



Introducción

El Centro de Cómputo del IDEAM constituye uno de los activos más sensibles de la institución, pues alberga servidores, sistemas de comunicaciones, redes, bases de datos y demás componentes que garantizan la disponibilidad, integridad y confidencialidad de la información. Por ello, se requiere establecer controles estrictos de acceso físico y procedimientos claros para proteger los equipos y los datos allí alojados.

El presente **Reglamento de Ingreso al Centro de Cómputo del IDEAM** define las normas, lineamientos y responsabilidades que deben cumplir funcionarios, contratistas, visitantes y personal técnico autorizado para acceder a estas áreas restringidas, garantizando la seguridad de la infraestructura tecnológica y la continuidad de los servicios informáticos institucionales.

Su cumplimiento es de carácter obligatorio y complementa las disposiciones establecidas en la Política de Seguridad de la Información, el Reglamento Interno de Trabajo y demás lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) adoptado por el IDEAM.

Objetivo

El presente reglamento tiene como objetivo establecer los lineamientos de acceso a funcionarios, contratistas, visitantes, personal de vigilancia, personal de servicios generales, a las instalaciones del Centro de Cómputo del IDEAM.

Alcance

Este documento presenta el marco de normatividad para políticas de seguridad de la información en el Instituto de Hidrología, Meteorología y Estudios Ambientales – IDEAM. Este reglamento describe los lineamientos de acceso al centro de cómputo.

Definiciones

Área Restringida:

Espacio físico dentro de las instalaciones del IDEAM cuyo acceso está limitado a personal autorizado debido a la naturaleza crítica de los equipos o información que allí se gestionan.

Centro de Cómputo:

Infraestructura física que alberga servidores, sistemas de almacenamiento, equipos de red, telecomunicaciones, sistemas de respaldo de energía y otros

	Sistema de Gestión Integrado Reglamento ingreso al centro de computo del IDEAM	Código: SGI-M011 Versión: 05 Fecha: 15/07/2025
--	--	---

componentes tecnológicos esenciales para el funcionamiento de los sistemas de información institucionales.

Control de Acceso:

Conjunto de medidas y procedimientos orientados a garantizar que solo el personal debidamente autorizado pueda ingresar al Centro de Cómputo, siguiendo protocolos establecidos de registro, verificación e identificación.

Ingreso Autorizado:

Permiso formal otorgado a una persona natural para acceder al Centro de Cómputo, bajo condiciones y tiempos específicos, previa validación de necesidad, identidad y acreditación.

Personal Autorizado:

Funcionarios, contratistas o proveedores que, por sus funciones o actividades, cuentan con la aprobación formal para ingresar al Centro de Cómputo, cumpliendo con los requisitos de seguridad establecidos.

Visitante:

Persona externa a la entidad o a la dependencia responsable del Centro de Cómputo, que requiere ingreso temporal para realizar actividades específicas, siempre bajo supervisión y autorización previa.

Seguridad Física:

Conjunto de medidas preventivas y de control para proteger la infraestructura tecnológica, instalaciones y recursos físicos frente a amenazas como accesos no autorizados, daños accidentales o actos malintencionados.

Siglas

No aplica

Marco Normativo

Ver normograma.

Descripción metodológica del tema a desarrollar

Con relación al Ingreso al Centro de Cómputo Visitantes Permanentes:

a. El Jefe de la Oficina de Informática debe definir y enviar vía correo electrónico la lista de las personas autorizadas para el ingreso al Centro de Cómputo al administrador del sistema biométrico. Cada persona debe tener su justificación.



Sistema de Gestión Integrado
Reglamento ingreso al centro de computo del IDEAM

Código: SGI-M011
Versión: 05
Fecha: 15/07/2025

- b. El administrador del sistema biométrico debe dar los permisos a las personas autorizadas por el Jefe de la Oficina de Informática.
- c. El administrador del sistema biométrico debe revisar mensualmente la lista de usuarios registrados como permanentes, revisar los eventos de acceso y reportar al Jefe de la Oficina de Informática y al Oficial de Seguridad los cambios de los usuarios e ingresos sospechosos.
- d. El ingreso para la administración de servidores debe ser limitado. Las tareas administrativas deben realizarse de forma remota en lo posible.

Con relación al Ingreso al Centro de Cómputo Visitantes No Permanentes:

- a. Para visitantes no permanentes la solicitud de ingreso se debe realizar con dos (2) días de anticipación, indicando las tareas a ejecutar y sobre qué elementos del Centro de Cómputo.
- b. El administrador del sistema biométrico debe informar la aprobación o denegación del ingreso.
- c. En el caso de que el visitante no permanente no sea funcionario del IDEAM, este debe estar acompañado por el responsable interno de la actividad y acompañarlo durante la ejecución de la tarea. El funcionario del IDEAM es directamente responsable de posibles acciones que atenten contra la Seguridad de las instalaciones del Centro de Cómputo y de la información que procesa.
- d. Los visitantes deben firmar la bitácora de visitantes colocando la justificación de ingreso.

Con relación al Ingreso al Centro de Cómputo del Personal de Vigilancia:

- a. La empresa de vigilancia designará un supervisor del turno de la mañana y un supervisor del turno de la noche, informando al Grupo de Recursos Físicos y a la Oficina de Informática las personas designadas para el ingreso al centro de cómputo en caso de emergencia.
- b. El personal de vigilancia designado debe firmar la bitácora de visitantes colocando la justificación de ingreso.
- c. La Oficina de Informática debe informar al personal de vigilancia designado un número de celular de contacto, **solo en caso de emergencia** el vigilante deberá informar por este medio el incidente ocurrido.

Con relación al Ingreso al Centro de Cómputo del Personal de Servicios Generales:

a. La empresa de servicios generales designará una persona para realizar las labores de aseo al centro de cómputo, informando al Grupo de Recursos Físicos y a la Oficina de Informática el horario establecido para realizar dichas labores.

b. El personal de servicios generales designado debe firmar la bitácora de visitantes colocando la justificación de ingreso.

Con relación al acceso al Centro de Cómputo de funcionarios, contratistas, visitantes, personal de vigilancia, personal de servicios generales:

a. Se prohíbe fumar al interior del Centro de Cómputo.

b. Se prohíbe ingresar comidas y bebidas.

c. Cuando se evidencie el acceso inadecuado, uso incorrecto de los servicios o recursos informáticos del Centro de Cómputo, la Oficina de Informática podrá revocar el derecho al acceso o uso de los mismos.

Así mismo se hace necesario cumplir con los siguientes requerimientos:

- La temperatura en cualquier punto del Centro de Cómputo debe oscilar entre 15° C y 25° C.
- La humedad debe estar entre el 20 y el 55%.
- Se debe controlar el acceso a través de un control biométrico.
- No debe existir puntos ciegos para el CCTV.

Debe estar equipado con sensores de movimiento.

- La UPS debe dar la suficiente autonomía según los planes de Continuidad del IDEAM.
- Debe estar equipado con un sistema de detección y de mitigación de incendios con agentes gaseosos.
- El ingreso para la administración de servidores debe ser limitado. Las tareas administrativas deben realizarse de forma remota en lo posible.
- Realizar mantenimientos preventivos a los equipos por lo menos dos veces al año, incluyendo sistemas de control.

Lo anterior sin detrimento de las consecuencias contractuales legales que pueda conllevar los actos realizados.

Los funcionarios, contratistas, visitantes deben dar uso adecuado a la información y/o los recursos y servicios informáticos que se encuentran alojados en el Centro de Computo, utilizando la autorización de acceso únicamente para realizar las actividades para las cuales fueron asignadas y evitando cualquier comportamiento que por acción u omisión conlleve a la violación de la privacidad,



confidencialidad e integridad de la información y/o la interrupción o disminución del desempeño de los servicios de información.

Los funcionarios, contratistas, visitantes, personal de vigilancia y personal de servicios generales serán responsables de cualquier hecho que vulnere la integridad o privacidad del Centro de Cómputo del IDEAM, que se derive de sus acciones u omisiones.

Todos los funcionarios, contratistas, visitantes, personal de vigilancia, personal de servicios generales son responsables de acatar los controles de acceso físico y por ningún motivo deben tratar de sobrepasarlos.

La seguridad es una obligación y responsabilidad de todos y cada uno de los funcionarios, contratistas, visitantes, personal de vigilancia y personal de servicios generales del Instituto en su día a día.

El incumplimiento de estas directrices y de los procedimientos que las respaldan podrá implicar sanciones disciplinarias.

Documentos relacionados en el SGI

No aplica

Bibliografía

ISO/IEC 27001:2022. *Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos.*

ISO/IEC 27002:2022. *Tecnología de la información — Código de prácticas para controles de seguridad de la información.*

Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.*

Manual para la Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC, Colombia.

Guía de Seguridad Física en Centros de Datos. Agencia Nacional Digital — MinTIC, Colombia.

Política de Gobierno Digital. Departamento Administrativo de la Función Pública y MinTIC.

Norma Técnica Colombiana NTC-ISO/IEC 27001:2013. ICONTEC — Instituto Colombiano de Normas Técnicas y Certificación.



Sistema de Gestión Integrado
Reglamento ingreso al centro de computo del IDEAM

Código: SGI-M011
Versión: 05
Fecha: 15/07/2025

Control de cambios

VERSIÓN	FECHA	DESCRIPCIÓN
01	18/02/2013	Versión inicial
02	20/02/2013	Revisión interna
03	26/02/2013	Entrega a IDEAM
04	05/04/2018	Se actualiza versión y codificación para cumplimiento decreto 415
05	15/07/2025	Se cambio código E-SGI-SI-M007 por SGI-M011, se ajusta imagen institucional.