CONTENIDO

1. OBJETIVO

Establecer los lineamientos necesarios para gestionar el acceso físico a las instalaciones y reforzar la seguridad de la información en zonas restringidas, mediante controles que minimicen el riesgo de fuga de datos por medios físicos o digitales.

2. ALCANCE

Inicia con los lineamientos de acceso a las zonas restringidas, continua con los lineamientos para la permanencia en estas zonas y finaliza con las directrices en caso de incumplimiento de los lineamientos generales.

3. AMBITO DE APLICACIÓN

El presente documento es aplicable en el proceso de Gestión de Emergencias y Gestión Tecnológica de Seguridad y Emergencia del Centro de Comando, Control, Comunicaciones y Computo – C4 Bogotá.

4. NORMATIVIDAD ASOCIADA

Ver Normas asociados del documento en https://portalmipg.scj.gov.co

5. DOCUMENTOS ASOCIADOS

Política de Seguridad y Privacidad de la Información PO-GT-01
Manual de Seguridad y Privacidad de la Información MA-GT-01
Compromiso de Confidencialidad y No Divulgación de la Información F-GH-807
Informe General del Turno NUSE 123 F-GE-1483

6. GLOSARIO

Activo de información: cualquier recurso que posee valor para una organización y que está relacionado con el procesamiento, almacenamiento o transmisión de información.

Área restringida: espacio físico dentro de una organización al que solo puede acceder personal autorizado, debido a la sensibilidad de la información, equipos o actividades que allí se manejan.

C4: Centro de Comando, Control, Comunicaciones y Computo de Bogotá

Confidencialidad: principio de seguridad que garantiza que la información solo sea accesible por personas autorizadas, protegiéndola contra accesos no permitidos o divulgaciones indebidas.

Contratista: persona natural o jurídica externa a una organización que es contratada para realizar un servicio específico o ejecutar una tarea, bajo los términos establecidos en un contrato.

Información sensible: aquella que, si se divulga, modifica o pierde sin autorización, puede causar daño a una persona, organización o entidad, ya sea en términos legales, financieros, operativos o reputacionales.

NUSE: Número Único de Seguridad y Emergencias

S.U.R.: Sala Unificada de Recepción

SOARS: Sala Operativa de Analítica, Respuesta y Seguimiento

7. DESCRIPCIÓN

Este documento es aplicable a todo el personal de contratistas, funcionarios, operadores, aliado tecnológico, terceros y visitantes que tengan que hacer ingreso físico a las instalaciones del Centro de Comando, Control, Comunicaciones y Computo de Bogotá; así mismo, este lineamiento tiene por objeto establecer pautas para evitar accesos no autorizados y aplicar mecanismos para mitigar los riesgos de fuga de información sensible de la entidad.

De manera complementaria este documento se alinea a los procedimientos de ingresos establecidos por la empresa de vigilancia encargada de la seguridad de las instalaciones del C4 y no debe ser tomado como lineamiento para el ingreso al edificio; en consecuencia, es adicional para el acceso a las zonas restringidas.

La entidad identifica como zonas restringidas los sitios donde se encuentran los siguientes activos de información

- Oficina Jefatura C4
- Sala Unificada de Recepción -SUR
- Sala Operativa de Analítica, Respuesta y Seguimiento SOARS
- Centro Automático de Despacho MEBOG
- Oficina del archivo central
- Cuartos de equipos técnicos de red eléctrica y datos.
- Centro de Operaciones de Emergencia
- Centro de Monitoreo de Operaciones (Motorola)
- Oficina de Monitoreo de Calidad de la Operación

7.1 Ingreso a las zonas restringidas

1. Los funcionarios, contratistas y/o terceros que no laboren dentro de las zonas restringidas y que requieran ingresar a una de éstas, deberán realizar una solicitud mediante correo

electrónico o el agendamiento de una cita previa, al responsable del área identificada como restringida; quien será el que autorice o no el respectivo ingreso remitiéndola por medio de correo electrónico al buzón de la recepción de ingreso.

2. Los funcionarios y/o contratistas que laboran de forma permanente en el área restringida, deben salvaguardar los activos de información, mediante el cumplimiento de las políticas del SGSI de la Secretaria de Convivencia, Seguridad y Justicia de Bogotá.
3. El responsable del área segura autorizará la entrada a dicha área, de los funcionarios, contratistas, terceros y/o visitantes y asignará una persona del área respectiva para el acompañamiento durante la visita. Si el ingreso no es autorizado, se dará respuesta y justificación por medio del correo electrónico al interesado.
4. Los funcionarios, contratistas, terceros y/o visitantes autorizados para el ingreso al área segura deben cumplir con los lineamientos acá descritos y permanecer acompañados por un funcionario del área restringida.
5. El funcionario, contratista, tercero y/o visitante, debe presentar el documento de identidad en el punto de recepción a fin de registrar su ingreso y salida al área restringida en el formato digital diseñado por la compañía de vigilancia.
6. El grupo de Integración Tecnológica junto con el Área de Tecnología del C4, de manera conjunta con la empresa de vigilancia, deberán velar por el correcto funcionamiento del circuito cerrado de videovigilancia y garantizar que se encuentre cubriendo de manera estratégica las zonas de ingreso a las zonas restringidas.

7.2 Lineamientos Generales para la permanencia en las zonas restringidas

1. Los funcionarios que laboran de forma permanente en las zonas restringidas deberán utilizar los mecanismos de acceso asignados (tarjetas, códigos, huellas dactilares, etc.).
2. Los visitantes deben ser acompañados por un funcionario autorizado durante su permanencia en las zonas restringidas.
3. Los colaboradores (Planta y Contratistas), proveedores, visitantes y las entidades que hagan parte del sistema C4 no podrán ingresar a las zonas restringidas, con dispositivos móviles, ni está permitido en ningún momento la toma de fotografías, videos o audios, sin previa autorización de la jefatura del C4.
4. El personal operativo de la SUR, SOARS y operadores de las agencias deberá hacer un uso adecuado de las herramientas tecnológicas disponibles para la operación; durante el turno no está permitido la navegación en redes sociales, revisión de correos electrónicos personales, consulta de páginas de juegos y cualquier otra página web o herramienta que no se encuentre asociada propiamente a la operación.
5. Todo el personal debe acatar las normativas de seguridad establecidas, incluyendo la evacuación en caso de emergencia.
6. La permanencia en zonas restringidas debe limitarse al tiempo estrictamente necesario para cumplir con las actividades autorizadas.

7. No está permitido ingresar a las zonas restringidas elementos tales como gorras y capuchas que impidan su plena identificación; así como maletines, bolsos, libros, revistas y demás elementos que no sean propios de la operación y/o misionalidad del C4.
8. Está estrictamente prohibido ingresar a estas zonas sin causa justificada o fuera de horario autorizado.
9. Está prohibido el ingreso y consumo de alimentos en las zonas restringidas.
10. Toda persona que acceda a estas zonas está obligada a mantener la confidencialidad de la información que pueda visualizar o manipular. En consecuencia, deberá hacer diligenciamiento y firma del documento Compromiso de Confidencialidad y No Divulgación de la Información F-GH-807, el cual será almacenado por el responsable del área definida como restringida.
11. Se prohíbe el ingreso a visitantes y/o colaboradores que muestren signos evidentes de estar bajo la influencia de alcohol, drogas u otras sustancias que puedan afectar su comportamiento.
12. Se prohíbe el ingreso funcionarios y/o visitantes que porten armas, objetos punzantes, explosivos u otros elementos que representen un riesgo para la seguridad.
13. Se prohíbe la entrada a personas menores de edad, a menos que autorizado por la Jefatura del C4 y estén acompañados por un adulto responsable.
14. No está permitido que los elementos que conforman las estaciones de trabajo y demás herramientas tecnológicas sean reubicados, trasladados, o cambiados de sus sitios originalmente establecidos, sin previa autorización.
15. No debe compartir ni dejar almacenados, los usuarios y claves asignados a cada funcionario para el acceso a las herramientas tecnológicas y sistemas de información, dispuestos por la Entidad para el desarrollo de su misionalidad.
16. De acuerdo con los lineamientos del Manual del Sistema de Gestión de Seguridad de la Información MA-GT-01, se prohíbe compartir usuarios, claves, tarjetas de acceso y demás que hayan sido asignados de manera individualizada a cada funcionario.
17. Todas las personas que ingresan a las zonas determinadas como restringidas, deberán acatar lo establecido en la Política de Seguridad y Privacidad de la Información PO-GT-01.

7.3 Directrices sobre el incumplimiento de los lineamientos generales

El incumplimiento de los lineamientos establecidos en el presente instructivo, el cual protege la seguridad física, informática y misional del C4, puede conllevar, además de sanciones administrativas o contractuales, responsabilidad penal, dependiendo de la gravedad y naturaleza de la conducta. Según el Código Penal Colombiano, las posibles sanciones pueden incluir:

1. Para funcionarios públicos:

- Prevaricato (Art. 413 y 414): Si incumplen deliberadamente normas que deben aplicar.

- Abuso de autoridad u omisión de denuncia (Art. 416-417): Por no reportar o actuar frente a una conducta indebida.
- Violación de medidas de seguridad (Art. 195): Cuando se compromete información o acceso sin autorización.
- Violación de datos personales (Art. 269F) Aplica si con su celular accede, copia, transfiere o fotografía datos personales de ciudadanos o información sensible del sistema 123

2. Para contratistas o terceros:

- Acceso abusivo a un sistema informático (Art. 269A): Si acceden o manipulan información o sistemas sin autorización.
- Daño informático (Art. 269D): Si alteran, borran o afectan datos sensibles.
- Violación de datos personales (Art. 269F) Aplica si con su celular accede, copia, transfiere o fotografía datos personales de ciudadanos o información sensible del sistema 123

Por otro lado, sumado a los procedimientos penales, si se presentan tres (3) infracciones a cualquiera de los lineamientos generales por parte de funcionarios administrativos o de operadores de las salas del C4, se procederá de la siguiente manera:

- Para empleados de planta: se iniciará el debido proceso disciplinario conforme a la normativa vigente.

- Para contratistas: se aplicará la suspensión del contrato correspondiente, según los términos establecidos.

3. Para visitantes:

En caso de evidenciarse el incumplimiento de alguno de estos lineamientos por parte de visitantes o terceros ajenos a la operación, el equipo de seguridad física procederá con el retiro inmediato de la persona de las instalaciones, así como con la restricción de acceso y veto de ingreso al edificio en futuras ocasiones.

Además, producto del ingreso a zonas restringidas sin autorización, podrían incurrir en procesos penales por las siguientes causas:

- Violación de habitación ajena o lugares privados (Art. 189).
- Violación ilícita de comunicaciones (Art. 192), si captan o divulgan información.
- Interceptación de datos informáticos (Art. 269C), si instala o usa aplicaciones para capturar comunicaciones, imágenes o información en tránsito dentro del sistema de emergencia.

Para el seguimiento y control de las infracciones, se tomará como insumo el documento de informe general del turno NUSE 123 F-GE-1483 y el reporte de generado por el operador tecnológico y/o la detección por parte del Jefe de Sala y/o el Supervisor de Turno, quienes están llamados a verificar y hacer cumplir el presente instructivo. De ser necesario, el responsable de

la operación podrá solicitar como soportes los registros de video del turno del incidente presentado.

Elaboró: Ana Catherine Mariño Rincón – Contratista C4

Revisó: Fabio Andrés Albornoz Quintero – Contratista C4
Sady Sofía Moreno Munévar – Contratista C4
Edith Nathalie Romero Barrera - Profesional Universitario
Sandra Milena Martínez Martínez – Contratista C4

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co