

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO	
VERSIÓN: 01	GESTIÓN DE INCIDENTES DE CONTINUIDAD	
EMISIÓN: 23 DIC 2024		

GESTIÓN DE INCIDENTES DE CONTINUIDAD

CONTROL DE GESTION DOCUMENTAL		
Elaboró: Proyecto de Actualización de Activos de Información ICFE 2024	Revisó y aprobó: Integrantes del Comité de desempeño Institucional	Aprobó: Cr. Ernesto Mejía Araque Director Instituto de Casas Fiscales del Ejército

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

1. INTRODUCCIÓN

El presente documento describe el procedimiento de atención de incidentes de continuidad del negocio, que le permitan al ICFE manejar adecuadamente los eventos materializados para los procesos y servicios tecnológicos críticos de negocio evaluados en el BIA en conjunto con el AIA, y de esta forma minimizar el impacto de eventos disruptivos mayores.

2. JUSTIFICACIÓN

La Resolución No 065 del 24 de mayo de 2016, del INSTITUTO DE CASAS FISCALES DEL EJÉRCITO, por medio de la cual se adopta la Directiva No 2014-18 del 19 de junio de 2014 “Políticas de Seguridad de la Información para el Sector Defensa”, establece la elaboración del Manual de Seguridad de la Información para el Instituto.

Para el año 2021, por medio de la resolución interna ICFE No. 0052 del 185 de febrero, la entidad adopta el Sistema de Gestión de Seguridad de la Información (SGSI), como parte del cumplimiento de normativas regulatorias del Ministerio de Defensa y del Departamento Administrativo de la Función Pública.

Este documento hace parte de los documentos del Sistema de Gestión de Continuidad del Negocio y está encaminado a gestionar los posibles incidentes que puedan derivar en la activación del BCP, DRP, el plan de emergencias o una combinación de los mismos, de acuerdo con la magnitud y alcance del incidente presentado; de forma que le permitan al Instituto responder adecuadamente ante un evento disruptivo mayor con características de desastre.

3. OBJETIVO

Gestionar de forma oportuna los incidentes de continuidad del negocio ante la materialización de un evento disruptivo mayor con características de desastre, de forma que se asegure la continuidad de las operaciones y/o servicios tecnológicos afectados y el Instituto pueda continuar prestando sus servicios de vivienda al personal militar.

4. ALCANCE

Aplica para la gestión de todos los incidentes de continuidad del negocio al interior del Instituto de Casas Fiscales del Ejército, iniciando desde el reporte hasta el cierre y finalización del incidente, comprendiendo las siguientes actividades:

- Reporte y registro del evento y/o incidente de seguridad de la información.
- Evaluación inicial del reporte.
- Análisis y evaluación del impacto.
- Aplicación de acciones de contención.
- Documentación de lecciones aprendidas.
- Notificación de cierre del evento y/o incidente.

5. DEFINICIONES

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su recurrencia. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.9]*

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO	
VERSIÓN: 01	GESTIÓN DE INCIDENTES DE CONTINUIDAD	
EMISIÓN: 23 DIC 2024		

- **Actividad:** Conjunto de una o más tareas con un resultado específico. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.1]*
- **Actividad priorizada:** Actividad a la cual se le da urgencia con el fin de evitar impactos indeseables para el negocio durante una interrupción. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.25]*
- **Acuerdo de confidencialidad:** Un acuerdo de confidencialidad es un documento que se firma entre partes, en el cual se comprometen a no divulgar ni compartir información que manejan por motivos de trabajo, o de participación en algún proyecto u emprendimiento. Es decir, se comprometen a mantener la confidencialidad de la información a la que tienen acceso. *[CoceptosJuridicos.com URL: <https://www.conceptosjuridicos.com/acuerdo-de-confidencialidad/>]*
- **Acuerdo de Nivel de Servicio (ANS o SLA por sus siglas en inglés):** Acuerdo documentado entre un prestador de servicios y un cliente, el cual identifica los servicios y los objetivos del servicio. *[Norma ISO 20000:2012, Capítulo 3, Términos y definiciones, numeral 3.3]*
- **Alta dirección:** Persona o grupo de personas que dirigen y controlan una organización en su más alto nivel. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.31]*
- **Análisis de impacto al negocio (BIA, por sus siglas en inglés):** Proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo, en la organización. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.5]*
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.2]*
- **Control:** Medida que modifica un riesgo. *[Norma ISO 27000:2017, Capítulo 2, Términos y definiciones, numeral 2.16]*
- **Competencia:** Habilidad de aplicar los conocimientos y las habilidades para lograr los resultados deseados. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.6]*
- **Conformidad:** Cumplimiento de un requisito. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.7]*
- **Continuidad del negocio:** Capacidad de una organización de continuar la oferta de productos y servicios dentro de un periodo de tiempo aceptable a una capacidad predefinida durante una interrupción. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.3]*

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		
GESTIÓN DE INCIDENTES DE CONTINUIDAD		

- **Desempeño:** Resultado medible. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.23]*
- **Disparador:** Evento que hace que el sistema inicie una respuesta. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.15]*
- **Eficacia:** Grado en el cual se realizan las actividades planeadas y se logran los resultados esperados. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.12]*
- **Equipos de continuidad del negocio:** Grupo de personas responsables del desarrollo, implementación, pruebas, mantenimiento y ejecución de los planes de continuidad de la organización. *[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]*
- **Estimación del riesgo.** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. *[Norma ISO 27005:2009, Capítulo 3, Términos y definiciones, numeral 3.5]*
- **Evitar el riesgo.** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. *[Norma ISO 27005:2009, Capítulo 3, Términos y definiciones, numeral 3.3]*
- **Fuente de riesgo:** Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo. *[Norma ISO 31000:2018, Capítulo 3, Términos y definiciones, numeral 3.4]*
- **Gestión de continuidad del negocio (BCM, por sus siglas en inglés):** Proceso general que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que, en caso de materializarse, y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.2]*
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar la organización con relación al riesgo. *[Norma ISO 31000:2018, Capítulo 3, Términos y definiciones, numeral 3.2]*
- **Impacto:** Resultado de una interrupción que afecta los objetivos. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.13]*
- **Incidente:** Evento que puede ser, o podría conducir a una interrupción *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.14]*
- **Información documentada:** Información que una organización tiene que controlar y

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		
GESTIÓN DE INCIDENTES DE CONTINUIDAD		

mantener, y el medio que la contiene. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.11]*

- **Interrupción:** Incidente, bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.10]*

- **Malware:** Abreviatura de software malicioso. Diseñado para infiltrarse, dañar u obtener información de un sistema informático sin el consentimiento del propietario **Nota:** El malware se considera comúnmente para incluir virus informáticos, gusanos, troyanos, spyware y adware. El spyware se utiliza generalmente con fines de marketing y, como tal, no es malicioso, aunque generalmente no es deseado. Sin embargo, el spyware se puede utilizar para recopilar información para el robo de identidad u otros fines claramente ilícitos. *[ISACA:2015 - Glosario de términos – URL: <https://www.isaca.org/resources/glossary>]*

- **MAO – Maximum acceptable outage** – Ver MTPD

- **Medición:** Proceso para determinar un valor. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.17]*

- **Mejoramiento continuo:** Actividad recurrente para mejorar el desempeño. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.8]*

- **Modo de falla:** Manera por la cual una falla es observada. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.9]*

- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.18]*

- **MTPD – Maximum tolerable period of disruption:** Tiempo que tomaría para que los impactos adversos, que pueden surgir como resultado de no proporcionar un producto/servicio o realizar una actividad, se vuelvan inaceptables *[Norma ISO 22300:2021, Capítulo 3, Términos y definiciones, numeral 3.1.151]*

- **Nivel de decisión estratégico:** El nivel de decisión estratégico relacionado con la continuidad del negocio se refiere a las decisiones que se toman a nivel ejecutivo para garantizar la supervivencia y la resiliencia de una organización frente a posibles interrupciones o desastres. *[Bajgoric, N., & Hadziahmetovic, N. (2019). Strategic Decision Making in the Field of Business Continuity Management: Conceptual Framework. Journal of Contemporary Management Issues, 24(1), 83-103.]*

- **Nivel de decisión operativo:** El nivel de decisión operativo relacionado con la continuidad del negocio se refiere a las decisiones que se toman a nivel de la línea de frente o de la ejecución diaria para garantizar la implementación efectiva de los planes y procedimientos establecidos a niveles estratégicos y tácticos. *[Elliot, S., Swartz, E., &*

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

Herbane, B. (2010). Business continuity management: A crisis management approach. In The Handbook of Crisis Communication (pp. 298-320). Wiley-Blackwell.]

- **Nivel de criticidad:** Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra. *[Guía Nro 10 para la preparación de las TIC para la continuidad del negocio, Capítulo 5, Glosario]*

- **Nivel de decisión táctico:** El nivel de decisión táctico relacionado con la continuidad del negocio implica tomar decisiones operativas a corto y mediano plazo para implementar los planes y estrategias establecidos a nivel estratégico. Estas decisiones se centran en la gestión de recursos y actividades específicas para mantener la continuidad de las operaciones durante situaciones de emergencia o crisis. *[Bajgoric, N., & Hadziahmetovic, N. (2019). Strategic Decision Making in the Field of Business Continuity Management: Conceptual Framework. Journal of Contemporary Management Issues, 24(1), 83-103]*

- **No conformidad:** Incumplimiento de un requisito. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.19]*

- **Objetivo:** Resultado a lograr. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.20]*

- **Objetivo mínimo de continuidad del negocio (Minimum Business Continuity Objective – MBCO, por sus siglas en inglés):** Mínimo nivel de servicios y/o productos que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.11]*

- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridad y relaciones para lograr sus objetivos. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.21]*

- **Parte interesada - término preferido- / Accionista (stakeholder) - término admitido:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. Ejemplo: Clientes, propietarios, personal de una organización, proveedores, banca, legisladores, sindicatos, socios o sociedad que pueden incluir competidores o grupos de presión con intereses opuestos. Se consideran partes interesadas las comunidades impactadas y las poblaciones locales se consideran partes interesadas. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.15]*

- **Plan de continuidad del negocio (BCP, por sus siglas en inglés):** Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.3]*

- **Plan de Recuperación ante Desastres de TIC (DRP):** Plan claramente definido y documentado el cual permite recuperar las capacidades de la tecnología y las

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

telecomunicaciones cuando se presenta una interrupción. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.14]*

- **Política:** Propósitos y dirección de una organización, como expresa formalmente la alta dirección. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.24]*
- **Probabilidad:** Posibilidad de que algo ocurra. *[Norma ISO 31000:2018, Capítulo 3, Términos y definiciones, numeral 3.7]*

• **Programas utilitarios:** Los programas utilitarios son programas que brindan una “utilidad” específica y no están diseñados para un tipo de usuario particular. Ejemplo, procesadores de texto, planillas de cálculo, videojuegos, navegadores para la web, etc.

• **Plan de continuidad del negocio:** Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.4]*

• **Preparación de las TIC para la continuidad de negocio (ICT Readiness for Business Continuity - IRBC, por sus siglas en inglés):** Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción, así como la recuperación de sus servicios de TIC. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.10]*

• **Proceso:** Conjunto de actividades interrelacionadas o que interactúan las cuales transforman entradas en salidas. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.26]*

• **Productos y servicios:** Salida o resultado que provee una organización a las partes interesadas. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.27]*

• **Punto objetivo de recuperación (RPO, Recovery Point Objective, por sus siglas en inglés):** Punto en el tiempo en el cual los datos deberían ser recuperados después de que una interrupción ocurra. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.12]*

• **Recursos:** Todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones, provisiones, suministros e información (bien sea electrónica o no) que una organización posee y que tienen que tener disponibilidad para usarse cuando sea necesario, con el fin de operar y lograr su objetivo. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.29]*

• **Reducción del riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. *[Norma ISO 27005:2009, Capítulo 3, Términos y definiciones, numeral 3.7]*

• **Registro vital:** Registro electrónico o en papel que es esencial para preservar, continuar

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.16]*

- **Requisito:** Necesidad o expectativa que se indica, generalmente implícita u obligatoria. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.28]*
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular. *[Norma ISO 27005:2009, Capítulo 3, Términos y definiciones, numeral 3.8]*
- **Resiliencia:** Habilidad para una organización para resistir al ser afectada por una interrupción. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.14]*
- **Riesgo:** Efecto de la incertidumbre en los objetivos. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.30]*
- **Riesgo residual:** Riesgo remanente después del tratamiento del riesgo. *[Norma ISO 27000:2017, Capítulo 2, Términos y definiciones, numeral 2.64]*
- **Servicios tecnológicos:** Conjunto de actividades basadas en la tecnología que buscan responder a las necesidades de los usuarios. Dentro de los servicios tecnológicos se encuentran, entre otros: los servicios tecnológicos de bases de datos, los servicios tecnológicos de comunicaciones LAN / WAN e internet, los servicios tecnológicos de seguridad, los servicios tecnológicos de almacenamiento y virtualización, los servicios tecnológicos de la nube (web, email y redes sociales).
- **Sistema de gestión:** Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr esos objetivos. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.16]*
- **Sitio alternativo:** Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.1]*
- **Subcontratar:** Realizar un acuerdo donde una organización externa realiza parte de una función o proceso de la organización. Nota: Una organización externa esta por fuera del alcance del sistema de gestión, aunque la función o proceso subcontratado esté dentro del alcance. *[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.22]*
- **Tercero / Proveedor:** Persona natural o jurídica con quien se vincula la Entidad para apoyar la ejecución de sus macroprocesos estratégicos, misionales, apoyo y evaluación en aras de cumplir los objetivos del negocio.
- **Tiempo objetivo de recuperación (RTO, Recovery Time Objective, por sus siglas en inglés):** Periodo de tiempo en el cual los mínimos niveles de servicios y/o productos y

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

los sistemas, aplicaciones o funciones que los soportan deben ser recuperados después de que una interrupción ocurra. *[ISO/IEC 27031:2016, Capítulo 3, Términos y definiciones, numeral 3.13]*

- **Transferencia del riesgo.** Compartir con otra de las partes la pérdida o la ganancia de un riesgo. *[Norma ISO 27005:2009, Capítulo 3, Términos y definiciones, numeral 3.9]2000*
- **WRT – Working Recovery Time:** Es la cantidad máxima tolerable de tiempo que tiene un equipo de recuperación ante desastres para verificar que los sistemas y la protección de datos estén en línea y operativos. WRT es la fase posterior a la restauración de los datos y las operaciones de misión crítica, cuando la organización debe concentrarse en volver a la normalidad.

6. NORMATIVIDAD

- Constitución Política de Colombia 1991.
- Ley 80 de 1993 “Estatuto General de contratación de la administración Pública”.
- Ley 87 de 1993 “Control interno en los organismos del Estado”.
- Ley 527 de 1999 “Comercio Electrónico”.
- Ley 594 del 2000 “Ley General de Archivo”.
- Ley 599 del 2000 “Código Penal Colombiano”.
- Ley 603 del 2000 “Control de legalidad del Software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Guía Nro 10 para la preparación de las TIC para la continuidad del negocio.
- Norma Técnica Colombiana NTC-ISO 22301 – Seguridad y resiliencia – Sistema de gestión de continuidad del negocio – Requisitos.
- Guía Técnica Colombiana – GTC-ISO/IEC 27031 Tecnologías de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de información y las comunicaciones para la continuidad del negocio.

7. VALIDEZ DEL PROCEDIMIENTO DE INCIDENTES DE CONTINUIDAD

El presente documento será válido hasta cuando se realice una nueva revisión de éste, mínimo una vez al año.

8. CLASIFICACIÓN DEL DOCUMENTO

Toda la documentación asociada a la gestión de incidentes se clasifica como **Información Pública Clasificada**

9. RESPONSABLES

Asesor de Gestión Integral:

- Asumir el rol de **Líder de Continuidad** con las funciones y responsabilidades asociadas tanto en operación normal como en operación en contingencia del BCP, definidas en el documento de gobierno de continuidad del negocio.
- Conocer, entender y ejecutar las actividades establecidas de su rol para el BCP, tanto en operación normal como en operación en contingencia.

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

- Revisar y actualizar el presente documento y la información de sus formatos asociados a nivel de BCP de forma periódica, mínimo una vez al año;
- Ser el dueño del presente documento y sus formatos asociados.

Coordinador o encargado del Grupo de Gestión de la Información y TIC

- Asumir el rol de **Líder de DRP** con las funciones y responsabilidades asociadas tanto en operación normal (Administración) como en operación en contingencia (Operación) del DRP, definidas en el documento de gobierno de continuidad del negocio.
- Conocer, entender y ejecutar las actividades establecidas de su rol para el DRP, tanto en operación normal (Administración) como en operación en contingencia (Operación) del DRP.
- Revisar y actualizar el presente documento y la información de sus formatos asociados a nivel de DRP de forma periódica, mínimo una vez al año;
- Informar de los cambios realizados a la evaluación de las estrategias de tecnología al Líder del BCP, para su conocimiento.

Dueños de procesos:

- Asumir el rol de **Líder del Equipo de Respuesta y Recuperación (LERyR)** del proceso del cual es dueño, con las funciones y responsabilidades asociadas tanto en operación normal como en operación en contingencia del BCP, definidas en el documento de gobierno de continuidad del negocio.
- Conocer, entender y ejecutar las actividades establecidas de su rol para el BCP, tanto en operación normal como en operación en contingencia.

Personal del proceso:

- Asumir el rol de **Miembro del Equipo de Respuesta y Recuperación (MERyR)** con las funciones y responsabilidades asociadas tanto en administración como en operación del BCP, definidas en el documento de gobierno de continuidad del negocio.
- Conocer, entender y ejecutar las actividades establecidas de su rol para el BCP, tanto en operación normal como en operación en contingencia, definidas en el documento de gobierno de continuidad del negocio.
- Conocer al **Líder de respuesta y recuperación** del proceso al cual pertenecen.

10. PROCEDIMIENTO

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN	DOCUMENTO O REGISTRO
1. Detección y/o reporte del incidente	Usuarios del ICFE (personal militar, contratista o de planta)	El incidente puede presentarse en cualquier momento y en cualquier lugar, por lo tanto, puede ser detectado por cualquier persona o colaborador del ICFE. Una vez se detecte que se ha presentado el incidente, se debe notificar a la Mesa de Ayuda. Ir a la actividad 2	Caso registrado en el sistema de Mesa de Ayuda

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO	
VERSIÓN: 01	GESTIÓN DE INCIDENTES DE CONTINUIDAD	
EMISIÓN: 23 DIC 2024		

2. Análisis del incidente	Mesa de Ayuda	La Mesa de Ayuda recibe el reporte del evento y/o incidente, lo identifica, registra, clasifica y evalúa si el mismo se puede resolver con contingencias internas, tanto de negocio como tecnológicas. Ir a la actividad 3	Caso registrado en el sistema de Mesa de Ayuda
3. Evaluar resolución con contingencias internas	Mesa de Ayuda	Si se puede resolver con contingencias internas de negocio o tecnológicas, ir a la actividad 4 . De no ser así, ir a la actividad 5	Caso registrado en el sistema de Mesa de Ayuda
4. Aplicar contingencias definidas	Mesa de Ayuda	Contingencias de negocio: Si existen contingencias internas de negocio, la Mesa de Ayuda solicita al proceso afectado la ejecución de las contingencias definidas. Contingencias tecnológicas: Si existen contingencias tecnológicas, la Mesa de Ayuda solicita al área de TI la ejecución de las contingencias establecidas para restaurar el servicio afectado. Ir a la actividad 5	Caso registrado en el sistema de Mesa de Ayuda
5. ¿Incidente resuelto?	Mesa de Ayuda	La Mesa de Ayuda evalúa, en conjunto con el proceso afectado o el área de TI, según corresponda; si el incidente disruptivo fue resuelto. Si fue resuelto, ir a la actividad 8 . En caso contrario, ir a la actividad 6	Caso registrado en el sistema de Mesa de Ayuda
6. Evaluar afectación	Mesa de Ayuda	La Mesa de Ayuda evalúa si el incidente disruptivo afecta la vida del personal del Instituto, las operaciones de los procesos y/o los servicios tecnológicos e informa a los integrantes del Comité de Gestión y Desempeño con funciones de continuidad de la situación. Ir a la actividad 7 .	Caso registrado en el sistema de Mesa de Ayuda

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO GESTIÓN DE INCIDENTES DE CONTINUIDAD	
VERSIÓN: 01		
EMISIÓN: 23 DIC 2024		

7. Activación de planes	Comité de Gestión y Desempeño con funciones de continuidad de la situación.	El personal del Comité de Gestión y Desempeño con funciones de continuidad evalúa la información recibida y ordena activar uno o varios de los siguientes planes, según la afectación y magnitud del evento disruptivo: 1. Activa el Plan de Emergencias para salvaguardar la vida del personal. 2. Activar el Plan de Continuidad del Negocio, si la operación de los procesos se ha visto comprometida por el evento disruptivo. 3. Activar el Plan de Recuperación ante Desastres, si la operación tecnológica del Instituto está comprometida. El Personal del Comité de Gestión y Desempeño con funciones de continuidad se renombra como Comité de Crisis para atender la situación, con las funciones y responsabilidades definidas en el documento de Gobierno de Continuidad del Negocio para su función en Operación en Contingencia. El manejo del incidente disruptivo se gestionará a través de las actividades definidas en cada uno de los diferentes planes activados y retornará a este flujo cuando la totalidad de dichas actividades de cada plan activado hayan finalizado su ejecución. Ir a la actividad 8.	Plan de Emergencias Plan de Continuidad del Negocio Plan de Recuperación ante Desastres
8. Registro de hallazgos y lecciones aprendidas	Líderes de Procesos Líder de BCP Líder de DRP	Registrar los hallazgos y las lecciones aprendidas una vez el incidente haya sido resuelto, así como de las actividades realizadas en cada una de las etapas de detección y análisis, contención, erradicación y recuperación. Ir a la actividad 9	Hallazgos Lecciones aprendidas

11. REGISTROS Y DOCUMENTOS ASOCIADOS

CÓDIGO	NOMBRE DEL DOCUMENTO
ICFE-P-113	PLAN DE CONTINUIDAD DEL NEGOCIO
ICFE-P-175	PLAN DE RECUPERACIÓN ANTE DESASTRES.

CÓDIGO: ICFE-P-191	INSTITUTO DE CASAS FISCALES DEL EJÉRCITO	
VERSIÓN: 01	GESTIÓN DE INCIDENTES DE CONTINUIDAD	
EMISIÓN: 23 DIC 2024		

CÓDIGO	NOMBRE DEL DOCUMENTO
ICFE-P-90	PLAN DE EMERGENCIAS – SEDE ADMINISTRATIVA ICFE

12. REGISTRO DE MODIFICACIONES (espacio exclusivo para calidad)

VERSIÓN	FECHA MODIFICACIÓN	NUMERAL MODIFICADO	NATURALEZA DEL CAMBIO
01	23-12-2024	Todo	Documento nuevo