RESOLUCIÓN 2022600278 DE 2022

(octubre 28)

Diario Oficial No. 52.205 de 1 de noviembre de 2022

INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS

Por la cual se declara la urgencia manifiesta para celebrar la contratación de bienes y servicios necesarios para conjurar y mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático ocasionado por la propagación de un código malicioso producto de un ataque con múltiples vectores contra la seguridad tecnológica del Invima.

EL SECRETARIO GENERAL DEL INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS (INVIMA),

en ejercicio de las facultades legales, la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto número 1082 de 2015, el Decreto número 2078 de 2012, la Resolución de Delegación de Funciones número 2012030802 del 19 de octubre de 2012, la Resolución número 2020006742 del 25 de febrero de 2020, Acta de Posesión número 040 del 25 de febrero de 2020, y

CONSIDERANDO QUE:

La Constitución Política de Colombia en su artículo 2o, contempla:

“**Artículo 2o.** Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares. (Subrayado fuera del texto).

Por medio del artículo 245 de la Ley 100 de 1993 se crea el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima) como establecimiento público del orden nacional, adscrito al Ministerio de Salud y Protección Social, con personería jurídica, patrimonio independiente y autonomía administrativa, cuyo objeto es la ejecución de las políticas en materia de vigilancia sanitaria y de control de calidad de medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y elementos médico-quirúrgicos, odontológicos, productos naturales homeopáticos y los generados por biotecnología, reactivos de diagnóstico, y otros que puedan tener impacto en la salud individual y colectiva.

Para tal fin el Decreto número 2078 de octubre de 2012 “Por el cual se establece la estructura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos -Invima y se determinan las funciones de sus dependencias”, en el numeral 1 de su artículo 4o, establece las funciones de la entidad entre las cuales se encuentra la siguiente:

Ejercer las funciones de inspección, vigilancia y control a los establecimientos productores y comercializadores de los productos a que hace referencia el artículo 245 de la Ley 100 de 1993 y en las demás normas que lo modifiquen o adicionen, sin perjuicio de las que en estas materias deban adelantar las entidades territoriales, durante las actividades asociadas con su producción, importación, exportación y disposición para consumo.

En tal sentido, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima) como organismo encargado de cumplir con las funciones de inspección, vigilancia y control de los productos de su competencia, le corresponde adelantar a través del talento humano (contemplando funcionarios y contratistas) que conforman y hacen parte del apoyo de las direcciones, oficinas, coordinaciones y demás grupos internos de trabajo de su estructura orgánica, las actividades necesarias para la efectiva prestación del servicio público que se brinda por la institución.

Así mismo, en el marco del proceso de transformación digital, la entidad cuenta con la infraestructura tecnológica que

soporta los múltiples sistemas de información, bases de datos y aplicativos necesarios para realizar las labores misionales y administrativas, y que se encuentra gestionada por la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico, con el cual garantiza que las actividades desarrolladas por la entidad se ejecuten, a través de los distintos aplicativos[(1)]; los cuales a pesar de haber sido impactados en el incidente cibernético del pasado 6 de febrero de 2022, al 2 de octubre de la presente anualidad se encontraban operativos, garantizando la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso.

El 3 de octubre de 2022, se evidenció un incidente de seguridad de la información[(2)] que comprometió la disponibilidad de los sistemas de información, bases de datos, plataformas y herramientas tecnológicas del Invima, generado por la instalación no autorizada de un código malicioso producto de un ataque con múltiples vectores contra la seguridad tecnológica del Invima[(3)], el cual bloquea el acceso a la información, afectando la operación de varios de los servidores y estaciones de trabajo cliente, así como los aplicativos y sistemas de información dispuestos para la operación del Instituto, de conformidad al informe denominado estado situacional[(4)].

Consonante a lo definido en el mentado estado situacional, se trata de un incidente tecnológico que tiene un despliegue de actos provocados por ciberdelincuentes que transitan desde:

1. Denegación del servicio del antivirus: ataque por medio de phishing (ingeniería social) y una vez comprometida la consola de antivirus (extensión ransomware.crypt, algunos troyanos y el.conti,) inhabilita las funcionalidades de protección, permitiendo la descarga de software maliciosos de diferentes orígenes con alta, media y baja complejidad que deja contaminado todo el ambiente tecnológico del instituto.

2. Instrucción abusiva de sistemas informáticos: circunstancia que se evidenció en procedimiento de encriptado de la información y los sistemas de información de la entidad, de forma masiva y generalizada.

3. Ransomware innominado: Como quiera que se evidenció en el mensaje de rescate donde se solicitó el pago por la liberación de la información a cambio de dinero, así como las múltiples caracterizaciones del cifrado encontrado, generando la capacidad de bloquear los dispositivos tecnológicos en uso de la entidad, sin que se refiriera a una familia de Ransomware específica.

4. Propagación de código malicioso de forma sistemática después de apagado los servicios de conectividad.

5. Daño sobre el servicio tecnológico que administra y soporta las copias de respaldo.

Circunstancia que generan evaluación como: “ataque cibernético con múltiples vectores[(5)]” de acuerdo con las conductas sistemáticas generada sobre los sistemas de información del Invima.

Dicho incidente ocasionó un problema de continuidad del negocio, afectando la ejecución de las actividades diarias del Instituto, toda vez que el mismo es considerado como “incidente de seguridad de la información”.

Es de precisar que, estas situaciones de ciberseguridad afectan de forma inesperada la estabilidad de los sistemas de información, toda vez que los vectores utilizados por los cibercriminales están dados desde la propagación de códigos maliciosos, virus, malware y ransomware, los cuales son cada vez más robustos, complejos y sofisticados, de forma tal que, a pesar de contar con los controles, políticas, lineamientos, planes y demás acciones relacionadas con el control y la seguridad de la información se hace casi imposible su detección y rastreo.

No obstante, derivado del primer ataque cibernético a la infraestructura de la entidad, ocasionado el 6 de febrero, el Invima desplegó una serie de acciones las cuales permitieron su habilitación de manera progresiva, y provisionar nuevamente los sistemas de información y aplicativos de la entidad, sin embargo estas acciones fueron complementadas mediante la ejecución de proyectos asociados al aseguramiento de la red del Instituto, obteniendo información valiosa que permitió definir y programar las acciones a desarrollar posteriormente, las cuales al momento del nuevo incidente se encontraban en ejecución con el ánimo de cerrar las brechas de seguridad digital encontradas; sin embargo, la implementación de algunas de estas acciones implican la gestión e inversión de recursos superiores a los ya asignados al Instituto, así como la vinculación del personal idóneo y con la experiencia requerida para la atención de este tipo de incidentes. Toda vez que el aumento de este tipo de ataques al sector estatal ha presentado un escalamiento vertiginoso que aprovecha el bajo dinamismo (por la ausencia de presupuesto) que en relación con los sistemas de información tiene el sector estado para perpetrar este tipo de ataques, ya no desde un código malicioso identificado, sino de a través de múltiples acciones encaminadas a generar la afectación y dar al traste con los desarrollos y seguridad perimetral que se pueda establecer entre uno y otro ataque, como quiera que se hace irresistible competir con este tipo de crímenes organizados que vienen golpeando la región como ha sucedido en países como Chile, México, Perú y reincidentemente en Colombia.

En relación con el incidente actual, la entidad implementó medidas, que van acorde con la implementación del plan de acción de riesgos de incidente de seguridad de la información, cuyo eje fundamental es “Garantizar la recuperación, disponibilidad y acceso a los sistemas de información, bases de datos y las redes de telecomunicaciones del Instituto Nacional de Vigilancia de Medicamento y Alimentos (Invima), afectados por una circunstancia constitutiva de fuerza mayor, relacionada con incidente informático a través de un ataque cibernético ocasionado por la propagación de un código malicioso, producto de un ataque con múltiples vectores contra la seguridad tecnológica del Invima”, para la reactivación de los servicios tecnológicos desde los que se despliega la misionalidad del Instituto, de conformidad a los aplicativos aludidos en el Anexo 1 (Relación de softwares) del presente documento, así mismo se configuraron trámites administrativos entre los que se encuentran la emisión de la Resolución número 2022600000 del 4 de octubre de 2022, “Por medio de la cual se adoptan medidas administrativas transitorias necesarias para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima)”.

De forma paralela, la entidad interpuso ante la Fiscalía General de la Nación denuncia bajo el Código de Noticia Criminal número 110016000050202231285 de fecha 05/10/2022, por el presunto delito de acceso abusivo a un sistema informático (artículo 269ª Ley 1273 de 2009), y se presentó el reporte a la Superintendencia de Industria y Comercio (SIC) sobre el incidente en el que quedaron cifrados datos personales (entidad), utilizando los medios indicados por la misma Superintendencia, con el usuario entregado para el Invima.

El 21 de octubre de 2022, se llevó a cabo Comité de Seguimiento Técnico**(6)**, integrado por el director general, los funcionarios y contratistas del Grupo de Soporte Tecnológico como de la Oficina de Tecnologías de la Información del Invima y la Oficial de Seguridad de la Información, quienes recomendaron realizar el análisis jurídico, económico, contractual y financiero para la declaratoria de urgencia manifiesta con el fin de:

1. Adquirir los recursos técnico-necesarios para garantizar la protección de equipos contra malware de próxima generación y la asistencia técnica para la visibilidad del tráfico cifrado, circunstancia que quedaría atendida a partir del licenciamiento y soporte técnico de los equipos SonicWall:

- Firewall (NSA 5600) solución en HA

- Firewall (NSA 4700)

- Firewall (NSA 4700)

- Equipo concentrador VPN SonicWall SMA 410

- Solución Global Management System de SonicWall

Así como la renovación del licenciamiento y soporte para el análisis de logs y modelamiento preventivo para la detención de ataques basados en la identificación temprana (técnicas, tácticas y procedimientos) de actos de ciberdelincuentes. De igual forma, la adquisición de una plataforma que permita a través de inteligencia artificial visibilizar comportamientos anómalos en la red hasta equipos de usuarios finales, circunstancias que redundarían en el aseguramiento y contención de códigos maliciosos que atentan contra la infraestructura en ambiente On-Premise.

2. Para efectos del restablecimiento de servicios y sistemas, en especial el Sistema de Información para los Laboratorios (Silab), a través del cual se gestiona la información de la oficina de Laboratorios y control de calidad del Instituto, y dada su afectación, como consecuencia de la encriptación de la información, se requiere la instalación, configuración, parametrización, pruebas y salidas a producción por parte del proveedor exclusivo del sistema y/o dueño del código fuente para efectos de superar el acceso al aplicativo y el reporte de informes, consulta de bases de datos e impresor de etiquetas de los trámites que lleva a cabo la Oficina de Laboratorios y Control de Calidad.

3. Restablecimiento del portal web, debido al incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la disponibilidad y acceso al portal WEB de la entidad. Por este motivo, se requiere contar con los servicios especializados para configurar, parametrizar, afinar, realizar pruebas y puesta en producción del portal web de la Entidad, soportado en la tecnología Liferay.

4. Análisis forense, dada la calificación del evento y teniendo en cuenta que se requiere un estado de seguridad y certeza respecto de lo ocurrido, se necesita identificar las evidencias para detectar las vulnerabilidades de la infraestructura y analizar las causas o causa raíz del evento que sufrió la entidad, circunstancia que permitirá mitigar y tratar este tipo de riesgos de manera efectiva y no quedar eventualmente expuestos respecto de estos ataques que a la fecha están en auge.

Bajo este contexto, y respecto a la importancia del cumplimiento de las labores de la entidad, teniendo en cuenta que la misionalidad del Instituto se basa en proteger y promover la salud de los colombianos, es claro que las actividades que desarrolla no se pueden paralizar; por lo cual se hace necesario activar la causal de contratación directa a través de urgencia manifiesta, de conformidad al plan de acción, en relación con las actividades anteriormente descritas establecidas en el Comité precitado y como medida conducente en el proceso de mitigación.

Así las cosas y, con el propósito de garantizar la disponibilidad y el acceso total a la información y las comunicaciones del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático, ocasionado por la propagación de un código malicioso producto de acciones generadas por múltiples vectores respecto la seguridad tecnológica irresistibles, por lo que se hace necesaria la contratación de bienes y servicios para conjurar, mitigar los efectos, y con ello restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como fortalecer la seguridad de la información de la Entidad.

Corolario, se requiere gestionar los trámites contractuales de forma inmediata, toda vez que no se cuenta con el plazo indispensable para adelantar el procedimiento ordinario de escogencia de contratistas[(7)], siendo viable acudir al mecanismo idóneo para adelantar las contrataciones, con atención a las situaciones anteriormente expuestas, garantizando una respuesta contigua de la administración.

En atención a la situación expuesta, se encuentra configurada la circunstancia de fuerza mayor contemplada en el artículo 42 de la Ley 80 de 1993[(8)], el cual refiere la condición de la urgencia manifiesta a partir de situaciones necesarias para conjurar contextos excepcionales relacionadas con esta.

En tal sentido, la Ley 1150 de 2007 (Literal a) numeral 4 del artículo 2o. De las modalidades de selección) refiere:

4. **Contratación directa.** La modalidad de selección de contratación directa solamente procederá en los siguientes casos:

(…)

a) Urgencia manifiesta;

Es preciso indicar que se acude a la excepción contemplada en el citado artículo, en atención a la situación de fuerza mayor descrita en la parte inicial del presente documento, en este orden y conforme a lo indicado en múltiples ocasiones por el Consejo de Estado[(9)], se entiende que la fuerza mayor debe ser:

1) Exterior: esto es que está dotado de una fuerza destructora abstracta, cuya realización no es determinada, ni aún indirectamente por la actividad del ofensor.

2) Irresistible: esto es que ocurrido el hecho el ofensor se encuentra en tal situación que no puede actuar sino del modo que lo ha hecho.

3) Imprevisible: cuando el suceso escapa a las previsiones normales, esto es, que ante la conducta prudente adoptada por quien lo alega, era imposible pronosticarlo o predecirlo.

En línea de lo anterior manifiesta la misma corporación frente a lo dicho por la Corte Suprema de Justicia a este respecto (Sentencia de 15 de junio de 2000, Expediente 12.423):

(...) La fuerza mayor solo se demuestra mediante la prueba de un hecho externo concreto (causa extraña). Lo que debe ser imprevisible e irresistible no es el fenómeno como tal, sino sus consecuencias (...) En síntesis, para poder argumentar la fuerza mayor, el efecto del fenómeno no solo debe ser irresistible sino también imprevisible, sin que importe la previsibilidad o imprevisibilidad de su causa. Además de imprevisible e irresistible debe ser exterior del agente, es decir, no serle imputable desde ningún ámbito.

Teniendo en cuenta la normatividad citada, es claro que no se trata de evadir los procedimientos legales ordinarios para este tipo de procesos sino de simplificarlos, en atención a las circunstancias excepcionales por las que atraviesa la Entidad, dado que no da espera a los tiempos de las modalidades típicas que se aplicarían ordinariamente para resolver este tipo de procesos, toda vez que los tiempos de gestión que implica realizar el procedimiento de selección correspondiente sería superior a 72 días[(10)].

Sobre el particular, la Corte Constitucional[(11)] indicó que:

“La “urgencia manifiesta” es una situación que puede decretar directamente por cualquier autoridad administrativa sin autorización previa, a través de acto debidamente motivado. Que ella existe o se configura cuando se acredite la existencia de uno de los siguientes presupuestos: - Cuando la continuidad del servicio exija el suministro de bienes, o la prestación de servicios o la ejecución de obras en el inmediato futuro. - Cuando se presenten situaciones relacionadas con los estados de excepción. - Cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, - en general cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o concursos públicos”.

El Consejo de Estado**(12)**, mediante pronunciamiento del 27 de abril de 2006, manifestó:

“Se observa entonces cómo la normatividad que regula el tema de la urgencia en la contratación estatal, se refiere a aquellos eventos en los cuales pueden suscitarse hechos que reclamen una actuación inmediata de la Administración, con el fin de remediar o evitar males presentes o futuros pero inminentes, provocados bien sea en virtud de los estados de excepción, o por la paralización de los servicios públicos, o provenientes de situaciones de calamidad o hechos constitutivos de fuerza mayor o desastres, o cualquier otra circunstancia similar que tampoco dé espera en su solución, de tal manera que resulte inconveniente el trámite del proceso licitatorio de selección de contratistas reglado en el estatuto contractual, por cuanto implica el agotamiento de una serie de etapas que se toman su tiempo y hacen más o menos largo el lapso para adjudicar el respectivo contrato, circunstancia que, frente a una situación de urgencia obviamente resulta entorpecedora, porque la solución en estas condiciones, puede llegar tardíamente, cuando ya se haya producido o agravado el daño. En estas estipulaciones, se hace evidente el principio de la prevalencia del interés general, en este caso, por encima de las formalidades de las actuaciones administrativas, puesto que si aquel se halla afectado o en peligro de serlo, el régimen jurídico debe ceder y permitir que las soluciones se den en la mayor brevedad posible, así ello implique la celebración de contratos sin el cumplimiento de los requisitos legales de selección del contratista y aún, la ejecución de los mismos, sin que medie la formalidad del contrato escrito, si la gravedad de las circunstancias así lo exige”.

En virtud de la obligación del Instituto de garantizar el derecho a la salud a través de la salvaguarda de la seguridad sanitaria del país, se requiere mantener la continua prestación del servicio de la entidad y, en atención a la imposibilidad, por razones de tiempo, de seleccionar a los contratistas mediante los procesos ordinarios de selección dispuestos por la Ley 80 de 1993 y demás normas reglamentarias, se requiere declarar la Urgencia Manifiesta, en aras de dar cumplimiento a la Constitución y la ley, teniendo en cuenta los recursos asignados para tal fin.

En razón a las causas y finalidades mencionadas y, de conformidad con los componentes técnicos en los que se justifica la necesidad de contratación suscrita por el Grupo de Soporte Tecnológico, la Oficina de Tecnologías de la Información y la Oficina Asesora de Planeación – Oficial de Seguridad de la Información; en este orden, los bienes y servicios que se adquirirán por vía de la contratación directa en el marco de la declaratoria de URGENCIA MANIFIESTA son los siguientes**(13)**:

TABLAS NO INCLUIDAS CONSULTAR ANEXO EN EL DIARIO OFICIAL IMPRESO O EN EL FORMATO PDF PUBLICADO EN LA WEB WWW.IMPRENTA.GOV.CO

Las necesidades anteriormente expuestas respecto a los bienes y servicios, conciernen únicamente a los requerimientos que, de acuerdo con su complejidad y especialidad, deben ser atendidos por proveedores expertos e idóneos, de conformidad con la plataforma, arquitectura, lenguaje de programación, ambiente de pruebas (QA) y producción, así como su calidad de proveedor exclusivo o canal autorizado del fabricante.

La duración de la Urgencia Manifiesta será hasta el 31 de diciembre de 2022 (inclusive), plazo dentro del cual se adoptarán las acciones para conjurar y mitigar los efectos ocasionados por el incidente de seguridad de la información, que no puedan ser atendidos con los recursos y el personal del Instituto.

En desarrollo del proceso de contratación directa, la entidad debe garantizar los principios que rigen la contratación estatal, consagrados en los artículos 24, 25 y 26 de la Ley 80 de 1993, referentes a los principios de transparencia, economía y responsabilidad**(15)**.

En mérito de lo expuesto, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima),

RESUELVE:

ARTÍCULO 1o. Declarar la URGENCIA MANIFIESTA en el **Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima)**, para celebrar la contratación de bienes y servicios necesarios para conjurar y

mitigar los efectos de la indisponibilidad de los sistemas de información, plataformas tecnológicas, y herramientas tecnológicas de la entidad, para restablecer la continuidad de la operación de las actividades misionales y administrativas en la infraestructura de comunicaciones e información, así como la seguridad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático ocasionado por la propagación de un código malicioso producto de un ataque con múltiples vectores contra la seguridad tecnológica del Invima.

PARÁGRAFO 1o. La duración de la Urgencia Manifiesta será hasta el 31 de diciembre de 2022 (inclusive), plazo dentro del cual se adoptarán las acciones para conjurar y mitigar los efectos ocasionados por el incidente de seguridad de la información, que no puedan ser atendidos con los recursos y el personal del Instituto.

ARTÍCULO 2o. Establecer como modalidad a aplicar para la contratación que aquí se trata, la contratación directa conforme a la causal prevista en el artículo 42 de la Ley 80 de 1993 de conformidad con lo señalado en el literal a) numeral 4 artículo 2o de la Ley 1150 de 2007, y el artículo 2.2.1.2.1.4.2. del Decreto número 1082 de 2015. y, en consecuencia, los bienes y servicios que se adquirirán por vía de la contratación directa en el marco de la declaratoria de URGENCIA son los siguientes:

ARTÍCULO 3o. Ordenar al Grupo de Gestión Contractual y Grupo Financiero y Presupuestal adelantar los trámites precontractuales pertinentes para la adquisición de los bienes y servicios relacionados en el artículo segundo de esta resolución.

ARTÍCULO 4o. Ordenar al Grupo Financiero y Presupuestal que se realicen los traslados presupuestales correspondientes para la adquisición de los bienes y servicios relacionados en el artículo segundo de esta resolución.

ARTÍCULO 5o. Disponer que, por el Grupo de Gestión Contractual, se conformen y organicen los expedientes respectivos, con copia de este acto administrativo, de los contratos originados en la presente urgencia manifiesta, y demás estudios y documentos precontractuales de orden técnico y administrativo, con el fin de que sean remitidos a la Contraloría General de la República, para el ejercicio del control fiscal pertinente, de conformidad con el artículo 43 de la Ley 80 de 1993.

ARTÍCULO 6o. La presente resolución rige a partir de la fecha de su publicación.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 28 de octubre de 2022.

El Secretario General,

Roy Galindo Wehdeking.

Anexo 1. Relación Software

Anexo 2. Estado situacional

Anexo 3. Acta Comité de Seguimiento Técnico

Anexo 4. Plan de Acción.

NOTAS AL FINAL:

1. Ver Anexo 1: Relación de software.

2. Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento de las actividades. Según www.piranirisk.com/es/blog/incidentes-en-la-seguridad-de-la-informacion.

3. Múltiples vectores de Ataque: Conjunto de ataques cibernéticos, que explotan tanto las debilidades de la red como aplicaciones, computadoras y correo electrónico; así como las falencias del personal mediante prácticas de ingeniería social. Tomado de https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/

Se puede obtener más información de:

https://www.cisa.gov/uscert/incident-notification-guidelines#attack-vectors

https://www.cisa.gov/uscert/incident-notification-guidelines

https://hackwise.mx/los-5-vectores-mas-comunes-de-ataques-ciberneticos-y-como-evitarlos/

4. Ver Anexo 2: Estado situacional.

5. Para efectos de este diagnóstico los múltiples vectores son las conductas descritas en la afectación de los sistemas de seguridad de la información realizadas por el intruso.

6. Ver Anexo 3: Acta Comité de Seguimiento Técnico

7. Licitación pública, selección abreviada, concurso de mérito, contratación mínima cuantía.

8. Artículo 42. De la urgencia manifiesta. <Aparte tachado derogado por el artículo 32 de la Ley 1150 de 2007> Existe urgencia manifiesta cuando la continuidad del servicio exige el suministro de bienes, o la prestación de servicios, o la ejecución de obras en el inmediato futuro; cuando se presenten situaciones relacionadas con los estados de excepción; cuando se trate de conjurar situaciones excepcionales relacionadas con hechos de calamidad o constitutivos de fuerza mayor o desastre que demanden actuaciones inmediatas y, en general, cuando se trate de situaciones similares que imposibiliten acudir a los procedimientos de selección o ~~concurso~~ públicos (…).

9. Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Expediente 13.833, sentencia de 26 de febrero de 2004, C. P. Germán Rodríguez Villamizar.

10. Circular número 109 del 1 de octubre de 2020, emitida por el Secretario General del Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima).

11. Corte Constitucional, Sentencia C-772 de 1998, 10 de diciembre de 1998. Magistrado Ponente: Fabio Morón Díaz.

12. Consejo de Estado, Sentencia del 27 de abril de 2006, Expediente número 14275. Consejero Ponente: Ramiro Becerra Saavedra.

13. En desarrollo de lo dispuesto en el Plan de Acción Incidente de Seguridad de la Información.

14.

15. Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera. Radicado Interno 37.044. Marzo 7 de 2011. Magistrado Ponente: Doctor Enrique Gil Botero.

16.


invima
Instituto Nacional de Vigilancia de Medicamentos y Alimentos.