IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

SGC
Sistema de Gestión de Calidad

SGA
Sistema de Gestión Ambiental

SGSST
Sistema de Gestión de la Seguridad y Salud en el Trabajo

SGD
Sistema de Gestión Documental

SCI
Sistema de Control Interno

SLNS
Sistema Laboratorio Nacional de Suelos

SGSI
Sistema de Gestión de Seguridad de la Información

IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

Guía

Trabajo en Áreas Seguras

Código: GI-GET-MN02-01 **Versión:** 1 **Vigente desde:** 15/08/2024

1. OBJETIVO

Establecer los lineamientos, controles de acceso físico y reglas de comportamiento en las áreas seguras donde se realice tratamiento o almacenamiento de información con el fin de gestionar adecuadamente el ingreso y realización de actividades por parte de funcionarios, contratistas o personal de proveedores, previniendo el acceso físico o retiro de activos de información no autorizados, el daño a la información o a las instalaciones de procesamiento o almacenamiento de información del IGAC.

2. ALCANCE

Inicia con la identificación de áreas seguras, continúa con la implementación de los lineamientos que son de obligatorio cumplimiento para todos los funcionarios, contratistas y los colaboradores vinculados de forma directa o subcontratada por otra empresa (tercerizada) del IGAC en Sede Central, Direcciones Territoriales y Puntos de Atención, cuando se realicen actividades en las áreas seguras definidas por la entidad y finaliza con la revisión del cumplimiento de los lineamientos establecidos en este documento.
Los lineamientos establecidos en esta guía se aplican a todas las áreas seguras (instalaciones) registradas en el inventario de activos de información del IGAC.

Este documento se alinea con los lineamientos establecidos en el Manual de Seguridad de la Información - MN-GET-02.

3. DEFINICIONES

- **Área Segura**: Las áreas seguras son sitios en los que se maneja información sensible o activos de información críticos. Son lugares donde se trata la información pública clasificada, pública reservada, datos personales semiprivados, privados o sensibles o donde se ubiquen los componentes, equipos de procesamiento, almacenamiento de información y comunicaciones críticos para la entidad. Por su naturaleza deben estar ubicadas en zonas de acceso restringido a personal no autorizado, empleando mecanismos de control de acceso como tarjetas de proximidad, esquemas biométricos, cerraduras, cámaras de vigilancia, entre otros según aplique.

- **Circuito Cerrado de Televisión CCTV**: Sistema de vigilancia interno accedido por el servicio de vigilancia contratado por la entidad, donde se capturan imágenes mediante cámaras, las cuales son monitoreadas por medio de monitores ubicados en los distintos pisos de la entidad y con el cual se graban las imágenes captadas, con el fin de supervisar las instalaciones de la entidad incluidas las áreas seguras y ejercer control de la seguridad física.

4. DESARROLLO

4.1 INVENTARIO DE ÁREAS SEGURAS

Con el fin de determinar las áreas consideradas cómo seguras en el IGAC, se debe registrar dentro del inventario de activos de información las áreas seguras, adicionalmente se debe establecer:

- Listado de funcionarios, contratistas o terceros con autorización permanente para ingresar a áreas seguras.
- Tipo de controles establecidos para asegurar el área.

4.1 TIPOS DE PERMISOS DE ACCESO A LAS ÁREAS SEGURAS

- **Accesos Permanentes**

  Los accesos permanentes a las áreas seguras son asignados por el jefe del área mediante correo electrónico, cuyas actividades diarias dependan de la verificación y configuración de los activos de información alojados allí. Toda solicitud de acceso permanente debe ser solicitada y justificada ante el jefe del área. Cada año se debe revisar y actualizar las personas que tienen acceso permanente o si se presentan novedades administrativas o contractuales con estas. Los datos a suministrar en el correo deben ser:

  - Nombres Apellidos/Razón social:
  - Dependencia:
  - Tipo de Vinculación: (Funcionario/Contratista/Proveedor)
  - Fecha de terminación del contrato: (Contratista/Proveedor)
  - Motivo/Justificación del permiso:

- **Acceso Especial o de Emergencia**

  Algunos funcionarios, contratistas o personal de proveedores pueden contar con un acceso especial a las áreas seguras para ejecución de soporte o mantenimiento correctivo en cualquier hora o día de la semana. Los accesos a las áreas seguras en caso de atención de una emergencia deben ser aprobados y comunicados por el jefe del área a las dependencias y roles correspondientes mediante correo electrónico indicando la fecha y hora y solo serán validos por el tiempo que sea necesario para la ejecución del soporte o mantenimiento correctivo.

- **Acceso Temporal**

  El acceso temporal a áreas seguras, como contratistas y proveedores externos, debe solicitarse previamente enviando un correo al jefe del área o quien designe relacionando la siguiente información:

  - Nombre de la empresa:
  - Nombre y número de cédula/NIT:
  - Motivo de la visita:
  - Fecha y horario de la visita:
  - Registro vigente de los parafiscales (salud, ARL, pensión)

  La confirmación de la solicitud será enviada por correo electrónico al solicitante. Confirmado la fecha y hora del acceso o planteando una fecha alternativa. En el momento de la visita se debe asignar una persona del IGAC para que realice el acompañamiento de manera permanente durante la duración de esta.

4.2 REGISTRO DE ACCESO A ÁREAS SEGURAS

Todas las personas que accedan a las áreas seguras con acceso permanente, accesos especial o de emergencia y temporales a las áreas seguras del IGAC deben registrarse en el formato vigente de "Control de Actividades Áreas Seguras", adicionalmente, el formato deberá estar custodiado por el responsable del área segura, en un espacio controlado con el fin de garantizar la integridad de los registros realizados.

4.3 REVISIÓN DE ACCESO A LAS ÁREAS SEGURAS

Se podrá realizar visitas a las áreas seguras como parte de una auditoría o de revisiones de seguridad de la información, con el fin de validar la efectividad de la implementación de controles según el tipo de área segura a validar. En el caso que, con estas visitas, se hayan identificado nuevos riesgos o sea necesario volver a evaluar o clasificar los riesgos de seguridad identificados con anterioridad se debe

actualizar la matriz de riesgos de seguridad de la información en las herramientas dispuestas por el Instituto.

4.4 LINEAMIENTOS DE TRABAJO EN ÁREAS SEGURAS

- No se debe ingresar sin autorización del responsable del área, equipos de cómputo, tablets, equipos de captura de imágenes, video o audio, tampoco equipos de transmisión o recepción de señales que puedan vulnerar las condiciones de seguridad del área y de la información. En el caso de ser necesario el ingreso se debe relacionar el tipo de equipo, el serial y la justificación en el formato "Control de Actividades Áreas Seguras" en el campo Actividad a Realizar.
- Las áreas seguras deben contar con los mecanismos de seguridad técnicos, físicos y/o administrativos que permitan proteger la información y activos de información ante cualquier posibilidad de pérdida de confidencialidad, integridad y disponibilidad, acceso no autorizado o riesgos ambientales.
- Se debe contar con cámaras de video vigilancia que permitan grabar el flujo de funcionarios, contratistas y/o terceros que entran y salen de las áreas seguras las 24 horas del día los 365 días del año. Estas grabaciones son almacenadas por la empresa de vigilancia en la Grabadora de Video Digital DVR de acuerdo a los criterios de retención de almacenamiento determinadas por la Subdirección Administrativa y Financiera, una vez cumplido este lapso de tiempo las grabaciones son sobrescritas, estas grabaciones solo pueden ser consultadas en los casos establecidos en la ley, en caso de ser necesarias para revisiones posteriores o una investigación originada por algún evento o incidente de seguridad.
- El acceso de funcionarios, contratistas, visitantes y/o proveedores (que no cuenten con acceso permanente) a las áreas seguras para la ejecución de mantenimientos, consultas, inspecciones, visitas, modificaciones y otras actividades a que haya lugar, se debe realizar con previa coordinación y autorización del responsable designado para el control del área segura de procesamiento o almacenamiento de información.
- Las labores de revisión que se realizan por parte de la DTIC en los centros de datos para verificar, temperatura, humedad, estado de los activos de información debe ser registrada en el formato vigente "Control de Actividades Áreas Seguras".
- Si la labor a realizar por un visitante es una actividad diaria, debe tratarse como visita permanente por un tiempo definido, para la cual se debería otorgar la autorización por el tiempo en que se realice la labor.
- De acuerdo con la criticidad de la información que se procese en el área segura, se implementarán controles adicionales para el resguardo de la información.
- Si es necesario realizar labores de aseo en las áreas seguras, estas deben estar acompañadas por el responsable del área o quien designe indicando cuales son las precauciones a seguir, teniendo en cuenta el tipo de material que se encuentra en el área con el fin de verificar que los activos de información funcionan correctamente antes, durante y después de ejecutar la labor de aseo dejando registro en formato vigente "Control de Actividades Áreas Seguras. Además, se prohibirá el ingreso de personal de limpieza con maletas o elementos distintos a su labor de limpieza y aseo.
- Se deben revisar y actualizar mensualmente los derechos de acceso a las áreas seguras, lo que debe realizar el líder o custodio a cargo de cada área.
- Las áreas seguras deben siempre permanecer limpias, ordenadas y libres de elementos innecesarios. Así mismo, los responsables de las áreas velarán porque se cumplan los controles de seguridad de la información, controles de seguridad y salud en el trabajo o controles de seguridad física y ambiental que determine el IGAC.
- Si se detecta el acceso no autorizado a un área segura se debe avisar inmediatamente al servicio de vigilancia y generar el evento de seguridad en la herramienta de gestión de la Mesa de Servicio de TI para que sea escalado al equipo de Seguridad de la Información.

5. FORMATOS ASOCIADOS

- Control de Actividades Áreas Seguras

6. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
15/08/2024	◦ Se adopta como versión 1 por corresponder a la creación del documento. Emisión Inicial Oficial. ◦ Hace parte del proceso de **Gestión Estratégica de Tecnología**. ◦ Se crea la guía "Trabajo en Áreas Seguras", código **GI-GET-MN02-01**, versión 1. ◦ Se encuentra asociado al Manual de Seguridad de la Información ◦ Se crea el formato "Control de Actividades Áreas Seguras" código **FO-GET-MN02-01,** versión 1.	**1**

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
Nombre: Juan de Jesús Aponte Buitrago. **Cargo:** Contratista. Dirección de Tecnologías de la Información y Comunicaciones.	**Nombre:** Diego Ramírez Pulido. **Cargo:** Contratista. Dirección de Tecnologías de la Información y Comunicaciones.	**Nombre:** Lida Carolina Zuleta Alemán. **Cargo:** Profesional Especializado. Oficina Asesora de Planeación. **Nombre:** Gabriel José Bolívar Acosta **Cargo:** Contratista. Oficina Asesora de Planeación.	**Nombre:** Perla Yadira Rojas Martínez. **Cargo:** Directora. Dirección de Tecnologías de la Información y Comunicaciones.