RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

EL DIRECTOR GENERAL DEL INSTITUTO DE DESARROLLO URBANO - IDU, en ejercicio de sus facultades legales y en especial las conferidas en el Acuerdo 19 de 1972 del Concejo de Bogotá D.C., y el Acuerdo No. 006 de 2021 del Consejo Directivo del IDU, y

CONSIDERANDO:

Qué el artículo 209 de la Constitución Política de Colombia establece que las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. Así mismo, determina que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la desconcentración y la delegación de funciones.

Qué el artículo 269 de la Constitución Política de Colombia establece que las entidades públicas, están obligadas a diseñar y aplicar según la naturaleza de sus funciones, métodos y procedimientos de control interno de conformidad con lo que disponga la ley.

Qué el Decreto Distrital 221 de 2023 reglamentó el Sistema de Gestión en el Distrito Capital de que trata el artículo 2.2.22.1.1 del Título 22 de la Parte 2 del Libro 2 del del Decreto Único Reglamentario 1083 de 2015, sustituido por el artículo 1 del Decreto Nacional 1499 de 2017, el cual se articula con el Sistema de Control Interno dispuesto en la Ley 87 de 1993 a través de la implementación del Modelo Integrado de Planeación y Gestión - MIPG; y las demás normas que lo modifiquen o sustituyan.

Que el Sistema de Gestión es el conjunto de entidades y organismos distritales, políticas de gestión y desempeño institucional, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados que satisfagan las necesidades de la ciudadanía y permitan el goce efectivo de los derechos en el marco de la legalidad y la integridad.

Que en el Comité Institucional de Gestión y Desempeño del Instituto en sesión del 22 de abril de 2021 aprobó la política MIPG-SIG, expidiéndose la Resolución IDU-1019 de 2021 que adopta el Sistema de Gestión MIPG-SIG, crea equipos Institucionales, y establece el marco de referencia para el actuar de los Subsistemas en el Instituto de Desarrollo Urbano, lo cual fue recogido por las Resolución IDU-6175 de 2021 y posteriormente en la Resolución IDU 4598 de 2022.

Que el MIPG opera a través de la puesta en marcha de siete (7) dimensiones que parten de una visión multidimensional de la gestión organizacional; en el IDU agrupan a su vez,

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

la implementación y mejora de los subsistemas de gestión, políticas, componentes, prácticas, procesos, herramientas o instrumentos con un propósito común, que adelantan las entidades públicas, y que, puestas en marcha de manera articulada e intercomunicada, permitirán que el Modelo opere eficaz y eficientemente, para transformar insumos en resultados que produzcan los impactos deseados, esto es una gestión y un desempeño institucional que genera valor público.

Que el Sistema Integrado de Gestión MIPG-SIG del IDU y sus 11 Subsistemas de Gestión articulados, se mantienen alineados con la intención de la Política del MIPG-

Que mediante Resolución 4151 de 2022, se actualizaron los roles y responsabilidades para la administración y mantenimiento del Subsistema de Gestión de Seguridad de la Información - SGSI, en el Instituto de Desarrollo Urbano, establecidos por la Resolución 761 de 2021.

Que mediante la Resolución IDU 2330 de 2023 se actualizó el Modelo Integrado de Planeación y Gestión -MIPG-SIG IDU, como un mecanismo que facilita la integración y articulación entre el Modelo Integrado de Planeación y Gestión, el Sistema Integrado de Gestión y el Sistema de Control Interno, y se constituye en el marco de referencia para la implementación, sostenibilidad y mejora continua del Sistema Integrado de Gestión - SIG del IDU y de los Subsistemas articulados; así mismo se definen sus elementos e instancias de coordinación para su establecimiento, implementación, mantenimiento y optimización, con el fin de optimizar el desempeño institucional y la consecución de resultados, en el marco de la legalidad, integridad y calidad en el servicio.

Que el artículo 4° de la citada Resolución define MIPG - SIG como el conjunto articulado de buenas prácticas que permiten en el Instituto, dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión con el fin de satisfacer a los grupos de valor e interés, cumplir con los instrumentos de planeación, en especial, el Plan Distrital de Desarrollo vigente, y contribuir bajo una política de integración, el cumplimiento de los fines esenciales del Instituto, sus propósitos organizacionales, su mejor desempeño institucional y la consecución de resultados; la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad.

Ibidem el artículo 8º, establece que el Sistema Integrado de Gestión MIPG-SIG se articula con once (11) Subsistemas en consonancia con las buenas prácticas internacionales, así:

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

Sigla	Subsistema	Norma base
SGAS	Gestión Antisoborno	ISO 37001
SGC	Gestión de Calidad	ISO 9001
SGA	Gestión Ambiental	ISO 14001
SGSST	Gestión de Seguridad y Salud en el Trabajo	ISO 45001
SGSI	Gestión de Seguridad de la Información	ISO 27001 ISO 27701
SIGA	Gestión Documental y Archivo	ISO 30301 ISO 15489
SGRS	Responsabilidad Social	ISO 26000
SGCN	Gestión de Continuidad del Negocio	ISO 22301
SGefr	Empresa Familiarmente Responsable	efr 1000-1
SGC&I	Gestión de Conocimiento e Innovación	ISO 30401
SARLAFT-IDU	Gestión para la Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo	Ley 2195 de 2022

Qué de conformidad con lo anterior, el Instituto de Desarrollo Urbano, adoptó e implementó el Subsistema de Gestión de Seguridad de la Información - SGSI, para generar las condiciones de seguridad necesarias en términos de confidencialidad, integridad y disponibilidad adecuadas a la información de la Entidad, en todos sus medios de conservación y divulgación, con los recursos asignados para administrar de forma efectiva los riesgos asociados a sus activos de información, aumentar la credibilidad y confianza de las partes interesadas, implementar estrategias para el mejoramiento continuo y cumplir con la normatividad vigente.

Qué los cuatro objetivos del SGSI, son:

1. Fortalecer la cultura de seguridad de la información en la Gente IDU.
2. Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos de seguridad de la información vigente.
3. Elevar el nivel de madurez de los controles de seguridad de la información, pasando el 65% de ellos a nivel L4 o superior y manteniendo el 35% restante en L3.
4. Evaluar los controles de seguridad de la información sobre el componente de privacidad, en cumplimiento de la norma ISO/IEC 27701:2019.

Que la Entidad el 9 de diciembre de 2019 obtuvo la certificación del Subsistema de Seguridad de la Información, bajo los estándares de la Norma Técnica ISO 27001:2013 y en noviembre del 2022 obtuvo la recertificación; la cual compromete a la Entidad a

RESOLUCIÓN NÚMERO 6135 DE 2023
"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

mantener y mejorar continuamente los mecanismos para la protección de los activos críticos de información frente a riesgos en disponibilidad, integridad y confidencialidad.

Qué de acuerdo con el inciso "d", del numeral 5.1 Liderazgo y compromiso y el numeral 5.3 Roles, responsabilidades y autoridades de la organización de la Norma NTC-ISO/IEC 27001: 2022, la Dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI y al efecto está obligado a:

> *"5.1 d) comunicar la importancia de una gestión eficaz de la seguridad de la información y de la conformidad con los requisitos del sistema de gestión de seguridad de la información; 5.3 Roles, responsabilidades y autoridades de la organización. La alta dirección debe asegurar que las responsabilidades y autoridades para los roles pertinentes para la seguridad de la información son asignados y comunicados dentro de la organización.*
>
> *La alta dirección debe asignar la responsabilidad y autoridad para:*
>
> *a) asegurarse de que el sistema de gestión de seguridad de la información es conforme con los requisitos de este documento.*
> *b) informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.*
>
> *NOTA: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de seguridad de la información dentro de la organización."*[1]

Que por lo anterior, debe actualizarse la Resolución 4151 de 2022 "Por la cual se actualizan los roles y responsabilidades para la administración y mantenimiento del Subsistema de Gestión de Seguridad de la Información - SGSI, en el Instituto de Desarrollo Urbano, establecidos por la Resolución 761 de 2021", en cuanto a los roles y responsabilidades para la administración y mantenimiento del Subsistema de Gestión de Seguridad de la Información - SGSI, establecidos en la Resolución 2330 de 2023 , regularizar la operación del sistema de seguridad de la información e incluir para todos los roles del subsistema experiencia, conocimientos y competencias.

En mérito de lo expuesto,

[1] Norma NTC ISO/IEC 27001:2022

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

RESUELVE:

ARTÍCULO PRIMERO. **Roles del Subsistema de Gestión de Seguridad de la Información - SGSI.** Dentro de la entidad se establecen los siguientes roles frente al SGSI:

1. Líder del SGSI (SGGC)
2. Subdirector(a) Técnico de Recursos Tecnológicos
3. Oficial de Seguridad de la Información
4. Equipo Operativo
5. Equipo Técnico (STRT)
6. Equipo Operativo de Gestores de activos de información
7. Líderes de Proceso
8. Supervisores de Proyectos
9. Gente IDU

En caso de que sea necesario, la entidad tomará medidas para que los roles descritos adquieran las competencias necesarias.

ARTÍCULO SEGUNDO. Líder del Subsistema de Gestión Seguridad de la Información. El(la) Subdirector(a) General de Gestión Corporativa - SGGC es el(la) líder del SGSI, quien tendrá a su cargo las siguientes responsabilidades:

a) Asignar el rol de Oficial de Seguridad de la Información a un directivo, servidor público del nivel profesional y/o contratista de prestación de servicios profesionales y de apoyo a la gestión.
b) Impulsar las actividades necesarias para la gestión y mantenimiento del SGSI.
c) Aprobar el Plan Estratégico de Seguridad y Privacidad de la Información.
d) Aprobar las políticas de seguridad de la información y la documentación del SGSI.
e) Verificar que se proporcionen los recursos necesarios para el SGSI.
f) Aprobar el "*Plan de toma de conciencia de seguridad de la información*".
g) Gestionar la implementación de las políticas y controles de seguridad de la información.
h) Promover la ejecución de auditorías al SGSI.
i) Apoyar las acciones de mejora continua del SGSI.
j) Realizar seguimiento al desempeño del SGSI.

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023
"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

k) Validar los cambios al SGSI.

Perfil
La educación, formación, experiencia y competencias del líder del SGSI están dados en el manual de funciones.

- **Conocimientos deseados**
  1. Sistemas de Gestión.
  2. Norma ISO 27001 versión 2013 o 2022. Deseable Certificado Auditor Interno ISO 27001.
  3. Modelo de operación del IDU para la atención de incidentes de ciberseguridad.
  4. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
  5. Conocimientos relativos a la Seguridad de la información, en:
     a) Modelo de Seguridad y Privacidad de la Información
     b) Confidencialidad, Integridad y Disponibilidad.
     c) Privacidad de los datos personales.
     d) Clasificación de la información del IDU.
     e) Amenazas, riesgos e incidentes de ciberseguridad.

ARTÍCULO TERCERO. El(la) Subdirector(a) Técnico(a) de Recursos Tecnológicos en el marco del SGSI tendrá las siguientes responsabilidades:

a) Gestionar la documentación asociada a ciberseguridad.
b) Gestionar la atención de incidentes de ciberseguridad.
c) Gestionar los informes técnicos de ciberseguridad.
d) Evaluar las mejoras en las plataformas tecnológicas de seguridad del IDU.
e) Coordinar la subsanación de hallazgos o no conformidades de auditorías.
f) Propender por la remediación de las vulnerabilidades técnicas.
g) Gestionar los cambios al Subsistema de Gestión de Seguridad de la Información - SGSI.

Perfil
La educación, formación, experiencia y competencias del (de la) Subdirector(a) Técnico(a) de Recursos Tecnológicos están dados en el manual de funciones.

- **Conocimientos deseados**
  1. Sistemas de Gestión.

RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

2. Norma ISO 27001 versión 2013 o 2022. Deseable Certificado Auditor Interno ISO 27001.
3. Arquitectura de seguridad del IDU.
4. Estructura de recuperación del IDU.
5. Modelo de operación del IDU para la atención de incidentes de ciberseguridad.
6. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
7. Conocimientos relativos a Seguridad de la información, en:
   a. Servicios de tecnología críticos.
   b. Funcionamiento de la Estrategia DRP del IDU.
   c. Tiempo de recuperación.
   d. Funcionamiento básico de herramientas de ciberseguridad.
   e. Arquitectura de ciberseguridad del IDU.
   f. Hacking ético, ingeniería social, análisis de vulnerabilidades, riesgos y atención de incidentes de ciberseguridad.
   g. Modelo de Seguridad y Privacidad de la Información

ARTÍCULO CUARTO. El(la) Oficial de seguridad de la información en el marco del SGSI tendrá las siguientes responsabilidades:

Política:

a) Definir y actualizar las políticas de seguridad de la información.
b) Hacer seguimiento al cumplimiento de las políticas de seguridad de la información.

Gestión:

c) Validar los diagnósticos realizados al SGSI.
d) Gestionar el contacto con autoridades y grupos de interés relacionadas con seguridad de la información, en los casos que sea necesario.
e) Coordinar la elaboración de la documentación del SGSI.
f) Coordinar las actividades del plan de comunicaciones y toma de conciencia del SGSI.
g) Promover el cumplimiento de los requisitos legales, en particular lo relacionado con la propiedad intelectual y de datos personales.
h) Realizar seguimiento a los indicadores del SGSI.
i) Promover y acompañar la ejecución de auditorías al SGSI.

Riesgos:

j) Participar de la definición de la estrategia de riesgos de seguridad de la información.

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

k) Gestionar la identificación, valoración y tratamiento de los riesgos asociados a los activos de información y hacer seguimiento.

Vulnerabilidades:

l) Coordinar la realización de análisis de vulnerabilidades de seguridad de la información.
m) Analizar los informes de vulnerabilidades encontradas en la plataforma de TI.

Incidentes:

n) Asignar al equipo de seguridad la atención de eventos o incidentes que puedan afectar la seguridad de la información.
o) Gestionar la elaboración de análisis forense de seguridad de la información en los casos que se requiera.

Activos de Información:

p) Realizar seguimiento a la actualización del inventario de activos de información de la Entidad.
q) Definir los lineamientos de clasificación y etiquetado de información.
r) Analizar e implementar soluciones de seguridad de la información de acuerdo con la necesidad.
s) Identificar requerimientos de seguridad de la información en los proyectos IDU.

Perfil

- **Experiencia**

  El oficial de seguridad debe tener experiencia en estas dos (2) actividades:

  1. Dos años desempeñando el rol de oficial de seguridad de la información.
  2. Un año en el diseño e implementación de estrategias de seguridad de la información.

- **Conocimientos**

  El oficial de seguridad debe tener conocimientos en todos los temas definidos a continuación:

  1. Postgrado en seguridad de la información, ciberseguridad, seguridad informática o afín.
  2. Norma ISO 27001 versión 2013 o 2022. Deseable Certificado Auditor Líder o Interno en ISO 27001 versión 2013 o superior.
  3. COBIT, ITIL o equivalentes. Deseable Certificado ITIL V4 y COBIT Foundation 2019.
  4. Seguridad de redes y sistemas.
  5. Criptografía.

6. Estrategias y controles con los que cuenta el IDU.
7. Conocimiento en concienciación y capacitación en seguridad de la información.
8. Conocimientos en ciberseguridad:
   a) Modelo de Seguridad y Privacidad de la Información
   b) Gestión de riesgos y activos de información.
   c) Protección de datos.
   d) Funcionamiento de la Estrategia DRP del IDU.
   e) Funcionamiento básico de herramientas de ciberseguridad.
   f) Arquitectura de ciberseguridad del IDU.
   g) Hacking ético, ingeniería social, análisis de vulnerabilidades y atención de incidentes.

- **Competencias**
  1. Toma de decisiones: Capacidad para analizar la información disponible, evaluar y elegir de varias alternativas la más adecuada de forma oportuna, anticipando y controlando los riesgos.
  2. Liderazgo: Llevar a cabo acciones para lograr los fines y objetivos establecidos en el Subsistema de Gestión de Seguridad de la Información.

ARTÍCULO QUINTO. Conformación y responsabilidades del Equipo operativo en el marco del SGSI. El Equipo operativo estará conformado por al menos un (1) representante de cada una de las siguientes dependencias: Oficina Asesora de Planeación - OAP, Subdirección General de Gestión Corporativa - SGGC, Dirección Técnica Administrativa y Financiera –DTAF y Subdirección Técnica de Recursos Tecnológicos - STRT, quienes serán designados(as) por el(la) respectivo(a) jefe inmediato(a) o supervisor de contrato, según sea el caso, mediante memorando u oficio, en un plazo no mayor a 30 días hábiles posteriores a la fecha de expedición de la presente Resolución.

Los(as) integrantes del Equipo operativo tendrán las siguientes responsabilidades:

Política:

a) Apoyar la identificación e implementación de las políticas de seguridad de la información.
b) Monitorear el cumplimiento de las políticas de seguridad de la información.

Gestión:

c) Verificar el diagnóstico del SGSI.

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023
"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

d) Realizar las actividades necesarias para la gestión y mantenimiento del Subsistema de Gestión de Seguridad de la Información - SGSI.
e) Apoyar la Identificación de los requisitos legales del SGSI.
f) Elaborar y mantener la documentación del SGSI.
g) Ejecutar los planes de acción del SGSI.
h) Acompañar la ejecución de auditorías de seguridad de la información.
i) Apoyar las acciones de mejora continua del SGSI.
j) Contactar autoridades y grupos de interés relacionadas con seguridad de la información.
k) Ejecutar el plan de comunicaciones y toma de conciencia del SGSI.
l) Aplicar las acciones de mejoramiento producto de las auditorías.
m) Implementar controles de seguridad de la información.
n) Generar informes de gestión de seguridad de la información.
o) Evaluar la madurez de los controles del SGSI.

Riesgos:
p) Participar de la identificación, valoración y tratamiento de los riesgos asociados a los activos de información y hacer seguimiento.
q) Consolidar información de la ejecución del plan de tratamiento de riesgos.

Incidentes:
r) Atender los incidentes de seguridad de la información.
s) Acompañar las actividades de análisis forense de seguridad de la información.

Vulnerabilidades:
t) Realizar análisis de vulnerabilidades de seguridad de la información y presentar los informes técnicos correspondientes.
u) Hacer revisión de código seguro.
v) Realizar seguimiento a la remediación de vulnerabilidades identificadas.

Activos de Información:
t) Gestionar la actualización del inventario de activos de información de la Entidad.
u) Apoyar la definición de lineamientos de clasificación y etiquetado de información.
v) Apoyar la identificación de requerimientos de seguridad de la información en los proyectos IDU.

Perfil
- **Experiencia**

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023
"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

1. Participación en por lo menos una auditoría de seguridad de la información o relacionada.

- **Conocimientos**
  Los integrantes del equipo operativo deben demostrar que conocen el SGSI, con temas como:
  1. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
  2. Tener conocimientos relativos a la Seguridad de la Información, en:
     a. Procesos críticos.
     b. Servicios de tecnología críticos.
     c. Confidencialidad, Integridad y Disponibilidad.
     d. Privacidad de los datos personales.
     e. Análisis y gestión de vulnerabilidades.
     f. Atención de incidentes de seguridad de la información.
     g. Gestión de activos y riesgos de seguridad de la información.
     h. Conocimiento en seguridad de aplicaciones o desarrollo seguro.
     i. Norma ISO 27001 versión 2013 o 2022. Deseable Certificado Auditor Interno ISO 27001 versión 2013 o superior.
     j. Modelo de Seguridad y Privacidad de la Información.
  3. Plan de seguridad de información de la vigencia.

- **Competencias**

1. Diligencia: Habilidad para llevar a cabo una tarea o gestión de manera oportuna.
2. Trabajo en equipo: Disposición para participar activamente en la consecución de una meta común, incluso cuando la colaboración conduce a una meta que no está relacionada con el interés propio.
3. Comunicación: Capacidad de escuchar, hacer preguntas, expresar conceptos e ideas en forma efectiva y exponer aspectos positivamente.

ARTÍCULO SEXTO. Conformación y responsabilidades del Equipo Técnico en el marco del SGSI. El Equipo Técnico de Seguridad de la Información estará conformado por el grupo funcional de infraestructura de tecnología de la STRT al que se le asignan las siguientes responsabilidades:

a) Implementar o acompañar la implementación de soluciones de seguridad de la información de acuerdo con la necesidad.
b) Generar informes técnicos de ciberseguridad.

c) Aplicar cambios en la plataforma de ciberseguridad.
d) Configurar y monitorear las herramientas de ciberseguridad.
e) Aplicar las recomendaciones de los informes de vulnerabilidades encontradas en la plataforma de TI.
f) Definir y aplicar el plan de remediación a las vulnerabilidades técnicas identificadas.
g) Realizar el monitoreo de las herramientas de ciberseguridad.

Perfil

- **Experiencia**
  1. Dos años en la administración de servidores y/o equipos y/o herramientas de seguridad perimetral y/o equipos de monitorización de activos de información.

- **Conocimientos**

  El equipo técnico debe dominar los siguientes temas referentes al SGSI:
  1. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
  2. Modelo de operación del IDU para la atención de incidentes de ciberseguridad Arquitectura de ciberseguridad del IDU.
  3. Tener conocimientos relativos a Seguridad de la Información, en:
     a. Conocimiento sólido de los sistemas operativos más comunes que se manejan en la Entidad (Windows y Linux) y saber cómo asegurarlos y protegerlos.
     b. Conocer y comprender los principios y algoritmos de la criptografía, así como su aplicación.
     c. Respuesta y gestión de los incidentes.
     d. Comprender los conceptos de redes, protocolos, firewalls, enrutadores y switches, así como las vulnerabilidades y amenazas asociadas a ellos.
     e. Administración de equipos de seguridad perimetral.
     f. Administración de herramientas de monitorización de activos de información.
     g. Conceptos básicos de redes de datos.

- **Competencias**

1. Diligencia: Habilidad para llevar a cabo una tarea o gestión de manera oportuna.
2. Trabajo en equipo: Disposición para participar activamente en la consecución de una meta común, incluso cuando la colaboración conduce a una meta que no está relacionada con el interés propio.
3. Comunicación: Capacidad de escuchar, hacer preguntas, expresar conceptos e ideas en forma efectiva y exponer aspectos positivamente.

RESOLUCIÓN NÚMERO 6135 DE 2023
"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

ARTIÍCULO SÉPTIMO. Conformación y responsabilidades del Equipo Operativo de Gestores de Activos de Información en el marco del SGSI. El equipo operativo de gestores de activos de información estará conformado por al menos una persona de cada uno de los procesos institucionales, quienes serán designados(as) por el(la) respectivo(a) jefe inmediato(a) o supervisor de contrato, según sea el caso, mediante memorando, en un plazo no mayor a 30 días hábiles posteriores a la fecha de expedición de esta Resolución. Se le asignan las siguientes responsabilidades:

a) Garantizar que el inventario de activos de su proceso se mantenga actualizado.
b) Acompañar la elaboración del inventario de activos de información.
c) Hacer uso adecuado de los activos de información y promover esta conducta en todos sus compañeros(as).
d) Gestionar la identificación, valoración y tratamiento de los riesgos asociados a los activos de información.
e) Elaborar el plan de tratamiento de riesgos de su proceso.
f) Participar de la identificación de los riesgos de seguridad de la información de su proceso y hacerles seguimiento.
g) Gestionar la aceptación del riesgo residual.
h) Apoyar las acciones de mejora continua del SGSI.

Perfil

- **Conocimientos deseados**

  El Equipo Operativo de Gestores de Activos de Información debe demostrar que ha apropiado los siguientes conceptos:

  1. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
  2. Gestión de activos de información.
  3. Tener conocimientos relativos a Seguridad de la Información, en:
     a. Confidencialidad, Integridad y Disponibilidad.
     b. Privacidad de los datos personales.
     c. Clasificación de la información del IDU.
     d. Amenazas, riesgos e incidentes de ciberseguridad.

- **Competencias**

1. Diligencia: Habilidad para llevar a cabo una tarea o gestión de manera oportuna.
2. Trabajo en equipo: Disposición para participar activamente en la consecución de una meta común, incluso cuando la colaboración conduce a una meta que no está relacionada con el interés propio.

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

3. Comunicación: Capacidad de escuchar, hacer preguntas, expresar conceptos e ideas en forma efectiva y exponer aspectos positivamente.

ARTIÍCULO OCTAVO. Conformación y responsabilidades de los Líderes de Procesos en el marco del SGSI. Los líderes de procesos son los directivos pertenecientes a la alta dirección y quienes toman las decisiones estratégicas de la entidad, quienes tendrán las siguientes responsabilidades:

a) Promover las actividades necesarias para la gestión y mantenimiento del Subsistema de Gestión de Seguridad de la Información - SGSI.
b) Aprobar las matrices de riesgos de seguridad de la información.
c) Aprobar el plan de tratamiento de riesgos de su proceso(s).
d) Aceptar expresamente el riesgo residual de seguridad de la información.

Perfil
La experiencia y competencias de los líderes de cada proceso están dadas en el manual de funciones respectivamente de acuerdo al cargo que ocupan.

- **Conocimientos deseados**

El equipo de Líderes de los Procesos debe demostrar que ha apropiado los siguientes conceptos:

1. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
2. Conocimientos relativos a Seguridad de la información, en:
   a) Confidencialidad, Integridad y Disponibilidad.
   b) Privacidad de los datos personales.
   c) Modelo de Seguridad y Privacidad de la Información
   d) Amenazas, riesgos e incidentes de seguridad de la información.

ARTÍCULO NOVENO. Conformación y responsabilidades de los Supervisores de Proyectos en el marco del SGSI. Asignar el rol de Supervisor de Proyectos, el cual será desempeñado por cada uno de los supervisores de contrato y/o profesionales de apoyo a la supervisión de contrato, quienes tendrán las siguientes responsabilidades:

a. Gestionar la identificación, valoración y tratamiento de los riesgos asociados a los activos de información involucrados en los proyectos a su cargo.
b. Identificar requerimientos de seguridad de la información en los proyectos del IDU a su cargo.

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

Perfil

- **Conocimientos deseados**
  1. Lineamientos del Subsistema de Gestión de Seguridad de la Información (Directriz, Alcance y Objetivos del Subsistema).
  2. Tener conocimientos relativos a Seguridad de la Información, en:
     a. Confidencialidad, Integridad y Disponibilidad.
     b. Privacidad de los datos personales.
     c. Modelo de Seguridad y Privacidad de la Información
     d. Amenazas, riesgos e incidentes de seguridad de la información.

ARTÍCULO DÉCIMO. **Conformación y responsabilidades de la Gente IDU.** Todos(as) los(as) servidores(as) públicos(as) y contratistas de prestación de servicios profesionales y de apoyo a la gestión del Instituto de Desarrollo Urbano IDU tendrán las siguientes responsabilidades:

a) Elaborar el inventario personal de activos de información.
b) Hacer uso adecuado de los activos de información.
c) Reportar eventos o incidentes que puedan afectar la seguridad de la información.
d) Conocer, entender y cumplir la directriz y las políticas del SGSI.
e) Cumplir con los requisitos legales, en particular lo relacionado con la propiedad intelectual y de datos personales.
f) Participar en los programas de capacitación, sensibilización y toma de conciencia de seguridad de la información.

ARTÍCULO UNDÉCIMO. Vigencia y derogatorias. La presente resolución rige a partir de su expedición y deroga la Resolución 4151 de 2022.

Dada en Bogotá D.C. en Diciembre 27 de 2023.

COMUNÍQUESE Y CÚMPLASE

DIEGO SANCHEZ FONSECA
Director General
Firma mecánica generada el 27-12-2023 06:13:24 PM autorizada mediante Resolución No. 400 de marzo 11 de 2021

Aprobó: HECTOR PULIDO MORENO-Subdirección Técnica de Recursos Tecnológicos

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15

RESOLUCIÓN NÚMERO 6135 DE 2023

"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"

Aprobó: MERCY YASMIN PARRA RODRIGUEZ-Dirección Técnica Administrativa y Financiera
Aprobó: MERCY YASMIN PARRA RODRIGUEZ-Subdirección General de Gestión Corporativa

Elaboró: ERIKA TATIANA QUINTERO QUINTERO-Subdirección Técnica de Recursos Tecnológicos
Héctor Andrés Mafla Trujillo – Profesional Especializado – STRT
Revisó: Ana Claudia Mahecha León – Asesor DG
Lorena Suárez – Contratista SGGC
Ángela Yamile Osorio – Profesional Especializado DTAF

Calle 22 No. 6 - 27
Código Postal 11031
Tel: 3386660
www.idu.gov.co
Info: Línea: 195
FO-DO-10_V15