



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

**INFORME DE AUDITORÍA Nº 55/2021  
MINISTERIO DE DEFENSA  
INSTITUTO DE INVESTIGACIONES CIENTÍFICAS  
Y TÉCNICAS PARA LA DEFENSA  
GERENCIA DE RECURSOS INFORMÁTICOS- SISTEMA CRISIS  
EVALUACION DEL CONTROL INTERNO IMPERANTE EN EL CICLO DE  
VIDA DEL DESARROLLO DEL SISTEMA CRISIS**

**Tabla de Contenidos**

<b>Informe Ejecutivo</b>	<b>1</b>
<b>Informe Analítico</b>	<b>3</b>
<b>Objetivo</b>	<b>3</b>
<b>Alcance</b>	<b>3</b>
<b>Tarea Realizada</b>	<b>4</b>
<b>Marco Normativo</b>	<b>4</b>
<b>Marco de Referencia</b>	<b>5</b>
<b>Descripción del Área Auditada</b>	<b>6</b>
<b>Antecedentes y Descripción del Proyecto</b>	<b>7</b>
<b>Conclusión</b>	<b>10</b>



*Ministerio de Defensa*  
Unidad de Auditoría Interna

**Informe Ejecutivo**

---

**INFORME DE AUDITORÍA Nº 55/2021  
MINISTERIO DE DEFENSA  
INSTITUTO DE INVESTIGACIONES CIENTÍFICAS  
Y TÉCNICAS PARA LA DEFENSA  
GERENCIA DE RECURSOS INFORMÁTICOS- SISTEMA CRISIS  
EVALUACION DEL CONTROL INTERNO IMPERANTE EN EL CICLO DE  
VIDA DEL DESARROLLO DEL SISTEMA CRISIS**

### **Objetivo**

---

Evaluar el control interno imperante en el CICLO de VIDA del desarrollo del Sistema de Crisis llevado a cabo por el INSTITUTO DE INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS PARA LA DEFENSA (CITEDEF) – Gerencia de Recursos Informáticos. El presente proyecto de auditoría se encuentra incluido en el Plan de Auditoría 2021, aprobado por la Sindicatura General de la Nación con fecha 12/02/2021 mediante NO-2021-12666234-APN-SIGEN.

### **Conclusión**

---

El Sistema Crisis tiene una arquitectura de alta complejidad, no sólo porque trabaja con cada uno de los componentes que lo conforman, sino también porque trabaja en la integración y homogeneidad de dichos componentes de modo de agilizar el flujo de datos con los diferentes nodos.

Durante el desarrollo de la auditoría se utilizaron diferentes herramientas que permitieron la evaluación del control interno imperante en el Ciclo de Vida del desarrollo del Sistema de Crisis, el análisis de factibilidades y de las funcionalidades del Sistema, la revisión de documentación suministrada y la realización de entrevistas con los funcionarios responsables del área considerada en el Marco de Referencia.

El proyecto CMC EMCO fue consecuencia de una línea de proyectos preparatorios que demostraron la factibilidad de desarrollo del Software para un Centro de Manejo de Crisis. La metodología exigió que se incluyera en la documentación de apertura, los estudios de factibilidad y otros antecedentes técnicos, realizándose una evaluación de la factibilidad por 3 instancias: Jefe de proyecto, Director o Gerente y la entonces Gerencia General.

Durante el desarrollo del Software del Sistema de Crisis, se realizó un proceso de monitoreo y seguimiento de proyectos para todas las actividades de desarrollo, a través del formulario Informe Trimestral de la Orden de Trabajo. Habiéndose cumplido en todo momento con los plazos y objetivos.

Desde junio de 2019 a la actualidad el Ministerio de Seguridad está usando a nivel nacional en forma permanente el Sistema de CRISIS CMC como



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

herramienta de gestión de emergencias, también conocido como el Sistema Nacional para la Gestión Integral del Riesgo y la Protección Civil (Proyecto SINAGIR etapa I) que tiene por objeto integrar las tareas para fortalecer y optimizar las acciones destinadas a la reducción de riesgos, el manejo de crisis y la recuperación.

En forma paralela el Ministerio de Seguridad ha tercerizado a Servicios técnicos especializados el desarrollo del Sistema de Gestión de Emergencias Específico (SINAGIR). Este proyecto está cercano a su finalización. (Proyecto SINAGIR Etapa II)

La tercera etapa (solo proyectada) consideró la implantación del sistema SINAGIR y la interrupción del uso del Sistema CRISIS CMC. Esta etapa aun no comenzó.

En opinión de esta Auditoría, CITEDEF ejecutó los controles en forma razonable y seleccionó una estrategia de diseño adecuada basada en un modelo de desarrollo evolutivo que permite la identificación de riesgos y la redefinición del diseño en cada iteración, producto de la evaluación de los usuarios y determinación de requerimientos, las veces que ello sea necesario.

Para permitir que el Ministerio de Defensa y las FFAA utilicen el Software desarrollado en el marco del Proyecto SINAGIR Etapa II, sería recomendable la publicación del código fuente del proyecto con autorización del Ministerio de Defensa. Esto permitiría que las instituciones adopten, mejoren y publiquen sus modificaciones al Software y que NO exista un potencial conflicto con el Ministerio de Seguridad por la propiedad intelectual del mismo.

Cabe destacar que actualmente en CITEDEF el Departamento de Modelado y Manejo de Crisis, área que desarrolló este software, está disuelto y no se cuenta con personal para dar continuidad al mantenimiento de estos sistemas.

Por lo expuesto, sería conveniente evaluar la utilización efectiva del sistema frente a requerimientos actuales en el ámbito del Ministerio de Defensa y de las Fuerzas Armadas, así como su adaptación y el desarrollo de componentes específicos de ser considerado de utilidad para la cobertura de necesidades específicas previamente definidas por los potenciales usuarios.

**BUENOS AIRES**, diciembre 2021



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

**Informe Analítico**

---

**INFORME DE AUDITORÍA Nº 55/2021  
MINISTERIO DE DEFENSA  
INSTITUTO DE INVESTIGACIONES CIENTÍFICAS  
Y TÉCNICAS PARA LA DEFENSA  
GERENCIA DE RECURSOS INFORMÁTICOS- SISTEMA CRISIS  
EVALUACION DEL CONTROL INTERNO IMPERANTE EN EL CICLO DE  
VIDA DEL DESARROLLO DEL SISTEMA CRISIS**

### **Objetivo**

---

Evaluar el control interno imperante en el CICLO de VIDA del desarrollo del Sistema de Crisis llevado a cabo por el INSTITUTO DE INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS PARA LA DEFENSA (CITEDEF) – Gerencia de Recursos Informáticos. El presente proyecto de auditoría se encuentra incluido en el Plan de Auditoría 2021, aprobado por la Sindicatura General de la Nación con fecha 12/02/2021 mediante NO-2021-12666234-APN-SIGEN.

### **Alcance**

---

La auditoría se llevó a cabo durante los meses de noviembre y diciembre de 2021, conforme a las Normas de Auditoría Gubernamental aprobadas por Resolución Nº 152/02SGN.

Las tareas de auditoría que comprendieron la evaluación del control interno imperante en el Ciclo de Vida del Desarrollo del Sistema de Crisisse efectivizaron en la División Computación Gráfica, ámbito del Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF).

Se sustentaron en verificar el cumplimiento de la Res 48/2005 Normas de Control Interno para Tecnología de Información (SGN) y el Instructivo de Trabajo 2/2005 GNYPE.

Los lineamientos de verificación del cumplimiento de los controles y su evaluación se circunscribieron específicamente a la fase Administración de Proyectos de la Cláusula Nº 6 del IT Nº 2/05 GNYPE del Anexo I – Circular Nº 3/05 SGN.

En virtud de las restricciones impuestas por la Ley Nº 27.541- Emergencia Sanitaria y el dictado de los Decretos Nros. 260/2020 Coronavirus (COVID19)- y 297/2020 y complementarios- Aislamiento Social Preventivo y Obligatorio- la presente auditoría se efectivizó complementándose la modalidad remota con relevamientos y controles in situ.



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

### **Tarea realizada**

---

La tarea realizada cuyo resultado se expone a lo largo del informe contempló los siguientes procedimientos de auditoría:

- Análisis del marco normativo vigente.
- Investigación preliminar.
- Entrevistas con los funcionarios responsables del área considerada en el Marco de Referencia.
- Análisis de factibilidades y de las funcionalidades del Sistema Crisis.
- Análisis de la información documentada y suministrada por el responsable del área considerada en el Marco de Referencia, producto del relevamiento efectuado a través del cuestionario del INSTRUCTIVO DE TRABAJO N° 2/2005 PROGRAMA DE TRABAJO DE EVALUACIÓN DEL CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN GNyPE en función de los lineamientos de la Cláusula N° 6 - Administración de Proyectos.
- Verificación de controles instrumentados en el Sistema.
- Evaluación de riesgos.
- Documentación de las tareas de campo y del análisis técnico-informático conformando los papeles de trabajo.

### **Marco Normativo**

---

Se identificó el marco normativo aplicable a las actividades de Tecnología de la Información (TI) integrado por las siguientes normas:

- Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.
- Resolución N° 152/2002 SIGEN.
- Resolución N° 48/2005 SIGEN.
- Instructivo de Trabajo N° 2/2015 - PROGRAMA DE TRABAJO DE EVALUACIÓN DEL CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN de la Gerencia de Normativa y Proyectos Especiales (GNyPE) – Anexo I – Circular N° 3/05 SGN.
- Disposición N° 1/2015 de la Oficina Nacional de Tecnología de la Información–ONTI.
- Decisión Administrativa N° 641/2021 de fecha 26 de junio de 2021- Requisitos mínimos de Seguridad de la Información para Organismos.
- Plan Estratégico de SI - Seguridad de la Información - Ministerio de Defensa, Subsecretaría de Ciberdefensa Año 2020/2021.



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

- Política de Seguridad de la Información aprobada el 27 de mayo de 2021.
- Ley N° 27.541 de Emergencia Sanitaria.
- DECNU-2020-260-APN-PTE-Disposiciones - Coronavirus (COVID-19).
- DECNU-2020-297-APN-PTE-Disposiciones - Aislamiento Social Preventivo y Obligatorio.
- Programa I+D CRISIS
- Disposición Normativa N° 23/2001 del Instituto de Investigaciones Científicas y Técnicas para la Defensa.
- Disposición Normativa N° 23/2001, ANEXO Apéndice N° 4, Formulario G – Solicitud de apertura CMC EMCO, de Órdenes de Trabajo de Actividades Científico –Tecnológicas del 21/02/2006.
- Disposición Normativa N° 23/2001, ANEXO Apéndice N° 11, Formulario IT – Informe de Avance Trimestral IT N° 14 del 01/04/2010 al 30/06/2010 realizado el 21/07/2010.
- Disposición Normativa N° 23/2001, ANEXO Apéndice N° 11, Formulario IT –Informe de Avance Trimestral IT N° 15 del 01/07/2010 al 30/09/2010.
- Orden de cierre CMC EMCO N° 08/2013 de la Orden de Trabajo 03 P 047/06 de octubre/2013.

## **Marco de Referencia**

CITEDEF es uno de los organismos desconcentrados del MINISTERIO DE DEFENSA dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa, dedicado a la ejecución de actividades de investigación, ciencia y tecnología. Forma parte del Polo Tecnológico Constitución, junto a la Comisión Nacional de Energía Atómica (CONEA), la Universidad Nacional de San Martín, el Instituto Nacional de Tecnología Industrial (INTI), el Instituto Nacional de Tecnología Agropecuaria (INTA) y el Servicio Nacional Geológico Minero Argentino (SEGEMAR). Integra también el Gabinete de Ciencia y Tecnología, en cumplimiento de la Ley N° 25.467 de Ciencia, Tecnología e Innovación Tecnológica.

Son sus principales objetivos:

- Investigar y desarrollar sistemas de armas hasta el nivel de prototipos.
- Transferir tecnología a las unidades de producción del Ministerio de Defensa y participar de la fase productiva posterior.
- Homologar equipos a los efectos de su clasificación como material de defensa.



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

- Mantener y actualizar las capacidades científicas y tecnológicas del instituto.
- Brindar asesoramiento técnico a los Ministerios de Defensa, de Relaciones Exteriores y Culto y de Economía y Finanzas Públicas.
- Desarrollar proyectos, productos y servicios para las Fuerzas Armadas y demás instituciones que integran el ámbito de la Defensa.
- Repotenciar y modernizar sistemas y equipos participando de este modo en la reestructuración del equipamiento de las Fuerzas Armadas.
- Participar en la reorientación del Sistema de Producción para la Defensa.
- Desarrollar tecnologías de uso Dual.
- Asesorar, evaluar, analizar y calibrar equipos a requerimiento de las Fuerzas Armadas, de otros organismos de la Administración Pública y de empresas privadas.
- Suscribir convenios y acuerdos de diverso orden con universidades u otras instituciones académicas y organismos nacionales e internacionales.

### **Descripción del Área Auditada**

El Sistema Crisis tuvo su origen entre los años 2006 y 2013, en el Departamento Modelado y Manejo de Crisis (DMMC) dependiente de la Gerencia de Recursos Informáticos. Dicha sección realizaba trabajos de investigación, análisis, diseño, desarrollo e implementación de sistemas informáticos con herramientas para el manejo de emergencias a escala nacional.

Actualmente el Departamento de Modelado y Manejo de Crisis se encuentra disuelto y no cuenta con personal para dar continuidad al mantenimiento del Sistema de Crisis; únicamente permanece en funciones un ingeniero, quien fue reubicado en la División Computación Gráfica, con el Grupo de Ingeniería de Software 3D. Esta División, ámbito de aplicación de esta auditoría, se encuentra bajo la órbita del Departamento Sistemas de Guiado y Simulación dependiente de la Gerencia de Tecnología de CITEDEF.

Este grupo de ingeniería cumple las siguientes funciones y tareas de desarrollo:

- Implementación de mejoras en la plataforma de simulación, en el modelo espacial de los simuladores y en la generación de escenarios a partir de información geoespacial.
- Implementación de mejoras en una aplicación destinada crear escenarios para ser utilizados en los simuladores generados en el área.



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

## **Antecedentes y Descripción del Proyecto**

**En el año 2003** se conforma un equipo de trabajo para el Laboratorio de Sistemas de Información Geográfica en CITEDEF (entonces CITEFA).

Como consecuencia de la gran inundación de Santa Fe de ese año, le asignan al laboratorio la misión de investigar y desarrollar herramientas informáticas para mejorar la respuesta ante emergencias de gran escala a nivel nacional.

Los primeros trabajos dieron sus pasos y consistieron en analizar lo actuado en respuesta a la inundación de Santa Fe y a otras emergencias históricas, tratando de identificar los problemas más frecuentes y sus causas, analizándose distintas alternativas para contribuir a reducir estas causas desde el punto de vista de mejorar la información para la toma de decisiones.

Se define también una línea de trabajo progresiva, ya que no existían herramientas que brindaran solución a esta problemática de forma integral y existían grandes dificultades para el intercambio de información entre diferentes instituciones. Las etapas del programa incluyeron un prototipo, luego un Sistema de Adiestramiento para manejo de Crisis y finalmente un Sistema de Gestión que fuera operativo en emergencias.

Es transcurrido este año 2003 que se desarrolla entonces, un prototipo de aplicación para el intercambio de información geográfica y tabular sobre emergencias. Con este Proyecto (CRISIS) se determinó que la capacidad de representación de los sistemas de información geográfica era adecuada para constituir la herramienta central de todo sistema de manejo de emergencias de gran escala, estableciéndose la factibilidad de compartir información de forma distribuida, donde las instituciones fueran responsables de la información que aportan y pudieran ver la situación de forma integrada.

**En el año 2004** se firma un acuerdo específico entre el Estado Mayor Conjunto de las FFAA, el Instituto Geográfico Militar y CITEFA para el desarrollo de herramientas de entrenamiento y coordinación de grupos multidisciplinares complejos. En el mismo se establecía que el Departamento Defensa Civil del EMCO (actualmente la Jefatura de Defensa Civil del COFFAA) pondría a disposición su metodología de trabajo en la coordinación del apoyo militar en emergencias; el Instituto Geográfico Militar (hoy IGN) pondría a disposición la información geográfica y que CITEFA (hoy CITEDEF) realizaría el desarrollo del software.

En ese marco, **entre los años 2004 y 2005** se desarrolla un sistema de Adiestramiento para Manejo de Crisis (AMC), que permitió la preparación, ejecución y evaluación de ejercicios de gabinete (o de toma de decisiones) con participantes de diferentes instituciones. Este sistema de adiestramiento permitió simular la información diferente que obraría en poder de las instituciones, y ponía a disposición un conjunto de componentes e hipótesis para que pudiera realizarse la coordinación de acciones interinstitucionales, unificación de la situación, comunicación segura, manejo colaborativo del





*Ministerio de Defensa*

*Unidad de Auditoría Interna*

ambiente geográfico. De este modo se pudo pasar a evaluar la pertinencia y eficacia de los componentes de hipótesis.

Con el sistema de adiestramiento funcional, se realizaron múltiples ejercicios con el Estado Mayor Conjunto de las Fuerzas Armadas (EMCO) en vistas de comprobar e identificar mejoras a los componentes y se formalizaron dos seminarios internacionales en los años 2005 y 2006.

**Del año 2006 a 2007** se capitalizaron las experiencias alcanzándose la segunda versión del Sistema de Adiestramiento para Manejo de CRISIS (AMaronC II); se apoyaron los ejercicios conjuntos combinados MASI 2007 con Bolivia, y HERMANDAD 2007 con PERÚ.

**Del año 2007 a 2008** (Proyecto CRISIS III PICTO CITEFA-ANPCyT) se avanzó en la investigación y modelización matemática de fenómenos obteniéndose un modelo de pandemia y un modelo de estimación del daño agudo por exposición a contaminantes en el aire. Estos modelos fueron integrados al AMC II para ser utilizados con fines de adiestramiento.

**En el año 2008** se dio apoyo al ejercicio conjunto combinado SOLIDARIDAD 2008, que tuvo particularidades muy especiales. Se trataba de un ejercicio de nivel estratégico nacional ya que altas autoridades de los ministerios de la Nación tomaron parte (Cancillería, Defensa, Interior, Justicia y Derechos Humanos, Planificación y Jefatura de Gabinete de Ministros). Del lado chileno participó una estructura semejante. El argumento del ejercicio fue de Pandemia de Influenza y se utilizó el modelo matemático de Pandemia desarrollado por la entonces División de Modelado y Manejo de Crisis (ex LABSIG). El resultado del ejercicio fue muy importante y se pudieron identificar aspectos a mejorar del Plan Nacional de Pandemia.

**A principios de año 2009** el MINISTERIO DE SALUD solicitó participación para mejorar el plan de pandemia, y en mayo de ese mismo año la Organización Mundial de la Salud (OMS) declaró la alerta epidemiológica influenza A H1N1. El MINISTERIO DE SALUD requirió entonces apoyo para la coordinación de acciones, el intercambio de información de la alerta, la unificación de cartas de situación y las corridas del modelo de pandemia para estimar la posible evolución de la amenaza. Se integraron terminales en Salud, Defensa, Interior, Jefatura de Gabinete y Desarrollo Social entre otros. Se decidió cumplir con el apoyo solicitado pese a estar en la etapa de adiestramiento, pues los sistemas desarrollados habían probado robustez suficiente durante múltiples ejercicios y seguimientos. Para este apoyo, la División proveyó el sistema AMC II, y el modelo matemático y las FFAA destinaron operadores ya formados del Sistema de Crisis para vincular las salas de situación de los diferentes Ministerios de la Nación. Esa red tenía su centro en el Ministerio de Salud.

**Ya en el año 2008** se había iniciado el proyecto de desarrollo del sistema de Gestión, pero la experiencia **del año 2009** obligó a un rediseño y **en año 2010**



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

se concluyó el desarrollo del sistema para el Centro de Manejo de Crisis del EMCFFAA (Proyecto CMC-EMCO). Ese mismo año se implementó el Sistema de manejo de Crisis en las tres Fuerzas Armadas hasta el nivel de Gran Unidad de Combate, se puso en vivo una instancia del software para acceso web (que continuó hasta el año 2018) y se determinó que el sistema sería la herramienta de coordinación en las operaciones de apoyo a la comunidad, dentro y fuera del país, en las que participen las FFAA. Ese mismo año se designó al EMCFFAA como el coordinador único de las FFAA en las operaciones de defensa civil, responsabilidad que pasó al COFFAA tras su conformación.

Se utilizó el sistema para coordinación durante la asistencia a la República de Chile por el terremoto y posterior tsunami del 27 de febrero de 2010. En particular se mantuvo enlace con representantes de la FFAA en el Hospital Reubicable emplazado en la localidad de CURICÓ.

**En el año 2011** se propuso a través del Ministerio de Defensa, al Consejo de Defensa Sudamericano, en el marco de la UNASUR, la adopción del Sistema Crisis como herramienta de coordinación para las actividades de apoyo que los países miembros se brindaran ante emergencias. Esta propuesta fue presentada como respuesta a una iniciativa de EE. UU. exhibida en la OEA, donde se invitaba a los países de América a centralizar su información de capacidades de apoyo, en un software y un servidor ubicado en el Comando Sur de las FFAA norteamericanas (SOUTHCOM).

**En el año 2012** se solicitó apoyo para utilizar el Sistema de Crisis en el Operativo de apoyo a la comunidad denominado Gral. José de San Martín. Este operativo conformaba el componente del Ministerio de Defensa dentro del Plan de Abordaje Integral (AHI), impulsado por el Consejo Nacional de Coordinación de Políticas Sociales, con el objetivo de mejorar las condiciones de vida e infraestructura en barrios carenciados de CABA y GBA. Participaron del Plan los Ministerios participantes del Consejo Coordinador de Políticas Sociales, a saber: Salud y Ambiente, Defensa, Educación, Seguridad, Trabajo, Desarrollo Social, Planificación Federal y Jefatura de Gabinete de Ministros. El proyecto de implantación denominado CRISIS JSM ha vinculado una red de 141 usuarios reunidos en 24 dependencias del Ministerio de Defensa, desde el nivel estratégico nacional (Unidad Ministerio), hasta el táctico operacional (Personal en el terreno). Dicha experiencia se fue desarrollando desde el mes de mayo de 2012 hasta el mes de junio de 2014. El sistema en esta escala barrial se lo utilizó fundamentalmente para coordinar acciones en el terreno utilizando el componente de tareas consistente en un C3I2 adaptado a operaciones cívico-militares de defensa civil.

**Entre los años 2013 y 2015** se desarrollaron prototipos para interoperar información geográfica para la gestión de riesgos (Proyecto MILCAPAS), la generación de avisos y alertas interoperables (Proyecto CAPRESSE), la explotación de alertas, avisos y noticias (Proyecto ESPRESSO), la modelización matemática de actividad eléctrica atmosférica (Proyecto



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

GEORAYOS), la integración de redes de sensores ambientales (Proyecto GEOUV), la modelización matemática de información LIDAR atmosférico (Proyecto GEOAEROSOLES), la Integración de información ambiental en la red SAVER-NET en el marco de un proyecto de cooperación con Japón y Chile.

**En el año 2016** fue solicitado por la Dirección Nacional de Protección Civil - Ministerio de Seguridad (MINSEG), el Sistema de CRISIS (una copia del CMC-EMCO), para coordinar la gestión de emergencias con la activación del SIFEM. Luego se derogó el Decreto N° 1250/99 del SIFEM y se sancionó la Ley N° 27.287 que creó el Sistema Nacional para la Gestión Integral del Riesgo y la Protección Civil (SINAGIR), con el objeto de integrar, fortalecer y optimizar las acciones destinadas a la reducción de riesgos, el manejo de crisis y la recuperación.

El proyecto **SINAGIR** se planificó en 3 etapas:

- La primera **2017 – 2018**, se implementó una instancia del sistema de CRISIS CMC<sup>(1)</sup>, brindándose capacitación a operadores de Protección Civil de todas las provincias del MINSEG y se relevaron los requerimientos para el Sistema Nacional de Monitoreo de Emergencias (SINAME), lugar donde MINSEG concentra todo lo que es monitoreo y manejo de emergencias (Proyecto SINAGIR Etapa I).

(1) **CRISIS CMC** programado en JAVA, utiliza una Base de Datos SQLITE3 y hosteado en [www.sistema-crisis.gob.ar](http://www.sistema-crisis.gob.ar)

- La segunda **2019 – 2022**, que contempló el uso en situaciones reales del sistema CRISIS CMC en el SINAME, mientras se realiza en paralelo el desarrollo del Sistema de Gestión de Emergencias específico para el SINAGIR<sup>(2)</sup>. Este proyecto está en curso cercano a su finalización. (Proyecto SINAGIR Etapa II).

(2) Sistema del **MINSEG** desarrollado en PYTHON sobre el FrameWork FLASK y utiliza Maria Db de Base de Datos.

- La tercera, solo proyectada, consideraría la implantación del sistema específico para el SINAGIR y la interrupción del uso del Sistema CRISIS CMC. (Proyecto SINAGIR Etapa III).

Esta etapa aun no comenzó, sin embargo, **desde junio de 2019**, el sistema CRISIS CMC está en uso permanente por el MINSEG como herramienta de gestión de emergencias.

## Conclusión

El Sistema Crisis tiene una arquitectura de alta complejidad, no sólo porque trabaja con cada uno de los componentes que lo conforman, sino también porque trabaja en la integración y homogeneidad de dichos componentes de modo de agilizar el flujo de datos con los diferentes nodos.



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

Durante el desarrollo de la auditoría se utilizaron diferentes herramientas que permitieron la evaluación del control interno imperante en el Ciclo de Vida del desarrollo del Sistema de Crisis, el análisis de factibilidades y de las funcionalidades del Sistema, la revisión de documentación suministrada y la realización de entrevistas con los funcionarios responsables del área considerada en el Marco de Referencia.

El proyecto CMC EMCO fue consecuencia de una línea de proyectos preparatorios que demostraron la factibilidad de desarrollo del Software para un Centro de Manejo de Crisis. La metodología exigió que se incluyera en la documentación de apertura, los estudios de factibilidad y otros antecedentes técnicos, realizándose una evaluación de la factibilidad por 3 instancias: Jefe de proyecto, Director o Gerente y la entonces Gerencia General.

Durante el desarrollo del Software del Sistema de Crisis, se realizó un proceso de monitoreo y seguimiento de proyectos para todas las actividades de desarrollo, a través del formulario Informe Trimestral de la Orden de Trabajo. Habiéndose cumplido en todo momento con los plazos y objetivos.

Desde junio de 2019 a la actualidad el Ministerio de Seguridad está usando a nivel nacional en forma permanente el Sistema de CRISIS CMC como herramienta de gestión de emergencias, también conocido como el Sistema Nacional para la Gestión Integral del Riesgo y la Protección Civil (Proyecto SINAGIR etapa I) que tiene por objeto integrar las tareas para fortalecer y optimizar las acciones destinadas a la reducción de riesgos, el manejo de crisis y la recuperación.

En forma paralela el Ministerio de Seguridad ha tercerizado a Servicios técnicos especializados externos el desarrollo del Sistema de Gestión de Emergencias Específico (SINAGIR). Este proyecto está cercano a su finalización. (Proyecto SINAGIR Etapa II)

La tercera etapa (solo proyectada) consideró la implantación del sistema SINAGIR y la interrupción del uso del Sistema CRISIS CMC. Esta etapa aun no comenzó.

En opinión de esta Auditoría, CITEDEF ejecutó los controles en forma razonable y seleccionó una estrategia de diseño adecuada basada en un modelo de desarrollo evolutivo que permite la identificación de riesgos y la redefinición del diseño en cada iteración, producto de la evaluación de los usuarios y determinación de requerimientos, las veces que ello sea necesario.

Para permitir que el Ministerio de Defensa y las FFAA utilicen el Software desarrollado en el marco del Proyecto SINAGIR Etapa II, sería recomendable la publicación del código fuente del proyecto con autorización del Ministerio de Defensa. Esto permitiría que las instituciones adopten, mejoren y publiquen sus modificaciones al Software y que NO exista un potencial conflicto con el Ministerio de Seguridad por la propiedad intelectual del mismo.



*Ministerio de Defensa*

*Unidad de Auditoría Interna*

Cabe destacar que actualmente en CITEDEF el Departamento de Modelado y Manejo de Crisis, área que desarrolló este software, está disuelto y no se cuenta con personal para dar continuidad al mantenimiento de estos sistemas.

Por lo expuesto, sería conveniente evaluar la utilización efectiva del sistema frente a requerimientos actuales en el ámbito del Ministerio de Defensa y de las Fuerzas Armadas, así como su adaptación y el desarrollo de componentes específicos de ser considerado de utilidad para la cobertura de necesidades específicas previamente definidas por los potenciales usuarios.

**BUENOS AIRES**, diciembre 2021