Gmail **Paiweb Risaralda <risaraldapaiweb@gmail.com>**

# Impacto de la nueva actualización de seguridad – Código PAI Web

3 mensajes

**Paiweb Risaralda** <risaraldapaiweb@gmail.com> 7 de abril de 2026 a las 11:54
Para: Monica Liliana Serrato Lanuza <mserrato@minsalud.gov.co>
Cc: Claudia Liliana Sosa Mesa <csosa@minsalud.gov.co>, bromero@minsalud.gov.co, Vacunación Secretaria de Salud <vacunacion@risaralda.gov.co>

Cordial saludo

Queremos dar a conocer las situaciones presentadas a raíz de la implementación del código de seguridad en el sistema Paiweb en el departamento de Risaralda.

## 1. Situación

| # | Situación | Consecuencia |
|---|---|---|
| 1 | **Bloqueo inmediato** ante cualquier error o demora en la digitación del código | El operador queda fuera del sistema y no puede continuar la vacunación |
| 2 | **No hay tolerancia** a condiciones del terreno (clima, conectividad, zona geográfica) | Municipios rurales o de difícil acceso son los más afectados |
| 3 | **No se puede verificar estado vacunal** de menores vacunados en otras sedes sin carnet | Riesgo de duplicidad o pérdida de seguimiento vacunal, errores programáticos |
| 4 | **La reactivación solo es manual** (vía administrador departamental) | Tiempos de espera prolongados; usuarios finales no esperan |
| 5 | **Saturación de solicitudes de desbloqueo** (15 solicitudes en solo 2 días, un solo municipio) | Desgaste operativo insostenible para el referente departamental |

**Problemas técnicos recurrentes.**

Error "la conexión no es privada" / certificados de seguridad, esto ocurre al acceder al Paiweb.
Acceso intermitente sin explicación técnica, siempre se mencionan fallos en internet.

**Solicitud concreta al Ministerio**

Como referente de sistemas del PAI Risaralda, solicité:

Mesa técnica con participación de los departamentos para conocer las situaciones presentadas que afectan la operación del programa
Ajustes al código de seguridad:
Ampliar tiempo de validez (codigo por día)
Implementar reactivación automática (SMS o correo)
Revisar problemas de certificados y compatibilidad de navegadores.
Revisar las políticas de bloqueo de usuarios
Establecer un canal directo de reporte desde los departamentos hacia el área técnica del ministerio.

"El nuevo código de seguridad está afectando la operatividad del PAI en Risaralda. Pasamos más tiempo desbloqueando usuarios que vacunando. Solicitamos una revisión urgente."

--
Farid Alexis Romero
**Sistemas de Información**
**Programa Ampliado de Inmunizaciones**
Risaralda




**Monica Liliana Serrato Lanuza** <mserrato@minsalud.gov.co> 21 de abril de 2026 a las 9:05
Para: Paiweb Risaralda <risaraldapaiweb@gmail.com>, Vacunación Secretaria de Salud <vacunacion@risaralda.gov.co>
Cc: Beatriz Eugenia Romero Tabima <bromero@minsalud.gov.co>, Claudia Liliana Sosa Mesa <csosa@minsalud.gov.co>, Mauricio Mosquera Gutierrez <mmosquera@minsalud.gov.co>

Cordial saludo.

En atención a la notificación recibida, se da respuesta a las inquietudes planteadas. Asimismo, se precisa que, cuando se realizan ajustes en el sistema que impactan a los usuarios, suele presentarse un período de estabilización en el uso de la herramienta.

Es importante aclarar que, en las zonas con difícil acceso a la red de internet, el ingreso a PAIWEB se ve limitado debido a que la plataforma funciona en línea. En este contexto, la implementación de la autenticación de doble factor no representa una barrera adicional, ya que la principal dificultad radica en la conectividad.

En este sentido, se solicita al departamento brindar apoyo a los usuarios en la aclaración de dudas, así como socializar las medidas dispuestas por este ministerio, con el fin de reducir progresivamente los inconvenientes relacionados con los bloqueos por parte de los usuarios al ingreso de la contraseña o código de verificación incorrecto

Como se informó en el oficio enviado el 5 de marzo de 2026 a las entidades territoriales, en relación con el “Fortalecimiento de los controles de acceso y la seguridad de la información en PAIWEB”, este Ministerio implementó la autenticación de doble factor como medida de seguridad para el acceso al sistema PAIWEB.

El Sistema de Información Nominal del Programa Ampliado de Inmunizaciones (PAIWEB) es una plataforma administrada por el Ministerio de Salud y Protección Social, destinada al registro, actualización y custodia de la información nominal sobre la aplicación de vacunas en la población residente en el país, así como en personas que transitan por zonas de frontera. Este sistema constituye el repositorio oficial del historial vacunal en Colombia.

Dado que PAIWEB almacena y gestiona datos sensibles, resulta indispensable implementar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información. En este sentido, es fundamental cumplir con lo dispuesto en la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1377 de 2013, así como con los lineamientos de seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Adicionalmente, estas medidas se alinean con la Ley 1273 de 2009, que tipifica los delitos informáticos y protege la información frente a accesos no autorizados, interceptación y uso indebido. El cumplimiento de este marco normativo fortalece la seguridad de PAIWEB y garantiza la protección de los derechos fundamentales de los ciudadanos respecto al tratamiento de sus datos personales.

La implementación del doble factor de autenticación adopta estándares de seguridad reconocidos en el sector tecnológico y utilizados en plataformas de uso cotidiano.

- **Mesa técnica con participación de los departamentos para conocer las situaciones presentadas que afectan la operación del programa.**

Desde el equipo de PAIWEB se han dispuesto canales oficiales para el reporte de novedades del sistema, siendo el correo electrónico el medio principal establecido para tal fin. Adicionalmente, frente a la implementación del servicio de autenticación de doble factor, se envió correo a las entidades territoriales que, en caso de requerir soporte técnico, podían solicitar sesiones de acompañamiento para aclarar inquietudes relacionadas con aspectos técnicos.

No obstante, desde el departamento de Risaralda no se ha recibido ninguna solicitud para la realización de sesiones de revisión o acompañamiento frente a las dudas que pudieran haberse presentado respecto a este servicio.

- **Ajustes al código de seguridad**

El código de autenticación es enviado únicamente desde la siguiente dirección de correo electrónico paiweb_noreply@paiweb.gov.co, el tiempo promedio en recibir el correo electrónico con el código de autenticación depende del servicio del correo electrónico que posea el usuario, de las configuraciones propias

del correo y de la estabilidad en la conexión de internet que tenga en el momento de consultar el correo. Desde el momento en que se solicita el código de autenticación de manera automática el sistema lo envía sin filtros y puede recibirse en un tiempo promedio menor a 60 segundos; de igual forma el tiempo de duración del código de autenticación, es de 5 minutos desde el momento de la solicitud.

- **Ampliar tiempo de validez (código por día)**

Ampliar el tiempo de validez del código de seguridad reduce la protección de los datos. Esto se debe a que, si un usuario deja su sesión abierta en un equipo, cualquier persona podría acceder sin que se le solicite nuevamente la autenticación. Esta situación facilita escenarios como los ya evidenciados, en los que se han detectado alteraciones de datos y los titulares argumentan que su contraseña estaba guardada en el equipo, permitiendo el acceso a terceros no autorizados.

En consecuencia, la implementación de esta medida busca minimizar los riesgos asociados a fraudes y a la manipulación indebida de la información. Adicionalmente, el tiempo promedio del proceso aumenta en aproximadamente 30 segundos, lo cual no representa una afectación significativa en la jornada laboral cada vez que se ingresa al sistema.

- **Implementar reactivación automática (SMS o correo)**

se implementó el uso del correo electrónico como método para la autenticación de doble factor. Esta medida se adopta porque el correo electrónico ofrece mayores niveles de seguridad, control y trazabilidad en comparación con otros mecanismos, especialmente en situaciones donde los números de teléfono pueden cambiar, ser reutilizados o estar expuestos a riesgos de suplantación.
El uso de este código permite validar la identidad del usuario de manera adicional, reduciendo el riesgo de accesos no autorizados y fortaleciendo la protección de la información. Se recomienda mantener seguro el correo electrónico y no compartir el código de verificación con terceros. Entre las razones para priorizar el correo electrónico como canal de autenticación se destacan: su estabilidad en el tiempo, su capacidad como identificador confiable de identidad digital, y la menor fiabilidad del teléfono móvil, que puede cambiar con frecuencia y constituye un canal más débil y volátil.
Para la definición e implementación del mecanismo de seguridad de la información, se llevó a cabo un análisis integral de las variables presentes en el contexto operativo al que está expuesto el sistema. Entre los factores más relevantes considerados se encuentran:

- La alta sensibilidad de la información gestionada, correspondiente a datos de historia clínica.
- La disponibilidad y el control directo del correo electrónico por parte del usuario, utilizado como canal de acceso estable.
- La elevada rotación de personal en las instituciones usuarias del sistema.
- Las deficiencias en la actualización oportuna de los datos de contacto de los usuarios por parte de los administradores.
- La alta probabilidad de cambios y portabilidad de números de telefonía móvil a nivel nacional.
- La desvinculación periódica de líneas móviles por parte de los operadores, asociada a condiciones de inactividad o falta de pago.
- El riesgo significativo de clonación de tarjetas SIM (SIM swapping).
- El reciclaje frecuente de números de telefonía móvil.
- La presencia recurrente de técnicas de ingeniería social.

En consideración de estos factores, se priorizó la adopción de mecanismos que reduzcan la dependencia de la infraestructura de telefonía móvil, garantizando un mayor control, trazabilidad y seguridad en el acceso al sistema.

- **Revisar problemas de certificados y compatibilidad de navegadores.**

Respecto al concepto de certificados de seguridad, es importante aclarar que estos son un estándar utilizado por todos los navegadores modernos (como Chrome, Edge, Firefox, Safari) para garantizar que las conexiones a los sitios web sean seguras.
En condiciones normales, los certificados de seguridad no generan problemas de compatibilidad. Por el contrario, son un requisito básico para que los navegadores permitan el acceso sin advertencias.
Sin embargo, pueden presentarse mensajes o alertas en casos como:

- Navegador web desactualizado (con caché y almacenamiento obsoleto) en el equipo del usuario.
- Sistemas operativos antiguos
- Fecha y hora incorrectas en el equipo del usuario
- Problemas temporales con el certificado del sitio
- Certificado vencido o en proceso de actualización en el sitio web que intenta cargar.

Cuando esto ocurre, no se trata de un problema de compatibilidad como tal, sino de una verificación de seguridad que no pudo completarse correctamente.
Los certificados de seguridad están diseñados para funcionar de manera compatible con todos los navegadores actuales y su objetivo es proteger la información del usuario, no generar inconvenientes.

Cuando los navegadores web identifican alguna novedad o situación como las previamente indicadas, automáticamente muestra un mensaje titulado “Conexión no es privada”, (el título del mensaje puede variar entre navegadores diferentes, pues es definido y generado por cada navegador).

El mensaje que indica "Conexión no es privada" es un mensaje estandarizado que todo navegador web muestra cuando se presenta novedad de actualización del certificado de seguridad que tiene almacenado en la caché dicho navegador en relación sobre cualquiera de los sitios (o páginas web) que el usuario esté intentando cargar desde el navegador.

Como ya se sabe, el sistema PAIWEB está alojado en la web y se accede por internet y para ello se requiere usar un navegador web actualizado siempre, de lo contrario, el mismo navegador por defecto mostrará alertas o mensajes.

PAIWEB siempre tiene sus certificados de seguridad actualizados y vigentes, por lo que no es una causa que aplique en situaciones en las que el navegador muestra el mensaje.

De manera resumida, el certificado de seguridad es un mecanismo que permite al navegador confirmar que la página es confiable y que la información que usted ingresa está protegida, por lo que cuando aparece esta advertencia se debe tener en consideración que:

“Conexión privada” indica que la información está segura, protegida.
“Conexión no privada” indica que no se puede garantizar la seguridad de la información.
Si tras la revisión, la situación de que el navegador web le sigue mostrando el mismo mensaje "Conexión no es privada" al intentar acceder a un determinado sistema, la recomendación es contactar al encargado técnico de la institución del área de sistemas.

- **Revisar las políticas de bloqueo de usuarios**

Respecto a las políticas de bloqueo de usuarios, como se ha indicado en las capacitaciones realizadas, el sistema cuenta con controles establecidos para la inactivación de usuarios debido a que se detecta un seguimiento insuficiente y se hizo necesario establecer estos controles. Las situaciones programadas que pueden derivar en la inactivación de un usuario son las siguientes:

1.Cuando se ingresan incorrectamente la contraseña o el código tres veces.
2.Al alcanzar la fecha de inactivación del usuario registrada en la creación de los usuarios.
3.Cuando se detectan cinco días de inactividad del usuario en el sistema.

Adicionalmente:

- El tiempo máximo de inactividad permitido durante una sesión activa es de 30 minutos.
- La duración máxima de una sesión continua es de 60 minutos.
- Se contemplan excepciones en fechas especiales, como Semana Santa y el cierre de año.

- **Establecer un canal directo de reporte desde los departamentos hacia el área técnica del ministerio.**

Desde el año 2025 se estableció un espacio de atención los días jueves, el cual fue retomado el pasado 10 de abril, una vez finalizadas las sesiones de inducción y reinducción al sistema, este espacio se denomina “Conectados con PAIWEB”. En este espacio, los administradores del sistema de los diferentes departamentos pueden conectarse para recibir apoyo del área técnica y resolver inquietudes o novedades. Sin embargo, el departamento de Risaralda no ha participado en dichas sesiones.

En este sentido, los canales y espacios de acompañamiento se encuentran habilitados; por lo tanto, es importante que el departamento de Risaralda haga uso de estos, asistiendo a las sesiones disponibles, con el fin de resolver y aclarar las dudas que se presenten.

Cordialmente,

Salud

**Mónica Liliana Serrato Lanuza**
Contratista
Subdirección de Enfermedades Transmisibles
Grupo de Gestión de Enfermedades Inmunoprevenibles
Tel: 330 5000 Ext. 0000
Cra. 13 No. 32-76, Bogotá D.C.
www.minsalud.gov.co

**De:** Paiweb Risaralda <risaraldapaiweb@gmail.com>
**Enviado:** martes, 7 de abril de 2026 11:54
**Para:** Monica Liliana Serrato Lanuza <mserrato@Minsalud.gov.co>
**Cc:** Claudia Liliana Sosa Mesa <csosa@Minsalud.gov.co>; Beatriz Eugenia Romero Tabima <bromero@Minsalud.gov.co>; Vacunación Secretaria de Salud <vacunacion@risaralda.gov.co>
**Asunto:** Impacto de la nueva actualización de seguridad – Código PAI Web

[El texto citado está oculto]

---

**Vacunación Secretaria de Salud** <vacunacion@risaralda.gov.co> 21 de abril de 2026 a las 9:07
Para: risaraldapaiweb@gmail.com, jessica sanchez correa <jessica.sanchezrisaralda@gmail.com>

[El texto citado está oculto]