Objetivo

Identificar y mantener actualizado el listado del personas clave y de los grupos de interés estratégico, responsables de brindar una respuesta oportuna, coordinada y eficaz ante cualquier incidente o evento que afecte los sistemas de información del Instituto, protegiendo la continuidad operativa, la seguridad de la información y la adecuada gestión de incidentes conforme a los protocolos establecidos.

Alcance

Establecer mecanismos y procedimientos eficaces para minimizar el impacto de eventos o incidentes inesperados que puedan afectar cualquier proceso, área o dependencia del IDEAM, protegiendo la continuidad operativa, la protección de los activos de información, la recuperación oportuna de los servicios críticos y la adecuada coordinación entre las partes involucradas, conforme a los lineamientos institucionales y mejores prácticas en gestión de incidentes.

Definiciones

Múltiples partes interesadas: Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil. (MSPI 2025)

COLCERT: Por sus siglas en inglés Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual se encuentra enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica cibernética del Estado Colombiano frente a emergencias de Ciberseguridad que atenten y comprometan la seguridad y defensa nacional. (MSPI 2025)

CSIRT: (Computer Security lncident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes. (MSPI 2025)

CSIRT Gobierno: Equipo de Respuesta a Incidentes de Seguridad en sus siglas en inglés (Computer Security Incident & Response Team), integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan medidas tendientes a prevenir y gestionar incidentes de ciberseguridad de las entidades del estado. (MSPI 2025)

CSIRT sectorial: Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones. (MSPI 2025)

CSIRT sectorial crítico: Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos. (MSPI 2025)

Siglas (si se requiere)

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia

CSIRT: (Computer Security lncident & Response Team)

PONAL: Policía nacional

Documentos relacionados en el SGI

- RESOLUCIÓN No. 063 del 22 de enero de 2025, Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del IDEAM
- Manual de políticas complementarias de seguridad y privacidad de la información
- Procedimiento de gestión de eventos e incidentes de seguridad

Recursos de Comunicación

Este apartado detalla los medios, herramientas y canales de comunicación disponibles para garantizar una interacción efectiva, oportuna y segura entre los miembros del Equipo de Atención de Incidentes y los funcionarios del Instituto, incluyendo tanto personal interno como externo (outsourcing). Estos recursos son fundamentales para coordinar acciones, compartir información crítica y asegurar una respuesta articulada ante cualquier incidente que afecte los sistemas de información del IDEAM.

Funcionaria Tecnico Operativo - Dhime	Servidores Dhime
Funcionario Tecnico Administrativo - Portal Web	Servidores del Portal Web
Contratista - Desarrollador - Utils	Servidores Utils
Contratista - Desarrollador - PCB	Servidores PCB
Contratista - Desarrollador - Renare	Servidor de Renare
Contratista - Desarrollador - Sisaire	Servidores de Sisaire
Contratista - Desarrollador - Orfeo	Servidores Orfeo
Contratista - Desarrollador - Smarmet, Goes	Servidores Smarmet
Contratista - Gerente de proyectos -FonVida	Servidores Siivra
Polaris	Servidores Polaris
Contratista - Desarrollador - RUA	Servidores Rua
Contratista - Pruebas y Requerimientos	Acceso a los aplicativos
Contratista - Seguridad Perimetral	Equipos de Seguridad Perimetral

Proveedores y terceros que prestan servicios al IDEAM

Servicio	Actividad	Nombre	Teléfono	correo
Soporte DIHME	Solución de incidencias	Cristian Tamayo		christian.tamayo@globalmvm.com
Soporte AQ Samples	Solución de incidencias	Soporte Aquarius Samples		

Servicio	Actividad	Nombre	Teléfono	correo
Soporte Chat Bot Pagina Web	Solución de incidencias	Pablo Fernandez		pfernandez@avantiit.co
Soporte Polaris	Solución de incidencias	Ana Guarecocu		a.guarecuco@siapmicros.com
Soporte y mantenimiento seguridad perimetral	Solución de incidencias	Soporte Datasec	601 7450145	soporte@datasec.com.co
Servicio conectividad IDEAM	Canal de comunicación backup	Jeffer Bohorquez	319 5023273	renata@ideam.gov.co
Soporte y mantenimiento equipo aire acondicionado de 15 TR - Datacenter	Equipo de aire acondicionado de 10 TR	Rene Moreno	3153699019	sergio.botero@opavsas.com
Soporte y mantenimiento equipo aire acondicionado de 10 TR - Datacenter	Equipo de aire acondicionado de 15 TR	Fabián Quintero	314 2449792	info@digitalservice.com.co
Soporte y mantenimiento equipos UPS	Planta electrica	Claudia Naranjo	3183574221	claudianaranjo@powersunups.com

Contacto Autoridades Externas

CSIRT PONAL Contacto equipo de respuesta a incidentes de seguridad

informática

- Correo: ponal.csirt@policia.gov.co o
- Teléfono: (601) 159090/ (601) 5159586

CCOCI Comando Conjunto Cibernético

- Gratuita Nivel Nacional +57 018000 952930 +57 (601)5804826 +57 3175765798
- Whatsapp: + 57 3175765798

COLCERT

- Teléfono Conmutador: +57 601 344 34 60 - Línea Gratuita: 01-800-0914014
- Línea Anticorrupción: 01-800-0912667
- Correo Institucional: minticresponde@mintic.gov.co
- Denuncias por actos de corrupción: soytransparente@mintic.gov.co
- Notificaciones judiciales:
- notificacionesjudicialesmintic@mintic.gov.co
- notificacionesjudicialesfontic@mintic.gov.co

FISCALÍA GENERAL DE LA NACIÓN

- Línea nacional gratuita (01 8000 9197 48)
- Desde su celular marque gratis al 122.
- Denuncie hechos de corrupción a través de las líneas del Centro de Contacto.
- Línea de Atención Dirección de Protección y Asistencia: 018000912280 - (+57) 601 7910758
- Correo Institucional: ges.documentalpqrs@fiscalia.gov.co
- Notificaciones Judiciales o Tutelas: jur.notificacionesjudiciales@fiscalia.gov.co

FORTINET – FIREWALL - WAF

- Teléfono: 018000423898 – Línea en Bogotá 57 1 4880058

UNIDAD ADMINISTRATIVA ESPECIAL CUERPO OFICIAL DE BOMBEROS DE BOGOTÁ

- Cl 18 No 99 – 38, Bogotá
- Teléfono: +57 316 473 95 99
- WhatsApp: +57 317 404 37 09

POLICÍA NACIONAL O CUADRANTE 38

Cr. 81 No 24 d / Cr. 98 # 16B-50

Celular: 3013460191 / 3203121620

Control de cambios

Versión	Fecha	Descripción
01	23/12/2016	Creación del documento.
02	23/11/2017	Se actualiza, versión y codificación para cumplimiento con el decreto 415 Se actualiza la información del documento dada la rotación del personal.
03	06/04/2018	Actualización del documento.
04	15/07/2025	Actualización del documento se ajusta código de E-SGI-SI-I003 por SGI-I003 y contactos.