**. Siempre que la notificación se inicie desde el **exterior de Tirea**, el Responsable de Comunicación interna y externa de Tirea convocará al Responsable del Comité de Crisis para **que participe en las evaluaciones iniciales**.

Con la información obtenida hasta el momento y el análisis inicial realizado por el Equipo de Evaluación Inicial, el Responsable del Comité de Crisis junto con el Responsable de Comunicación interna y externa de Tirea valorarán el impacto inicial del incidente y decidirán activar o no el Comité de Crisis.

Según el tipo de incidente se podrá valorar activar al Comité de Crisis o simplemente informar sobre el desarrollo de la contingencia.

Además, en el momento de activar el Comité de Crisis, el Equipo de Evaluación inicial valorará el envío de una comunicación global a las entidades participantes del ecosistema CIMA sobre el incidente ocurrido.

Será necesario activar el Comité de Crisis cuando se de alguno de los siguientes supuestos:

- **Escenario robo de Información**:
  - Si se ha producido un acceso no autorizado en la Plataforma CIMA, aunque no esté confirmado el robo de información.
  - Si el robo de información se ha producido en la Plataforma CIMA.
  - Si el robo de información se ha producido fuera de la Plataforma CIMA, pero afecta a información relacionada con el ecosistema CIMA. La información confidencial se encuentra dentro de los anexos de este documento.

- **Indisponibilidad del ecosistema CIMA**:

  - Si la incidencia supone un problema de indisponibilidad de la Plataforma CIMA de manera total.
  - Si la incidencia de inaccesibilidad afecta a un número elevado de usuarios y supone un problema en la operativa de la Plataforma CIMA.

Además, de manera general se establecen los siguientes criterios para tomar la decisión de activar el Comité de Comité de Crisis:

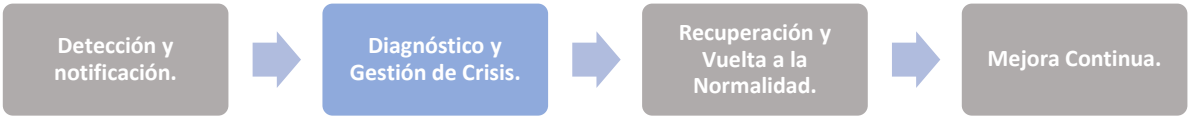
- **Criterio 1:** el incidente afecta a un número masivo de miembros del ecosistema CIMA y no pueden continuar prestando servicio.
- **Criterio 2**: existe una pérdida de datos relacionada con el ecosistema CIMA.
- **Criterio 3**: indisponibilidad de la Plataforma CIMA estimadas en más de 8 horas.
- **Criterio 4**: si se produce un daño reputacional severo (incidente reflejado en los medios de comunicación, multitud de quejas de clientes, posible pérdida masiva de clientes…).
- **Criterio 5**: si se produce un acceso no autorizado a entornos CIMA o a información relacionada con el ecosistema CIMA.

En el momento en el que se de alguno de los criterios descritos estaremos ante un incidente suficientemente grave como para tener que activar el Comité de Crisis.

Por último, según el tipo de incidente se deberá valorar realizar acciones iniciales como:

- Implementar **medidas de seguridad** para mitigar el impacto del incidente.
- **Notificar a los actores** que han detectado el incidente indicando la recepción de la alerta y la puesta en marcha de los equipos.
- El **Equipo de Evaluación Inicial valorará el envío de una comunicación global a los intervinientes del ecosistema CIMA** sobre el incidente ocurrido.
- **Valorar la realización de algún tipo de comunicación al exterior.**
- Valorar realizar la **notificación inicial** del incidente a la **DGSFP dentro de las primeras 24 horas** desde la notificación del incidente. La comunicación se realizará de manera particular por cada interviniente del ecosistema CIMA afectado.

8.2. Diagnóstico y Gestión de Crisis



Objetivo	El Comité de Crisis deberá evaluar el incidente y tomar decisiones para disminuir el impacto.
Involucrados	• Comité de Crisis. • Responsable del Comité de Crisis. • Responsable de comunicación interna y externa de Tirea.

Una vez se ha decidido activar el Comité de Crisis (en la fase de Detección y notificación), será el Responsable del Comité de Crisis quién activará las alarmas pertinentes a través del Grupo de WhatsApp del Comité de Crisis para la convocatoria de los miembros del Comité de Crisis.

La convocatoria del Comité de Crisis deberá contener, al menos, la siguiente información:

- Fecha, hora y lugar de la convocatoria.
- Resumen de lo sucedido.
- Breve resumen del Impacto del incidente.

El Responsable del Comité de Crisis coordinará el proceso de gestión de incidentes establecido en el presente procedimiento, velando por la gestión y funcionamiento de los canales de transmisión de información.

Una vez reunido el Comité de Crisis, el Responsable del Comité de Crisis, junto con la Responsable de Comunicación interna y externa de Tirea, informarán sobre la evaluación inicial realizada por el Equipo de evaluación inicial, así como de la previsión de evolución de los efectos de la contingencia para la activación o no de otros planes y medidas.

Si se considera necesario, el Comité de crisis recabará la información de última hora poniéndose en contacto con el Equipo de evaluación inicial que están trabajando en el incidente, siempre a través de la Responsable de Comunicación interna y externa de Tirea.

Será necesario:

- **Concluir con los tiempos estimados** que pudieran ser de interés (si procede):
  - Tiempo estimado en realizar las acciones mínimas para recuperar parte de la operativa.
  - Tiempo estimado en recuperar la operativa normal.

- Considerando los hechos conocidos, valorar las siguientes posibilidades:
  - **Cancelar la situación de Alerta**, y detener cada acción de recuperación que pudo haber sido iniciada.
  - **Declarar inmediatamente la situación de contingencia**.

En caso de haber decidido declarar la situación como contingencia, el Comité de Crisis deberá tomar las siguientes acciones:

- **Robo de Información**:
  - Proponer medidas mitigadoras a implementar para reducir el impacto actual.
  - Identificar las medidas que están adoptando los intervinientes del ecosistema CIMA afectados.
  - Identificar las comunicaciones internas y externas a realizar y el responsable de su comunicación.
  - Valorar ponerse en contacto con (cada interviniente del ecosistema CIMA será responsable de hacerlo):
    - Fuerzas y Cuerpos de Seguridad del Estado.
    - Agencia Española de Protección de Datos (AEPD).
    - INCIBE-CERT.
    - Valorar realizar la **notificación intermedia** del incidente a la DGSFP dentro de las primeras 72 horas desde la notificación inicial. La comunicación se realizará de manera particular por cada interviniente del ecosistema CIMA afectado.
    - Interesados afectados
- **Indisponibilidad del Ecosistema CIMA**:
  - Proponer la activación de los equipos de recuperación del interviniente del ecosistema CIMA afectado.

- Proponer la activación de las estrategias alternativas del interviniente del ecosistema CIMA afectado.
- Proponer a los actores implicados la activación de sus planes de continuidad.
- Identificar las comunicaciones a realizar a terceros y el responsable de su comunicación.
- Valorar ponerse en contacto con (cada interviniente del ecosistema CIMA afectado será responsable de hacerlo):
  - Fuerzas y Cuerpos de Seguridad del Estado.
  - Agencia Española de Protección de Datos (AEPD).
  - INCIBE-CERT.
  - Valorar realizar la **notificación intermedia** del incidente a la DGSFP dentro de las primeras 72 horas desde la notificación inicial. La comunicación se realizará de manera particular por cada interviniente del ecosistema CIMA afectado.
  - Interesados afectados.

Además, el **Comité de Crisis valorará el envío de una comunicación** global a los intervinientes del ecosistema CIMA sobre el avance de la contingencia.

El Comité deberá estar informado en todo momento sobre el desarrollo del incidente, para ello se establecerán unos tiempos de reporte entre:

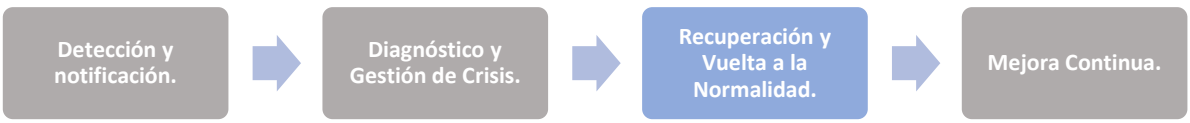
- El Comité de Crisis y la Responsable de Comunicación interna y externa de Tirea en caso de que el incidente se produzca en la plataforma CIMA. Por ende, también se deberá decidir el tiempo de reporte entre el Equipo de evaluación inicial y el Responsable de comunicación interno y externo de Tirea.

- El Comité de Crisis y el interviniente del Ecosistema CIMA que ha notificado el incidente, cuyo nexo de unión será responsabilidad del Responsable de Comunicación interno y externo de Tirea.

- Entre el Comité de Crisis y el Ecosistema CIMA en caso de haber tomado la decisión de reportar el incidente de manera global.

En base a los nuevos acontecimientos que se pudieran dar durante la gestión de la contingencia, el Comité de Crisis irá tomando diferentes decisiones.

8.3. Recuperación y Vuelta a la Normalidad



Objetivo	Iniciar la recuperación de la plataforma CIMA y la Vuelta a la normalidad

Involucrados	• Comité de Crisis. • Responsable del Comité de Crisis. • Equipo de Evaluación inicial.

Una vez se han adoptado las decisiones encaminadas a mitigar el impacto de la contingencia y el incidente se encuentra controlado, el Comité de Crisis deberá tomar decisiones en relación con la vuelta a la normalidad.

Con el objetivo de facilitar la toma de decisiones al Comité de Crisis se deberán tener en cuenta los siguientes aspectos según el escenario de la contingencia:

- **Robo de Información**:
  - Proponer las medidas para recuperar la información (en caso de ser necesario).
  - Identificar las comunicaciones de cierre y vuelta a la normalidad del incidente a quién corresponda.
  - El **Responsable del Comité de Crisis valorará el envío de una comunicación global a los intervinientes del ecosistema CIMA** sobre el incidente ocurrido.

- **Indisponibilidad del ecosistema CIMA**:

  - Identificar los responsables de recuperar aquellos sistemas impactados en el entorno de CIMA.
  - Proveer los medios necesarios a los equipos de recuperación para devolver la normalidad al entorno CIMA.
  - Desactivar los Planes de Continuidad de Negocio de los intervinientes afectados.
  - El **Responsable del Comité de Crisis valorará el envío de una comunicación global a los intervinientes del ecosistema CIMA** sobre el incidente ocurrido.

Una vez los involucrados en la contingencia comuniquen la vuelta a la normalidad el Responsable del Comité de Crisis desactivará el Comité de Crisis:

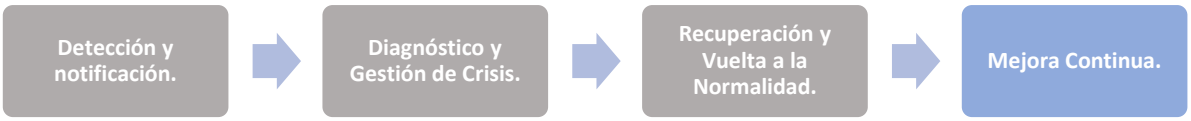
- **Robo de Información**:
  - El Representante(s) del interviniente afectado deberá confirmar el cese de la contingencia a través del buzón de gestión de incidentes del ecosistema CIMA.

- **Indisponibilidad del ecosistema CIMA.**

  - El Representante del interviniente afectado que anuncio el incidente a través del buzón de gestión de incidentes del ecosistema CIMA deberá confirmar el cese de la contingencia.

Una vez, se verifica que el incidente ha sido contenido y se está procediendo con la vuelta a la normalidad, el Responsable del Comité de Crisis podrá desactivar el Comité.

8.4. Mejora Continua



Objetivo	Definir un plan de acción según las lecciones aprendidas.
Involucrados	• Comité de Crisis. • Responsables de Comunicación interna y externa de Tirea.

De manera individual cada entidad afectada será la encargada de realizar un informe final del incidente, se espera que se tengan en cuenta los siguientes puntos:

- La rapidez en las respuestas ante las alertas y la rapidez en identificar el impacto del incidente.
- La eficacia de las comunicaciones internas y externas.
- La eficacia de la activación de los equipos y procedimientos que han intervenido en la resolución del incidente.
- La calidad y rapidez del análisis forense (si procede).

Para la correcta definición de los planes de acción y el cumplimiento de normativas, como DORA, será necesario que se definan y ejecuten pruebas de resiliencia ante escenarios similares.

Cada interviniente del ecosistema CIMA será quien apruebe la implementación de las acciones identificadas, se asignará un responsable a cada plan de acción y serán los encargados de dar seguimiento a los planes y reportar el estado de implementación en los Comités pertinentes.

Todos los incidentes reportados al buzón de gestión de incidentes del ecosistema CIMA deberán ser inventariados, la información a contener será la siguiente:

- La información que ha sido reportada mediante la plantilla de evaluación inicial por parte del afectado.
- Bitácora de las acciones tomadas por el Comité de Crisis.
- Informes realizados por cada interviniente afectado.

El registro de estos incidentes se llevará a cabo a través del Excel "Registro de incidentes CIMA" el cual se podrá encontrar dentro del repositorio en el siguiente enlace:

01 Registro de incidentes

Este protocolo se deberá revisar de manera anual y cuando se identifique como plan de acción al ocurrir un incidente o ejecutarse alguna prueba de este procedimiento.

En el caso de haber notificado el incidente a DGSFP, cada interviniente deberá remitir un informe final en un periodo máximo de un mes.

8.5. Listado de tareas a realizar durante la Gestión de la contingencia.

Cod.	Tarea	Responsable
01	Notificar el incidente	Cualquier persona del ecosistema CIMA destinado para realizarlo.
02	Activar al Equipo de evaluación inicial	Responsable de Comunicación interna o externa.
03	Evaluación inicial del Incidente	Equipo de Evaluación inicial.
04	Activar el Comité de Crisis	Responsable del Comité de Crisis.
05	Notificar el suceso a las entidades que forman parte del ecosistema CIMA.	Responsable del Comité de Crisis.
06	Activar medidas iniciales	Cada entidad de manera individual. El Comité de Crisis será conocedor del detalle ejecutado por cada entidad.
07	Activar los equipos de respuesta, estrategias y planes alternativos.	Cada entidad de manera individual. El Comité de Crisis será conocedor del detalle ejecutado por cada entidad.
08	Notificar el incidente a los grupos de interés.	Cada interviniente afectado de manera individual. El Comité de Crisis será conocedor del detalle ejecutado por cada interviniente.
09	Tomar las medidas necesarias para la vuelta a la Normalidad.	Cada interviniente afectado de manera individual. El Comité de Crisis será conocedor del detalle ejecutado por cada interviniente

Cod.	Tarea	Responsable
10	Realizar el informe final	Cada interviniente afectado de manera individual.
11	Mantener un inventario de todos los incidentes notificados.	Equipo de Evaluación inicial.

9. Anexos

9.1. Datos confidenciales

- Datos de la entidad aseguradora: Pólizas, recibos, siniestros, liquidaciones y cuentas de efectivo enviados por la entidad aseguradora.
- Datos del corredor: Pólizas, recibos, siniestros, liquidaciones y cuentas de efectivo enviados por la entidad aseguradora.
- Credenciales del corredor facilitadas por la entidad aseguradora.
- Firmantes: Datos identificativo y de contacto.
- Datos propios de la Entidad: número de Póliza, Producto, Ramo.
- Documentos: Póliza, Condiciones Generales, Particulares, Documento LOPD/RGPD, Cuestionario Salud, Pack de bienvenida, Solicitud de seguro, Suplemento, Boletín de adhesión, Recibo, Liquidación, Comunicación Notificación, Certificado, Documento de información previa, Clausulado, Solicitud, Mandato SEPA, IDDM, IPID, entre otros.
- Otros datos: plazos de firma, plazos de almacenamiento, URL a la que redirigir al firmante tras la firma, eventos, ID de la solicitud en el proveedor, motivos de rechazo, etc.
- Administrativos: Datos personales y de contacto de usuarios.
- Consultas Tecnológicas: información sobre los corredores que operan por tecnológica.
- Costes: por proveedor, solicitud, entidad y corredor.

9.2. Plantilla de Notificación del Incidente

Información general del Incidente

Cuestión	Detalle
Nombre del interviniente y Representante que notifica el incidente	
Fecha y hora del inicio del incidente:	
Fecha y hora de la detección del incidente:	

Cuestión	Detalle
Lugar del incidente:	
Origen/Fuente de la alerta:	
Alcance del impacto:	
Descripción de la alerta:	

Información específica del incidente

Cuestión	Detalle
¿La alerta está vinculada a una disponibilidad de los servicios CIMA?	
¿Se ha producido un acceso no autorizado al ecosistema CIMA?	
¿Existe fuga de información relacionada con el ecosistema CIMA?	
¿Se ha notificado a las autoridades competentes?	
Medidas implementadas hasta el momento	

9.3. Plantilla de evaluación inicial

Preguntas para valorar el incidente

Val.01	¿El incidente afecta a la disponibilidad, integridad o confidencialidad de la información del ecosistema CIMA?	[Sí / No]
Val.02	¿Un número masivo de miembros del ecosistema CIMA están afectados y no pueden continuar prestando servicio?	[Sí / No]
Val.03	¿Existe una pérdida de datos relacionada con el ecosistema CIMA?	[Sí / No]
Val.04	¿Existe una indisponibilidad de los servicios CIMA por más de 12 horas?	[Sí / No]
Val.05	¿Existe un daño reputacional severo (incidente reflejado en los medios de comunicación, multitud de quejas de clientes, posible pérdida masiva de clientes…) o puede haberlo en las próximas horas?	[Sí / No]
Val.06	¿Se ha producido un acceso no autorizado a entornos CIMA o a información relacionada con el ecosistema CIMA?	[Sí / No]
Val.07	¿Hay algún grupo de ciberdelincuentes detrás del incidente?	[Sí / No]

Valoración Tipo de incidente

☐ Incidencia (no se ha respondido de manera afirmativa a ninguna valoración)

☐ Incidente (solo se responsade de manera afirmativa la valoración Val.01)

☐ Incidente grave (Existen dos o más valoraciones positivas)

Valoración de la activación del Comité de Crisis

☐ Se trata de una incidencia, no se activa el Comité de Crisis ni se notifica el incidente al Responsable del Comité de Crisis.

☐ Se trata de una incidencia, no se activa el Comité de Crisis, pero sí se notifica el incidente al Responsable del Comité de Crisis.

☐ Se notifica el incidente al Responsable del Comité de Crisis para valorar la activación del Comité de Crisis.

9.4. Contactos Claves

Interviniente del Ecosistema CIMA	Rol
Generali	Responsable del Comité de Crisis
TIREA	Responsable comunicación interna y externa TIREA Responsable Técnico
Equipo de Evaluación Inicial	
TIREA	Responsable de sistema de información TIREA
TIREA	Responsable Tecnología
TIREA	Responsable Seguridad Lógica y Continuidad de Negocio TIREA
TIREA	DPO (Responsable de protección de datos) TIREA
TIREA	Responsable Explotación
TIREA	Responsable Gestores CIMA de Tirea
TIREA	Gestor CIMA de Tirea
TIREA	Responsable SAU CIMA TIREA
TIREA	Responsable Técnico
Personal designado por la empresa afectada del Ecosistema CIMA	Personal designado por la empresa afectada del Ecosistema CIMA
Comité de Crisis	
Entidad: Allianz	CISO de Allianz
Entidad: Axa	CISO y Responsable Resiliencia Operacional
Entidad: Caser	Pendiente de información
Entidad: Generali	CISO de Generali

Interviniente del Ecosistema CIMA	Rol
Entidad: Mapfre	DPO MAPFRE ESPAÑA. Directora de Seguridad
Entidad: Occident	CISO de Occident
Entidad: Reale	CISO de Reale
Entidad: Segurcaixa Adeslas	CISO - director de Área Seguridad Digital y Continuidad
Entidad: Zurich	CISO - director de Área Seguridad Digital y Continuidad
Entidad: Fiatc	Pendiente de información
Asociaciones De Corredores: Adecose	CISO de Adecose
Asociaciones De Corredores: CGCMS	Directora General
Gestor de la Plataforma CIMA: TIREA	Medios y Tecnología
Tecnológica: AETMA	CTO

9.5. Plantillas de Mensajes

9.5.1. Plantilla para la detección y notificación del incidente

Estimados [Destinatarios],

Se ha detectado un posible incidente de seguridad con relación a [descripción del incidente: robo de información / indisponibilidad del Ecosistema CIMA] en [empresa afectada]. El equipo de evaluación inicial interno está realizando un análisis preliminar para determinar el alcance y naturaleza del incidente. [Adjuntar Plantilla de Notificación del Incidente cumplimentada]

9.5.2. Plantilla para Activación del Comité de Crisis

Estimados miembros del Comité de Crisis,

El incidente detectado el [Fecha] relacionado con [robo de información / indisponibilidad del servicio] ha sido evaluado como crítico, por lo que es necesario activar el Comité de Crisis para coordinar las acciones correspondientes.

Acciones inmediatas:

- Reunión del comité de crisis: [Fecha, hora y canal]

- Información disponible hasta el momento: [Adjuntar Plantilla de evaluación inicial cumplimentada]

Solicitamos su asistencia para coordinar la respuesta inmediata a este incidente.

9.5.3. Plantilla inicial de Comunicaciones Internas del Ecosistema CIMA durante la Gestión de Crisis

Estimados,

Les informamos que ha ocurrido un incidente de seguridad relacionado con [robo de información / indisponibilidad del servicio]. El equipo de evaluación procede a activar al Comité de Crisis. Se está trabajando en contener el impacto y recuperar los servicios afectados.

Por favor, manténganse disponibles para recibir instrucciones adicionales y colaborar en las acciones necesarias.

9.5.4. Plantilla de Actualización de Información del Ecosistema CIMA Durante la Gestión de Crisis

Estimados,

Les proporcionamos información sobre el estado actual del incidente de seguridad relacionado con [robo de información / indisponibilidad del servicio] que está siendo gestionado por el Comité de Crisis y los equipos de respuesta.

Situación actual: [Breve descripción del estado actual del incidente]

Impacto de la afectación: [Descripción del impacto en los servicios]

Se agradece la colaboración de todos los equipos y la disponibilidad para coordinar las acciones necesarias. Mantendremos este canal abierto para futuras actualizaciones sobre el progreso.

9.5.5. Plantilla para Comunicación de recuperación del Ecosistema CIMA

Estimados,

Nos complace informar que el incidente de seguridad relacionado con [robo de información / indisponibilidad del servicio] ha sido gestionado, y los sistemas afectados han sido recuperados. La operación normal de los servicios se ha restablecido.

Seguiremos monitoreando los sistemas para garantizar su correcto funcionamiento y evitar recurrencias.

9.6. Lista de riesgos a valorar

En este listado se incluyen las amenazas de cada escenario que obtuvieron una calificación inferior a los riesgos prioritarios, deben seguir siendo monitoreadas y

gestionadas de acuerdo con su nivel de importancia, para asegurar que no escalen hacia situaciones de alta criticidad, este enfoque garantiza una gestión integral del riesgo.

Además, se incluyen las amenazas de desastres naturales y errores humanos involuntarios, que podrían impactar la disponibilidad del ecosistema CIMA o permitir la obtención ilegítima de información. Estas amenazas, aunque no son el enfoque principal del documento actual, deben ser consideradas en un desarrollo posterior debido a su potencial para comprometer la operatividad y la seguridad del ecosistema CIMA.

Escenario	Amenazas	Probabilidad	Impacto	Riesgo Inherente	Nivel de riesgo
Robo de información	Vulnerabilidades de software y explotación de fallos de seguridad	4	4	16	Muy Alto
	Ataques de fuerza bruta y credential stuffing	4	4	16	Muy Alto
	Ataques de insiders maliciosos	3	5	15	Muy Alto
	Ataques a la cadena de suministro	3	4	12	Alto
	Ingeniería Social	4	3	12	Alto
	Ataques Man-in-the-Middle (MitM)	3	4	12	Alto
	Acceso físico no autorizado	3	3	9	Medio
Indisponibilidad del Ecosistema CIMA	Fallas en los sistemas de backup o recuperación	3	4	12	Alto
	Errores en la configuración	3	4	12	Alto
	Problemas en la cadena de suministro de servicio tecnológico	3	4	12	Alto
	Ataques a la infraestructura de suministro de energía	2	5	10	Alto
	Desastres naturales	2	4	8	Medio
	Condiciones ambientales extremas	2	4	8	Medio
	Errores humanos	3	3	9	Medio
	Acciones malintencionadas	3	3	9	Medio