Campos de respuesta

No.	Nombre del campo	Tipo de dato	Longitud permitida	Valores permitidos	Obligatorio
0	Resultado	A	50	Código para seguimiento de la solicitud	SI
1	Mensaje	A	200	Mensaje de respuesta a la solicitud.	SI
2	Código	A	10	Código de respuesta a la solicitud. Código: Mensaje 200: OK E: Campos de entrada incompletos GE01: Estructura de los datos de entrada incorrectos	SI

4. Características técnicas de Intercambio de información con SAT

Las características de los servicios Web que se implementan tanto en SAT, como en las administradoras de pensiones, para el envío de la información de solicitudes, son:

1. **Lenguaje del Servicio Web.** Los servicios web deben ser desarrollados haciendo uso de los siguientes elementos:

- Datos de entrada y salida en formato JSON
- Servicios RESTful
- Documentación de los servicios en Swagger

Las respuestas de los servicios estarán documentadas en el Swagger que se disponga, y tendrán por lo menos un código resultado acorde a:

Código	Descripción
200	Éxito en la transacción
400	Datos no enviados correctamente
401	Autenticación fallida
500	Error interno del servidor. Cuando al realizar la transacción el servicio no puede responder

2. **Esquema de seguridad.** Para el acceso a los servicios Web, el SAT y las administradoras contarán con el siguiente esquema de seguridad para la interoperabilidad.

a) Para el envío de las solicitudes de afiliación retracto y el reporte de inicio y terminación de la relación laboral, e inicio y retiro del trabajador independiente a las administradoras de pensiones, el SAT tendrá en cuenta los siguientes requerimientos:

- Esquema de seguridad OAuth2. Una vez implementado, cada administradora debe enviar al Ministerio de Salud y Protección Social la información de ClientID y Password. Se recomienda que la información de la clave pueda ser modificada posteriormente vía Web por el Ministerio de Salud y Protección Social, cada vez que se considere necesario.
- Cifrado de mensajes. El Ministerio de Salud y Protección Social enviará los mensajes de las solicitudes por canal SSL, por lo que la información viajará cifrada, por ello no se realizará cifrado adicional a los mensajes.
- Registros de auditoría. El Ministerio de Salud y Protección Social guardará registro de traza de cada solicitud, a nivel de qué envía y qué respuesta obtiene. Así mismo, construirá un servicio de consulta para esta traza, con los siguientes datos:

Campos de entrada

No.	Nombre del campo	Tipo de dato	Longitud permitida	Valores permitidos	Obligatorio
1	Resultado	A	50	Código para seguimiento de la solicitud	SI

Campos de respuesta

No.	Nombre del campo	Tipo de dato	Longitud permitida	Valores permitidos	Obligatorio
1	Código	A	10	Código de respuesta a la solicitud. Código: Mensaje 200: OK E: Campos de entrada incompletos GE01: Estructura de los datos de entrada incorrectos	SI
2	Mensaje	A	200	Mensaje de respuesta a la solicitud.	SI
3	Datos de entrada	A	N.A.	Estructura de entrada en formato JSON	SI
4	Datos de respuesta	A	N.A.	Estructura de salida en formato JSON	SI
5	Fecha de la transacción asociada al resultado	A	19	Fecha de la transacción asociada al resultado en formato AAAA-MM-DDTHH:mm:SS	SI

b) Para el envío de las respuestas de las administradoras de pensiones a las solicitudes de afiliación y retracto y el reporte de inicio y terminación de la relación laboral, e inicio y retiro del trabajador independiente al SAT, las administradoras tendrán en cuenta los siguientes requerimientos:

- *Esquema de seguridad OAuth2*. El Ministerio de Salud y Protección Social habilitará la funcionalidad de administración de servicios Web para que cada administradora de pensiones pueda conocer la información de ClientID de cada servicio web dispuesto, usuario a utilizar y pueda asignar su clave.
- *Cifrado de mensajes*. Las administradoras enviarán la información de cada servicio web a través de canal SSL, por lo que la información viajará cifrada, por ello no se realizará cifrado adicional a los mensajes.
- *Registros de auditoría*. La administradora guardará registro de traza de cada reporte, a nivel de qué envía y qué respuesta obtiene. Así mismo, construirá un servicio de consulta para esta traza, con los siguientes datos:

Campos de entrada

No.	Nombre del campo	Tipo de dato	Longitud permitida	Valores permitidos	Obligatorio
1	Resultado	A	50	Código para seguimiento de la solicitud	SI

Campos de respuesta

No.	Nombre del campo	Tipo de dato	Longitud permitida	Valores permitidos	Obligatorio
1	Código	A	10	Código de respuesta a la solicitud. Código: Mensaje 200: OK E: Campos de entrada incompletos GE01: Estructura de los datos de entrada incorrectos	SI
2	Mensaje	A	200	Mensaje de respuesta a la solicitud.	SI
3	Datos de entrada	A	N.A.	Estructura de entrada en formato JSON	SI
4	Datos de respuesta	A	N.A.	Estructura de salida en formato JSON	SI
5	Fecha de la transacción asociada al resultado	A	19	Fecha de la transacción asociada al resultado en formato AAAA-MM-DDTHH:mm:SS	SI

(C. F.).

CIRCULARES EXTERNAS

CIRCULAR EXTERNA NÚMERO 0000022 DE 2021

(marzo 17)

PARA: ENTIDADES PROMOTORAS DE SALUD (EPS) DE LOS REGÍMENES CONTRIBUTIVO Y SUBSIDIADO, ENTIDADES ADAPTADAS, ADMINISTRADORES DE LOS REGÍMENES ESPECIAL Y DE EXCEPCIÓN, INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD (IPS), SECRETARÍAS DE SALUD O ENTIDADES QUE HAGAN SUS VECES, POBLACIÓN MAYOR DE 80 AÑOS, PROFESIONALES INDEPENDIENTES DE SALUD.

DE: MINISTRO DE SALUD Y PROTECCIÓN SOCIAL.

ASUNTO: AGENDAMIENTO PARA VACUNACIÓN DE LA POBLACIÓN MAYOR DE 80 AÑOS Y PROFESIONALES INDEPENDIENTES DE SALUD DEL PNV, QUE AÚN NO SE HAN INMUNIZADO EN EL MARCO DEL PLAN NACIONAL DE VACUNACIÓN CONTRA LA COVID-19.

FECHA: 17 de marzo de 2021

Este Ministerio en ejercicio de sus funciones constitucionales y legales como órgano rector del Sector Salud y de Protección Social, encargado de la dirección, orientación y conducción del Sistema General de Seguridad Social en Salud (SGSSS) en desarrollo de lo establecido en el Decreto número 109 de 2021, instruye a los destinatarios de esta circular sobre algunas medidas para agilizar el agendamiento e inmunización de la población mayor de 80 años y profesionales independientes de salud, previas las siguientes consideraciones:

1. El Gobierno nacional expidió el Decreto número 109 de 2021, a través del cual se adopta el Plan Nacional de Vacunación contra la COVID-19 y se establece la población objeto, los criterios de priorización, las fases y la ruta para la aplicación de la vacuna, las responsabilidades de cada actor tanto del Sistema General de Seguridad Social en Salud, como de los administradores de los regímenes Especial y de Excepción.
2. El objetivo del Plan Nacional de Vacunación contra la COVID-19 es reducir la morbilidad grave y la mortalidad específica por esta enfermedad, disminuir la incidencia de casos graves y proteger a la población que tiene alta exposición al virus, reducir el contagio en la población general, y de esta manera controlar la transmisión y contribuir a la inmunidad colectiva en el país.
3. El artículo 7° del citado Decreto número 109 de 2021, dividió el Plan Nacional de Vacunación contra la COVID-19 en dos (2) fases y cinco (5) etapas. La primera fase está integrada por tres (3) etapas, siendo lo propio en la Etapa 1, vacunar al personal cuya actividad principal está involucrada con la atención de pacientes que tienen diagnóstico confirmado de COVID-19 y las personas de 80 años y más.

Por lo anterior, con el fin de agilizar de forma organizada la finalización de la Etapa 1, se instruye a los destinatarios de la presente circular:

1. Agendamiento de la población mayor de ochenta (80) años que aún no han sido vacunadas.

El proceso de agendamiento para los mayores de 80 años que aún no han sido inmunizados por dificultades en el proceso de contactabilidad, actualización de datos o quienes no pudieron cumplir la cita asignada, deberán acercarse a cualquier punto de vacunación de la red de su EPS o al punto de vacunación COVID más cercano a su domicilio o al lugar donde sea más accesible a su cuidador, del 16 al 21 de marzo de 2021, con cédula de ciudadanía y un acompañante mayor de edad, preferiblemente no adulto mayor.

Con el propósito de evitar aglomeraciones en estos espacios, se recomienda a las entidades territoriales disponer medidas como "*pico y cedula*", "*pico y género*" o cualquier otra que consideren pertinente para facilitar la vacunación de esta población, sin exponerlos al riesgo de contagio.

En caso de que el mayor de 80 años tenga agendada la aplicación de la vacunación, se debe cumplir con la cita en la fecha y el horario establecido.

2. Agendamiento de los profesionales independientes que aún no han sido vacunados.

Los prestadores de servicios de salud clasificados como profesionales independientes que aún no han sido vacunados, accederán a la vacunación de la siguiente forma:

2.1 El Ministerio de Salud y Protección Social dispondrá a las EPS los listados cargados en la plataforma PISIS, que se encuentren en MI VACUNA, tanto del talento humano en salud, apoyo logístico y administrativo.

2.2 A partir de este listado, las EPS entregarán la información a las IPS vacunadoras de su red de prestadores de servicios de salud, quienes procederán a realizar el proceso de agendamiento, una vez se realice la verificación previa de su inclusión en el aplicativo MIVACUNA.

2.3 Los profesionales y el personal de apoyo logístico y administrativo, asistirán a la IPS vacunadora determinada por cercanía a su domicilio o a su lugar de trabajo para la aplicación de la vacuna contra la COVID-19.

Finalmente, es necesario señalar que en caso de que se agende a una persona como parte del proceso de vacunación en una IPS que no corresponda a la de su ciudad de residencia, el ciudadano podrá comunicarse o acercarse a una IPS cercana a su residencia para solicitar el agendamiento de vacunación contra la COVID-19, el único requisito será la verificación de la priorización en el aplicativo MIVACUNA, independientemente de su condición de aseguramiento.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 17 de marzo de 2021.

El Ministro de Salud y Protección Social,

Fernando Ruíz Gómez.

(C. F.).

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

RESOLUCIONES

RESOLUCIÓN NÚMERO 00500 DE 2021

(marzo 10)

por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

La Ministra de Tecnologías de la Información y las Comunicaciones, en ejercicio de sus facultades legales, en especial las que le confiere el parágrafo del artículo 16 del Decreto número 2106 de 2019, y

CONSIDERANDO QUE

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2° de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto número 1078 de 2015 (DUR-TIC), *por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*, la Política de Gobierno Digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Según el numeral 2, del artículo anteriormente citado, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad y privacidad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

El parágrafo del artículo 16 del Decreto número 2106 de 2019, *por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública*, señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Por lo anterior, es necesario que MinTIC establezca los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

En mérito de lo expuesto,

RESUELVE:

Artículo 1°. *Objeto*. La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

Artículo 2°. Ámbito de aplicación. Serán sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto número 1078 de 2015 (DUR-TIC), *por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*.

Artículo 3°. *Lineamientos generales*. Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.

Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura crítica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

Artículo 4°. *Sistema de gestión de seguridad de la información y seguridad digital*. Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia.

Artículo 5°. *La estrategia de seguridad digital*. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto número 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

1. Ser aprobada a través de un acto administrativo de carácter general.
2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.
4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones (PIC), o el que haga sus veces.