invima	GESTIÓN DIRECTIVA		DIRECCIONAMIENTO ESTRATÉGICO	
	FORMATO DE ACTA			
	Código: GDI-DIE-FM001	Versión: 01	Fecha de Emisión: 2019-02-08	Página 1 de 1

El tratamiento de los datos personales se realiza de acuerdo a los requerimientos de la ley 1581 de 2012 y a lo establecido en la política de tratamiento y Protección de datos personales GDI-DIE-PL018 disponible en www.invima.gov.co

Tema: Formateo de Servidores del Invima

Lugar: TEAMS		Acta No
Fecha: 2022-03-15		**1250-006-2022**
Hora de inicio: 06:00 pm	**Hora de finalización:**	

ASISTENTES

Nombre Completo	Cargo
María Margarita Jaramillo Pineda	**Jefe Oficina Asesora Jurídica**
Juan Manuel Palacio Posada	**Jefe de la Oficina de Tecnologías de la Información**
Eliodoro Rojas Ochoa	**Profesional Especializado - Coordinador Grupo Soporte Tecnológico**
Nidia Nayibe González Pinzón	**Contratista - Oficial de Seguridad de la Información**
Camilo Andrés Guzmán Camacho	**Profesional Especializado – Coordinador Grupo de Informática**
Miguel Fernando Diaz Peña	**Profesional Especializado – Coordinador Grupo Gestión de la Información**

SEGUIMIENTO A COMPROMISOS PREVIOS

Compromiso	Responsable	Observaciones

ORDEN DEL DÍA

1. Revisión estado entrega de información a la DIJIN y la SIC
2. Selección y aprobación de las acciones a seguir con el formateo y reinstalación de los servidores

DESARROLLO ORDEN DEL DÍA

1. Revisión estado entrega de información a la DIJIN y la SIC

El día 25/02/2022 se realizó la entrega de la información solicitada por la DIJIN, sobre los servidores afectados en el Invima, como parte de las pruebas del proceso penal que se inició ante la Fiscalía General de la Nación con denuncia penal NC_110016000050202201569.

El 28/02/2022 se realizó la entrega de la información solicitada por el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante, "GTIFSD") de la Superintendencia de Industria y Comercio - SIC, para el análisis forense a realizar sobre el incidente de seguridad de la información presentado en el Instituto.

El miércoles 2 de marzo de 2022 a través de correo electrónico el intendente Alejandro González Franco Suboficial Centro Cibernético Policial, en coordinación con el Mayor Félix Daniel Miranda Herrera responsable del despliegue del PMU Ciber Electoral, informa a la oficial de seguridad de la información del Invima que una vez recolectadas las muestras de software malicioso y de los servidores afectados, el centro cibernético policial ya inició el análisis y las actividades investigativas y forenses, por lo que no

van a requerir formación. Por lo anterior se puede disponer de los servidores. Se adjunta imagen del correo electrónico recibido:

RV: Informando requerimiento

Policía Nacional Dios y Patria

Buenas tardes, respetuosamente me permito informar a la señora NIDIA NAYIBE GONZÁLEZ PINZÓN Oficial de Seguridad de la Información de INVIMA, que una vez recolectadas las muestras de software malicioso y de los servidores afectados, el Centro Cibernético Policial ya inicio el análisis y demás actividades investigativas y forenses, por lo anterior ya no se requiere de algún otro requerimiento y ni ninguna interrupción por parte de ustedes en la activación de los servicios de INVIMA.

Por otra parte, esta decisión se toma en coordinación con mi Mayor FELIX DANIEL MIRANDA HERRERA, responsable del despliegue del PMU Ciber electoral.

Quedamos atentos a cualquier solicitud y a la información adicional que nos puedan aportar.

Atentamente,

Intendente
ALEJANDRO GONZÁLEZ FRANCO
Suboficial Centro Cibernético Policial
Teléfonos 5159700 Ext. 30428
www.policia.gov.co/dijin

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

Después de recibir la comunicación se determina esperar hasta el 15/03/2022 para dar inicio al proceso de formateo y reinstalación de los servidores, para dar espacio a cualquier requerimiento adicional por parte de la Superintendencia de Industria y Comercio - SIC.

2. Acciones para seguir con el formateo y reinstalación de los servidores

Luego de realizar un análisis de la información que puede ser vital para determinar hallazgos o recuperar información importante para la gestión de la seguridad y operatividad técnica, se decide seleccionar el servidor AZURE, para los correspondientes a los aplicativos SESUITE y BI, almacenándola de forma segura.

El proceso de formateo se realizará de forma ordenada informando a cada responsable de la información contenida en los servidores que estos se formatearán y reconfigurarán para su uso posterior en el marco de la recuperación de los servicios que presta el Invima. A continuación, se presenta una lista de los servidores físicos y virtuales que se formatearán:

No.	Nombre del Servidor	IP	Descripción
1	SRVVCLUSQL01	172.16.10.21	SERVIDOR SKYPE
2	SRVVCOLOMBIA	172.16.10.128	SERVIDOR JAGUAR
3	SRVVCONOF365	172.16.10.196	CONNECT OFFICE 365
4	SRVVKAS	172.16.10.98	SERVIDOR ANTIVIRUS KASPERSKY Y WSUS
5	SRVVDHCP01	172.16.10.61	SERVIDOR DHCP
6	SRVVMOSCU	172.16.10.102	SERVIDOR DE BASE DE DATOS ACCESS

No.	Nombre del Servidor	IP	Descripción
7	SRVVMYSQLWEB01	172.16.10.218	SERVIDOR WEB BASE DE DATOS – DESARROLLO
8	SRVVNGINXWEB01	172.16.10.52	SERVIDOR LIFERAY DE PRODUCCION
9	SRVVSAPIENS01	172.16.10.198	HV_SAPIENS
10	SRVVSERTRAMI	172.16.10.148	SERVIDOR TRAMITES EN LINEA
11	SRVVWEBDES03	172.16.10.219	SERVIDOR DESARROLLO PAGINA WEB - APP.INVIMA
12	SRVVWFLY01	172.16.10.80	SERVIDOR MASTER WILDFLY 8
13	SRVVWFLY9FV	172.16.10.65	WILDFLY
14	SRVV3MBX	172.16.10.177	SERVIDOR CORREO EXCHANGE MAILBOX
15	SRVVACCESO	172.16.10.79	SERVIDOR PARA EL CONTROL DE ACCESO
16	SRVVRELAY	172.16.80.15	MAQUINA RELAY CORREO LINUX
17	SRVVSESBDPRU	172.16.10.171	SERVIDOR SESUITE BD QA
18	SRVVSOLARW01	172.16.10.152	SERVIDOR MONITOREO SOLARWINDS
19	SRVVWHD	172.16.10.159	SERVIDOR SOLAR WINDS HELP DESK
20	SRVVSAPIENS01	172.16.10.198	SERVIDOR SQL SERVER
21	SRVVAPPEONPROD	172.16.10.55	APP APPEON Productivo
22	SRVV1CAS	172.16.10.175	SERVIDOR CAS DE CORREO EXCHANGE
23	SRVV3SESPRU	172.16.10.82	SERVIDOR DE PRUEBAS DE SESUITE
24	SRVVPAPERCUT	172.16.40.14	Administrador de Impresión – ERT
25	SRVVNAGIOS	172.16.10.197	Monitoreo Nagios Free
26	SRVVAULA	172.16.10.113	SERVIDOR DE SERVICIOS Y APLICACIONES WEB -AULA VIRTUAL
27	SRVVSESAPPRU	172.16.10.172	SERVIDOR DE APLICACIONES SESUITE DE PRUEBAS
28	SRVVMILANFL	172.16.10.194	SERVIDOR DE ARCHIVOS VIEJO
29	SRVVCOLOMBIA_CLON02	172.16.10.127	SERVIDOR JAGUAR
30	SRVV6SENT	172.16.10.36	MOBILE IRON - security.invima.gov.co
31	SVV5CORE	172.16.10.35	MOBILE IRON - mobile.invima.gov.co - CORE
32	SRVVSESAPPRO	172.16.10.181	SERVIDOR SESUITE APLICACIÓN DE PRODUCCION VERSION 2 2017
33	BOG1DMP-WVD-0	172.17.0.16	ESCRITORIOS VIRTUALES
34	BOG1DMP-WVD-1	172.17.0.8	ESCRITORIOS VIRTUALES
35	BOG1DMP-WVD-2	172.17.0.13	ESCRITORIOS VIRTUALES
36	BOG1DMP-WVD-3	172.17.0.6	ESCRITORIOS VIRTUALES
37	BOG1DMP-WVD-4	172.17.0.14	ESCRITORIOS VIRTUALES
38	BOG1DMP-WVD-5	172.17.0.12	ESCRITORIOS VIRTUALES
39	BOG1DMP-WVD-6	172.17.0.11	ESCRITORIOS VIRTUALES
40	BOG1DMP-WVD-7	172.17.0.9	ESCRITORIOS VIRTUALES
41	BOG1DMP-WVD-8	172.17.0.5	ESCRITORIOS VIRTUALES

42	BOG1DMP-WVD-9	172.17.0.17	ESCRITORIOS VIRTUALES
43	BOG1DMP-WVD-10	172.17.0.10	ESCRITORIOS VIRTUALES
No.	**Nombre del Servidor**	**IP**	**Descripción**
44	BOG1DMP-WVD-11	172.17.0.7	ESCRITORIOS VIRTUALES
45	BOG1DMP-WVD-12	172.17.0.15	ESCRITORIOS VIRTUALES
46	BOG1DMP-WVD-13	172.17.0.18	ESCRITORIOS VIRTUALES
47	BOG1DMP-WVD-14	172.17.0.4	ESCRITORIOS VIRTUALES
48	ControladorDeDominioAzureInvima	172.17.0.52-52.247.8.221	ESCRITORIOS VIRTUALES

Cada seis (6) meses se realizará una reunión para analizar y verificar la situación de la información resguardada y se tomarán las decisiones sobre mantenerla o eliminarla de acuerdo a la realidad del Instituto en ese momento. Sobre esta revisión periódica se dejarán actas para el respectivo seguimiento.

COMPROMISOS ADQUIRIDOS:		
Compromiso	**Responsable** *(Nombre –Cargo)*	**Fecha de Ejecución**
Realizar copias de seguridad a los servidores	Grupo de Soporte Tecnológico	25 de marzo del 2022
Formateo y reinstalación de los servidores	Grupo de Soporte Tecnológico	22 de marzo del 2022

SUSCRIBEN EL ACTA	
Nombre completo	**Firma**
María Margarita Jaramillo Pineda	M. Margarita Jaramillo P.
Juan Manuel Palacio Posada	
Eliodoro Rojas Ochoa	
Nidia Nayibe González Pinzón	
Camilo Andrés Guzmán Camacho	
Miguel Fernando Diaz Peña	
Visto Bueno Asesor Dirección General	Ok DG

Tema: COMITÉ TÉCNICO DE SEGUIMIENTO CONTINGENCIA

Lugar: Auditorio Invima

Fecha: 2022-03-16

Hora de inicio: 9:00 am | **Hora de finalización: 1:00 pm**

Acta No 1250-07-2022

ASISTENTES

Nombre Completo	Cargo
Juan Manuel Palacio Posada	Jefe de Oficina de Tecnología (OTI) / INVIMA
Miguel Fernando Díaz Peña	Coordinador del Grupo de Gestión de la Información / OTI /INVIMA
Camilo Andrés Guzmán Camacho	Coordinador del Grupo de Informática / OTI/ INVIMA
Eliodoro Rojas Ochoa	Coordinador del Grupo de Soporte Tecnológico/ Secretaría General (SG)/INVIMA
Cristhian Hernando Pinzón Camacho	Profesional Especializado Grupo de Soporte Tecnológico/ SG/ INVIMA
Freddy Holman Pulido Granados	Profesional Especializado Grupo de Soporte Tecnológico/ SG/ INVIMA
Jhorbis Ramses Rios Chaves	Contratista OTI/INVIMA
Nidia Nayibe González	Oficial de Seguridad de la Información / Oficina Asesora de Planeación/ INVIMA
Leidy Diana García Arevalo	Contratista OTI/INVIMA

SEGUIMIENTO A COMPROMISOS PREVIOS

Compromiso	Responsable	Observaciones
N/A	N/A	N/A

ORDEN DEL DÍA

1. Actividades realizadas para la contención del incidente tecnológico
2. Necesidades de la entidad para restablecer los servicios.

DESARROLLO ORDEN DEL DÍA

Siendo las 9:00 am en el auditorio del Invima, se reúnen los grupos de la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico de la Secretaria General, así como la Oficial de Seguridad de la Información de la Oficina Asesora de Planeación y demás personas que suscriben como intervinientes la presenta acta.

El objetivo de la reunión tiene el fin de evaluar y concluir con las alternativas para que el Jefe de la Oficina de Tecnologías de la Información y la Dirección General avancen en la intervención de las medidas idóneas para conjurar la crisis en la que se encuentran los sistemas de información e infraestructura tecnológica de la Entidad debido al incidente acontecido del pasado domingo 6 de febrero de 2022.

1. Como antecedente se contextualiza, dando lectura al anexo 1. Estado situacional.
2. En el uso de la palabra el Jefe de Tecnologías de la Información, procede a realizar un análisis de avance por cada sistema de información de conformidad al estado anteriormente indicado y en relación con las gestiones que con el recurso técnico y humano desde el Invima se han desarrollado

N.	NOMBRE SOFTWARE, SISTEMA DE INFORMACIÓN.	TIPO DE PLATAFORMA	LENGUAJE DE PROGRAMACION	SE TIENE EL CODIGO FUENTE?	% AVANCE DE RESTAURACION	RECURSO HUMANO DE LA ENTIDAD
1	SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO	ON PREMISE[1]	POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
2	SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA	ON PREMISE	POWER BUILDER	SI	0%	-
3	SOLUCIÓN WEB DE TRÁMITES EN LÍNEA	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
4	SISTEMA DE INFORMACIÓN DE SIVICOS MOVILES-CIS	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
5	SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS – SESUITE	ON PREMISE	PHP – JAVA	SAAS	0%	-
6	SOLUCIÓN WEB ADMIN	ON PREMISE	JAVA	SI	0%	
7	SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA	ON PREMISE	JAVA JSP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
8	SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA.	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
9	SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS.	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
10	SOLUCIÓN WEB CÓDIGO ÚNICO DE MEDICAMENTOS (CUM).	ON PREMISE	JAVA – POWER BUILDER	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
11	SOLUCIÓN WEB ACIDOS.	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
12	SOLUCIÓN WEB FARMACOVIGILANCIA.	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
13	SOLUCIÓN WEB TRANSPARENCIA	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
14	SOLUCIÓN WEB REGISTRO – RECAUDOS	ON PREMISE	Delphi JAVA	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
15	SOLUCIÓN WEB IVC/SOA.	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
16	SOLUCIÓN WEB REACTIVOVIGILANCIA.	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico
17	SOLUCIÓN WEB TECNOVIGILANCIA.	ON PREMISE	JAVA JEE7	SI	80%	Grupo de Informática Grupo de Soporte Tecnológico

[1] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

18	SOLUCIÓN WEB – IVC SOA PUERTOS.	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
19	SOLUCION WEB PROTOCOLOS DE INVESTIGACIÓN -	ON PREMISE	JAVA JEE7	SI	0%	Grupo de Informática Grupo de Soporte Tecnológico
20	SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS	ON PREMISE	JAVA JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
21	SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA	ON PREMISE	Java JEE7	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
22	SISTEMA DE INFORMACIÓN DE LABORATORIOS – SILAB	ON PREMISE	C#, TSQL, HTML5, CSS, TypeScript	NO	0%	-
23	PORTAL WEB INSTITUCIONAL	ON PREMISE	CMS LifeRay – Java	SI	50%	Grupo de Informática Grupo de Soporte Tecnológico
24	SOLUCIÓN WEB KAWAK	NUBE	N/A	NO	100%	Servicio SaaS externo
25	SOLUCION WEB ITSM ARANDA	NUBE	N/A	NO	100%	Servicio SaaS externo
26	HERRAMIENTA ANTIVIRUS KASPERSKY	ON PREMISE	N/A	NO	100%	Servicio Externo
27	SOLUCION WEB OFICINA VIRTUAL	ON PREMISE	MySQL y PHP	SI	90%	Grupo de Informática Grupo de Soporte Tecnológico
28	DIRECTORIO ACTIVO		N/A	NO	90%	Grupo de Soporte Tecnológico
29	CORREO ELECTRONICO	HIBRIDO	N/A	NO	70%	Grupo de Soporte Tecnológico
30	SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO)	NUBE	JAVA	En construcción	-	-
31	SISTEMA DE INFORMACION WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL – SIVICOS (PROYECTO EN DESARROLLO)	NUBE	JAVA	En construcción	-	-

3. Destaca el Jefe de Oficina de la Información que las actividades hasta aquí desglosadas están acompañadas de forma paralela con las actuaciones administrativas y jurídicas (de índole judicial) se vienen desarrollando con el apoyo de la Oficina Asesora Jurídica, la Oficial de Seguridad de la Información y la Coordinación del Grupo de Soporte Tecnológico:
   - Resolución 2022500000 del 9 de febrero de 2022 y la Resolución 2022500001 del 15 de febrero de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites.
   - Circular · 1000-001-22, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso – Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.

4. Adicionalmente se presenta como punto coyuntural que para efectos de poder continuar las labores de limpieza, formateo y vuelta a la operación de los servidores afectados, se debe tener en cuenta lo consignado en el Acta de Formateo de Servidores del Invima que se realizó el día inmediatamente anterior y que establece el que se puede realizar el formateo de los servidores afectados.

En consonancia, el comité técnico estudia las actividades que deben ser realizadas por terceros de la siguiente manera:

1. **Aseguramiento de la Infraestructura Tecnológica:** La entidad requiere el aseguramiento de la infraestructura para lograr la identificación y mitigación de brechas, minimizando riesgos de incidentes tecnológicos que puedan presentarse en la entidad.

   En este sentido, se encuentra que las actividades de aseguramiento requeridas por la entidad son las siguientes:

   - Hacking Ético: Este servicio va orientado a la identificación y explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información.
   - Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.

2. **Restablecimiento de Servicios y Sistemas:**

   - **Sistema de Información para laboratorios SILAB (SAMPLER):** este es el sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), y que permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad. Este sistema y toda su información se encuentra encriptada y se requiere de la instalación, configuración, parametrización, pruebas y salida a producción de este por parte del proveedor exclusivo del sistema y dueño del código fuente la empresa Caudales y Muestreos SAS.
   - **Sistema de Información Gestor Documental Sesuite – Correspondencia y PQRDS:** Este sistema de información contiene los módulos del Gestor Documental de la Entidad y de PQRDS y correspondencia. Es un sistema transversal en el cual reposa la información de los tramites solicitados en la entidad y que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima.
   - **Software Comisión Revisora:** El software de comisión revisora es un software que se integra técnicamente con el software de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de la Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los módulos que habían sido entregados por parte del contratista. Este software fue desarrollado y entregado al Invima por parte de Innpulsa mediante convenio de cooperación 180 de 2021.

3. **Buzones de correo electrónico:** Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. Teniendo en cuenta el incidente

presentado en la entidad, se encuentra comprometida la disponibilidad de recursos como los correos electrónicos configurados On-Premise afectando su funcionamiento, por lo tanto, se requiere que se creen nuevos correos electrónicos para su uso en los aplicativos de la entidad. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.

4. **Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos:** Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados, los servicios tecnológicos de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no hay capacidad de almacenamiento para subir y poner operativos todos los servicios. Por lo anterior se deben adquirir discos de estado sólido y mecánico para el restablecimiento de los servicios.

5. **Aumento (temporal) del ancho de banda para cargue de información y Debido** al incidente se propone por parte del comité técnico cargar en el espacio que brinda Microsoft Sharepoint la información que se encuentra en los servidores comprometidos para poder formatearlos y usarlos para el despliegue de sistemas y servicios en los mismos.

6. **Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión:** Así mismo se requiere del apoyo por parte del contratista ERT en el alistamiento de los computadores y servicios de impresión de la Entidad, en observancia que para cumplir con los cronogramas establecidos no se cuenta con personal suficiente en la entidad.

7. **Instalación de los proyectos de transformación digital en desarrollo y entregados:**

   - **Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo):** El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que una vez desarrollado permitirá ejecutar en línea las actividades misionales de los procesos "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los procedimientos que habían sido entregados por parte del contratista en las fases de desarrollo y codificación del proyecto como se observa en el siguiente cuadro:

PROCEDIMIENTO	% DE EJECUCIÓN DEL PROCEDIMIENTO	% DE EJECUCIÓN FRENTE A PROYECTO
aic-ast- pr001- procedimiento información y atención al ciudadano	100%	33,78%
Ass- ayc- pr001- procedimiento auditorias y certificaciones	100%	
Ass-rsa- pr001- procedimiento registro sanitario nuevo o renovación con estudio previo"	100%	

Ass-rsa- pr002- procedimiento de expedición de registros sanitarios, permisos sanitarios, notificaciones sanitarias sin estudio previo y control / revisión posterior	100%
Ass-rsa- pr003- procedimiento asignación de código de notificaciones sanitarias obligatorias, reconocimientos, renovaciones con firma digital y cambios asociados.	100%
Ass-rsa- pr011- procedimiento cancelación de registro sanitario y pérdida de ejecutoriedad	100%
Ass-rsa- gu029- guía para la elaboración de certificación de vo.bo. De exclusión de IVA con registro sanitario	100%
Ass-rsa-pr005-procedimiento modificación de registros sanitarios	100%
Ass-rsa-pr006-procedimiento certificación	100%
Ass-rsa-pr007-procedimiento autorización	100%
Ass-rsa-pr008-procedimiento visto bueno de importación	100%
Ass-rsa-pr010-procedimiento revisión de oficio	100%
Ass-rsa- pr013- procedimiento evaluación técnica científica	100%
Ass-rsa- pr014- procedimiento de evaluación y seguimiento a protocolos de investigación	100%
Ass-rsa- pr015- procedimiento para la aprobación previa de publicidad	100%
Ass-rsa- pr016- procedimiento de autorizaciones relacionadas con material es, objetos, envases y equipamientos destinad os a entrar en contacto con alimentos y bebidas para consumo humano	100%
Ass-rsa- pr019- procedimiento de autorización, cesión o modificación de uso exclusivo en alimentación y salud humana de organismos vivos modifica dos	100%
Ass-rsa- pr021- procedimiento autorización, renovación, modificación y/o cancelación de licencia de fabricación de derivado s de cannabis para uso medicinal y científico	100%
Ivc-vig- in043- instructivo para la inscripción de recurso humano que presta servicios de mantenimiento a equipos biomédicos	100%

Ivc-ins- pr004- procedimiento de inspección para importación y exportación de alimentos, materias primas o ingrediente secundario para la industria de alimentos en sitios de control de primera barrera, zonas francas y depósitos	100%	

- **Sistema de Información SIVICOS III (En desarrollo):** El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Con respecto a este sistema se deben instalar, configurar, parametrizar, hacer pruebas y salir a producción con los ambientes y desarrollos de los módulos que habían sido entregados por parte del contratista en la fase de Sistematización y Automatización de conformidad con el siguiente cuadro:

MÓDULOS ENTREGADOS SIVICOS	PORCENTAJE HITO
Integración Tramites en línea, Gestión de traza (Reconocimiento de requerimientos, modelado, diseño y simulación, Desarrollo e implementación, Realización de pruebas, Entrega de manual de usuario y técnico, Transferencia de conocimiento, Despliegue en ambiente de pruebas y producción)	11,42%
Módulo para programación, gestión de visitas y otras actividades de IVC	12,81%
Terminar e Integrar Certificado de inspección sanitaria 2 (CIS2), Actas paramétricas, Sincronizador IVC Actas paramétricas, e-Certificates Países Bajos y Traces, Farmacovigilancia	16,49%
Módulo de la Dirección de Operaciones Sanitarias	36,38%
Módulo de la Dirección de Responsabilidad Sanitaria	1,28%
Módulo de la Dirección de Medicamentos y Productos Biológicos	20,24%
Módulo Administrativo y de Gestión del Sistema de Información – Sección para Gestión de Usuarios, Claves, Roles y Permisos de Aplicación, Sección para Diseño y Creación Paramétrica de Reportes, Sección para Gestión de Parámetros de Fuentes IVC SOA e IVC SOA Puertos, Sección para Gestión y Parametrización de la Automatización	10,25%

Conclusiones:

En atención a los análisis realizados, al avance estimado, y a las actividades por desarrollar se concluye en la mesa las siguientes recomendaciones:

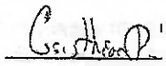
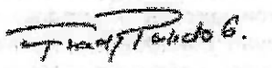
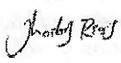
1. Teniendo en cuenta que ya han sido tomadas como parte del material probatorio las evidencias por la fiscalía, para efectos de los temas judiciales correspondientes a la acción penal que ha iniciado el Instituto, se hace procedente realizar el formateo y restauración de los servidores; situación que permitirá el almacenamiento correspondiente para la instalación, configuración, parametrización, pruebas y salida a producción de los sistemas de información SeSuite (Módulos de Gestión Documental y PQRDS/Correspondencia), Silab y el portal web.
2. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales concernientes a la contratación para la instalación, configuración, parametrización, pruebas, salida a producción y soporte técnico del Sistema de Información de los Laboratorios Silab, con el proveedor exclusivo y dueño del código fuente del sistema, que lo hacen titular de la obra Sampler, en la que se encuentra desarrollado el sistema de los laboratorios del Instituto.
3. De igual forma, realizar los análisis jurídicos, tecnológicos, financieros y contractuales para la contratación de la instalación, configuración, parametrización, pruebas y salida a producción del software SeSuite (Módulos Gestor Documental y Correspondencia/ PQRDS), con el proveedor que realizó los desarrollos concernientes al componente utilitario (Componente del Software SeSuite) y componente radicador (Componente del Módulo Correspondencia y PQRDS), que fueron desarrollados exclusivamente para el Invima y cuyo código fuente pertenece al canal autorizado de las tecnologías.
4. En atención a las sugerencias de los numerales 2 y 3, se recomienda que las mismas deben hacerse operativas en el menor tiempo posible, para dar continuidad a la interoperabilidad de los proyectos en desarrollo, para Sivicos y la Nueva Plataforma de Trámites y Servicios, así como la usabilidad del actual sistema de registros sanitarios y correspondencia y PQRDS.
5. Como acción de prevención se debe viabilizar la contratación de las actividades de aseguramiento de hacking ético y pruebas de seguridad, para la publicación de cada servicio de la entidad, y así mitigar la ejecución de riesgos asociados a este tipo de incidentes tecnológicos.
6. Dado que los sistemas de información están parametrizados con correos electrónicos en la infraestructura dispuesta por el Invima (On-Premise[2]) y que no se encuentran disponibles debido al incidente presentado, se requieren más licencias de correos en nube, que permitan la disponibilidad de los correos recibidos y enviados por los sistemas de información a los usuarios internos y externos de la Entidad; dicha suscripción debe realizarse con el mismo proveedor con el que se contrataron el uso de las licencias de correo en el servicio de Microsoft Office 365.
7. Dadas las necesidades de realizar copias de seguridad a los servidores y sistemas de información impactados, así como la adecuación para el alojamiento de los sistemas de información actualmente en desarrollo por parte del Instituto, se requiere garantizar el espacio de almacenamiento necesario, mediante la compra de discos de estado sólido para alojar esta información.
8. Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se sugiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft, para esto se recomienda aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, y así poder contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad. Adicionalmente, se requiere el acompañamiento técnico para el alistamiento de los computadores del Instituto y habilitación de los servicios de impresión, los cuales pueden ser brindados por el proveedor de apoyo a la gestión tecnológica.
9. Con el fin de habilitar el módulo de la comisión revisora entregado por Innpulsa, que también se encuentra afectado, se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción de este, para continuar su integración en el proyecto de Nueva Plataforma de Trámites y Servicios.

[2] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

10. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto, respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de desarrollo y codificación para la Nueva Plataforma de Trámites y Servicios, proyecto transversal a la transformación tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.
11. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de sistematización y automatización para el Proyecto Sivicos, proyecto transversal a la Transformación Tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.

COMPROMISOS ADQUIRIDOS:		
Compromiso	**Responsable** *(Nombre –Cargo)*	**Fecha de Ejecución**
Asociar estas medidas al Plan de contingencia.	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022
Reunirse con las diferentes dependencias de la Entidad para la socialización de estas medidas (Grupo de Gestión Contractual, Secretaria General, Oficina Asesora Planeación, Dirección General)	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022
Solicitar cotizaciones a los proveedores identificados	Oficina Tecnologías de la Información – Grupo de Soporte Tecnológico	Marzo de 2022

SUSCRIBEN EL ACTA	
Nombre completo	**Firma**
Juan Manuel Palacio Posada	
Miguel Fernando Díaz Peña	
Camilo Andrés Guzmán Camacho	
Eliodoro Rojas Ochoa	

Cristhian Hernando Pinzón Camacho	
Freddy Holman Pulido Granados	
Jhorbis Ramses Rios Chavez	
Nidia Nayibe González Pinzón	
Leidy Diana García Arevalo	

invima	GESTIÓN DIRECTIVA		DIRECCIONAMIENTO ESTRATÉGICO	
	FORMATO DE ACTA			
	Código: GDI-DIE-FM001	Versión: 01	Fecha de Emisión: 08/02/2019	Página 1 de 22

El tratamiento de los datos personales se realiza de acuerdo a los requerimientos de la ley 1581 de 2012 y a lo establecido en la política de tratamiento y Protección de datos personales GDI-DIE-PL018 disponible en www.invima.gov.co

Tema: Comité Asesor de Contratación

Lugar: Virtual

Acta No 011

Fecha: 04 de abril de 2022.

Hora de inicio: 10:00 a.m. **Hora de finalización:** 7:00 p.m.

ASISTENTES – MIEMBROS DEL COMITÉ ASESOR DE CONTRATACIÓN

Nombre Completo	Cargo
Roy Luis Galindo Wehdeking	Secretario General.
Larry Sadit Álvarez Morales	Asesor de la Dirección General
María Margarita Jaramillo	Jefe de la Oficina Asesora Jurídica.
Daladier Medina Niño	Jefe de Oficina Asesora de Planeación
Marlon Simón Ortega Ordosgoitia	Asesor de la Dirección General con delegación de funciones del Grupo Financiero y Presupuestal.
Norma Constanza García Ramírez	Jefe de la Oficina de control interno.
Luis Alejandro Delgado España	Coordinador del Grupo de Gestión Administrativa.
María Margarita Cárdenas Cortes	Asesora de la Dirección General con Delegación de Funciones de Coordinación del Grupo de Gestión Contractual.

ASISTENTES – INVITADOS

Nombre Completo	Cargo
Saaibi Arenas Moreno	Oficina de Tecnologías de la Información
Sandra Patricia Bello	Oficina de Tecnologías de la Información
Leidy Diana Garcia Arevalo	Oficina de Tecnologías de la Información
Eliodoro Rojas Ochoa	Coordinador de Soporte Tecnologico
Juan Manuel Palacio	Jefe de la Oficina de la Tecnologías de la Información
Jhonny Fabricio Tocua	Oficina de Tecnologías de la Información

María Laura Olivella Dangond	Contratista – Grupo de Gestión Contractual
María José Amaya López	Contratista – Grupo de Gestión Contractual
Karla Mayelis Mengual Redondo	Contratista – Grupo de Gestión Contractual
Marta Mengual Quintero	Contratista – Grupo de Gestión Contractual
Dany Daniela Valdez Orozco	Contratista – Grupo de Gestión Contractual
Astrid Lorena Bernal Rincon	Grupo de Gestión Contractual
Elsa Stefania Valderrama Ovalle	Oficina Asesora de Planeación

ORDEN DEL DÍA

El comité se desarrolla de manera virtual, con el siguiente orden del día:

1. Instalación del Comité Asesor de Contratación y verificación del Quorum.
2. Presentación de temas objeto de comité, votos y recomendaciones.

DESARROLLO ORDEN DEL DÍA

1.INSTALACIÓN DEL COMITÉ ASESOR DE CONTRATACIÓN Y VERIFICACIÓN DEL QUORUM.

Mediante correo electrónico (enviado el viernes 01/04/2022), se convocó a los miembros con voz y voto del Comité Asesor de Contratación para que realizaran la votación del día 04/04/2022, de conformidad con los artículos 3° y 6° de la Resolución No. 2020021292 del 30 de junio de 2020 "por medio de la cual se adoptan disposiciones acerca del Comité Asesor de Contratación del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA y derogan las Resoluciones No. 2016000364 del 8 de enero y 2016014483 del 26 de abril ambas 2016."

El correo electrónico fue enviado a los siguientes destinatarios:

Roy Luis Galindo Wehdeking rgalindow@invima.gov.co
Larry Sadit Álvarez Morales lalvarezm@invima.gov.co
Daladier Medina Niño dmedinan@invima.gov.co
María Margarita Jaramillo Pineda mjaramillop@invima.gov.co
Marlon Simón Ortega Ordosgoitia mortegao@invima.gov.co
Norma Constanza García Ramírez ngarciar@invima.gov.co
Luis Alejandro Delgado España ldelgadoe@invima.gov.co
María Margarita Cárdenas Cortes mcardenasc@invima.gov.co
Juan Manuel Palacio- jpalaciop@invima.gov.co
Saaibi Arenas Moreno sarenasm@invima.gov.co
Leidy Diana Garcia Arevalo- lgarciaa@invima.gov.co

Sandra Patricia Bello- sbellov@invima.gov.co
Maria Laura Olivella Dangond – molivellad@invima.gov.co
Karla Mayelis Mengual Redondo - kmengualr@invima.gov.co
Eliodoro Rojas Ochoa- erojaso@invima.gov.co
Jhonny Fabricio Tocua Jimenez -jtocuaj@invima.gov.co
María José Amaya López-mamayal@invima.gov.co
Astrid Lorena Bernal Rincon -abernalri@invima.gov.co
Elsa Stefania Valderrama Ovalle- evalderramao@invima.gov.co
Valeria Isabel Saurith -vsaurithl@invima.gov.co

2. PRESENTACIÓN DE TEMAS OBJETO DE COMITÉ, VOTOS Y RECOMENDACIONES:

1. Trámite contractual – Aseguramiento de la Infraestructura Tecnológica.
2. Trámite contractual – El Sistema De Información De Laboratorios (SILAB)
3. Trámite contractual – SOFTWARE GESTOR DOCUMENTAL, COMPONENTES Y MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS Microsoft Adición Contrato 624 De 2022
4. Trámite contractual – MICROSOFT ADICIÓN CONTRATO 624 DE 2022
5. Trámite contractual -Adquirir 18 Discos De 7.68 Tb
6. Trámite contractual -Resciliación Contrato *No 469-2022 Caudales & Muestreos S.A.S*

Es este sentido una vez iniciado el comité se recibieron los siguientes votos:

1.Tema: ***Aseguramiento de la Infraestructura Tecnológica****:*

1	***Solicitud***	***Trámite contractual – Aseguramiento de la Infraestructura Tecnológica.***
	Objeto:	***PRESTAR SERVICIOS ESPECIALIZADOS PARA EL ACOMPAÑAMIENTO EN EL DESARROLLO DE ACTIVIDADES DE ASEGURAMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL INVIMA, AFECTADA POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE***
	Plazo de ejecución inicial	Noventa (90) días, previo el cumplimiento de los requisitos legales de perfeccionamiento del presente contrato.
	Valor inicial	***DOSCIENTOS NOVENTA Y OCHO MILLONES TRES MIL DOSCIENTOS CINCUENTA Y UN PESÓS M/CTE ($298.003.251.oo) incluido IVA y demás impuestos, tasas y contribuciones de ley a que haya lugar.***
	Modalidad:	***Contratación Directa***
	Área interesada:	*Grupo de Informática– Oficina de Tecnologías de la Información*
	Abogado	*Jorge Andrés Galindo Barrios – jgalindob@invima.gov.co*
	Técnico encargado	*Leidy Diana Garcia Arevalo- lgarciaa@invima.gov.co*

	Documentos adjuntos	*Trámite contractual* *Presentación, CDP y estudios previos*
	Votos	*Voto de la doctora María Margarita Cárdenas Cortes presentado mediante correo electrónico mcardenasc@invima.gov.co de fecha lunes 04/04/2022 14:48 p.m., manifestando lo siguiente:* *"Buenas tardes. De conformidad con los temas sometidos a conocimiento por parte de este Comité en la fecha señalada, me permito dar las siguientes recomendaciones* • *Votación Tema 1: Recomiendo al ordenador del gasto seguir adelante con el trámite previsto para esta necesidad, la cual debe gestionarse en el marco de la urgencia manifiesta decretada por la Entidad. Esta recomendación se realiza de conformidad con la justificación presentada por el área técnica".* *Voto del doctor Marlon Simón Ortega Ordosgoitia presentado mediante correo electrónico sortegao@invima.gov.co de fecha martes 04/04/2022 15:04 p.m., manifestando lo siguiente:* *Cordial saludo miembros del Comité de Contratación,* *"En atención al comité de contratación de fecha 4 de abril de 2022, el cual fue enviado el 1 de abril de 2022, me permito manifestar lo siguiente a cada uno de los puntos citados, así,* • *me permito recomendar al Sr. Ordenador del Gasto continuar con el trámite contractual, es importante hacer la mención que mi recomendación está dada de acuerdo con la justificación dada por el área técnica solicitante y en virtud del ataque cibernético sufrido por la entidad, la cual hace parte de la presente citación y la revisión legal de parte del Grupo de Gestión Contractual".* *Voto de la doctora María Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., manifestando lo siguiente:* *Buenas tardes para todos los miembros del Comité.* *"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy:* • *Recomiendo continuar con los trámites contractuales en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta".*

Voto del doctor Daladier Medina Niño presentado mediante correo electrónico dmedinan@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

"Buena tarde Con el presente, de manera atenta y atendiendo la citación realizada para el comité del día de hoy, frente a los diferentes temas propuestos, procedo a dar respuesta de la siguiente manera:

- *"De acuerdo a la información presentada en el actual comité del día 04/04/2022, recomiendo continuar con el Trámite contractual de "PRESTAR SERVICIOS ESPECIALIZADOS PARA EL ACOMPAÑAMIENTO EN EL DESARROLLO DE ACTIVIDADES DE ASEGURAMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL INVIMA, AFECTADA POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE".*
  Dicha recomendación se da únicamente con base en la necesidad presentada por el área interesada, en atención a las respectivas justificaciones argumentadas; teniendo en cuenta la información allegada o presentada por el grupo contractual a través del presente medio, sin tener conocimiento de los demás detalles del proceso. Adicionalmente, la presente recomendación se atiene a lo dispuesto en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta."

Voto del doctor Larry Sadit Álvarez Morales presentado mediante correo electrónico lalvarezm@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

	PROCESO	OBJETO	RECOMENDACIÓN
1	Contratación Directa	Prestar servicios especializados para el acompañamiento en el desarrollo de actividades de aseguramiento de la infraestructura tecnológica del Invima, afectada por el incidente de seguridad de la información generado por el ataque de un RANSOMWARE	SE RECOMIENDA CONTINUAR CON EL TRÁMITE DEL PROCESO.

Observaciones	N/A

De conformidad a lo anterior, los miembros del Comité Asesor de Contratación ***RECOMIENDAN*** *seguir adelante con el tema contractual antes expuesto.*

2. ***Tema: Trámite contractual*** *–SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB).*

2	***Solicitud***	***Trámite contractual*** *–SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB).*
	Objeto:	*INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN, GARANTIZANDO EL SOPORTE FUNCIONAL PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER, AFECTADO POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE.*
	Plazo de ejecución inicial	Treinta (30) días, previo el cumplimiento de los requisitos legales de perfeccionamiento del presente contrato.
	Solicitud de trámite	***Contratación Directa***
	Área interesada:	*Grupo de Informática– Oficina de Tecnologías de la Información*
	Abogado	*Karla Mayelis Mengual Redondo - kmengualr@invima.gov.co*
	Área Técnica encargada	*Saaibi Arenas Moreno sarenasm@invima.gov.co*
	Documentos adjuntos	*Trámite contractual Presentación, CDP, Estudios Previos*
	Votos	*Voto de la doctora María Margarita Cárdenas Cortes presentado mediante correo electrónico mcardenasc@invima.gov.co de fecha lunes 04/04/2022 14:48 p.m., manifestando lo siguiente:* *"Buenas tardes. De conformidad con los temas sometidos a conocimiento por parte de este Comité en la fecha señalada, me permito dar las siguientes recomendaciones* • *Votación Tema 2: Recomiendo al ordenador del gasto seguir adelante con el trámite previsto para esta necesidad, la cual debe gestionarse en el marco de la urgencia manifiesta decretada por la Entidad. Esta recomendación se realiza de conformidad con la justificación presentada por el área técnica".*

Voto del doctor Marlon Simón Ortega Ordosgoitia presentado mediante correo electrónico sortegao@invima.gov.co de fecha martes 04/04/2022 15:04 p.m., manifestando lo siguiente:
Cordial saludo miembros del Comité de Contratación,

"En atención al comité de contratación de fecha 4 de abril de 2022, el cual fue enviado el 1 de abril de 2022, me permito manifestar lo siguiente a cada uno de los puntos citados, así,

- *me permito recomendar al Sr. Ordenador del Gasto continuar con el trámite contractual, es importante hacer la mención que mi recomendación está dada de acuerdo con la justificación dada por el área técnica solicitante y en virtud del ataque cibernético sufrido por la entidad, la cual hace parte de la presente citación y la revisión legal de parte del Grupo de Gestión Contractual, como también a lo relacionado en el punto 6 del presente comité".*

Voto de la doctora María Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., manifestando lo siguiente:

Buenas tardes para todos los miembros del Comité.

"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy:

- *Considero viable y necesario continuar con los trámites contractuales conforme a lo establecido en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta".*

Voto del doctor Daladier Medina Niño presentado mediante correo electrónico dmedinan@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

"Buena tarde Con el presente, de manera atenta y atendiendo la citación realizada para el comité del día de hoy, frente a los diferentes temas propuestos, procedo a dar respuesta de la siguiente manera:

> *"De acuerdo a la información presentada en el actual comité del día 04/04/2022, recomiendo continuar con el Trámite contractual de "INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN, GARANTIZANDO EL SOPORTE FUNCIONAL PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER, AFECTADO POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE". Dicha recomendación se da únicamente con base en la necesidad presentada por el área interesada, en atención a las*

		respectivas justificaciones argumentadas; teniendo en cuenta la información allegada o presentada por el grupo contractual a través del presente medio, sin tener conocimiento de los demás detalles del proceso. Adicionalmente, la presente recomendación se atiene a lo dispuesto en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta..” *Voto del doctor Larry Sadit Álvarez Morales presentado mediante correo electrónico lalvarezm@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:*

	PROCESO	***OBJETO***	***RECOMENDACIÓN***
2	*Contratación Directa*	*Instalar, configurar, parametrizar, realizar pruebas y puesta en producción, garantizando el soporte funcional para el sistema de información de laboratorios (SILAB) basado en el software SAMPLER, afectado por el incidente de seguridad de la información generado por el ataque de un RANSOMWARE.*	*SE RECOMIENDA CONTINUAR CON EL TRÁMITE DEL PROCESO.*

	Observaciones	*No aplica*

*De conformidad a lo anterior, los miembros del Comité Asesor de Contratación **RECOMIENDAN** seguir adelante con el tema contractual antes expuesto.*

3. *Tema: **Trámite contractual** – SOFTWARE GESTOR DOCUMENTAL, COMPONENTES Y MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS:*

3	***Solicitud***	***Trámite contractual** – SOFTWARE GESTOR DOCUMENTAL, COMPONENTES Y MÓDULOS SESUITE Y CORRESPONDENCIA - PQRDS*

57

	Objeto:	*INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN DEL SOFTWARE GESTOR DOCUMENTAL, COMPONENTES Y MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS PARA EL INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS – INVIMA AFECTADOS POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE*
	Plazo de ejecución inicial	Treinta (30) días, para hacer entrega de los compotentes y modilos SESUITE, *CORRESPONDENCIA –PQRDS configurados parametrizados e instalados y en funcionamiento de la plataforma disponible en ambiente de producción una vez cumplidos los requisitos legales del contrato.*
	Solicitud de trámite	***Contratación Directa***
	Área interesada:	*Grupo de Informática– Oficina de Tecnologías de la Información*
	Abogado	*María José Amaya López-mamayal@invima.gov.co*
	Área Técnica encargada	*Sandra Patricia Bello- sbellov@invima.gov.co*
	Documentos adjuntos	*Trámite contractual Presentación, CDP, Estudios Previos*
	Votos	*Voto de la doctora María Margarita Cárdenas Cortes presentado mediante correo electrónico mcardenasc@invima.gov.co de fecha lunes 04/04/2022 14:48 p.m., manifestando lo siguiente:* *"Buenas tardes. De conformidad con los temas sometidos a conocimiento por parte de este Comité en la fecha señalada, me permito dar las siguientes recomendaciones* • *Votación Tema 3: Recomiendo al ordenador del gasto seguir adelante con el trámite previsto para esta necesidad, la cual debe gestionarse en el marco de la urgencia manifiesta decretada por la Entidad. Esta recomendación se realiza de conformidad con la justificación presentada por el área técnica".* *Voto del doctor Marlon Simón Ortega Ordosgoitia presentado mediante correo electrónico sortegao@invima.gov.co de fecha martes 04/04/2022 15:04 p.m., manifestando lo siguiente:* *Cordial saludo miembros del Comité de Contratación,* *"En atención al comité de contratación de fecha 4 de abril de 2022, el cual fue enviado el 1 de abril de 2022, me permito manifestar lo siguiente a cada uno de los puntos citados, así,*

- *me permito recomendar al Sr. Ordenador del Gasto continuar con el trámite contractual, es importante hacer la mención que mi recomendación está dada de acuerdo con la justificación dada por el área técnica solicitante y en virtud del ataque cibernético sufrido por la entidad, la cual hace parte de la presente citación y la revisión legal de parte del Grupo de Gestión Contractual".*

Voto de la doctora María Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., manifestando lo siguiente:

Buenas tardes para todos los miembros del Comité.

"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy:

- *Sobre este contrato, si bien entiendo la mejor opción que tenemos es continuar con el proceso contractual y adelantarlo prontamente, tengo tres observaciones que agradezco sean tenidas en cuenta en la ejecución y supervisión del contrato: 1) El plazo de ejecución a 30 días no responde a las necesidades actuales del Invima, por lo que sugiero que atendiendo la situación y lo establecido en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta, se revise este plazo frente a las características del software y las necesidades apremiantes de la entidad. 2) Con esta contingencia se ha evidenciado que en las condiciones en las que se configuró previamente este software, los MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS no se han podido restablecer ni han brindado soluciones prácticas para la entidad. En este sentido, más allá de instalar y configurar lo mismo que ya teníamos, sugiero que se analice de manera preventiva desde el INVIMA, cómo pueden mejorar las condiciones de funcionamiento de este aplicativo para garantizar la seguridad en la gestión documental del Instituto frente a eventos como el que ya estamos atravesando. 3) La instalación y puesta en marcha debe ser óptima para el Invima, recuperando la estabilidad del sistema de información y permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto. No es el instituto el que debe ajustarse a las condiciones del contratista.".*

Voto del doctor Daladier Medina Niño presentado mediante correo electrónico dmedinan@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

"Buena tarde Con el presente, de manera atenta y atendiendo la citación realizada para el comité del día de hoy, frente a los diferentes temas propuestos, procedo a dar respuesta de la siguiente manera:

"De acuerdo a la información presentada en el actual comité del día 04/04/2022, recomiendo continuar con el Trámite contractual de "INSTALAR, CONFIGURAR, PARAMETRIZAR, REALIZAR PRUEBAS Y PUESTA EN PRODUCCIÓN DEL SOFTWAREGESTOR DOCUMENTAL, COMPONENTES Y MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS PARA EL INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS – INVIMA AFECTADOS POR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN GENERADO POR EL ATAQUE DE UN RANSOMWARE". Dicha recomendación se da únicamente con base en la necesidad presentada por el área interesada, en atención a las respectivas justificaciones argumentadas; teniendo en cuenta la información allegada o presentada por el grupo contractual a través del presente medio, sin tener conocimiento de los demás detalles del proceso. Adicionalmente, la presente recomendación se atiene a lo dispuesto en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta y coadyuvo las recomendaciones realizadas por la Dra. Jaramillo" al presente proceso, especialmente el plazo de ejecución de 30 días, diapositiva 7.

Voto del doctor Larry Sadit Álvarez Morales presentado mediante correo electrónico lalvarezm@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

	PROCESO	***OBJETO***	***RECOMENDACIÓN***
3	Contratación Directa	Instalar, configurar, parametrizar, realizar pruebas y puesta en producción del software gestor documental, componentes y módulos SESUITE y correspondencia - PQRDS para el instituto nacional de vigilancia de medicamentos y alimentos – Invima afectados por el incidente de seguridad de la información generado por el ataque de un RANSOMWARE	SE RECOMIENDA CONTINUAR CON EL TRÁMITE DEL PROCESO.

	Observaciones	*Voto de la doctora Maria Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., presento observaciones a este trámite contractual sin embargo recomienda el seguir con el tramite contractual vota, manifestando lo siguiente:* *Buenas tardes para todos los miembros del Comité.* *"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy* *Sobre este contrato, si bien entiendo la mejor opción que tenemos es continuar con el proceso contractual y adelantarlo prontamente, tengo tres observaciones que agradezco sean tenidas en cuenta en la ejecución y supervisión del contrato: 1) El plazo de ejecución a 30 días no responde a las necesidades actuales del Invima, por lo que sugiero que atendiendo la situación y lo establecido en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta, se revise este plazo frente a las características del software y las necesidades apremiantes de la entidad. 2) Con esta contingencia se ha evidenciado que en las condiciones en las que se configuró previamente este software, los MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS no se han podido restablecer ni han brindado soluciones prácticas para la entidad. En este sentido, más allá de instalar y configurar lo mismo que ya teníamos, sugiero que se analice de manera preventiva desde el INVIMA, cómo pueden mejorar las condiciones de funcionamiento de este aplicativo para garantizar la seguridad en la gestión documental del Instituto frente a eventos como el que ya estamos atravesando. 3) La instalación y puesta en marcha debe ser óptima para el Invima, recuperando la estabilidad del sistema de información y permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto. No es el instituto el que debe ajustarse a las condiciones del contratista.* *De acuerdo a las observaciones dela Dra. Maria Margarita Jaramillo, la parte técnica, según correo electrónico por la Contratista Leidy Diana Garcia de la Oficina de Tecnología de la Información responde a cada uno de los interrogantes:* ***1) Sobre este contrato, si bien entiendo la mejor opción que tenemos es continuar con el proceso contractual y adelantarlo prontamente, tengo tres observaciones que agradezco sean tenidas en cuenta en la ejecución y supervisión del contrato:*** ***1) El plazo de ejecución a 30 días no responde a las necesidades actuales del Invima, por lo que sugiero que atendiendo la situación y lo establecido en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta, se revise este plazo frente a las características del software y las necesidades apremiantes de la entidad.***

Respuesta: De acuerdo a la observación referente al plazo de ejecución de los 30 días, atentamente se informa que, revisando con el contratista, las actividades que deben realizar contemplan el tiempo indicado ya que comprenden:

- Preparación y validación de los pre-requisitos de hardware y software para la instalación del software documental SeSuite, componentes y módulos Sesuite y correspondencia-PQRDS, así como verificación de conectividad y recursos de red, puertos y reglas de seguridad.
- Configuraciones de conexión del software sesuite, base de datos, directorios controlados para el almacenamiento de documentos, configuración de sincronización con directorio activo y de prueba del servidor de correo para notificaciones del sistema, así como inicialización de servicios.
- Verificación funcional del software SeSuite, flujos, componentes y Módulos configurados y parametrizados, corrección y ajustes de incidencias presentadas, así como de la verificación de los requisitos tecnológicos para el despliegue en ambiente de producción en el servidor dispuesto en la plataforma del Invima.

Dadas las actividades técnicas en mención, se requiere el tiempo de ejecución estipulado en el proceso.

2) Con esta contingencia se ha evidenciado que en las condiciones en las que se configuró previamente este software, los MÓDULOS SESUITE Y CORRESPONDENCIA -PQRDS no se han podido restablecer ni han brindado soluciones prácticas para la entidad. En este sentido, más allá de instalar y configurar lo mismo que ya teníamos, sugiero que se analice de manera preventiva desde el INVIMA, cómo pueden mejorar las condiciones de funcionamiento de este aplicativo para garantizar la seguridad en la gestión documental del Instituto frente a eventos como el que ya estamos atravesando.

Respuesta: De acuerdo a la observación referente a mejorar condiciones de funcionamiento de este aplicativo, atentamente se informa que en este proceso de contratación no contempla mejoras solo instalación, configuración, parametrización del Software documental módulos Sesuite y correspondencia- PQRDS, posteriormente se realizará la contratación de ajustes de mejoras del software, en el cual se contemplará lo solicitado.
Este proceso que se está realizando de acuerdo a la urgencia manifiesta, solo contempla la instalación del software en su última versión.

3) La instalación y puesta en marcha debe ser óptima para el Invima, recuperando la estabilidad del sistema de información y permitiendo la gestión oportuna de los documentos, la

		correspondencia y las PQRDS del Instituto. No es el instituto el que debe ajustarse a las condiciones del contratista. **Respuesta:** De acuerdo a la observación referente a la instalación y puesta en marcha de manera óptima del software, atentamente les informo que revisando con el contratista, las actividades que se deben realizar contemplan el tiempo indicado de los 30 días y de acuerdo al cronograma revisado con el equipo técnico de la OTI se valida que este tiempo de ejecución es necesario para garantizar la instalación, configuración, parametrización, pruebas y puesta en producción del software.

4. Tema: **MICROSOFT ADICIÓN CONTRATO 624 DE 2022**

4	***Solicitud***	***Trámite contractual* – MICROSOFT ADICIÓN CONTRATO 624 DE 2022**
	Objeto:	RENOVACION DE SUSCRIPCIONES DE OFFICE 365, ADQUISICÓN Y ACTUALIZACIÓN DE OTROS PRODUCTOS MICROSOFT PARA INSTITUTO NACIONAL DE VIGILANCIA DE MEDIAMENTOS Y ALIMENTOS INVIMA.
	Plazo de ejecución inicial	*2022*
	Solicitud de trámite	***Contratación Directa***
	Área interesada:	*Grupo de Informática– Oficina de Tecnologías de la Información*
	Abogado	Astrid Lorena Bernal Rincon -*abernalri@invima.gov.co*
	Área Técnica encargada	*Jhonny Fabricio Tocua Jimenez -itocuaj@invima.gov.co* *Leidy Diana Garcia Arevalo- lgarciaa@invima.gov.co*
	Documentos adjuntos	*Trámite contractual Presentación, CDP, Estudios Previos*
	Votos	*Voto de la doctora María Margarita Cárdenas Cortes presentado mediante correo electrónico mcardenasc@invima.gov.co de fecha lunes 04/04/2022 14:48 p.m., manifestando lo siguiente:* *"Buenas tardes. De conformidad con los temas sometidos a conocimiento por parte de este Comité en la fecha señalada, me permito dar las siguientes recomendaciones* • *Votación Tema 4: Recomiendo al ordenador del gasto seguir adelante con el trámite previsto para esta necesidad, la cual debe*

gestionarse en el marco de la urgencia manifiesta decretada por la Entidad. Esta recomendación se realiza de conformidad con la justificación presentada por el área técnica.".

Voto del doctor Marlon Simón Ortega Ordosgoitia presentado mediante correo electrónico sortegao@invima.gov.co de fecha martes 04/04/2022 15:04 p.m., manifestando lo siguiente:
Cordial saludo miembros del Comité de Contratación,

"En atención al comité de contratación de fecha 4 de abril de 2022, el cual fue enviado el 1 de abril de 2022, me permito manifestar lo siguiente a cada uno de los puntos citados, así,

- *me permito recomendar al Sr. Ordenador del Gasto continuar con el trámite contractual, es importante hacer la mención que mi recomendación está dada de acuerdo con la justificación dada por el área técnica solicitante y en virtud del ataque cibernético sufrido por la entidad, la cual hace parte de la presente citación y la revisión legal de parte del Grupo de Gestión Contractual."*

Voto de la doctora María Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., manifestando lo siguiente:

Buenas tardes para todos los miembros del Comité.

"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy:

- *Recomiendo continuar con los trámites contractuales en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta".*

Voto del doctor Daladier Medina Niño presentado mediante correo electrónico dmedinan@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

"Buena tarde Con el presente, de manera atenta y atendiendo la citación realizada para el comité del día de hoy, frente a los diferentes temas propuestos, procedo a dar respuesta de la siguiente manera:

- *"De acuerdo a la información presentada en el actual comité del día 04/04/2022, recomiendo continuar con el Trámite contractual de ADICIÓN CONTRATO 624 DE 2022 "RENOVACION DE SUSCRIPCIONES DE OFFICE 365, ADQUISICÓN Y ACTUALIZACIÓN DE OTROS PRODUCTOS MICROSOFT PARA INSTITUTO NACIONAL DE VIGILANCIA DE MEDIAMENTOS Y ALIMENTOS INVIMA". Dicha*

		recomendación se da únicamente con base en la necesidad presentada por el área interesada, en atención a las respectivas justificaciones argumentadas; teniendo en cuenta la información allegada o presentada por el grupo contractual a través del presente medio, sin tener conocimiento de los demás detalles del proceso. Adicionalmente, la presente recomendación se atiene a lo dispuesto en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta." *Voto del doctor Larry Sadit Álvarez Morales presentado mediante correo electrónico lalvarezm@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:*
	Observaciones	*No aplica*

	PROCESO	***OBJETO***	***RECOMENDACIÓN***
4	Contratación Directa	Renovación de suscripciones de office 365, adquisición y actualización de otros productos Microsoft para instituto nacional de vigilancia de medicamentos y alimentos Invima	SE RECOMIENDA CONTINUAR CON EL TRÁMITE DEL PROCESO.

5. Tema: **ADQUIRIR 18 DISCOS DE 7.68 TB**

5	***Solicitud***	***Trámite contractual* – ADQUIRIR 18 DISCOS DE 7.68 TB**
	Objeto:	ADQUIRIR 18 DISCOS DE 7.68 TB CADA UNO, PARA LOGRAR UNA CAPACIDAD DE ALMACENAMIENTO EFECTIVA DE 103.52 TB Y USABLE DE 98.45TB, PARA LA CAJA DE DISCOS IBM FLASHSYSTEM 5000 MODELO: 2072-3N4 SERIAL: 781K1Y6; Y LOS SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN, SOPORTE Y GARANTÍA DE HARDWARE POR 3 AÑOS BAJO EL MODELO 7X24X4 IBM STORAGE.
	Plazo de ejecución inicial	Treinta (30) días, previo el cumplimiento de los requisitos legales de perfeccionamiento del presente contrato.

61

Solicitud de trámite	***Contratación Directa***
Área interesada:	*Grupo de Informática– Oficina de Tecnologías de la Información*
Abogado	Valeria Isabel Saurith López - *vsaurithl@invima.gov.co*
Área Técnica encargada	*Eliodoro Rojas Ochoa- erojaso@invima.gov.co*
Documentos adjuntos	*Trámite contractual Presentación, CDP, Estudios Previos*
Votos	*Voto de la doctora María Margarita Cárdenas Cortes presentado mediante correo electrónico mcardenasc@invima.gov.co de fecha lunes 04/04/2022 14:48 p.m., manifestando lo siguiente:* *"Buenas tardes. De conformidad con los temas sometidos a conocimiento por parte de este Comité en la fecha señalada, me permito dar las siguientes recomendaciones* • *Votación Tema 5: Recomiendo al ordenador del gasto seguir adelante con el trámite previsto para esta necesidad, la cual debe gestionarse en el marco de la urgencia manifiesta decretada por la Entidad. Esta recomendación se realiza de conformidad con la justificación presentada por el área técnica.".* *Voto del doctor Marlon Simón Ortega Ordosgoitia presentado mediante correo electrónico sortegao@invima.gov.co de fecha martes 04/04/2022 15:04 p.m., manifestando lo siguiente:* *Cordial saludo miembros del Comité de Contratación,* *"En atención al comité de contratación de fecha 4 de abril de 2022, el cual fue enviado el 1 de abril de 2022, me permito manifestar lo siguiente a cada uno de los puntos citados, así,* • *me permito recomendar al Sr. Ordenador del Gasto continuar con el trámite contractual, es importante hacer la mención que mi recomendación está dada de acuerdo con la justificación dada por el área técnica solicitante y en virtud del ataque cibernético sufrido por la entidad, la cual hace parte de la presente citación y la revisión legal de parte del Grupo de Gestión Contractual."* *Voto de la doctora María Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., manifestando lo siguiente:* *Buenas tardes para todos los miembros del Comité.*

"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy:

- *Considero necesario y viable continuar con los trámites contractuales en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta".*

Voto del doctor Daladier Medina Niño presentado mediante correo electrónico dmedinan@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

"Buena tarde Con el presente, de manera atenta y atendiendo la citación realizada para el comité del día de hoy, frente a los diferentes temas propuestos, procedo a dar respuesta de la siguiente manera:

- *"De acuerdo a la información presentada en el actual comité del día 04/04/2022, recomiendo continuar con el Trámite contractual de "ADQUIRIR 18 DISCOS DE 7.68 TB CADA UNO, PARA LOGRAR UNA CAPACIDAD DE ALMACENAMIENTO EFECTIVA DE 103.52 TB Y USABLE DE 98.45TB, PARA LA CAJA DE DISCOS IBM FLASHSYSTEM 5000 MODELO: 2072-3N4 SERIAL: 78J1K1Y6; Y LOS SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN, SOPORTE Y GARANTÍA DE HARDWARE POR 3 AÑOS BAJO EL MODELO 7X24X4 IBM STORAGE". Dicha recomendación se da únicamente con base en la necesidad presentada por el área interesada, en atención a las respectivas justificaciones argumentadas; teniendo en cuenta la información allegada o presentada por el grupo contractual a través del presente medio, sin tener conocimiento de los demás detalles del proceso. Adicionalmente, la presente recomendación se atiene a lo dispuesto en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta."*

Voto del doctor Larry Sadit Álvarez Morales presentado mediante correo electrónico lalvarezm@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

	PROCESO	***OBJETO***	***RECOMENDACIÓN***
5	Contratación Directa	Adquirir 18 discos de 7.68 TB cada uno, para lograr una capacidad de almacenamiento	SE RECOMIENDA CONTINUAR CON EL TRÁMITE DEL PROCESO.

62

				efectiva de 103.52 TB y usable de 98.45tb, para la caja de discos IBM FLASHSYSTEM 5000 modelo: 2072-3n4 serial: 781k1y6; y los servicios de instalación, configuración, soporte y garantía de hardware por 3 años bajo el modelo 7x24x4 IBM STORAGE	
	Observaciones	*No aplica*			

6. Tema: Resciliación Contrato *No 469-2022 Caudales & Muestreos S.A.S*

6	***Solicitud***	Resciliación Contrato *No 469-2022 Caudales & Muestreos S.A.S*
	Objeto:	RENOVAR EL SERVICIO DE SOPORTE TÉCNICO PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER RENOVAR EL SERVICIO DE SOPORTE TÉCNICO PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER.
	Plazo de ejecución inicial	*La vigencia del soporte técnico y servicios conexos serán por un año (1), a partir del día 7 de abril de 2022. La entrega del certificado de renovación del soporte técnico y los Acuerdos de Niveles de Servicios (ANS) deberá realizarse 10 días calendarios siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. El certificado de renovación debe especificar la fecha de inicio y finalización del soporte técnico.*
	Solicitud de trámite	***Contratación Directa***
	Área interesada:	*Grupo de Informática– Oficina de Tecnologías de la Información*
	Abogado	*Maria Laura Olivella Dangond – molivellad@invima.gov.co*
	Área Técnica encargada	*Saaibi Arenas Moreno sarenasm@invima.gov.co*
	Documentos adjuntos	*Trámite contractual Presentación, CDP, Estudios Previos*

	Votos	*Voto de la doctora María Margarita Cárdenas Cortes presentado mediante correo electrónico mcardenasc@invima.gov.co de fecha lunes 04/04/2022 14:48 p.m., manifestando lo siguiente:* *"Buenas tardes. De conformidad con los temas sometidos a conocimiento por parte de este Comité en la fecha señalada, me permito dar las siguientes recomendaciones* • *Votación Tema 6: Recomiendo al ordenador del gasto seguir adelante con el trámite previsto para esta necesidad, la cual debe gestionarse en el marco de la urgencia manifiesta decretada por la Entidad. Esta recomendación se realiza de conformidad con la justificación presentada por el área técnica.".* *Voto del doctor Marlon Simón Ortega Ordosgoitia presentado mediante correo electrónico sorteqao@invima.gov.co de fecha martes 04/04/2022 15:04 p.m., manifestando lo siguiente:* *Cordial saludo miembros del Comité de Contratación,* *"En atención al comité de contratación de fecha 4 de abril de 2022, el cual fue enviado el 1 de abril de 2022, me permito manifestar lo siguiente a cada uno de los puntos citados, así,* • *me permito recomendar al Sr. Ordenador del Gasto continuar con el trámite contractual de resciliación, es importante hacer la mención que mi recomendación está dada de acuerdo con la justificación dada por el área técnica solicitante y en virtud del ataque cibernético sufrido por la entidad, y a la respuesta dada por el proveedor de servicios suscrito por el contratista la cual hace parte de la presente citación y la revisión legal de parte del Grupo de Gestión Contractual en dicha materia."* *Voto de la doctora María Margarita Jaramillo Pineda presentado mediante correo electrónico mjaramillop@invima.gov.co de fecha miércoles 04/04/2022 17:01 p.m., manifestando lo siguiente:* *Buenas tardes para todos los miembros del Comité.* *"A continuación, mis recomendaciones y observaciones frente a los temas puestos a consideración en la sesión de hoy:* • *Recomiendo continuar con los trámites contractuales en los términos previstos en la Resolución No. 2022500010 del 10 de marzo de 2022, por medio de la cual se declaró la Urgencia Manifiesta.".* *Voto del doctor Daladier Medina Niño presentado mediante correo electrónico dmedinan@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:*

63

"Buena tarde Con el presente, de manera atenta y atendiendo la citación realizada para el comité del día de hoy, frente a los diferentes temas propuestos, procedo a dar respuesta de la siguiente manera:

- *"De acuerdo a la información presentada en el actual comité del día 04/04/2022, recomiendo continuar con el Trámite contractual de RESCILIACIÓN CONTRATO No 469-2022 CAUDALES & MUESTREOS S.A.S "RENOVAR EL SERVICIO DE SOPORTE TÉCNICO PARA EL SISTEMA DE INFORMACIÓN DE LABORATORIOS (SILAB) BASADO EN EL SOFTWARE SAMPLER". Dicha recomendación se da únicamente con base en la necesidad presentada por el área interesada, en atención a las respectivas justificaciones argumentadas; teniendo en cuenta la información allegada o presentada por el grupo contractual a través del presente medio, sin tener conocimiento de los demás detalles del proceso."*

Voto del doctor Larry Sadit Álvarez Morales presentado mediante correo electrónico lalvarezm@invima.gov.co de fecha martes 04/04/2022 18:33 p.m., manifestando lo siguiente:

	PROCESO	OBJETO	RECOMENDACIÓN
6	Contratación Directa	Renovar el servicio de soporte técnico para el sistema de información de laboratorios (SILAB) basado en el software SAMPLER	SE RECOMIENDA CONTINUAR CON EL TRÁMITE DEL PROCESO.

Observaciones	*No aplica*

COMPROMISOS ADQUIRIDOS:

Compromiso	Responsable (Nombre –Cargo)	Fecha de Ejecución
N/A	N/A	*N/A*

SUSCRIBEN EL ACTA

Nombre completo	Firma

Roy Luis Galindo Wehdeking Secretario General.	
María Margarita Jaramillo Pineda Jefe de Oficina Asesora de Jurídica	M. Margarita Jaramillo P.
Marlon Simón Ortega Ordosgoitia Asesor de la Dirección General con delegación de funciones del Grupo Financiero y Presupuestal.	
Larry Sadit Álvarez Morales Asesor de la Dirección General	
Daladier Medina Niño Jefe de Oficina Asesora de Planeación	
María Margarita Cárdenas Cortes Asesora de la Dirección General con Delegación de Funciones de Coordinación del Grupo de Gestión Contractual.	

Proyectó: Emilia Alexandra Correa Rodríguez

La salud es de todos | Minsalud

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

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 1082 de 2015, el Decreto 2078 de 2012, la Resolución de Delegación de Funciones No. 2012030802 del 19 de octubre de 2012, la Resolución No. 2020006742 del 25 de febrero de 2020, acta de posesión No. 040 del 25 de febrero de 2020 y,

CONSIDERANDO QUE:

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

> "ARTICULO 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 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 4, 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.*

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

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, para realizar las labores misionales y administrativas, 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 la correcta ejecución de sus oficios, administrada 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]; situación que se venía cumpliendo efectivamente en las diferentes sedes de la entidad de forma presencial y virtual, garantizando la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso.

El domingo 6 de febrero 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 el ataque de un ransomware[3] llamado Blackbyte el cual encriptó[4] la información de la entidad, restringiendo su acceso, 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 estado situacional[5].

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*"[6].

En este orden, la entidad implementó medidas, que van desde la contención del incidente hasta la activación de un plan de contingencia, cuyo eje fundamental fue 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 de este acto administrativo. Estos servicios se

[1] Ver Anexo 1: Relación de softwares.
[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] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com
[4] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos
[5] Ver anexo 2: Estado situacional.
[6] Debe precisarse que respecto del incidente, y conforme a lo evaluado por la Oficina de Tecnologías de la Información y el Grupo de soporte Tecnológico, no se evidencian indicios de fuga de la información sin embargo, la entidad se atiene al resultado del análisis forense que fue solicitado a la Superintendencia de Industria y Comercio - SIC, y a lo definido en la investigación penal que adelanta la Fiscalía General de la Nación con apoyo de la Policía Nacional – Dirección de Investigación Criminal e Interpol.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos Invima
Oficina Principal: Cra 10 N° 64 - 28 Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

restauraron de forma paulatina con la gestión de las actividades tecnológicas y jurídicas correspondientes, que a su vez desplegó la entidad, como lo son: la actualización e implementación del plan de acción y medidas de contingencia frente a los posibles efectos o consecuencias del incidente cibernético, la emisión de las medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, emitiendo los siguientes actos administrativos:

- Resolución 2022500000 del 9 de febrero de 2022; la Resolución 2022500001 del 15 de febrero de 2022; 2022500002 del 22 de febrero de 2022; 2022500003 del 25 de febrero de 2022; 2022500005 del 8 de marzo de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites, y la Resolución No. 2022500009 del 16 de marzo de 2022, por medio de la cual se adoptaron decisiones y se actualizaron las medidas administrativas transitorias necesarias para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto.

- Circular 1000-001-22 del 18 de febrero de 2022, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso - Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.

- Circular 1000-002-22 del 25 de febrero de 2022, a través de la cual se otorga la ampliación de empresas beneficiadas por formato de contingencia para autorización de traslado de alimentos, materias primas, otros alimentos perecederos, desde el sitio de ingreso a otro sitio que cumplan con las condiciones sanitarias para su almacenamiento.

De forma paralela la entidad con las actividades anteriormente descritas, interpuso ante la Fiscalía General de la Nación denuncia penal Expediente CAD N° 110016000050202201569 por el presunto delito de acceso abusivo a un sistema informático, tipificado en el artículo 269 A de la Ley 1263 de 2009, actuación de la que se desprendieron las consecuentes investigaciones, iniciando con las practicas del recaudo del material probatorio y/o evidencia física sobre los servidores y equipos diagnosticados con la transmisión o inoculación del virus ransomware. En consecuencia, la policía judicial realizó las actividades forenses correspondientes, extrayendo las que conformarían el caudal probatorio que soporta la denuncia en cita, actividad que fue desplegada hasta el 15 de marzo de 2022, fecha en la que se emite el acta que autoriza proceder con el uso para formateo de los servidores afectados, en relación con el acta de formateo de servidores del Instituto[7].

El 16 de marzo de 2022, se llevó a cabo Comité Técnico de Seguimiento[8], integrado por 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:

1. Teniendo en cuenta que ya han sido tomadas como parte del material probatorio las evidencias por la fiscalía, para efectos de los temas judiciales correspondientes a la acción

[7] Ver anexo 3: Acta formateo servidores del Invima.
[8] Ver anexo 4: Comité Técnico de Seguimiento Contingencia.

penal que ha iniciado el Instituto, se hace procedente realizar el formateo y restauración de los servidores; situación que permitirá el almacenamiento correspondiente para la instalación, configuración, parametrización, pruebas y salida a producción de los sistemas de información SeSuite (Módulos de Gestión Documental y PQRDS/Correspondencia), Silab y el portal web.

2. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales concernientes a la contratación para la instalación, configuración, parametrización, pruebas, salida a producción y soporte técnico del Sistema de Información de los Laboratorios Silab, con el proveedor exclusivo y dueño del código fuente del sistema, que lo hacen titular de la obra Sampler, en la que se encuentra desarrollado el sistema de los laboratorios del Instituto.
3. De igual forma, realizar los análisis jurídicos, tecnológicos, financieros y contractuales para la contratación de la instalación, configuración, parametrización, pruebas y salida a producción del software SeSuite (Módulos Gestor Documental y Correspondencia/ PQRDS), con el proveedor que realizó los desarrollos concernientes al componente utilitario (Componente del Software SeSuite) y componente radicador (Componente del Módulo Correspondencia y PQRDS), que fueron desarrollados exclusivamente para el Invima y cuyo código fuente pertenece al canal autorizado de las tecnologías.
4. En atención a las sugerencias de los numerales 2 y 3, se recomienda que las mismas deben hacerse operativas en el menor tiempo posible, para dar continuidad a la interoperabilidad de los proyectos en desarrollo, para Sivicos[9] y la Nueva Plataforma de Trámites y Servicios[10], así como la usabilidad del actual sistema de registros sanitarios y correspondencia y PQRDS.
5. Como acción de prevención se debe viabilizar la contratación de las actividades de aseguramiento de hacking ético y pruebas de seguridad, para la publicación de cada servicio de la entidad, y así mitigar la ejecución de riesgos asociados a este tipo de incidentes tecnológicos.
6. Dado que los sistemas de información están parametrizados con correos electrónicos en la infraestructura dispuesta por el Invima (On-Premise[11]) y que no se encuentran disponibles debido al incidente presentado, se requieren más licencias de correos en nube, que permitan la disponibilidad de los correos recibidos y enviados por los sistemas de información a los usuarios internos y externos de la Entidad; dicha suscripción debe realizarse con el mismo proveedor con el que se contrataron el uso de las licencias de correo en el servicio de Microsoft Office 365.
7. Dadas las necesidades de realizar copias de seguridad a los servidores y sistemas de información impactados, así como la adecuación para el alojamiento de los sistemas de información actualmente en desarrollo por parte del Instituto, se requiere garantizar el

[9] Sivicos es la denominación utilizada para referirse al proyecto que comprende el desarrollo de una solución que consiste en un software que permite la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima.

[10] El proyecto de nueva plataforma es el relacionado con el desarrollo de una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para la ejecución en línea, de las actividades misionales de los procesos: "Registros sanitarios y tramites asociados" y "Auditorias y certificaciones" del instituto.

[11] On-Premise: En las instalaciones propias. "In situ". Utilización de servidores y entorno informático propios de la empresa

Instituto Nacional de Vigilancia de Medicamentos y Alimentos Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

espacio de almacenamiento necesario, mediante la compra de discos de estado sólido para alojar esta información.

8. Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se sugiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft, para esto se recomienda aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, y así poder contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad. Adicionalmente, se requiere el acompañamiento técnico para el alistamiento de los computadores del Instituto y habilitación de los servicios de impresión, los cuales pueden ser brindados por el proveedor de apoyo a la gestión tecnológica.
9. Con el fin de habilitar el módulo de la comisión revisora entregado por Innpulsa, que también se encuentra afectado, se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción de este, para continuar su integración en el proyecto de Nueva Plataforma de Trámites y Servicios.
10. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto, respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de desarrollo y codificación para la Nueva Plataforma de Trámites y Servicios, proyecto transversal a la transformación tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.
11. Realizar los análisis jurídicos, tecnológicos, financieros y contractuales para efectos de garantizar la continuidad del proyecto respecto de los desarrollos, instalaciones, configuraciones, parametrizaciones, pruebas y salida a producción que se encuentran encriptados, y que de conformidad al plazo contractual fueron recibidos y alojados en los ambientes de pruebas (QA) y producción en los servidores de la Entidad, permitiendo en este orden que se pueda completar la fase de sistematización y automatización para el Proyecto Sivicos, proyecto transversal a la Transformación Tecnológica del Instituto. Estas actividades se deben ejecutar por el proveedor que está realizando los desarrollos.

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 acogidas por la Entidad 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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte, 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[12], siendo viable acudir al mecanismo idóneo para adelantar las contrataciones, con atención a las situaciones anteriormente expuestas, garantizando una respuesta contigua de la administración.

De igual manera, debe tenerse en cuenta la prohibición establecida en el marco de Ley de garantías, contemplada en el artículo 33 de la Ley 996 de 2005, el cual dispone:

> **Artículo 33. Restricciones a la contratación pública.** Durante los cuatro (4) meses anteriores a la elección presidencial y hasta la realización de la elección en la segunda vuelta, si fuere el caso, queda prohibida la contratación directa por parte de todos los entes del Estado.
>
> Queda exceptuado lo referente a la defensa y seguridad del Estado, los contratos de crédito público, los requeridos para cubrir las emergencias educativas, sanitarias y desastres, así como también los utilizados para la reconstrucción de vías, puentes, carreteras, infraestructura energética y de comunicaciones, en caso de que hayan sido objeto de atentados, acciones terroristas, desastres naturales o casos de fuerza mayor, y los que deban realizar las entidades sanitarias y hospitalarias. Adicionalmente se exceptúan aquellos gastos inaplazables e imprescindibles que afecten el normal funcionamiento de la administración[13].

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[14], el cual refiere la condición de la urgencia manifiesta a partir de situaciones necesarias para conjurar contextos excepcionales relacionadas con la fuerza mayor, para este caso, en concordancia con la excepción dispuesta en el artículo 33 de la citada Ley 996 de 2005.

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

---

[12] Licitación pública, selección abreviada, concurso de mérito, contratación mínima cuantía.
[13] Texto subrayado declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia C-1153 de 2005; el resto del artículo fue declarado EXEQUIBLE, condicionado a que se entienda que para el Presidente o el Vicepresidente de la República se aplique desde que manifiestan el interés previsto en el artículo 9º.
[14] 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 (...).

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 0121
www.invima.gov.co

> 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[15], 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, Exp. 12.423):

> (...) La fuerza mayor sólo 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 sólo 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[16].

Sobre el particular, la Corte Constitucional[17] indicó que:

---

[15] 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.

[16] Circular No. 109 del 1 de octubre de 2020, emitida por el Secretario General del Instituto Nacional de Vigilancia de medicamentos y Alimentos- Invima.
[17] Corte Constitucional, Sentencia C-772 de 1998, 10 de diciembre de 1998. Magistrado Ponente: Fabio Morón Díaz.

> *"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[18], 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.

---

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

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

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[19]:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la	• Hacking Ético: interno de caja blanca para 160 IP[20]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.

[19] En desarrollo de lo dispuesto en el Plan de Acción Incidente de Seguridad de la Información.
[20] IP: Internet Protocol – Protocolo de comunicaciones de Internet

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**1. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log. **ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓI DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		2. **Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto. Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios • Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de Insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td>requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.</td><td>

Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos.
Revisión portales y reportes.
Ajustes y corrección de incidencias portales y reportes.
Revisión de integridad para el componente de documentos vs directorios controlados.
Acompañamiento de casa matriz.

Fase de estabilización

Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información.

Fase cuatro: Actividad de Salida a producción
El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado.

Operación en producción
Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores.

Tecnológicos para ambiente de producción
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>128 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>32 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>800 Gygas</td><td>Dos Discos (1) 300 y (1) 500 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>24 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>1 Tera</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteProducción y Utilitario</td><td></td></tr>
<tr><td colspan="3">Servidor de configuración y paso</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos: (1) de 150 Gygas (1) de 350 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">File server</td></tr>
<tr><td>Sistema de archivos</td><td>NTFS</td><td></td></tr>
<tr><td>Capacidad</td><td>20 Teras</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>
Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.
Características Especiales
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo
Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log
Respaldo de los archivos nuevos cargados al File Server diario.
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta

Tecnológicos para ambiente de pruebas
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos de 150 y 250 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>16 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>500 Gygas</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteproduccion y Utilitario</td><td></td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
<tr><td colspan="3">Backup de las bases de datos 1 Diario completo y cada 3 horas Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S</td></tr>
<tr><td colspan="3">Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td colspan="3">Configuración de una estrategia de seguridad robusta.</td></tr>
</table>
</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEA SAP</td><td>Microsoft®ExchangeOnlinePlan 2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.</td></tr>
</table>
</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS			
	contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima. En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad. Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin.				• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas. • Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection • Más información en: https://www.microsoft.com/es-co/microsoft-365/exchange/compare-microsoft-exchange-online-plans
		2	KF5-00002EAEA SAP	Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP	• Protección de próxima generación que incluye protección antimalware y antivirus robusta. • Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad. Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad.	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	de las ventanas de tiempo acordadas. • Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y Servicios de conformidad a las condiciones técnicas del proyecto.	máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor de Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Instalación del Ambiente de Producción: Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

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 por un término aproximado de seis (6) meses, 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[21].

En mérito de lo expuesto, el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA,

RESUELVE:

ARTÍCULO PRIMERO: 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, 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 del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, afectados por una circunstancia constitutiva de fuerza mayor relacionada con incidente informático a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte.

PARÁGRAFO PRIMERO: La duración de la Urgencia Manifiesta será por un término aproximado de seis (6) meses, 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 SEGUNDO: 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 2° de la Ley 1150 de 2007, y el artículo 2.2.1.2.1.4.2. Del Decreto 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:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de	• Hacking Ético: interno de caja blanca para 160 IP[22]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration

[21] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera. Radicado interno 37.044. marzo 7 de 2011. Magistrado Ponente: Doctor Enrique Gil Botero.
[22] IP: Internet Protocol – Protocolo de comunicaciones de Internet

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del	**3. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log.

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma. **4. Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto.	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td>Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema.

Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.</td><td>• Restauración de la base de datos de INVIMA (SeSuite)

Configuración SE Suite
• Ejecutar procedimientos de activación de SE Suite
• Pruebas de conectividad con el directorio activo
• Configuración de la sincronización con el Directorio Activo
• Configuración y prueba del servidor de correo para SE Suite Notificaciones

Configuración de almacenamiento de archivos
• Configuración de directorios controlados de acuerdo con la entrega de insumos por parte de Invima.
• Configuración y prueba de vínculos de documento con SeSuite

Fase tres: Actividad de Pruebas
• Verificación integridad del software Gestor Documental SeSuite y componentes-módulos
• Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos.
• Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos.
• Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos.
• Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos.
• Revisión portales y reportes.
• Ajustes y corrección de incidencias portales y reportes.
• Revisión de integridad para el componente de documentos vs directorios controlados.
• Acompañamiento de casa matriz.

Fase de estabilización
• Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información.

Fase cuatro: Actividad de Salida a producción
El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado.

Operación en producción
Tareas por revisar/ (enlistar)iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores.

Tecnológicos para ambiente de producción
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>128 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>32 cores</td><td></td></tr>
</table>
</td></tr>
</table>

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS

Disco Duro	800 Gygas	Dos Discos (1) 300 y (1) 500 Gygas
Sistema Operativo	Windows Server 2019 Datacenter	
Servidor de Base de datos		
Memoria	64 Gygas	
Procesador	24 cores	
Disco Duro	1 Tera	
Engine	SQL Server 2017 Enterprise Edition	
Bases de Datos	SeSuiteProducción y Utilitario	
Servidor de configuración y paso		
Memoria	64 Gygas	
Procesador	8 cores	
Disco Duro	400 Gygas	Dos Discos: (1) de 150 Gygas (1) de 350 Gygas
Sistema Operativo	Windows Server 2019 Datacenter	
File server		
Sistema de archivos	NTFS	
Capacidad	20 Teras	
Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.		
Características Especiales		
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo		
Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log		
Respaldo de los archivos nuevos cargados al File Server diario.		
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura		
Configuración de una estrategia de seguridad robusta		

Tecnológicos para ambiente de pruebas

REQUERIMIENTOS	CARACTERISTICAS	
Servidor de Aplicaciones		
Memoria	64 Gygas	
Procesador	8 cores	
Disco Duro	400 Gygas	Dos Discos de 150 y 250 Gygas
Sistema Operativo	Windows Server 2019 Datacenter	
Servidor de Base de datos		
Memoria	16 Gygas	
Procesador	8 cores	
Disco Duro	500 Gygas	
Engine	SQL Server 2017 Enterprise Edition	
Bases de Datos	SeSuiteproduccion y Utilitario	
Características Especiales		
Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo		

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>Backup de las bases de datos 1 Diario completo y cada 3 horas
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta.</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima.

En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEA SAP</td><td>Microsoft®ExchangeOnlinePlan 2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.
• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas.
• Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection
• Más información en: https://www.microsoft.com/es-co/microsoft-</td></tr>
</table>
</td></tr>
</table>

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS			
	buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad. Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin. Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y				365/exchange/compare-microsoft-exchange-online-plans
		2	KF5-00002EAEA SAP	Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP	• Protección de próxima generación que incluye protección antimalware y antivirus robusta. • Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativa: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del Invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad. Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	de los servidores que se encuentran en el Datacenter de la entidad.	
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro de las ventanas de tiempo acordadas. • Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y Servicios de conformidad a las condiciones técnicas del proyecto.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	**Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades:

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		• Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato. Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 742 2121
www.invima.gov.co

República de Colombia
Ministerio de Salud y Protección Social
Instituto Nacional de Vigilancia de Medicamentos y Alimentos – INVIMA

RESOLUCIÓN No. 2022500010 DEL 23 DE MARZO DE 2022

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.

ARTÍCULO TERCERO: 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 CUARTO: 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 QUINTO: Desígnese un comité de seguimiento y acompañamiento respecto de la ejecución de las actividades enunciadas en el artículo segundo del presente acto administrativo a la Oficina de Tecnologías de la Información y al Grupo de Soporte Tecnológico, desde el rol administrativo, jurídico y financiero a:

- La Oficina Asesora de Planeación, representada por el Jefe de Oficina y el Oficial de Seguridad.
- El Grupo Financiero y Presupuestal, representado por el Asesor de la Dirección delegado para el Grupo Financiero y Presupuestal.
- La Oficina Asesora Jurídica, representada por el Jefe de Oficina.

"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 a través de un tipo de programa dañino conocido como ransomware denominado Blackbyte".

- Asesor de la Dirección General Delegado para tal fin.

ARTÍCULO SEXTO: 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 SÉPTIMO: La presente resolución rige a partir de la fecha de su publicación.

Dada en Bogotá D.C., el 23 de marzo de 2022.

PUBLÍQUESE Y CÚMPLASE

ROY GALINDO WEHDEKING
Secretario General

Proyectó: María José Amaya López - Abogada contratista Grupo de Gestión Contractual.
María Laura Olivella Dangond – Abogada contratista Grupo de Gestión Contractual.
Leidy Diana García Arevalo – Contratista Oficina de Tecnologías de la Información.

Aprobó: María Margarita Cárdenas – Asesora de la Dirección General con delegación de funciones del Grupo de Gestión Contractual.
María Margarita Jaramillo P- Jefe de la Oficina Asesora Jurídica.
Juan Manuel Palacio Posada- Jefe de Oficina de Tecnologías de la Información.
Eliodoro Rojas Ochoa- Coordinador del Grupo de Soporte Tecnológico.
Camilo Guzmán Camacho- Coordinador del Grupo de Informática.
Miguel Díaz Peña- Coordinador del Grupo de Gestión de la Información.
Nidia Nayibe González Pinzón- Oficial de Seguridad de la Información de la Oficina Asesora de Planeación.

Anexo 1: Relación Software
Anexo 2: Estado situacional
Anexo 3: Acta Formateo Servidores
Anexo 4: Acta Comité Seguimiento Técnico
Anexo 5: Plan de Acción
Anexo 6: Anexo Técnico

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 Bogotá
Administrativo: Cra 10 N° 64 - 60
(60)(1) 743 3121
www.invima.gov.co

ANEXO 2

ESTADO SITUACIONAL Y DIAGNÓSTICO INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN 06 DE FEBRERO DE 2022

1. INTRODUCCIÓN

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos Invima, de conformidad con las funciones asignadas por Ley, es un establecimiento público del orden nacional, de carácter científico y tecnológico, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Salud y Protección Social y perteneciente al Sistema de Salud.[1]

Su objetivo consiste en actuar como institución de referencia nacional en materia sanitaria y ejecutar las políticas formuladas por el Ministerio de Salud y Protección Social en materia de vigilancia sanitaria y de control de calidad de los 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 de conformidad con lo señalado en el artículo 245 de la Ley 100 de 1993 y en las demás normas que la modifiquen, adicionen o sustituyan.

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 recurso humano (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, para realizar estas labores misionales, en el marco del proceso de transformación digital, la entidad cuenta con la infraestructura tecnológica que soporta los múltiples sistemas de información y aplicativos necesarios para la correcta ejecución de sus oficios, administrada por la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico, con el cual garantiza que las actividades misionales y administrativas de la entidad se ejecuten, a través de los distintos aplicativos como lo son:

1. SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO.
2. SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA.
3. SOLUCIÓN WEB DE TRÁMITES EN LÍNEA.
4. SISTEMA DE INFORMACIÓN DE CÍVICOS MOVILES -CIS.
5. SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS – SESUITE.

[1] Artículo 1 del Decreto 2078 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"*

6. SOLUCIÓN WEB ADMIN.
7. SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA.
8. SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA.
9. SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS.
10. SOLUCIÓN WEB CÓDIGO ÚNICO DE MEDICAMENTOS (CUM).
11. SOLUCIÓN WEB ACIDOS.
12. SOLUCIÓN WEB FARMACOVIGILANCIA.
13. SOLUCIÓN WEB TRANSPARENCIA.
14. SOLUCIÓN WEB REGISTRO – RECAUDOS.
15. SOLUCIÓN WEB IVC/SOA.
16. SOLUCIÓN WEB REACTIVOVIGILANCIA.
17. SOLUCIÓN WEB TECNOVIGILANCIA.
18. SOLUCIÓN WEB - IVC SOA PUERTOS.
19. SOLUCION WEB PROTOCOLOS DE INVESTIGACIÓN.
20. SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS.
21. SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA.
22. SISTEMA DE INFORMACIÓN DE LABORATORIOS – SILAB.
23. PORTAL WEB INSTITUCIONAL.
24. SOLUCIÓN WEB KAWAK.
25. SOLUCION WEB ITSM ARANDA.
26. HERRAMIENTA ANTIVIRUS KASPERSKY.
27. SOLUCION WEB OFICINA VIRTUAL.
28. DIRECTORIO ACTIVO.
29. CORREO ELECTRONICO.
30. SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO).
31. SISTEMA DE INFORMACION WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL - SIVICOS (PROYECTO EN DESARROLLO).

De dichos aplicativos se venía haciendo uso de forma efectiva desde las diferentes sedes de la entidad de manera presencial y virtual, conforme a la capacidad diagnosticada y operativamente válida para garantizar la prestación del servicio y la seguridad de la información, acorde a las frecuencias de uso. Sin embargo, el 6 de febrero de 2022 el Coordinador (E) del Grupo de Soporte Tecnológico informa a su equipo de trabajo de la caída de la página web de la entidad, generando la indisponibilidad de los sistemas de información, plataformas tecnológicas y herramientas tecnológicas que soportan las actividades operacionales y administrativas de la Entidad.

En tal sentido, es procedente realizar en desarrollo de las políticas, lineamientos y estándares adoptados por la Entidad el siguiente diagnostico que consta de los puntos que a continuación se tratan, para efectos de tomar las decisiones y acciones procedentes para mitigar los posibles eventos adversos generados como consecuencia de la indisponibilidad.

2. ANTECEDENTES

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información[2] que comprometió la disponibilidad de la información del Invima, este se dio por el ataque de un ransomware[3] llamado Blackbyte el cual encriptó[4] la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto.

En consecuencia, se procedió a dar paso al Procedimiento Gestión de Incidentes Tecnológicos:

- **Identificar los posibles eventos de seguridad de la información:** El Coordinador (E) del Grupo de Soporte Tecnológico estuvo monitoreando el fin de semana del 5 de febrero de 2022 el funcionamiento de la página web del Instituto, el domingo 6 de febrero de 2022 a las 7:30 de la mañana detectó que la página dejo de funcionar, comunicándose de forma inmediata con el ingeniero Cristian Pinzón para que se realizara la revisión de la infraestructura correspondiente (servidores), indicándose que existía una anomalía, por lo que el funcionario Pinzón se comunica con el ingeniero Jhorbis Ríos, quienes de manera mancomunada proceden a revisar la infraestructura.

  El reporte telefónico indica que se encontró un cambio de contraseña en el administrador, y se percató por parte del Ingeniero Ríos que existían discos encriptados, se observa que uno de los principales servidores Directorio Activo se encontraba encriptado e infectado; de conformidad a lo sucedido y en atención a la experiencia se presumió de forma inmediata que la indisponibilidad obedecía a un ataque.

- **Reportar el evento:** Se procede a informar al oficial de seguridad de la información, al jefe de la Oficina de Tecnologías de la Información y al Coordinador titular del cargo. Quienes tomaron la decisión de comunicarse con el contratista de la entidad Empresa de Recursos Tecnológicos - ERT para que procediera a desconectar los canales de comunicación, de igual forma como medidas de seguridad se comienzan a apagar los servidores de forma gradual y a la elaboración del inventario de los servidores impactados, también se realizó al apagado de suiches de distribución.

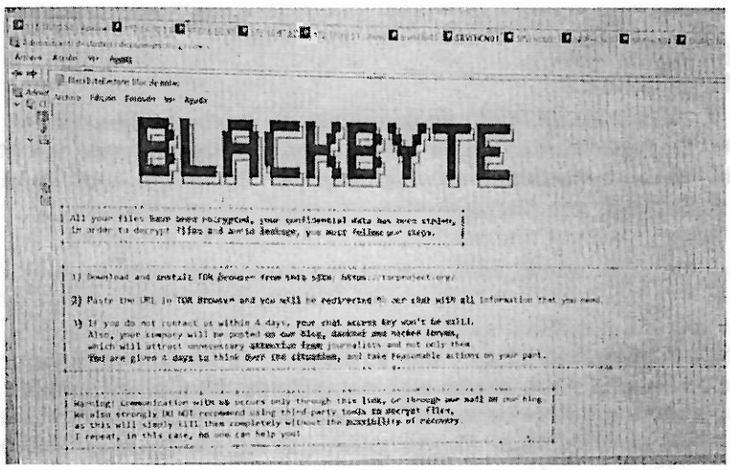
  Según el archivo .txt se observa que es un Ransoware Blackbyte

---

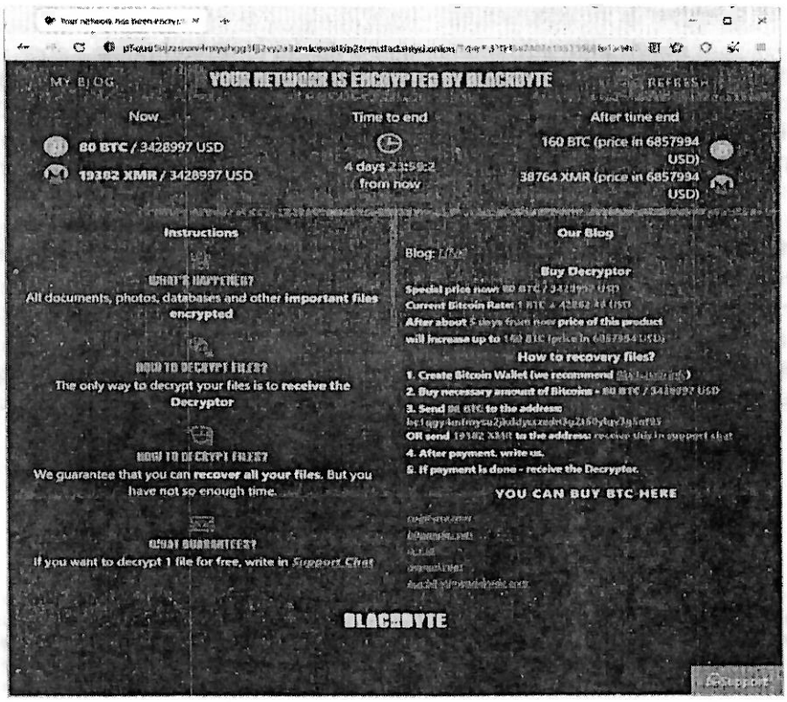
[2] Incidente de seguridad de la información: Un incidente se reporta cuando de manera ilegal se tiene acceso a la información confidencial o a datos privados de una organización con fines delictivos o en pro de usurpar posiciones para adquirir algún dato en particular afectando el normal funcionamiento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

[3] Ransomware: Es un tipo de software malicioso, que secuestra archivos y, en ocasiones, equipos o dispositivos móviles enteros. Según este comportamiento los ciberdelincuentes solicitan el pago de un rescate a cambio de liberar la información y así devolverles el acceso. Según www.avast.com

[4] Encriptar: Significa ocultar información a simple vista, de manera que haga falta una llave o clave específica para poder acceder a su contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información. Según www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos



Finalizado el cifrado del equipo se identificó una nota de rescate que indica:



El incidente se reportó vía telefónica y vía WhatsApp al Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL el día 6 de febrero de 2022 a las 10:07, de conformidad al Instructivo de Relaciones con Autoridades y Grupos de Interés, con el propósito de solicitar apoyo en el manejo de dicha situación.

- **Realizar evaluación preliminar del evento:** Se dispuso la elaboración de la evaluación de los equipos, de la cual se obtuvo el siguiente resultado:

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\AD_DNS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\AD_DNS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\APP	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\APP	1-Sin Acceso	Microsoft Windows Server 2012 Datacenter	Si
INVIMA\APP_BIO_STAR	0-Comprometida	Microsoft® Windows Server® 2008 Standard	Si
INVIMA\DHCP	1-Sin Acceso	WINDOWS SERVER 2012 STANDARD	Si
INVIMA\DHCP	1-Sin Acceso	WINDOWS SERVER 2019 STANDARD	Si
INVIMA\EXCHANGE	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\EXCHANGE	1-Sin Acceso	WINDOWS SERVER 2008 R2 Enterprise - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	0-Comprometida	Microsoft Windows Server 2012 Standard	Si
INVIMA\FS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\FS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\FS	1-Sin Acceso	Microsoft Windows Server 2012 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\FS_IIS	1-Sin Acceso	WINDOWS 10 PRO - 64 BIT	Si
INVIMA\FS_IIS	1-Sin Acceso	WINDOWS SERVER 2008 R2 - 64BIT	Si
INVIMA\FS_IIS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Datacenter	Si
INVIMA\FS_ISS_P_SERVER	1-Sin Acceso	WINDOWS SERVER 2008 R2 Enterprise - 64BIT	Si
INVIMA\FS_ISS_P_SERVER	0-Comprometida	WINDOWS SERVER 2008 R2 - 64BIT	Si
INVIMA\HYPER_V\CLUSTER_CONT_01	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_CONT_01	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	Microsoft Windows Server 2012 R2 Datacenter	Si
INVIMA\HYPER_V\CLUSTER_HV_02	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_03	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTER_HV_03	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	Microsoft Windows Server 2019 Datacenter	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	Microsoft Windows Server 2019 Datacenter	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\CLUSTERHV04	0-Comprometida	SIN INFO	Si
INVIMA\HYPER_V\SRVHCICLINV	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\HYPER_V\SRVHCICLINV	1-Sin Acceso	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\IIS	2-Aislada / apagada	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\IIS- ARANDA	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\IIS_RDS_POWER_BI	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Datacenter	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\NPS_RADIUS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\OTROS	2-Aislada / apagada	SIN INFO	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	SIN INFO	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows 7 Professional	Si
INVIMA\OTROS	2-Aislada / apagada	WINDOWS SERVER 2012 R2 STANDARD	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows 8.1 Pro	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2019 Standard	Si
INVIMA\OTROS	2-Aislada / apagada	Microsoft Windows Server 2008 R2 Enterprise	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2008 R2 ENTERPRISE - 64 BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	Windows Server 2012 R2 estandar	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 2012 R2	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 2012 R2	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2016 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2016 STANDARD - 64 BIT	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows Server 2016 Standard	Si
INVIMA\OTROS	0-Comprometida	Microsoft Windows 8.1 Pro	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 DATACENTER - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS 10 PRO - 64 BIT	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\OTROS	1-Sin Acceso	Microsoft Windows Server 2019 Standard	Si
INVIMA\OTROS	0-Comprometida	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\OTROS	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\SFB	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SFB	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si
INVIMA\SFB	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL	1-Sin Acceso	Microsoft Windows Server 2012 Standard	Si
INVIMA\SQL	1-Sin Acceso	WINDOWS SERVER 2012 R2 STANDARD - 64BIT	Si

Rol	Estado Hoy	OS	Administrada (Si / No)
INVIMA\SQL_CLUSTER	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	0-Comprometida	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SQL_CLUSTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
INVIMA\SYSTEM_CENTER-SQL	1-Sin Acceso	Microsoft Windows Server 2012 R2 Standard	Si
		Microsoft Windows Server 2012 R2 Standard	No
		Microsoft Windows Server 2012 R2 Standard	No
		Microsoft Windows Server 2008 R2 Enterprise	No
		Microsoft Windows Server 2016 Standard	No
		Microsoft Windows Server 2016 Datacenter	No
		Microsoft Windows Server 2016 Standard	No

- **Evaluar el evento:** De conformidad al procedimiento la oficial de seguridad de la información, junto con la persona que reporta y el equipo de la mesa de ayuda, establecieron que el incidente presentado sobre los sistemas de información y comunicaciones del Instituto se trata de:

Malware:	Ransomware
Disponibilidad:	Sabotaje
Compromiso de Información:	Acceso no autorizado a información
Fraude:	Uso ilegitimo de credenciales
Política de Seguridad:	Acceso a servicios no autorizados
Clasificación de peligrosidad	10 / 10

- **Características más predominantes de BlackByte:**
  - Tiene funcionalidad de gusano en donde realiza consulta de otros posibles equipos objetivo, al conocer el alcance de infección, procede a propagarse a través de la red.

- Paquete Wake-on-LAN en donde se puede controlar de manera remota los equipos afectados al encenderlos cuando están apagados, hibernando o suspendidos. (Ver Anexo: Alerta de Seguridad Ransonware BlackByte).

- **¿Se considera un incidente de Seguridad de la Información?:** Si. (Ver Anexo: Formato de Reporte de Incidentes – CSIRT Gobierno Invima V1).

- **Contener el incidente**: Una vez se presentó el suceso el Invima tomó las siguientes acciones como medida de contención frente a la propagación del programa dañino identificado en los sistemas de información, plataformas tecnológicas y herramientas tecnológicas:

  - Se apagaron de forma gradual los servidores de la entidad, para limitar la expansión del código malicioso en la red que pudiera impactar la información del instituto (servidores de datos compartidos).
  - Se identificó que los computadores de los usuarios estaban afectados, por lo que se desconectó físicamente toda la red.
  - Se desconectaron las interfaces de red y se desactivó toda la red (incluido wifi) para evitar la expansión del virus y afectación de otros servidores.
  - Se procedió a la revisión de los logs y al monitoreo de la herramienta de control de software y antivirus, para efectos de comprobar la finalización de la ejecución del proceso dañino, identificando que los atacantes lograron ganar acceso completo a la infraestructura tecnológica sobre la 1:00 a.m. del 6 de febrero de 2022, con el cambio de la contraseña maestra del Directorio Activo.
  - Se identificó que respecto de las copias de seguridad de la entidad (backup) toda la data e información del Invima se encuentra protegida y no fue objeto de sustracción por parte de los atacantes.
  - Se realizó un levantamiento de información con el propósito de determinar qué información se encontraba encriptada.
  - Como metodología de trabajo se realizó el análisis del comportamiento de este tipo de ataque que se actúa como un virus, respecto de las herramientas de seguridad con la que cuenta la entidad (antivirus, firewall y fireeye). En tal sentido, se estableció como necesidad y dada la clasificación de peligrosidad comportada por este tipo de virus se debe estructurar una estrategia de contención que va desde parchar los servidores, obtener una auditoria forense para delimitar los principales puntos débiles que deben tenerse en cuenta en la evaluación de riesgos por ciberataques atendiendo criterios de razonabilidad, así como mantener actualizadas para posibles nuevas amenazas cibernéticas respecto de los ransomware.
  - Finalmente se instauró denuncia penal bajo el código de noticia criminal No. 110016000050202201569 de fecha 18 de febrero de 2022, por el presunto delito de accedo abusivo a un sistema informático (Artículo 269ª Ley 1273 de 2009).

- **Evaluar el incidente de seguridad:** Al confirmarse que el evento corresponde a un incidente de seguridad de la información se procedió a evaluarlo de acuerdo con el instructivo Gestión de incidentes Tecnológicos lo que conlleva a identificar:

1. Se valida el tipo de incidente, especificando el impacto potencial, la cantidad de usuarios afectados.
2. Se evidencia la indisponibilidad de los servicios tecnológicos del instituto que se encuentran dentro del catálogo de servicios y de los servidores de la entidad

Se procede a categorizar el incidente de seguridad de la información teniendo cuenta la siguiente tabla:

Niveles de prioridad de los incidentes

Prioridad	Descripción
Prioridad 1 (Alta)	Causa una completa pérdida del servicio, sin importar el ambiente en el que se está trabajando (producción, pruebas, desarrollo, etc.). La operación no puede continuar de una manera razonable y no puede ser restablecida inmediatamente.
Prioridad 2 (Media)	Causa una pérdida mínima del servicio. El problema o defecto tiene un impacto menor o no produce inconvenientes. Comprende características importantes inoperables, pero con una solución alterna o características no tan importantes inoperables sin solución alterna.
Prioridad 3 (Baja)	No causa pérdida del servicio. El resultado del problema es un error menor, comportamiento incorrecto o error en la documentación que, de ninguna manera, impide la operación del sistema.

Adicionalmente se identifica una falla masiva es decir en más de 10 usuarios en los siguientes aspectos:

1. Interrupción del servicio en alguna de las aplicaciones o sistemas de información de Invima.
2. Falla al ingresar o realizar alguna operación en aplicativos o sistemas de información del Invima.
3. Falla en alguna de las operaciones o en la generación de reportes
4. Falla es reportada en uno o varios elementos de configuración.
5. Falla de telecomunicaciones o conexión de red o wifi
6. Reducción de la calidad del servicio masiva, no planificada del servicio, determinando si fue producida por la implementación de un cambio.
7. Falla de uno o más servicios que se encuentran activos en el catálogo de servicios

Lo anterior nos lleva a valorar el incidente con un nivel de **Prioridad Alto** y una **Criticidad Alta**, por lo que se procede a aplicar lo establecido en el documento TIC-GTI-IN008 - INSTRUCTIVO GESTIÓN DE PROBLEMAS DE LOS SERVICIOS DE TI (TIC-GTI-IN008).

- **Definir estrategia de atención del incidente:** La estrategia de atención se encuentra registrada en el documento Plan de Acción Riesgo Incidente de Seguridad de la Información

- **Erradicar fallas:** En proceso de análisis
- **Recuperar activos de información:**

  Conforme a lo evaluado por la Oficina de Tecnologías de la Información y el Grupo de soporte Tecnológico, no ha existido fuga de información, sin embargo, la entidad se atiene a lo dispuesto en el análisis forense realizado por la SIC, entidad competente para determinar la perdida de la información.

- **Registrar lecciones aprendidas:** En proceso de análisis
- **Cerrar el incidente:** En proceso

ANEXO 1

INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS - INVIMA
RELACION DE SOFTWARE, SISTEMAS DE INFORMACIÓN Y/O HERRAMIENTAS TECNOLOGICAS INVIMA
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

NÚMERO	NOMBRE SOFTWARE, SISTEMA DE INFORMACIÓN, APLICATIVOS TECNOLÓGICOS, PLATAFORMAS TECNOLÓGICAS, HERRAMIENTAS TECNOLÓGICAS Y/O APLICACIONES	DESCRIPCIÓN	ARQUITECTURA	TIPO DE PLATAFORMA	ES MISIONAL?	PROCESO DUEÑO DE LOS DATOS	LENGUAJE DE PROGRAMACION
1	SISTEMA DE INFORMACIÓN DE REGISTRO SANITARIO	El sistema de información "Registros Sanitarios", se encarga de apoyar las actividades relacionadas con el proceso de expedición de registros sanitarios y trámites asociados de los productos competencia del INVIMA.	CLIENTE - SERVIDOR	ON PREMISE	SI	Aseguramiento Sanitario	POWER BUILDER
2	SISTEMA DE INFORMACIÓN DE COMISIÓN REVISORA	El sistema de información "COMISIÓN REVISORA", se utiliza para relacionar los radicados enviados a la comisión revisora, permite generar un documento que se adiciona al expediente, para informarle a la comisión. Además, permite generar un consolidado con los datos específicos del producto de las actas de la comisión.	CLIENTE - SERVIDOR	ON PREMISE	SI	Aseguramiento Sanitario	POWER BUILDER
3	SOLUCIÓN WEB DE TRÁMITES EN LÍNEA	Este sistema web de "TRAMITES EN LÍNEA", permite hacer uso de los siguientes módulos: Consulta estado trámite, Certificado de Venta Libre, Cambio de Clave, Actualizar Datos, Pago Electrónico de Tarifas, Solicitud Certificado de Inspección Sanitaria en Puertos – Alimentos, Solicitud Certificado de Inspección Sanitaria en Puertos - Bebidas Alcohólicas, Adjuntar documentos.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
4	SISTEMA DE INFORMACIÓN DE SIVICOS MOVILES-CIS	El sistema de información "SIVICOS", permite realizar la inspección in situ de las importaciones/exportaciones en puertos, aeropuertos y pasos fronterizos. Así mismo, genera reportes de eventos y reacciones adversas y la consulta de reportes enviados al INVIMA. Inspección PAPF: Solución informática implementada para ser utilizada con tableta en Windows, Android, utilizada como herramienta por los inspectores al momento de realizar la inspección sanitaria de alimentos, materias primas, insumos y bebidas alcohólicas, expide el certificado.	CLIENTE - SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
5	SISTEMA DE INFORMACION CORRESPONDENCIA Y PQRDS - SESUITE	El sistema de información "CORRESPONDENCIA", permite gestionar y realizar el control de correspondencia interna y externa del INVIMA.	ON PREMISE	ON PREMISE	SI	Transversal a todos los procesos	PHP - JAVA
6	SOLUCIÓN WEB ADMIN	Este sistema web "ADMIN", es interna y permite su gestión diariamente, y genera los reportes diarios y mensuales sobre los siguientes módulos: Certificaciones por Entregar, Notificación por Aviso, Autos por Estado, Registros Cancelados, Registros Negados, Registros o Renovaciones por periodo, Resoluciones Pendientes por Notificar.	WEB	ON PREMISE	NO	Aseguramiento Sanitario	JAVA
7	SOLUCIÓN WEB CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTOS, AEROPUERTOS Y PASOS DE FRONTRERA	Este sistema web "CERTIFICADOS DE INSPECCIÓN SANITARIA EN PUERTO", permite consultar los certificados inspección sanitaria en puerto.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JSP
8	SOLUCIÓN WEB VALIDAR DOCUMENTOS DE APOSTILLE CANCILLERÍA	Este sistema web "DOCUMENTOS DE APOSTILLE CANCILLERIA", permite validar los documentos apostillados.	WEB	ON PREMISE	SI	Aseguramiento Sanitario	JAVA - POWER BUILDER
9	SOLUCIÓN WEB CONSULTA DE DOCUMENTOS EMITIDOS.	Este sistema web "CONSULTA DE DOCUMENTOS EMITIDOS", permite consultar los documentos con firma digital.	WEB	ON PREMISE	NO	Aseguramiento Sanitario	JAVA - POWER BUILDER
10	SOLUCIÓN WEB CODIGO UNICO DE MEDICAMENTOS (CUM).	El Servicio Web "CODIGO UNICO DE MEDICAMENTOS (CUM)", le proporciona al Ministerio de Salud la información de los Códigos Únicos de Medicamentos.	SERVICIO WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA - POWER BUILDER
11	SOLUCIÓN WEB ACIDOS.	Este sistema web "ACIDOS", (Decreto 1033/2014) Sistema de información que soporta el registro de control para la comercialización de ácidos, álcalis o sustancias similares o corrosivas, quien intervenga en el proceso de comercialización de cualquier sustancia sujeta al registro de control, reportará la información que permita la trazabilidad sobre su procedencia, así como la individualización de cada uno de los actores que intervinieron en la operación de comercialización.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
12	SOLUCIÓN WEB FARMACOVIGILANCIA.	Este sistema web "FARMACOVIGILANCIA", permite que usuarios externos reporten información de eventos adversos.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
13	SOLUCIÓN WEB TRANSPARENCIA	Este sistema web "TRANSPARENCIA", permite consultar los registros o renovaciones otorgados en una fecha determinada.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
14	SOLUCIÓN WEB REGISTRO - RECAUDOS	Este sistema móvil "Registro - Recaudos", es una solución que permite realizar el cargue manual de los archivos de los pagos recibidos en las ventanillas de Davivienda a través de la lectura del código de barras.	WEB	ON PREMISE	SI	Inspección, Vigilancia y Control / Aseguramiento Sanitario	Delphi JAVA
15	SOLUCIÓN WEB IVC/SOA.	Este sistema web "IVC/SOA", es una solución Web que permite calcular los Índices de severidad, ocurrencia y afectación, desde los grupos de productos por Dirección misional, hasta el consolidado denominado IRA (Índice de Riesgo Asociado), para cada Dirección misional y el Instituto.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
16	SOLUCION WEB REACTIVOVIGILANCIA.	Este sistema web "REACTIVOVIGILANCIA", permite la notificación, registro y evaluación sistemática de los problemas relacionados con los reactivos de diagnostico in vitro.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
17	SOLUCIÓN WEB TECNOVIGILANCIA.	Este sistema web "TECNOVIGILANCIA", permite el reporte de eventos e incidentes adversos serios e indeseados producidos asociados con los dispositivos médicos.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
18	SOLUCIÓN WEB - IVC SOA PUERTOS.	Este sistema de IVC SOA Puertos, fue construida como una herramienta para consultar, calcular y/o modificar información relacionada con el Modelo IVC SOA Puertos.	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7
19	SOLUCION WEB PROTOCOLOS DE INVESTIGACIÓN -	Este sistema web "PROTOCOLOS DE INVESTIGACIÓN", herramienta del INVIMA, desde la cual se podrá solicitar el trámite de evaluación inicial de protocolos de investigación con productos en investigación/medicamentos desde la comodidad de su casa u oficina.	WEB	ON PREMISE	NO	Inspección, Vigilancia y Control / Aseguramiento Sanitario	JAVA JEE7
20	SOLUCIÓN WEB INSCRIPCIÓN ESTABLECIMIENTOS	Este sistema web "ESTABLECIMIENTOS", permite el registro de establecimientos nacionales y extranjeros, (censo de establecimientos de alimentos).	WEB	ON PREMISE	SI	Inspección Vigilancia y Control	JAVA JEE7

21	SISTEMA DE INFORMACION CERTIFICACIÓN ELECTRÓNICA DEL PROYECTO DE PAÍSES BAJOS Y COLOMBIA	El proyecto de Países Bajos y Colombia se divide en dos frentes: 1. La aplicación SivicosMoviles: La utilizan los funcionarios en Tablet o Windows para las operaciones que manejan en los puertos. 2. Los microservicios desarrollados en OpenShift: Es la lógica que contiene el desarrollo de los servicios para interactuar con Países Bajos.	CLIENTE SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	Java JEE7
22	SISTEMA DE INFORMACIÓN DE LABORATORIOS - SILAB	Es una solución tecnológica, para la gestión de la información generada por los laboratorios desde sus procesos analíticos, que permite la gestión integral de las muestras desde el ingreso al laboratorio hasta la generación del informe de resultados. permitiendo la total trazabilidad en custodia, calidad y control de los datos del informe de resultados.	CLIENTE - SERVIDOR	ON PREMISE	SI	Inspección Vigilancia y Control	C#, TSQL, HTML5, CSS, TypeScript
23	PORTAL WEB INSTITUCIONAL	Plataforma que ofrece al ciudadano de forma integrada información del instituto y servicios que esta presta de forma virtual o a través del internet. Principalmente está dirigida para apoyar a resolver las inquietudes y necesidades del ciudadano y los tramites que este requiere.	WEB	ON PREMISE	SI	Servicio Transversal para todos los procesos	CMS LifeRay - Java
24	SOLUCIÓN WEB KAWAK	Plataforma para administrar el Sistema Integrado de Gestión del Instituto	WEB	NUBE	NO	Administración del Sistema de Gestión Integrado	N/A
25	SOLUCION WEB ITSM ARANDA	Aplicativo que agrupa un conjunto de recursos tecnológicos para brindar o prestar servicios con la posibilidad de gestionar y solucionar de manera integral requerimientos relacionados con tecnología y recursos tecnológicos.	WEB	NUBE	NO	Procesos de Apoyo	N/A
26	HERRAMIENTA ANTIVIRUS KASPERSKY	Programa cuyo objetivo es detectar y eliminar virus informáticos, además los bloquea, desinfecta archivos y puede prevenir la infección o daño que los virus puedan ocasionar a la información.	N/A	ON PREMISE	NO	Gestión de Tecnologías de la Información	N/A
27	SOLUCION WEB OFICINA VIRTUAL	Herramienta que permite la interacción del instituto con el ciudadano a través de medios digitales	WEB	ON PREMISE	SI	Inspección, Vigilancia y Control / Aseguramiento Sanitario	MySQL y PHP
28	DIRECTORIO ACTIVO	Base de datos y conjunto de servicios que conecta a los usuarios de la entidad con los recursos de red que se requieren para realizar su trabajo, esto incluye información crítica sobre el entorno tecnológico incluidos los usuarios, los computadores y acceso a la información, así como la definición de permisos.	ON PREMISE Y NUBE		NO	Gestión de Tecnologías de la Información	N/A
29	CORREO ELECTRONICO	Sistema que permite el intercambio de mensajes entre los diferentes usuarios de la entidad y con otros usuarios externos a la misma.	N/A	HIBRIDO	NO	Servicio Transversal para todos los procesos	N/A
30	SISTEMA DE INFORMACIÓN WEB NUEVA PLATAFORMA DE TRÁMITES Y SERVICIOS (PROYECTO EN DESARROLLO)	Solución tecnológica que se encuentra en desarrollo y permitirá ejecutar en línea las actividades misionales de los procesos "Registros Sanitarios Y Tramites Asociados" Y "Auditorias Y Certificaciones" Del Instituto Nacional De Vigilancia De Medicamentos Y Alimentos – Invima. Para este proyecto se encuentra afectada la información de la arquitectura y los ambientes de calidad y producción que ya habían sido implementados en la plataforma OpenShift y la implementación de la tecnología RPA.	WEB	NUBE	SI	Aseguramiento Sanitario	JAVA
31	SISTEMA DE INFORMACION WEB PARA LA INSPECCIÓN, VIGILANCIA Y CONTROL - SIVICOS (PROYECTO EN DESARROLLO)	Solución tecnológica que se encuentra en desarrollo que permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de Inspección, Vigilancia y Control (basado en un enfoque de riesgo de los reglmenos sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. Para este proyecto se afectó la información de la arquitectura y los ambientes de calidad donde se habían iniciado pruebas funcionales y el ambiente de producción implementados en la plataforma openshift	WEB	NUBE	SI	Inspección, Vigilancia y Control	JAVA
32	REQUERIMIENTOS TRANSVERSALES	Requerimientos generales para mantener evidencia del material probatorio y aprovechar la capacidad de almacenamiento; 80 discos de 900 GB Mecánico					

La salud es de todos | Minsalud

ANEXO 5

PLAN DE ACCIÓN
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN DEL 6 DE FEBRERO DE 2022
Actualización del 25 de Febrero de 2022

1. OBJETIVO

Garantizar la disponibilidad y acceso a la información y las comunicaciones 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 tipo de programa dañino conocido como ransomware denominado Blackbyte.

2. ANÁLISIS DEL RIESGO

A continuación, se presenta el riesgo identificado y gestionado dentro del Sistema de Gestión Integrado del Instituto, en el cual se establece la descripción, causa, efectos y control de este, tal como se observa en la siguiente tabla:

Riesgo	Posibilidad de afectación de la operación de la entidad, por la indisponibilidad del activo de información, debido a las fallas de software y hardware del centro de datos.
Descripción	Imposibilidad de acceso a la información por parte de la entidad cuando se presente una falla en la infraestructura y herramientas tecnológicas del centro de datos (hardware y software).
Causas	Incidente a las vulnerabilidades de los sistemas informáticos de la Entidad que pueden afectar la operación del servicio (origen: Externo, factor: Tecnológico
Efectos	• Pérdida de información. • Demoras en los procesos y/u operación • Atención parcial o nula al ciudadano • Pérdida de imagen Institucional • Insatisfacción de los usuarios internos del Invima • Daños irreversibles en equipos y herramientas tecnológicas • Disminución o pérdida de productividad
Control	Monitoreo y mantenimiento de herramientas para control incidentes informáticos
Descripción del control	Se cuenta con un antivirus y herramientas de control de software dañino que son monitoreados periódicamente por los administradores del centro de datos de acuerdo al procedimiento de administración del centro de datos TIC-GTI-PR004, como soporte se cuentan con logs y reportes de eventos de este monitoreo.

Respecto a lo anterior, se relacionan los posibles efectos o consecuencias de la materialización del riesgo antes mencionado, con sus respectivas acciones y medidas de contingencia frente al incidente cibernético para garantizar la continuidad en la prestación de los servicios y trámites a cargo del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima.

3. PLAN DE ACCIÓN Y MEDIDAS DE CONTINGENCIA FRENTE A LOS POSIBLES EFECTOS O CONSECUENCIAS DEL INCIDENTE CIBERNÉTICO

Posibles efectos	Acciones y medidas de contingencia.
Pérdida de información	A la fecha no se evidencia pérdida de la información, ya que se implementó uno de los controles establecidos frente a este riesgo que consistió en "Disponer de copias de seguridad (backps) para restablecer la plataforma y disponibilidad de la información, así como la aplicación del procedimiento interno "TIC-GSI-PR003- PROCEDIMIENTO GENERACIÓN DE COPIAS DE RESPALDO DE A INFORMACIÓN DE LOS SERVIDORES DEL CENTRO DE CÓMPUTO" lo que ha permitido la continuidad de la operatividad y la prestación servicios de la entidad.
Demoras en los procesos y/o operación	• Emitir medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto. A la fecha se han emitido las siguientes: ▪ Resolución 2022500000 del 9 de febrero de 2022 y la Resolución 2022500001 del 15 de febrero de 2022, sobre medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto, donde se suspenden los términos legales de algunos trámites. ▪ Circular · 1000-001-22, con el fin de agilizar el proceso de nacionalización de alimentos, materias primas y otros alimentos perecederos desde el sitio de ingreso - Puertos, Aeropuertos y Pasos de Frontera, a otros sitios que cumplan con las condiciones sanitarias para su almacenamiento.
Atención parcial o nula al ciudadano	• Activar la gestión manual de los trámites sin suspensión de términos (posteriormente estos se incluirán en las bases de datos correspondientes). • Activar la opción de pago de trámites a través de transferencia bancaria. • Activar radicación y atención de PQRDS.
Pérdida de imagen Institucional	• Mantenido la comunicación e información mediante los distintos canales digitales de la entidad respecto a las medidas de acciones de contingencia para el restablecimiento del servicio. • Desarrollar reuniones con la Presidencia de la República, MinTIC, MINCIT y mesas de trabajo con los diferentes gremios, asociaciones para garantizar la continuidad de la prestación del servicio.
Insatisfacción de los usuarios internos del Invima	• Garantizar el uso de equipos de navegación a internet mediante módems y routers a las diferentes dependencias de la entidad, para la continuidad operativa de los funcionarios y contratistas de la entidad.

Posibles efectos	Acciones y medidas de contingencia.
	• Restablecer Internet en áreas misionales y críticas de la entidad, puertos (Buenaventura, Cartagena, Barranquilla y Santa Marta) y aeropuerto del dorado.
Daños irreversibles en equipos y herramientas tecnológicas	• A la fecha no se han identificado daños irreversibles en equipos y herramientas tecnológicas
Disminución o pérdida de productividad	• Realizar la priorización del restablecimiento de la plataforma SIVICOS para los trámites de certificados de inspección sanitaria en PAPF. • Hacer ampliación del horario de trabajo de funcionarios en puertos, aeropuertos y pasos de frontera para estudio de trámites manuales hasta las 8:00 p.m. así como sábados y domingos jornada completa. • Reforzar la capacidad operativa de los Grupos en Puertos, Aeropuertos y Pasos de Frontera y Ventanilla Única de Comercio Exterior, mediante reasignación de funciones. • Reconstruir el directorio activo, correo electrónico en Microsoft Office 365 • Hacer verificación de los servidores y PC afectados • Realizar alistamiento del administrador del antivirus para servidores y pc con la posibilidad de identificar el virus • Realizar formateo de los equipos (equipos de cómputo, y servidores) y erradicación de cualquier rastro dejado por el incidente, garantizando la desinfección y puesta a punto de la infraestructura • Restaurar copias de seguridad • Reactivar la plataforma Sivicos (Operación en Puertos, Aeropuertos y Pasos de Frontera) • Reactivar el sistema de información de Registros Sanitarios • Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad • Ampliar de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración • Adquirir servicios de infraestructura a través del modelo IAAS, SAAS y/o modelo PAAS • Configurar Portal Web, Oficina Virtual y de sistemas de información de la Entidad en la nube • Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad • Restablecer los demás servicios del Instituto

4. RECURSOS

El desarrollo y ejecución de este plan queda sometido a la disponibilidad de recursos humano, tecnológico y presupuestales que deben ser gestionados por el Instituto, entidades aliadas y el gobierno nacional.

El Equipo de Trabajo está conformado por la totalidad de los servidores públicos del Invima.

5. CRONOGRAMA Y RUTA CRITICA

Ítem	Semanas Previas (Febrero)			Semanas (Marzo, Abril y Mayo)										
	1	2	3	1	2	3	4	5	6	7	8	9	10	11
Actividades Administrativas														
Emisión de Resoluciones con medidas administrativas transitorias para garantizar la continuidad en la prestación de los servicios y trámites del Instituto	■	■	■											
Hacer ampliación del horario de trabajo de funcionarios en puertos, aeropuertos y pasos de frontera para estudio de trámites manuales hasta las 8:00 p.m. así como sábados y domingos jornada completa.	■	■	■											
Reforzar la capacidad operativa de los Grupos en Puertos, Aeropuertos y Pasos de Frontera y Ventanilla Única de Comercio Exterior, mediante reasignación de funciones.	■	■	■											
Mantener la comunicación e información mediante los distintos canales digitales de la entidad respecto a las medidas de acciones de contingencia para el restablecimiento del servicio.	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Desarrollar reuniones con la Presidencia de la República, MinTIC, MINCIT y mesas de trabajo con los diferentes gremios, asociaciones para garantizar la continuidad de la prestación del servicio.		■	■	■	■	■	■	■	■	■	■	■	■	■
Actividades Operacionales y Técnicas														
Reconstruir el directorio activo, correo electrónico en Microsoft Office 365 (RC)	■	■												
Hacer verificación de los servidores y PC afectados (RC)	■	■	■	■	■	■	■	■						
Realizar alistamiento del administrador del antivirus para servidores y pc con la posibilidad de identificar el virus	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Realizar formateo de los equipos (equipos de cómputo, y servidores) y erradicación de cualquier rastro dejado por el incidente, garantizando la desinfección y puesta a punto de la infraestructura		■	■	■	■	■	■	■	■	■	■	■	■	■
Restaurar copias de seguridad (RC)			■	■	■	■	■	■	■	■	■	■	■	■
Reactivar la plataforma Sivicos (Operación en Puertos, Aeropuertos y Pasos de Frontera)				■	■									

Ítem	Semanas Previas (Febrero) 1	2	3	Semanas (Marzo, Abril y Mayo) 1	2	3	4	5	6	7	8	9	10	11
Reactivar el sistema de información de Registros Sanitarios				■	■	■	■	■	■	■	■	■		
Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad			■	■	■	■	■							
Ampliar de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración (RC)			■	■	■	■	■	■	■					
Adquirir servicios de infraestructura a través del modelo IAAS, SAAS y/o modelo PAAS				■	■	■	■	■	■	■	■	■	■	■
Configurar Portal Web, Oficina Virtual y de sistemas de información de la Entidad en la nube					■	■	■	■						
Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad				■	■	■	■	■	■	■	■	■	■	■
Restablecer los demás servicios del Instituto								■	■	■	■	■	■	■

Las actividades marcadas con **(RC)** conforman la ruta crítica del plan de acción

ANEXO 6

ANEXO TECNICO

El domingo 6 de febrero de 2022, se evidenció un incidente de seguridad de la información que comprometió la disponibilidad de los sistemas de información, plataformas tecnológicas y herramientas tecnológicas del Invima, generado por el ataque de un ransomware llamado Blackbyte el cual encriptó la información de la entidad afectando los servidores, y los aplicativos dispuestos para la operación del Instituto.

De conformidad con el Plan de Acción socializado por la entidad para el manejo del incidente, mediante la realización de estos procesos contractuales se da cumplimiento a las siguientes acciones:

- Requerir servicios especializados en seguridad digital para determinar el origen del incidente y establecer medidas de contención frente a potenciales incidentes futuros, así como el aseguramiento de la infraestructura tecnológica de la entidad.
- Ampliación de la capacidad de almacenamiento e infraestructura de cómputo a través de la compra de discos de estado sólido y mecánico y servidores que garanticen infraestructura disponible, y que incluye instalación y configuración.
- Garantizar la suficiencia de licencias de correo para servicios y cuentas genéricas de la entidad.

Es por ello que se deben realizar las siguientes actividades desde la Oficina de Tecnologías de la Información – OTI y el Grupo de Soporte Tecnológico así:

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Aseguramiento de la Infraestructura Tecnológica	El aseguramiento de la infraestructura Tecnológica va orientado a actividades que conduzcan de manera efectiva a la identificación y mitigación de brechas, minimizando riesgos que atenten contra la confidencialidad, la disponibilidad e integridad de la información, así como la de los activos y plataformas que los soportan. El ejercicio de estas actividades se desarrollará basado en las siguientes líneas de servicio: • Hacking Ético: Este servicio va orientado a la explotación de las posibles vulnerabilidades existentes en los sistemas de manera controlada, haciendo pruebas de intrusión que permitan evaluar y obtener un panorama preciso sobre el estado de la seguridad física y lógica de los sistemas de información, portales web, servidores físicos y virtuales, bases de datos entre otros activos de información.	• Hacking Ético: interno de caja blanca para 160 IP[1]s. Se realizará una (1) prueba en el periodo de ejecución del servicio, por lo cual se debe entregar los resultados de las pruebas en un formato que incluya como mínimo y sin limitarse a las explicaciones de los hallazgos, las evidencias, la ruta de ataque, el impacto, la criticidad y la solución. El servicio de pruebas de penetración debe ejecutarse con personal certificado en Penetration Testing o Ethical Hacking. La Prueba de Penetración no debe afectar los servicios del Invima y dicha prueba debe realizarse en coordinación con el supervisor, por lo cual en caso de presentarse una falla producto de dicha prueba, se debe presentar un informe donde se especifique con evidencias, las actividades realizadas y los detalles del servicio afectado. • Pruebas de seguridad para la publicación de cada servicio de la Entidad: El alcance de las pruebas de seguridad a aplicar está dirigido específicamente a los sistemas de información que se vayan restaurando progresivamente y de manera previa a su despliegue en ambiente productivo, de tal forma que se puedan tomar las medidas preventivas y correctivas ante un escenario de riesgo. El total de los sistemas de información que se encuentran en etapa de restauración es de 31 en ambientes web y cliente-servidor.

[1] IP: Internet Protocol – Protocolo de comunicaciones de Internet

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	• Pruebas de seguridad para la publicación de cada servicio de la Entidad: Esta línea de servicio está orientada a la identificación, clasificación y mitigación de debilidades que comprometan la seguridad de cualquiera de los sistemas de información que son soportados por la Infraestructura TI de la entidad, dichas debilidades pueden generar perdida de la información, accesos no autorizados, perdida de gestión de la infraestructura o en efecto pérdida total de las operaciones.	
Sistema de Información para laboratorios SILAB (SAMPLER)	El sistema de Información para Laboratorios de ensayos SILAB (SAMPLER), con el que cuenta el Invima, permite la gestión de la información de la Oficina de Laboratorios de Control y Calidad desde la entrada de las muestras hasta la generación de informes. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando la configuración y acceso a los aplicativos y bases de datos del Sistema de Información de los laboratorios - SILAB - de la entidad, razón por la cual, no es posible acceder desde las máquinas de escritorio a los módulos LIMS (sistema central), recursos (Inventarios), Reportes, BI (consultas de bases de datos), QAQC (sistema de calidad), impresor de etiquetas, instrumental, entre otros. Por este motivo, se requiere que el proveedor del Sistema de Información (SILAB) dueño del código fuente, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores y de máquinas de escritorio que disponga el Invima para su despliegue en ambiente productivo; procedimientos que requieren del conocimiento y experticia del proveedor, para garantizar la estabilidad de este sistema de información en la última versión y con las últimas actualizaciones y desarrollos del software.	**1. Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** **ETAPA UNO – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE BASE DE DATOS** Para este proceso se requiere que la Oficina de Tecnologías de la Información (OTI) del Invima provea el backup de la base de datos a febrero 04 de 2022 y el personal del proveedor hará el montaje de todos los archivos que la base de datos requiere para operar, incluidos los archivos de Log. **ETAPA DOS – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WEB** **Instalación, configuración y parametrización de los Servicios WCF de Sampler y los AplicativosWeb** En los servidores de aplicación se configurarán los módulos LIMS, Recursos, Administrativo, QAQC, Indicadores, Validador, Uploader, Reportes, Gestor Documental, Interactivo y Receptor deMuestras, tanto los aplicativos como los servicios web que los alimentan asegurándose además de documentar el Checklist de Control de cambios. **Instalación, configuración y parametrización de los Servicios Windows** El servicio de Sampler Notificaciones se configurará sobre el servidor de base de datos y se configurará una cuenta de correo del dominio Invima para que envié los correos de notificaciones hacia los buzones de correo de los funcionarios Invima. **ETAPA TRES – INSTALACIÓN, CONFIGURACIÓN Y PARAMETRIZACIÓN DE APLICATIVOS WIN** Los módulos Impresor de Etiquetas, Instrumental, Visor BI, Sampler Tools y Lanzador serán parametrizados en los equipos que Invima designe hasta un total de 120 máquinas, en las sedes de Montevideo y CAN. La parametrización se desarrollará por parte de un funcionario de forma presencial. **ETAPA CUATRO – PRUEBAS Y PUESTA EN MARCHA DEL SISTEMA** El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios de la Oficina de Laboratorios y Control de Calidad y la Oficina de Tecnologías de la Información del Invima, durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado. Así

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		mismo, acompañará el proceso de ajustes de configuración que se requieran para la entrada en operación de la plataforma. **2. Condiciones técnicas del servicio de soporte técnico:** **NIVELES DE SOPORTE:** Soporte de nivel 1 (N1) Este soporte técnico se basa en la asistencia en primera línea o soporte Front-End, donde el técnico tendrá que reunir toda la información relativa al problema. El objetivo es determinar exactamente qué es lo que ocurre y definir cuál es la causa que lo produce. Una vez definido el problema y descubierta su causa, se procede a ser resuelto por el proveedor. **Soporte de nivel 2 (N2)** En este nivel de soporte se cuenta con personal de mayor experiencia y conocimiento, ya que se trata de profesionales especializados en áreas de Help Desk, contando con conocimientos en redes, sistemas microinformáticos, bases de datos, laboratorio y del negocio. Lo habitual es que el soporte de nivel 2, se encargue de problemas que no han podido ser resueltos por los técnicos del nivel 1 al requerir tareas más complejas. **Soporte de nivel 3 (N3)** Es un soporte de alto nivel o soporte de Back-End, y se encarga de los problemas más complejos y técnicos, proporcionando soluciones eficientes a los mismos. El personal de soporte asignado a la solución de estas incidencias, disponen de profundos conocimientos y experiencia en la resolución de problemas de Sampler (SILAB) y cuentan con conocimientos técnicos de productos y servicios informáticos, con habilidades avanzadas de análisis y resolución de problemas y con excelentes habilidades de comunicación. **Soporte de nivel 4 (N4)** Este nivel de soporte este asignado a personal de desarrollo de la plataforma Sampler (SILAB) y tiene que ver con la resolución de incidencias que involucran la manipulación del código fuente. El personal asignado corresponde a ingenieros de sistemas desarrolladores. **Soporte Excepcional** El Invima podrá contar con un servicio de soporte por fuera del horario establecido del 5*8 por hasta 2 incidencias urgentes en un mes, con solución en las siguientes 4 horas hábiles, en un horario de reporte de estas incidencias hasta las 8:00 p.m. de lunes a viernes.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
Sistema de Información Gestor Documental SeSuite – Correspondencia y PQRDS	El sistema de Información Gestor Documental Se Suite (solución SoftExpert ECM Premium), está compuesto por los módulos Componente Utilitario que permite realizar un correlacionamiento de los documentos de los diferentes tramites que son radicados ante el Instituto; de igual manera permite consultar, descargar y generar reportes de los documentos relacionados con la información del sistema y por otro lado, se tiene el módulo de PQRDS que atiende las solicitudes que realiza el ciudadano relacionado con Peticiones, Quejas, Reclamos, Solicitudes y Denuncias. Por último, se cuenta con el módulo de Correspondencia que se encarga de administrar y gestionar la correspondencia entrante, saliente e interna que maneja el Invima a través de los flujos de trabajo definidos. Todos los componentes de este sistema se encuentran alojados, instalados y parametrizados de forma local en los Servidores del Instituto. Teniendo en cuenta que el incidente cibernético ocurrido afectó la infraestructura tecnológica del Invima, se pudo comprobar la encriptación de la información, afectando el Sistema de Información de Gestor Documental Se Suite y Correspondencia y al módulo PQRDS de la entidad, razón por la cual, no es posible acceder a las funcionalidades y a la información que se tiene en el sistema. Por este motivo, se requiere que el proveedor del Sistema de Información, Representante en Colombia de SoftExpert, fabricante del aplicativo, realice la instalación, configuración, parametrización, pruebas y salida a producción del software y de las bases de datos en la infraestructura de servidores que disponga el Invima para su despliegue; procedimientos que requieren del conocimiento y experticia del proveedor y del fabricante, garantizando de este modo una nueva instalación y puesta en marcha óptima para el Invima, recuperando la estabilidad del sistema en la última versión y con los últimos desarrollos entregados por el proveedor a la entidad	**Fase uno: Actividades de instalación** Preparación de prerrequisitos • Configuración y verificación de conectividad y recursos de red. • Verificación conexión con directorio activo. • Configuración de puertos y reglas de seguridad. • Revisión de recursos del servidor. • Descarga de prerrequisitos de instalación SeSuite. • Instalación y configuración de Visual Studio. • Instalación y configuración de Microsoft Office. • Instalación y configuración del Servidor de Base de Datos. • Instalación y configuración del motor de base de datos. • Configuración opciones de red de la base de datos • Instalación Aplicación SeSuite. • Instalación de SeSuite 2.1.6. • Instalación de parche. **Fase dos: Actividades de configuración y parametrización** Configuración del servidor (Producción) • Instalación y configuración Java JRE. • Instalación y configuración de IIS. • Instalación y configuración de "Certificado Digital" • Creación y configuración de usuario de aplicación (SeSuite) • Instalación y configuración del Apache Tomcat. **Ecualización de la base de datos** • Configuración conexión SeSuite y la base de datos • Prueba e inicialización de Servicios • Restauración de la base de datos de INVIMA (SeSuite) **Configuración SE Suite** • Ejecutar procedimientos de activación de SE Suite • Pruebas de conectividad con el directorio activo • Configuración de la sincronización con el Directorio Activo • Configuración y prueba del servidor de correo para SE Suite Notificaciones **Configuración de almacenamiento de archivos** • Configuración de directorios controlados de acuerdo con la entrega de Insumos por parte de Invima. • Configuración y prueba de vínculos de documento con SeSuite **Fase tres: Actividad de Pruebas** • Verificación integridad del software Gestor Documental SeSuite y componentes-módulos • Revisión y ajustes del software Gestor Documental SeSuite y Componentes-Módulos. • Revisión y ajustes de configuración del software Gestor Documental SeSuite y componentes-módulos. • Verificación funcional de flujos del software Gestor Documental SeSuite y componentes-módulos. • Corrección de incidencias con flujos en ejecución del software Gestor Documental SeSuite y componentes-módulos. • Revisión portales y reportes. • Ajustes y corrección de incidencias portales y reportes. • Revisión de integridad para el componente de documentos vs directorios controlados. • Acompañamiento de casa matriz.

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td>permitiendo la gestión oportuna de los documentos, la correspondencia y las PQRDS del Instituto.</td><td>
Fase de estabilización
• Reporte de incidentes y temas relacionados con el registro y puesta a punto de la información.

Fase cuatro: Actividad de Salida a producción
El proveedor acompañará a los líderes funcionales, analistas y/o funcionarios del Grupo de Gestión Documental y de la Oficina de Tecnologías de la Información durante el proceso de revisión/validación/pruebas de usuario que buscan confirmar que la plataforma se comporta de acuerdo con lo esperado.

Operación en producción
Tareas por revisar/ (enlistar)Iniciar/detener los servicios y/o los aplicativos SeSuite, ajustar la configuración para mantener la operatividad del sistema, monitorear el desempeño de los diferentes indicadores de ejecución en los servidores.

Tecnológicos para ambiente de producción
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>128 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>32 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>800 Gygas</td><td>Dos Discos (1) 300 y (1) 500 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>24 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>1 Tera</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteProducción y Utilitario</td><td></td></tr>
<tr><td colspan="3">Servidor de configuración y paso</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos: (1) de 150 Gygas (1) de 350 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td colspan="3">File server</td></tr>
<tr><td>Sistema de archivos</td><td>NTFS</td><td></td></tr>
<tr><td>Capacidad</td><td>20 Teras</td><td></td></tr>
<tr><td colspan="3">Determinar cuál es la mejor manera de emplear este recurso y que el servidor de Aplicaciones pueda acceder la información.</td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
<tr><td colspan="3">Backup de las bases de datos 1 Diario completo y cada 3 horas backup del log</td></tr>
<tr><td colspan="3">Respaldo de los archivos nuevos cargados al File Server diario.</td></tr>
<tr><td colspan="3">Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura</td></tr>
<tr><td colspan="3">Configuración de una estrategia de seguridad robusta</td></tr>
</table>

Tecnológicos para ambiente de pruebas
<table>
<tr><th>REQUERIMIENTOS</th><th colspan="2">CARACTERISTICAS</th></tr>
<tr><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td>Memoria</td><td>64 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>400 Gygas</td><td>Dos Discos de 150 y 250 Gygas</td></tr>
<tr><td>Sistema Operativo</td><td>Windows Server 2019 Datacenter</td><td></td></tr>
<tr><td colspan="3">Servidor de Base de datos</td></tr>
<tr><td>Memoria</td><td>16 Gygas</td><td></td></tr>
<tr><td>Procesador</td><td>8 cores</td><td></td></tr>
<tr><td>Disco Duro</td><td>500 Gygas</td><td></td></tr>
<tr><td>Engine</td><td>SQL Server 2017 Enterprise Edition</td><td></td></tr>
<tr><td>Bases de Datos</td><td>SeSuiteproduccion y Utilitario</td><td></td></tr>
<tr><td colspan="3">Características Especiales</td></tr>
<tr><td colspan="3">Respaldo del Servidor Aplicaciones - Verificar estrategia de Activo - Pasivo</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>SERVICIOS Y/O SOFTWARE</th><th>JUSTIFICACIÓN TÉCNICA</th><th>CONDICIONES TÉCNICAS</th></tr>
<tr><td></td><td></td><td>Backup de las bases de datos 1 Diario completo y cada 3 horas Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma S
Acceso por Escritorio Remoto al Servidor de Aplicaciones de Forma Segura
Configuración de una estrategia de seguridad robusta.</td></tr>
<tr><td>Buzones de correo electrónico</td><td>Office 365 es el conjunto de programas informáticos de ofimática que contiene entre otras, correo, calendarios, programas de procesamiento de texto y hojas de cálculo y que se adquiere anualmente para los funcionarios y contratistas. El Invima cuenta desde el año 2019 con licenciamiento de Office 365 el cual fue puesto en funcionamiento y asignado en febrero de 2020 con un número inicial de 1505 suscripciones. Para la vigencia 2022 se consolidaron todas las licencias bajo suscripciones de Office 365 E3 y se incrementó en 50 suscripciones más, permitiendo contar con un total de 1755 suscripciones de Office 365 E3 para funcionarios y contratistas del Invima.

En este sentido, el Invima cuenta con una configuración hibrida entre su infraestructura local (On-Premise) y en la nube de Microsoft Exchange, con el propósito de permitir la correcta migración, creación, parametrización y gestión de los buzones de correos electrónicos de cada usuario y de los buzones compartidos de la entidad.

Teniendo en cuenta que, la entidad sufrió un ataque cibernético en el mes de febrero de 2022, ocasionando entre otros, que se viera afectada la disponibilidad de recursos tales como, sistemas de información, aplicaciones y</td><td>
<table>
<tr><th>No</th><th>CÓDIGO CATALOGO</th><th>DESCRIPCIÓN DEL PRODUCTO</th><th>CARACTERÍSTICAS TÉCNICAS</th></tr>
<tr><td>1</td><td>TQA-00001EAEASAP</td><td>Microsoft®ExchangeOnlinePlan2 ShrdSvr AllLng MonthlySubscriptions-VolumeLicense MVL 1License PerUsr_EA_EAS_AP</td><td>• Cada usuario dispone de un buzón con 100 GB de espacio de almacenamiento y puede enviar mensajes de hasta 150 MB de tamaño
• 100 GB en el buzón principal del usuario y, además, 1.5 TB en el buzón de archivo del usuario.
• Conexión con versiones compatibles de Outlook a Exchange Online.
• Control de datos empresariales confidenciales con directivas de prevención de pérdida de datos (DLP) integradas.
• Todos los buzones están protegidos con protección premium contra correo no deseado y malware mediante Exchange Online Protection
• Más información en: https://www.microsoft.com/es-co/microsoft-365/exchange/compare-microsoft-exchange-online-plans</td></tr>
<tr><td>2</td><td>KF5-00002EAEASAP</td><td>Microsoft® Defender O365 P1 Subscription Per User_EA_EAS_AP</td><td>• Protección de próxima generación que incluye protección antimalware y antivirus robusta.
• Acciones de respuesta manual, como enviar un archivo a cuarentena en dispositivos o</td></tr>
</table>
</td></tr>
</table>

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS			
	correos electrónicos creados y/o configurados de manera local (On-Premise) afectando su funcionamiento y quedando indisponibles, razón por la cual en este momento no permite que se creen nuevos correos electrónicos y aprovisionar de forma correcta los buzones para su uso en los aplicativos de la entidad. Al respecto, el Grupo de Puertos Aeropuertos y pasos de frontera [PAPF] antes de la afectación presentada, desarrollaba las actividades de notificación con los usuarios internos y externos mediante correos electrónicos On-premise de Microsoft para el envió de correos adjuntando los documentos expedidos por el Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima desde el aplicativo SivicosMoviles, por lo cual al momento de presentarse la indisponibilidad de los servicios de buzón de correos electrónicos On-Premise, se vieron afectados los correos que se usaban para tal fin. Así mismo para los aplicativos: Fármaco, Tecno y Reactivo Vigilancia que apoya el proceso Inspección, Vigilancia y Control (IVC) se requieren cuentas de correo electrónico adicionales para notificar a los usuarios e instituciones de los registros y actualización. En este mismo sentido, se contempla la necesidad de asignar cuentas de correo electrónico online para el aplicativo de SeSuite, correspondencia y PQRSD y suscripciones de correo electrónico que deben ser asociados al aplicativo denominado: Certimail, ya que a través de esta plataforma de Correo Electrónico Certificado el Invima cuenta con un servicio de notificación electrónica por e-mail. Por medio de estas cuentas de correo electrónico y su respectivo aseguramiento se espera poder reestablecer de la gestión de información con usuarios externos, la remisión de documentos y correspondencia, garantizando la integridad y la trazabilidad de los mensajes de datos y archivos enviados por el Instituto. El aprovisionamiento de correos electrónicos en ambiente de nube (Cloud), permitirá el almacenamiento en				archivos cuando se detectan amenazas • Capacidades de reducción de la superficie de ataque que fortalecen los dispositivos, evitan los ataques de día cero y ofrecen un control granular sobre el acceso y los comportamientos de los terminales. • Configuración y administración centralizadas con el portal de Microsoft 365 Defender e integración con Microsoft Endpoint Manager • Protección para una variedad de plataformas, incluidos dispositivos Windows, Mac OS, iOS y Android • Más información en: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1?view=o365-worldwide

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	la nube de Microsoft de la información gestionada a través de estos correos, permitiendo disponibilidad permanente de los servicios, acceso en diferentes equipos electrónicos y desde diferentes lugares geográficos a través de una conexión a internet.	
Gestionar el aumento de la capacidad de almacenamiento de información a través de la compra de discos de estado sólido y mecánico que garanticen infraestructura disponible, y que incluye instalación y configuración	Los componentes de los sistemas de información del invima se encuentran alojados localmente en el datacenter de la Entidad. Dado que la mayoría de los servidores se encuentran encriptados debido al incidente tecnológico, los servicios de la entidad se han tenido que ir restableciendo gradualmente, toda vez que no se cuenta con la capacidad de almacenamiento para subir y mantener operativos todos los servicios requeridos por la entidad. Adicionalmente, los discos con los que cuenta la entidad (una vez sean formateados) no tienen la capacidad de almacenamiento necesario para realizar el restablecimiento de los servicios de manera óptima y rápida debido a la limitación de estos, por lo que se tardaría más tiempo del necesario en restablecer sistemas de información que impactan en los servicios que presta la entidad al ciudadano. Por otro lado, la entidad ha seguido operando algunos servicios de manera manual, por lo que se advierte que una vez restablecidos los servicios se necesitará más espacio para almacenar la información que se ha generado a partir de los procesos manuales, además de los Backups o copias de seguridad que se deben realizar y las pruebas de recuperación y de seguridad, teniendo en cuenta que se actualizaron las políticas de backup de la entidad por las situaciones derivadas del incidente mencionado. Estas nuevas políticas serán más exhaustivas, incluyendo las máquinas virtuales y los LOGs de tráfico de la red. En este sentido, se requiere la adquisición de discos de estado sólido y mecánico para garantizar infraestructura disponible para restaurar los servicios y ejecutar las copias y/o backups necesarios para el resguardo de la información de la entidad.	**Discos:** 18 Discos duros para el dispositivo del almacenamiento IBM Flashsystem 5000 Serial: 781k1y6.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Es importante resaltar que se hizo el debido estudio a los acuerdos marco de precio de Colombia Compra Eficiente – Agencia Nacional de Contratación Pública, y no se encontraron los discos con las especificaciones técnicas requeridas por la Entidad.	
Aumento (temporal) del ancho de banda para cargue de información	Respecto de la información encriptada que se encuentra contenida en los servidores de la entidad, se requiere que sea cargada en el espacio en nube de la plataforma SharePoint de Microsoft. Para esto se requiere aumentar el ancho de banda para la velocidad de subida de la data, lo que permitirá que el cargue de la información se haga de forma más ágil, lo que permitirá contar con la disponibilidad de los servidores que se encuentran en el Datacenter de la entidad.	Se realizará la ampliación del canal actual de Internet Dedicado (Enlace Principal/CMREZ77 y Backup/CMREZ78). El enrutador con el que actualmente se cuenta es un equipo Huawei 6120 el cual soporta hasta un 1Gb, pero por condiciones técnicas de seguridad se amplía hasta 900 Mbps, por lo anterior se propone ampliar el servicio a 900 Mbps, de manera que no sea necesario cambiar el enrutador y el servicio pueda ser ampliado en tres (3) días hábiles.
Apoyo técnico para el aseguramiento, alistamiento y puesta en funcionamiento de los computadores, portátiles y servicios de impresión	Se requiere del apoyo técnico para lograr el alistamiento de todos los computadores y servicios de impresión de la Entidad. Para cumplir con los cronogramas establecidos, no se cuenta con personal suficiente en la entidad. Las actividades a realizar son las siguientes: • Realizar la validación inicial de los casos identificando el requerimiento o incidencia a solucionar. • Tipificación de los casos generados en la herramienta de Gestión Aranda. • Realizar el escalamiento al siguiente nivel registrando el diagnóstico y documentación requerida por el siguiente nivel. • Recibir, atender, solucionar y cerrar los casos asociados a un incidente o requerimiento reportado por el usuario. • Recibir los casos escalados por la mesa de servicio por los medios habilitados. • Anotar las acciones realizadas durante la resolución, indicando la verdadera causa que motivó el caso. • Solucionar los casos escalados por la mesa de servicios, cumpliendo los Acuerdos de Niveles de Servicio (ANS) convenidos. • Hacer seguimiento a actividades específicas para la solución dentro de las ventanas de tiempo acordadas.	Los horarios del servicio para el soporte técnico en sitio en Bogotá serán de lunes a viernes de 8:00 am a 6:00 pm o en el horario que sea requerido por la entidad, sin sobrepasar el tiempo máximo establecido para que cada agente labore diariamente cumpliendo con la reglamentación colombiana y para que la entidad cuente siempre con la disponibilidad del servicio. Los requerimientos de servicios que sean necesarios para cubrir la contingencia serán establecidos entre las partes acorde al análisis de necesidades de la entidad.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	• Priorizar las necesidades / requerimientos sobre los procesos atendidos. • Participar en las reuniones de seguimiento según la periodicidad acordada en el contrato o acta de inicio del contrato. • Realizar el Análisis de los procesos del servicio y las mediciones de los Niveles de Servicio, identificando desvíos y acordando las acciones preventivas y correctivas que apliquen. • Gestionar los riesgos que puedan afectar la operación normal del servicio.	
Sistema de Información Nueva Plataforma de Trámites y Servicios (en desarrollo)	El sistema de Información de Nueva Plataforma de Trámites y Servicios es un sistema de información que, una vez desarrollado, permitirá ejecutar en línea las actividades misionales de los procesos: "registros sanitarios y trámites asociados" y "auditorias y certificaciones" de la Entidad. Este sistema se encuentra en proceso de desarrollo por el contratista SOAIN Software Associates SAS de conformidad con el contrato 710 de 2020 con objeto: desarrollar una solución tecnológica consistente en la implementación de la nueva plataforma de trámites y servicios para ejecutar en línea, las actividades misionales de los procesos: "registros sanitarios y tramites asociados" y "auditorias y certificaciones" del Instituto Nacional de vigilancia de Medicamentos y Alimentos - Invima. A partir del Incidente tecnológico se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat y RPA AA) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes, así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de desarrollo y codificación para la Nueva Plataforma de Tramites y	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Servicios de conformidad a las condiciones técnicas del proyecto.	desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Sistema de Información SIVICOS III (En desarrollo)	El sistema de información de Sivicos fase III es un sistema de información que una vez desarrollado permitirá la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control que se ejecutan por parte de las direcciones misionales del Invima. Este sistema se encuentra en proceso de desarrollo por la Unión Temporal SOAIN BS Sivicos de conformidad con el contrato 760 de 2020 con objeto: desarrollar una solución consistente en un software que permita la sistematización, automatización, gestión de visitas, integración, interoperabilidad, realización y seguimiento de las actividades del macroproceso de inspección, vigilancia y control (basado en un enfoque de riesgo de los regímenes sanitarios) que se ejecutan por parte de las direcciones misionales del Invima. A partir del incidente tecnológico, se afecta la instalación, configuración y parametrización de la plataforma tecnológica (Todos los componentes de Redhat) en ambientes de QA y Producción, las configuraciones, parametrizaciones y desarrollos de todos los entregables realizados hasta finales del 2021 para ambos ambientes y así como las pruebas y verificaciones de funcionalidad realizadas en cada una de las etapas de los entregables con los usuarios. Por lo tanto, se requiere completar la fase de sistematización y automatización para el proyecto de Sivicos de conformidad a las condiciones técnicas del proyecto.	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa instalación, Configuración y Parametrización:** **Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue.

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		Despliegue Base de Datos: Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.
Modulo Comisión Revisora	El Módulo de comisión revisora es un software que se integra con el Sistema de Información de Nueva Plataforma de Trámites y Servicios para automatizar los procesos de La Comisión Revisora de la Dirección de Medicamentos y Productos	**Condiciones técnicas del servicio de instalación, configuración, parametrización, pruebas y salida a producción:** • **Etapa Instalación, Configuración y Parametrización:**

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
	Biológicos del Instituto de Vigilancia y Alimentos y Medicamentos Este sistema fue desarrollado en el marco del convenio de cooperación con Innpulsa Numero 180 de 2021. Teniendo en cuenta el incidente cibernético ocurrido y que afectó la infraestructura tecnológica del Invima, se pudo comprobar que se comprometieron las configuraciones y los desarrollos realizados en el marco del mencionado contrato. Con el fin de habilitar el módulo de la comisión revisora se requiere realizar la instalación, configuración, parametrización, pruebas y salida a producción del mismo, para continuar su integración en el proyecto de Nueva Plataforma.	**Configuración VPN:** Se procede a configurar una Red Privada Virtual C2S, para garantizar la seguridad al momento de ingresar a la plataforma y hacer de manera confiable el envío de la información de los diferentes componentes que se tienen en la solución. Una correcta implementación de esta tecnología va a permitir y asegurar la confidencialidad e integridad de todos los datos y la información que se transmite por medio de la red. La capa extra de seguridad que otorga una VPN es especialmente útil cuando se conecta a una red pública y quieres acceder a información privada de la entidad. De no hacerlo así, sería relativamente sencillo para una persona ajena a la entidad capturar los paquetes sin cifrar y obtener las cuentas de usuario. Con la conexión VPN los paquetes se envían cifrados, de manera que aquel que intercepte la información no podrá descifrar la información y, por ende, no podrá hacer nada con ella. **Implementación Openshift:** Se debe garantizar que los requisitos mínimos requeridos para la instalación de la plataforma estén garantizados, además de confirmar que los accesos necesarios para el equipo que debe realizar el proceso se encuentren habilitados. Antes de instalar se deben revisar los requisitos del sistema de cada uno de los productos y el dimensionamiento de la ocupación. **Implementación Automation Anywhere:** Se verifican los accesos necesarios a la infraestructura, se configura la base de datos de la plataforma y finalmente se instalan las licencias de Office necesarias para hacer la ejecución de los agentes. Control Room se implementa en servidores de centros de datos. Los requisitos mínimos de hardware de Automation Anywhere incluyen: tipo de servidor, tipo de máquina, procesador, RAM, espacio de almacenamiento en disco y red. **Implementación DevOps:** Para el proceso de integración y despliegue continuo se va a utilizar Jenkins que es la herramienta encargada de hacer la ejecución de los Pipelines, la cual se debe instalar y sobre esta realizar la configuración de los pipelines para los diferentes ambientes tanto producción como calidad. Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito. Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue. **Despliegue Base de Datos:** Se hace la creación en el ambiente de calidad del modelo de datos necesario para todos los proyectos, además de los procedimientos almacenados, funciones y secuencias que son necesarios en cada una de las entidades. Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominadas comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos

SERVICIOS Y/O SOFTWARE	JUSTIFICACIÓN TÉCNICA	CONDICIONES TÉCNICAS
		servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. **Instalación del Ambiente de Calidad:** la Instalación en el ambiente de Calidad de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. **Instalación del Ambiente de Producción:** Instalación en el ambiente de Producción de las herramientas de Automatización en el servidor del Control Room, con lo cual se procede a hacer la configuración del Control Room para hacer la gestión de los agentes y se configuran los servidores del Boot Runer los cuales se encargan de levantar los agentes y hacer el seguimiento de la ejecución de cada uno de estos. • Para este caso se contempla la instalación del entorno de calidad y producción On premises donde se realizan las siguientes actividades: • Instalación de la Herramienta Automation Anywhere en el Server Control Room • Configuración del Control Room en Herramienta Automation Anywhere • Configuración Herramienta Automation Anywhere en Servidores BotRunner • **Etapa Pruebas y salida a Producción:** **Despliegue Aplicaciones:** Se procede en el ambiente de calidad y posteriormente de producción a hacer el despliegue de cada microservicios desde el Registry de OpenShift, y se verifica que el proceso de escalamiento de la solución esté funcionando perfectamente, además se debe hacer la publicación de cada endpoint por medio de api gateway, y la configuración del SSO para garantizar las políticas de autenticación y autorización para capa endpoint del API de la solución, posteriormente este proceso se comienza a controlar desde los pipelines de despliegue continuo.