SECRETARÍA DE INNOVACIÓN Y GOBIERNO ABIERTO

ELABORA	REVISA	ADMINISTRA
RÚBRICA Karina Onofre Martínez Directora General de Gobierno Digital y Soporte Tecnológico	RÚBRICA Cintia Smith Secretaria de Innovación y Gobierno Abierto	RÚBRICA María Fernanda Araujo Meza Directora de Planeación, Enlace y Proyectos Estratégicos

Con fundamento en lo dispuesto en los artículos 1, 88, 89 y 96 de la Ley de Gobierno Municipal del Estado de Nuevo León; 5, 11, 14, 16 fracción IX, 113, 114, 115, 116 fracciones VII, XVIII, XIX, XXII y XXX, 117 fracciones XVI, XIX y XXV, 118 fracciones VI y XII del Reglamento de la Administración Pública Municipal de Monterrey; artículo 1, 2 fracción V, 3 fracción XXXII, 6 fracciones XVI, XIX y XX, 7, 8 fracción XV, 23, 24 fracción II, 121, 122 del Reglamento de Gobernanza Tecnológica para el Municipio de Monterrey y demás ordenamientos y disposiciones jurídicas aplicables.

La Secretaría de Innovación y Gobierno Abierto, a través de la Dirección General de Gobierno Digital y Soporte Tecnológico, tiene a bien elaborar el presente lineamiento con el fin de resguardar, prevenir, detectar, retrasar, disuadir y responder a amenazas cibernéticas, así como controlar y proteger la infraestructura y sistemas informáticos de la Administración Pública Municipal y Paramunicipal de Monterrey.

I. OBJETIVO

Establecer criterios y buenas prácticas para la gestión de los diferentes estándares de Seguridad Informática dentro de la Administración Pública Municipal y Paramunicipal de Monterrey, con la finalidad de promover un manejo de la información de forma responsable, segura y eficiente; que cuenten con estándares de seguridad informática.

II. ALCANCE

Este lineamiento es aplicable a los Sujetos Obligados de las Entidades y Dependencias de la Administración Pública Municipal y Paramunicipal de Monterrey que cuenten con acceso a los equipos y redes de telecomunicaciones municipales.

III. DEFINICIONES

Análisis de Riesgo. Proceso realizado por la Secretaría, a través de la Dirección General de Gobierno Digital y Soporte Tecnológico, que tiene como propósito identificar las circunstancias adversas a las que están expuestas en el desarrollo de sus actividades y analizar los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias que permitan administrarlos y, por lo tanto, contribuir al logro de los objetivos, metas y programas.

Confiabilidad. Se refiere a la provisión de información actual, objetiva, creíble y legítima para la Administración en las Dependencias y Entidades Municipales y Paramunicipales.

Confidencialidad. Se refiere a la protección de la información contra su divulgación no autorizada.

Dependencias. Las señaladas en el artículo 16 del Reglamento de la Administración Pública del Municipio de Monterrey.

Desembalarlas. Acto de sacar o extraer algo que está embalado o empaquetado.

Deserializan. Proceso de convertir datos serializados (generalmente en forma de bytes) en un formato que pueda ser interpretado y utilizado por un programa.

Direcciones. Dirección de Gobierno Digital y la Dirección de Soporte e Infraestructura de la Dirección General de Gobierno Digital y Soporte Tecnológico de la Secretaría de Innovación y Gobierno Abierto del Municipio de Monterrey.

Entidades. Las Entidades Públicas Descentralizadas creadas por el R. Ayuntamiento con aprobación del H. Congreso del Estado.

Información Sensible. Conjunto de datos definidos por el propietario de la información cuya revelación, alteración, pérdida o destrucción puede producir daños importantes a la Administración Pública Municipal.

OWASP. Proyecto de Seguridad de Aplicaciones Web Abiertas, es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

Personas Servidoras Públicas. Toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la Administración Pública Municipal de Monterrey.

Privacidad. Disposición de niveles de seguridad adecuados que garanticen la protección de datos personales y datos personales sensibles, de conformidad con lo establecido en los ordenamientos legales aplicables.

Ransomware. Malware o código malicioso que impide la utilización de los equipos o sistemas que infecta.

Routers de red. Dispositivos de hardware que sirven de punto de conexión entre una red local e internet. Los routers gestionan o enrutan el tráfico web y los datos entre dispositivos de diferentes redes, mediante paquetes que contienen, a su vez, distintos tipos de datos como archivos, comunicaciones y transmisiones simples como interacciones web, y permiten que varios dispositivos compartan la misma conexión a internet.

Secretaría. Secretaría de Innovación y Gobierno Abierto del Municipio de Monterrey.

Seguridad Informática. Garantía tecnológica de protección y niveles diferenciados de acceso de la información contenida en los sistemas digitales de información que no sea de carácter público, en consideración de datos personales o información estratégica para el buen funcionamiento del gobierno del municipio.

Serialización. Proceso de convertir datos o estructuras de datos en un formato específico que puede ser almacenado o transmitido y luego reconstruido en su forma original.

Sistema 5inco. Sistema organizacional que permite administrar los diversos folios de solicitudes y/o reportes realizados a la Dirección de Soporte e Infraestructura de la Dirección General de Gobierno Digital y Soporte Tecnológico de la Secretaría de Innovación y Gobierno Abierto de Monterrey.

SQL. Lenguaje de programación diseñado para administrar y manipular bases de datos relacionales.

SSRF. Es una vulnerabilidad de seguridad en la que un atacante puede manipular las solicitudes que realiza una aplicación desde el lado del servidor.

Sujetos Obligados. Todas las Dependencias y Entidades de la Administración Pública Municipal y Paramunicipal.

Switch de red. Es un dispositivo que permite la conexión de múltiples dispositivos a una misma red, actuando como puente entre estos, permitiendo que la información se transfiera entre ellos a través de paquetes de datos, mejorando a su vez, el rendimiento, la seguridad y fiabilidad de la red.

URL. Secuencia de caracteres que proporciona la dirección única de un recurso en la web.

IV. DESCRIPCIÓN

Criterios y estándares de seguridad informática

El lineamiento de criterios y estándares de seguridad informática del Municipio de Monterrey es emitido y será actualizado por la Secretaría de Innovación y Gobierno Abierto, a través de la Dirección General de Gobierno Digital y Soporte Tecnológico y la supervisión de la Dirección de Gobierno Digital y la Dirección de Soporte e Infraestructura, según corresponda. Este lineamiento establece las directrices para lograr una responsable gestión de la seguridad informática de la Administración Pública Municipal y Paramunicipal de Monterrey, implicando la observancia de lo dispuesto en el presente lineamiento y los demás ordenamientos jurídicos aplicables.

A efecto de garantizar la seguridad informática, y en cumplimiento con la Ley de Gobierno Municipal para el Estado de Nuevo León, el Reglamento de la Administración Pública Municipal de Monterrey, así como el Reglamento de Gobernanza Tecnológica para el Municipio de Monterrey, se determinan los siguientes lineamientos:

4.1. Disposiciones Generales

4.1.1. Las Direcciones promoverán una cultura de estándares idóneos de seguridad informática.

4.1.2. Los Sujetos Obligados deberán asegurar que las personas Servidoras Públicas conozcan las disposiciones generales en términos de Seguridad Informática.

4.1.3. Las Direcciones establecerán los procedimientos necesarios para el cumplimiento de los estándares municipales de seguridad informática, contemplando lo siguiente:

a) Atender las capacitaciones en la presente materia.
b) Cumplir con lo establecido en el Reglamento de Gobernanza Tecnológica para el Municipio de Monterrey, **L-SIG-GGD-08** *Lineamiento de Criterios y Estándares de Interoperabilidad*, así como el presente Lineamiento.
c) Otorgar opinión técnica para la adquisición o desarrollo en materia de tecnologías de la información y comunicaciones.

4.1.4. Todo intercambio de información entre los Sujetos Obligados debe cumplir con las buenas prácticas establecidas en el presente lineamiento, observando a la par lo dispuesto en las leyes nacionales y estatales sobre protección de datos personales.

4.1.5. Los Sujetos Obligados deberán informar mediante oficio dirigido a la persona titular de la Dirección General de Gobierno Digital y Soporte Tecnológico, marcando con copia a la persona titular de la Secretaría de Innovación y Gobierno Abierto del Municipio de Monterrey, el nombre completo, número de nómina y correo institucional de las personas Servidoras Públicas que se integran a sus dependencias o nuevos encargos indicando el perfil o permisos necesarios para el uso de sistema, para otorgarles claves de acceso a los sistemas. Así mismo, deberán informar cuando sean separados de su cargo o comisión, solicitando la baja de los accesos y permisos, evitando vulnerabilidades a la información.

4.2. Estándares de Seguridad Informática

La actual Administración Pública Municipal de Monterrey cuenta con estándares de seguridad que permiten garantizar la confidencialidad, integridad y disponibilidad de la información en todos los equipos electrónicos habilitados y utilizados por las personas Servidoras Públicas autorizadas.

4.2.1. **Antivirus**

La solución de protección por medio de antivirus deberá proveer protección ante diferentes amenazas cibernéticas que puedan comprometer la disponibilidad, integridad y confidencialidad de la información contenida en los distintos puntos de acceso a internet del municipio.

4.2.1.1. La Secretaría, a través de la Dirección de Soporte e Infraestructura de la Dirección General de Gobierno Digital y Soporte Tecnológico, será la encargada de dictaminar y establecer la solución o en su caso, soluciones de antivirus que se deberán ejecutar en la totalidad de las dependencias y entidades de la Administración Pública Municipal de Monterrey.

4.2.1.2. La Dirección de Soporte e Infraestructura garantizará la seguridad de la información contenida en los dispositivos electrónicos y redes informáticas autorizadas para operar dentro de la Administración Pública Municipal de Monterrey, por lo que éstos deberán contar con la última versión de actualización de la solución de antivirus.

4.2.1.3. Los Sujetos Obligados tendrán la responsabilidad de asegurar que el equipo de cómputo cuente con las últimas actualizaciones, por lo que cada Sujeto Obligado deberá reportar a la Dirección de Soporte e Infraestructura cualquier alerta o mensaje emergente en relación, a fin de que se realice la acción correspondiente, observando lo dispuesto en el punto 4.4.1. del presente lineamiento.

4.2.2. **Protección de la red**

Para garantizar la protección de la red es necesario realizar acciones que permitan la optimización del manejo del tráfico de la red, el cumplimiento de las condiciones de seguridad de los servicios con el usuario final y la atención inmediata de problemas de congestión, seguridad de la red y privacidad. Para tal fin, la Secretaría, a través de la Dirección de Soporte e

Infraestructura, atenderá de manera continua las distintas medidas de seguridad dirigidas a todos los Sujetos Obligados que intervengan en el proceso de tráfico por la red. Esto se realizará mediante los presentes lineamientos y atendiendo en todo momento las especificaciones relativas al eje de seguridad contemplado en el punto 4.2 del **L-SIG-GGD-08** *Lineamiento de Criterios y Estándares de Interoperabilidad.*

4.2.2.1. La Administración Pública Municipal y Paramunicipal de Monterrey deberá contar con un programa de protección informática, que será administrado por las Direcciones, garantizando la seguridad de la información, atacando directamente cualquier intento de acceso no autorizado a las redes de la Administración, así como aquellas amenazas que deriven de algún virus informático malicioso.

4.2.2.2. Las personas Servidoras Públicas que cuenten con cualquiera de los distintos niveles de internet a que se refiere el punto 4.2.1 del **L-SIG-SOI-01** *Lineamiento para Altas, Bajas y Modificación de Cuentas de Correo Institucional y Google Workspace*, deberán acceder a internet desde los dispositivos, así como las redes informáticas autorizadas por la Dirección a fin de disminuir posibles vulnerabilidades de la información de la Administración Pública Municipal y Paramunicipal de Monterrey, en atención lo dispuesto en el punto 4.2.2.3 del presente lineamiento.

4.2.2.3. Será obligación de la Direcciones contar con al menos una solución de seguridad de correo electrónico que brinde protección a la Administración Pública Municipal de Monterrey contra el espectro completo de amenazas basadas en correo electrónico, tales como suplantación de identidad, ransomware, ataques de día cero y ataques de compromiso de correo electrónico comercial; los rubros enlistados anteriormente se entenderán de manera enunciativa, más no limitativa.

4.2.2.4. Atendiendo a lo dispuesto en el punto 4.4 y demás relativos del presente lineamiento, será responsabilidad de cada una de las personas Servidoras Públicas con acceso a la red informática monitorear los recordatorios y mensajes emergentes así como los avisos de actualizaciones de la o las distintas soluciones de seguridad informática, debiendo notificar cualquier irregularidad para que el personal de la Dirección de Soporte e Infraestructura lleve a cabo la implementación de medidas paliativas y se asegure el buen uso de los equipos electrónicos que le hayan sido proporcionados por la Administración Pública Municipal y Paramunicipal de Monterrey.

4.2.2.5. Con la finalidad de reforzar la seguridad en los dispositivos electrónicos, la Dirección de Soporte e Infraestructura realizará actualizaciones a las contraseñas de éstos de manera periódica en los equipos en red y, en el caso de correo electrónico, se solicitará a la persona usuaria actualizar trimestralmente.

4.2.2.6. En el supuesto de alguna omisión a los presentes lineamientos, será responsabilidad de cada Sujeto Obligado la protección de la información que tengan en su posesión, derivado del desempeño de sus funciones en la Administración.

4.2.3. **Equipos de telecomunicaciones**

Los equipos de telecomunicaciones son todos aquellos que permiten y auxilian en los procesos de emisión, transmisión y recepción de la información de la Administración Pública Municipal y Paramunicipal de Monterrey a través de hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos aplicables.

4.2.3.1. Además de los equipos de telecomunicaciones, existen herramientas y accesorios electrónicos tales como switches y routers, entre otros, que sirven de auxilio en los procesos de simplificación técnica para el desempeño de las funciones propias de las personas Servidoras Públicas.

4.2.3.2. La Secretaría, a través de la Dirección de Soporte e Infraestructura de la Dirección General de Gobierno Digital y Soporte Tecnológico, será la única facultada para definir y llevar a cabo la instalación de los dispositivos de telecomunicación, herramientas y accesorios que podrán operar dentro de la Administración Pública Municipal y Paramunicipal de Monterrey.

4.2.3.3. La Dirección de Soporte e Infraestructura podrá retirar inmediatamente cualquier dispositivo externo que haya sido detectado, debiendo elaborar un acta circunstanciada en la que se detalle la Dependencia, Dirección, nombre completo y número de nómina del o la responsable de la incidencia, así como la descripción de la misma, a fin de evitar vulnerabilidades de la información.

4.3. Open Web Application Security Project (Proyecto Abierto de Seguridad de Aplicaciones Web)

Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. Entre otras cosas, publica la guía OWASP la cual es una guía amplia de criterios de seguridad que deben utilizar las aplicaciones web.

Para las aplicaciones web publicadas en infraestructura del Municipio, deben cumplirse la mayor cantidad posible de criterios de la guía OWASP, se debe mostrar evidencia de análisis de cumplimiento de las recomendaciones OWASP en las que aplique, considerando como mandatorios a la Dirección de Gobierno Digital al menos los que se establecen en el presente lineamiento a continuación, considerando en caso de haber una nueva edición de OWASP Top 10 actualizar la guía vigente como línea base de criterios mínimos:

4.3.1. A01:2021-Broken Access Control (Control de acceso roto)

El Control de acceso hace referencia a un sistema que controla cual usuario accede a cuál información o funcionalidad. Los controles de acceso que no funcionan permiten a los atacantes saltarse la autorización y realizar tareas como si fueran usuarios privilegiados, como los administradores. Por ejemplo, una aplicación web podría permitir que una persona usuaria cambie la cuenta con la que ha iniciado sesión solo modificando una parte de la url, sin ninguna otra verificación.

Los controles de acceso pueden protegerse al asegurar que una aplicación web utilice tokens de autorización y establezca controles estrictos sobre los mismos.

4.3.2. A02:2021-Cryptographic Failures (Fallas criptográficas)

Si las aplicaciones web no protegen los datos confidenciales, como la información financiera y las contraseñas, los atacantes pueden acceder a esos datos y venderlos o utilizarlos con fines maliciosos. Un método popular para robar información confidencial es el uso de un ataque en ruta.

El riesgo de exposición de datos puede minimizarse al cifrar todos los datos confidenciales, y al desactivar el almacenamiento en caché de cualquier información confidencial. Además, los desarrolladores de aplicaciones web deben asegurarse de que no están almacenando innecesariamente ningún dato confidencial.

4.3.3. A03:2021-Injection (Inyección)

Los ataques de inyección ocurren cuando se envían datos que no son de confianza a un intérprete de código a través de la entrada de un formulario o algún otro envío de datos a una aplicación web. Por ejemplo, un atacante podría introducir código de base de datos SQL en un formulario que espera un nombre de usuario en texto plano. Si la entrada

del formulario no está asegurada de forma adecuada, se acabaría ejecutando el código SQL. Esto se conoce como un ataque de inyección de código SQL.

Los ataques de inyección pueden evitarse al validar o sanear los datos enviados por la persona usuaria (la validación significa rechazar los datos que tienen un aspecto sospechoso, mientras que la sanitización hace referencia a la limpieza de las partes de aspecto sospechoso de los datos).

Además, la persona responsable de administrar la base de datos puede establecer controles para minimizar la cantidad de información que puede sacar a la luz un ataque de inyección.

4.3.4. **A04:2021-Insecure Design (Diseño inseguro)**

Se enfoca ampliamente en el diseño de aplicaciones y fallas arquitectónicas que conducen a mayores riesgos de seguridad. Cuando una aplicación está inherentemente diseñada de manera insegura, incluso una implementación perfecta de los controles y riesgos de seguridad no puede compensar esas debilidades de diseño. Los actores de amenazas sofisticados eventualmente encontrarán y explotarán las fallas de diseño.

A un alto nivel, uno de los consejos de mitigación más importantes es exigir el uso de modelos de amenazas para los equipos de desarrollo de software. El modelado de amenazas debe usar la estructura y el flujo de datos inherentes a una aplicación web específica para rastrear las amenazas técnicas clave que podrían explotar el sistema.

4.3.5. **A05:2021-Security Misconfiguration (configuración incorrecta de seguridad)**

La desconfiguración de la seguridad es la vulnerabilidad más común de la lista y suele ser el resultado de usar configuraciones por defecto o de mostrar errores excesivamente detallados. Por ejemplo, una aplicación podría mostrar a la persona usuaria errores demasiado descriptivos que

mostraran vulnerabilidades en la aplicación. Esto se puede mitigar mediante la eliminación de cualquier función no utilizada en el código y al asegurarse de que los mensajes de error sean más generales.

4.3.6. A06:2021-Vulnerable and Outdated Components (Componentes vulnerables y obsoletos)

Es frecuente utilizar piezas de software que ayuden a los desarrolladores a evitar el trabajo redundante y a ofrecer la funcionalidad necesaria; un ejemplo común son los marcos frontales como Vue y las bibliotecas más pequeñas que se utilizan para añadir iconos compartidos o pruebas a/b. Algunos atacantes buscan vulnerabilidades en estos componentes que luego pueden utilizar para orquestar ataques. Algunos de los componentes más famosos se utilizan en cientos de miles de sitios web; un atacante que encuentre un agujero de seguridad en uno de estos componentes podría dejar cientos de miles de sitios vulnerables.

Los desarrolladores de componentes suelen ofrecer parches de seguridad y actualizaciones para tapar las vulnerabilidades conocidas, pero los desarrolladores de aplicaciones web no siempre tienen las versiones parcheadas o más recientes de los componentes que se ejecutan en sus aplicaciones. Para minimizar el riesgo de ejecutar componentes con vulnerabilidades conocidas, los desarrolladores deben eliminar de sus proyectos los componentes que no utilicen, así como asegurarse de que reciben componentes de una fuente de confianza y de que estos estén actualizados.

4.3.7. A07:2021-Identification and Authentication Failures (Fallos de identificación y autenticación)

Las vulnerabilidades en los sistemas de autenticación (login) pueden dar a los atacantes acceso a las cuentas de las personas usuarias e incluso tener la capacidad de poner en riesgo todo un sistema mediante el uso de una cuenta de administrador. Por ejemplo, un atacante puede coger una lista con miles de combinaciones conocidas de nombres de usuarios y

contraseñas conseguidas durante una fuga de datos, y utilizar un script para probar todas esas combinaciones en un sistema de inicio de sesión para ver si funciona alguna.

Algunas estrategias para mitigar las vulnerabilidades de autenticación son pedir la autenticación de doble factor (2FA), así como limitar o retrasar los intentos repetidos de inicio de sesión mediante el uso de la limitación de velocidad.

4.3.8. **A08:2021-Software and Data Integrity Failures (Fallos de integridad de datos y software)**

Esta amenaza se dirige a las numerosas aplicaciones web que serializan y deserializan datos con frecuencia. La serialización implica tomar objetos del código de la aplicación y convertirlos en un formato que pueda ser utilizado con otro objetivo, como almacenar los datos en el disco o transmitirlos. La deserialización es justo lo contrario: convertir los datos serializados de nuevo en objetos que la aplicación pueda utilizar. La serialización es como meter los muebles en cajas antes de una mudanza, y la deserialización es como sacarlos de las cajas y volver a montarlos después de la mudanza. Un ataque de deserialización inseguro es como si la empresa de mudanzas manipulara el contenido de las cajas antes de desembalarlas.

Una explotación de deserialización insegura es el resultado de la deserialización de datos desde fuentes no confiables, y puede tener graves consecuencias, como los ataques DDoS y los ataques de ejecución remota de código. Aunque se pueden tomar medidas para intentar atrapar a los atacantes, como la supervisión de la deserialización y la implementación de comprobaciones de tipo, la única forma segura de protegerse antes los ataques de deserialización insegura es prohibir la deserialización de datos desde fuentes no fiables.

4.3.9. **A09:2021-Security Logging and Monitoring Failures (Fallas de registro y monitoreo de seguridad)**

El registro y la supervisión ayudan a proporcionar responsabilidad de seguridad, visibilidad de eventos, alertas de incidentes y análisis forense. Cuando hay fallas en estas capacidades, la capacidad de su empresa para detectar y responder a las infracciones de aplicaciones se ve gravemente comprometida. Para mitigar, use herramientas de código abierto o propietarias para correlacionar registros, implementar monitoreo y alertas y crear una estrategia de respuesta y recuperación de incidentes utilizando pautas establecidas, como NIST 800-61r2 (guía publicada por el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos, titulada "Computer Security Incident Handling Guide", proporciona pautas detalladas para la gestión y respuesta a incidentes de seguridad informática).

4.3.10. **A10:2021-Server-Side Request Forgery (falsificación de solicitudes del lado del servidor)**

Falsificación de solicitud del lado del servidor (SSRF) es uno de los dos riesgos Top Ten de OWASP agregados según la encuesta de la comunidad en lugar de los datos de las aplicaciones web. La mayoría de las aplicaciones web actuales requieren recursos externos para su funcionalidad, a los que generalmente se accede a través de URL. SSRF ocurre cuando los piratas informáticos pueden hacer que los servidores realicen solicitudes que ellos controlan. La vulnerabilidad típica es que la aplicación web no valida la URL proporcionada por la persona usuaria, lo que podría permitir el acceso a servicios o recursos internos al pasar por alto los controles de acceso. El concepto estratégico de defensa en profundidad es importante aquí; múltiples controles en las capas de aplicación y red pueden ayudar a prevenir SSRF. Los datos de entrada proporcionados por el/la cliente deben validarse y desinfectarse, mientras que la segmentación de la red también puede ayudar.

4.4. **De las incidencias**

En el caso de que ocurran uno o varios eventos que atenten contra la confidencialidad, la integridad y la disponibilidad de la información, y/o que violenten la seguridad de la información de la Administración Pública Municipal y Paramunicipal de Monterrey, deberán ser atendidos conforme a lo siguiente:

4.4.1. Las incidencias deberán ser reportadas directamente a la línea telefónica de la recepción de la Dirección de Soporte e Infraestructura, salvo que por circunstancias particulares no sea posible. Para tales casos se podrá realizar el o los reportes de incidencias, únicamente a través de correo institucional: helpdesk@monterrey.gob.mx

4.4.2. La persona Servidora Pública que detecte cualquier anomalía o comportamiento fuera de lo normal en alguno de los equipos, dispositivos o accesorios instalados por la Dirección de Soporte e Infraestructura, deberá comunicarse inmediatamente para realizar el reporte de incidencia correspondiente, atendiendo lo dispuesto en el punto que antecede.

4.4.3. A través del sistema 5inco, el personal de la Dirección de Soporte e Infraestructura generará y turnará el ticket al área de Soporte Técnico de esa misma Dirección, el cual permitirá la atención de la incidencia que haya motivado el reporte.

4.4.4. El personal de soporte técnico de la Dirección de Soporte e Infraestructura canalizará el ticket al personal a su cargo o bien, al área según corresponda, para que, en un plazo no mayor a 24 horas, sea atendido.

4.4.5. Una vez atendido el incidente, la Dirección de Soporte, elaborará un reporte de riesgos, en el que se detallarán las acciones implementadas, cumplimiento y estatus de los equipos y/o dispositivos involucrados.

4.4.6. En caso de que la situación requiera de una mayor atención por la naturaleza del incidente se valorará la situación por parte de la persona titular de la Dirección de Soporte e Infraestructura con la persona titular de la Dependencia involucrada para definir las acciones conducentes.

V. REFERENCIAS Y/O BIBLIOGRAFÍA

- **L-SIG-GGD-08** *Lineamiento de Criterios y Estándares de Interoperabilidad.*
- **L-SIG-SOI-01** *Lineamiento para Altas, Bajas y Modificación de Cuentas de Correo Institucional y Google Workspace.*
- *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. https://owasp.org
- *OWASP Application Security Verification Standard | OWASP Foundation*. https://owasp.org/www-project-application-security-verification-standard/
- *OWASP Top Ten | OWASP Foundation*. https://owasp.org/www-project-top-ten/
- *OWASP Application Security Verification Standard 4.0.3* *https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-es.pdf*

VI. ANEXOS

N/A.

VII. CONTROL DE CAMBIOS

VERSIÓN	FECHA	MOTIVO
01	30/04/24	Creación del lineamiento.