



PLAN DE CONTINUIDAD PARA LA UNIDAD DE INVESTIGACIÓN CRIMINAL DE LA DEFENSA S.A.S.

1. Introducción

La Unidad de Investigación Criminal de la Defensa reconoce la importancia de consolidar un Plan de Continuidad Operativa (PCO) para establecer los procedimientos y estrategias que garanticen la continuidad de las operaciones esenciales de la UID, en caso de incidentes que puedan interrumpir su funcionamiento normal.

2. Objetivos

- Asegurar la disponibilidad y continuidad de los servicios críticos de la UID.
- Reducir el impacto de incidentes que puedan comprometer las investigaciones, peritajes y la seguridad de la información.
- Facilitar una recuperación eficiente y organizada de las operaciones.

3. Alcance

Este plan se aplica a todas las áreas funcionales de la UID, incluyendo personal, infraestructura, sistemas de información y comunicaciones.

4. Análisis de Riesgos

Se identifican los principales riesgos que podrían afectar la continuidad operativa:

- Ciberataques (ransomware, phishing, accesos no autorizados).
- Desastres naturales (terremotos, inundaciones, incendios).
- Fallas tecnológicas (caídas de servidores, pérdida de datos).
- Amenazas internas (errores humanos, sabotaje, fuga de información).

5. Estrategias de Continuidad

- Redundancia de Infraestructura: Implementación de servidores de respaldo y almacenamiento en la nube. Se implementarán data centers en ubicaciones geográficas distintas y se establecerán procedimientos de replicación en tiempo real para asegurar la disponibilidad de los sistemas en caso de una interrupción.
- Seguridad de la Información: Implementación de protocolos de cifrado de extremo a extremo, autenticación multifactor en todos los accesos críticos y almacenamiento seguro de registros sensibles. Se realizarán auditorías de seguridad periódicas para evaluar vulnerabilidades y aplicar medidas correctivas.
- Planes de Respuesta a Incidentes: Desarrollo de manuales de actuación para distintos tipos de incidentes, incluyendo ciberataques, intrusiones físicas y sabotajes internos. Los equipos deben estar preparados para ejecutar procedimientos de contención, mitigación y recuperación en un tiempo mínimo para reducir el impacto en las operaciones.
- Capacitación del Personal: Programas continuos de entrenamiento en ciberseguridad, gestión de crisis y manejo de información clasificada. Se realizarán simulacros y ejercicios prácticos que permitan evaluar la capacidad de respuesta del equipo ante situaciones reales.

- Planes de Comunicación de Emergencia: Definición de canales de comunicación alternativos y seguros, incluyendo redes privadas virtuales (VPN), sistemas de mensajería cifrada y protocolos de comunicación fuera de línea. Se deben establecer listas de contactos prioritarios y procedimientos para informar rápidamente sobre incidentes a las partes interesadas.
- Gestión de la Continuidad Operativa: Implementación de un modelo de gestión basado en el ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar), con revisiones periódicas del PCO para adaptarlo a nuevos riesgos y tecnologías emergentes.

6. Procedimientos de Recuperación

- Evaluación del Incidente: Identificación del impacto y notificación a los funcionarios y/o autoridades correspondientes.
- Activación del PCO: Implementación de protocolos de recuperación según el tipo de incidente.
- Restauración de Servicios: Recuperación de sistemas, acceso a datos de respaldo y verificación de integridad.
- Evaluación Post-Incidente: Análisis de fallas, mejoras al PCO y documentación del evento.

7. Revisión y Mantenimiento del Plan

El PCO se revisará anualmente y tras cada incidente significativo para asegurar su eficacia y actualización según nuevas amenazas y tecnologías emergentes.

8. Contactos de Emergencia

Lista de contactos clave dentro de la UID y entidades de respuesta ante incidentes.

- Contacto Yefrin Garavito- Director UID: 3173468593
- Contacto Damián Guevara- Director Suplente UID: 3115572711
- Emergencias: 123
- Policía: 112
- Bomberos: 119
- Cruz Roja: 132
- Línea Púrpura: 01 8000 112137
- Acueducto: 116
- Fiscalía General de la Nación: 01 80009197 48



YEFRIN ALEXIS GARAVITO NAVARRO
REPRESENTANTE LEGAL



DAMIÁN LEANDRO GUEVARA HERNÁNDEZ
REPRESENTANTE LEGAL SUPLENTE