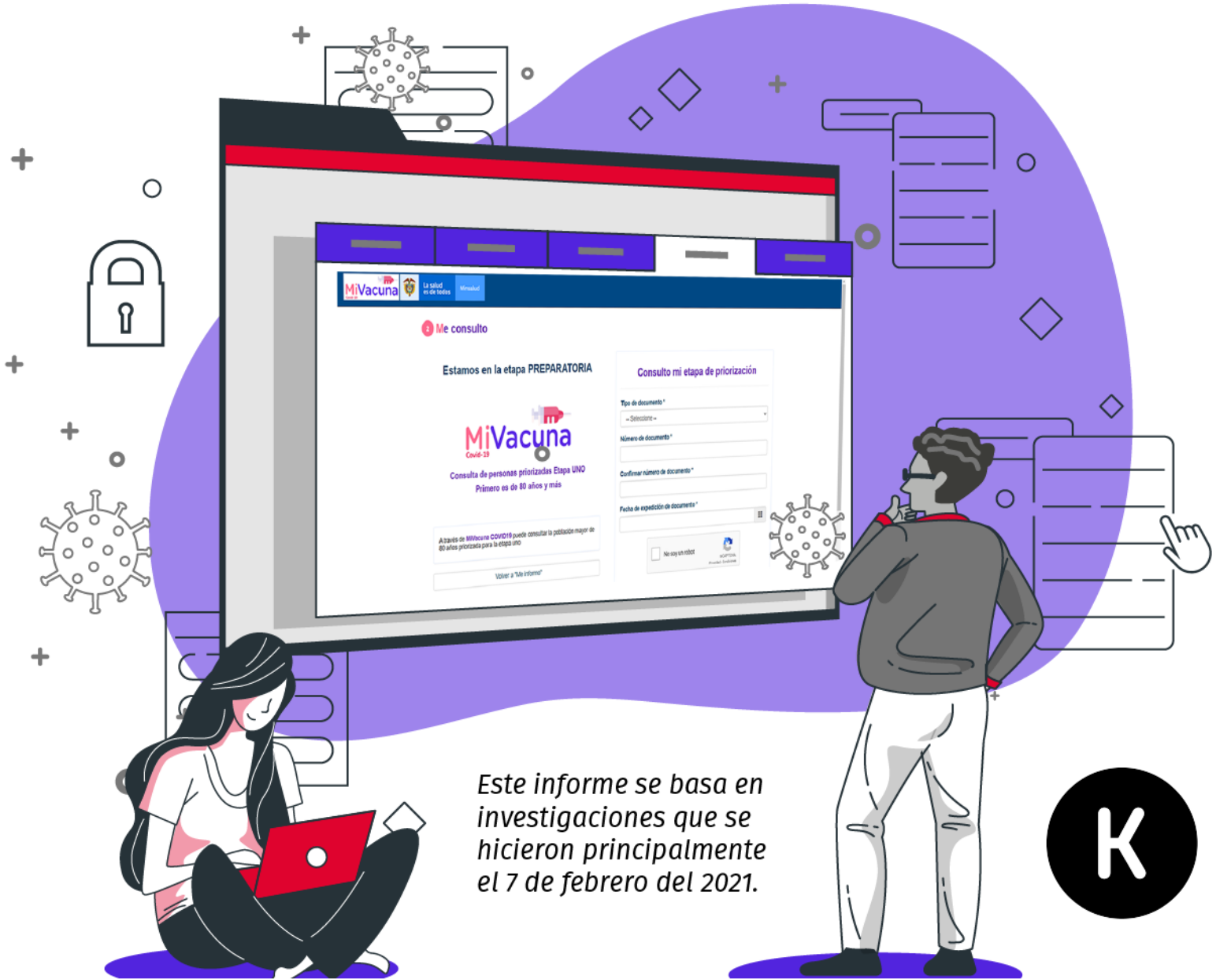
Informe sintético

<K+LAB>

Análisis del formulario del Ministerio de Salud de consulta de poblaciones priorizadas para vacunación contra el COVID-19

MiVacuna
Covid-19



Este informe se basa en investigaciones que se hicieron principalmente el 7 de febrero del 2021.

Fundación
Karisma

1. Contexto

La página “Mi Vacuna” es un portal que pertenece al sitio web del Ministerio de salud y protección social desarrollado en el contexto de la vacunación contra el COVID-19. Al momento de este análisis, permite a las personas mayores de 80 años verificar que estén en la lista para vacunación en la primera fase. Cómo lo declaro el Ministro de la salud:

“*Más que un aplicativo será un portal dentro de la página web de la entidad. Se les pedirá su número de identificación y la EPS a la que pertenecen, y podrán ver si se encuentran en las poblaciones priorizadas para ser programadas.*”

La URL de este portal es la siguiente:

https://mivacuna.sispro.gov.co/MiVacuna/Account/Login

Carolina Botero, directora de Fundación Karisma, publicó una columna el 12 de febrero en El Espectador[1], socializando el punto de vista de Fundación Karisma sobre este portal y adelantando los hallazgos que para ese momento habían aparecido en el análisis del laboratorio de privacidad y seguridad digital, K+Lab.

Este informe constituye la base de esa columna presentando los elementos técnicos y evidencias específicas de cada punto en sus anexos.

[1] https://www.elespectador.com/opinion/hablemos-de-mi-vacuna/

2. Tabla sintética del análisis del formulario "MiVacuna"

Categoría	Descripción
Información y política de privacidad	No hay política de privacidad o información sobre la protección de los datos personales en el portal "Mi Vacuna". Se puede deducir que aplica la política de la página web del Ministerio de Salud, al ser parte de su sitio, pero no es expreso y no hay enlace desde la página principal. En todos casos, no puede decirse que esté completo para el tipo de gestión que la solución parece hacer de los datos personales, en particular porque supone tomar datos de diversas fuentes y seguramente entregarlos a varias otras para apoyar la logística de vacunación, lo que por ejemplo no se explica en ese documento. Además la política de uso y privacidad del portal web del Ministerio de salud y protección social es un documento que no se ha actualizado desde el año 2012[2]. **Recomendación: Es necesario crear y publicar una política de protección de datos (o privacidad) específica al portal "Mi Vacuna".**
Hosting	El servidor web tiene la dirección IP 204.199.87.236 y se ubica en la empresa CTL Colombia.
Cifrado y autenticación	El portal usa de forma predeterminada el protocolo seguro HTTPS (HTTP+TLS) con un certificado de la empresa DigiCert a nombre del Ministerio de salud y protección social [Ver Anexo 1].
Envío de los datos personales y autenticación	Los datos personales transmitidos en los formularios (cédula, fecha de expedición, departamento y municipio) se envían con el protocolo HTTPS y el método POST. Se transmiten únicamente a la URL "https://mivacuna.sispro.gov.co/MiVacuna/Account/Login". En respuesta, el servidor instala una cookie (llamada "a") que permite autenticar la sesión [Ver Anexo 2].
Tecnologías usadas y actualizaciones	El servidor web es un servidor Microsoft IIS versión 10.0, que usa el framework Bootstrap [Ver Anexo 3]. La página usa también la herramienta de Google reCAPTCHA para detectar/bloquear tráfico procedente de robots. Nuestro análisis, de carácter no intrusivo, no permite verificar si el servidor IIS y el framework Bootstrap cuentan con las últimas actualizaciones de seguridad. **Recomendación: Es importante asegurarse de la actualización del servidor web y de todos sus componentes.**

[2] Este documento (disponible aquí: https://www.minsalud.gov.co/Documents/Ministerio/Terminos%20y%20Condiciones%20de%20uso%20del%20portal%20web_Octubre%202012x.pdf) tiene una fecha de última modificación del 22 de octubre del 2012.

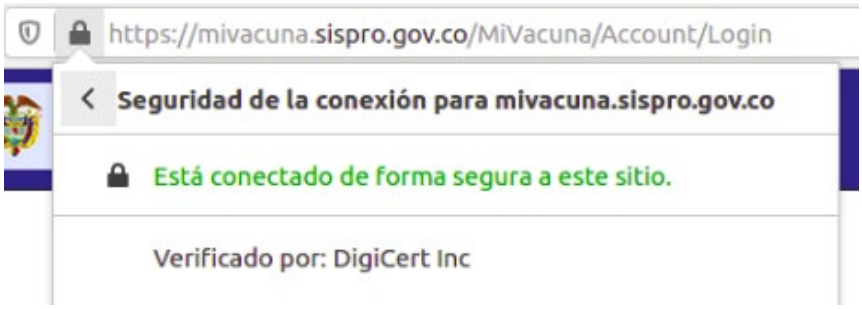
Protecciones adicionales	El sitio web implementa varias protecciones adicionales, que en su mayoría se pueden observar en las respuestas HTTP(S). Podemos mencionar las siguientes [Ver Anexo 4]: Uso de la política "*HTTP Strict Transport Security*" (HSTS) que garantizar el uso exclusivo del protocolo HTTPS y así protege contra ciertos ataques y errores ; Protección de las cookies internas de sesión/autenticación con los parámetros "secure" y "HTTPOnly", que garantizan que sean transmitidas sólo con el protocolo HTTPS (protección en las transmisión) y que sean accedidos sólo del lado del servidor web, vía el protocolo HTTP(S) (protección en el acceso); Uso de protección contra los ataques de tipo "Cross Site Scripting" ("X-XSS-Protection"). Adicionalmente haciendo pruebas con VPN, pudimos notar que sólo se autorizan las conexiones desde direcciones IP ubicadas en Colombia.
Rastreo y cookies de tercero	La única cookie de terceros que puede ocasionar un rastreo es la cookie de Google asociada al servicio "GRECAPTCHA" [Ver Anexo 5]. Sin embargo, teniendo en cuenta la eficiencia de este servicio en términos de seguridad, se puede entender la decisión de implementarlo, a pesar del rastreo generado por su uso.

Conclusión

La aplicación Mi Vacuna parece haber sido diseñada pensando en seguridad digital, se deduce del análisis que se toman decisiones en este sentido y por eso muchos de los problemas que se identifican en otros desarrollos para el Estado, en este caso no aparecen.

ANEXOS – Referencias técnicas

[1] Uso del protocolo HTTPS y certificado criptográfico



Certificado

mivacuna.sispro.gov.co	DigiCert TLS RSA SHA256 2020 CA1

Nombre del asunto

País	CO
Localidad	Bogota
Organización	MINISTERIO DE SALUD Y PROTECCION SOCIAL
Nombre común	mivacuna.sispro.gov.co

Nombre del emisor

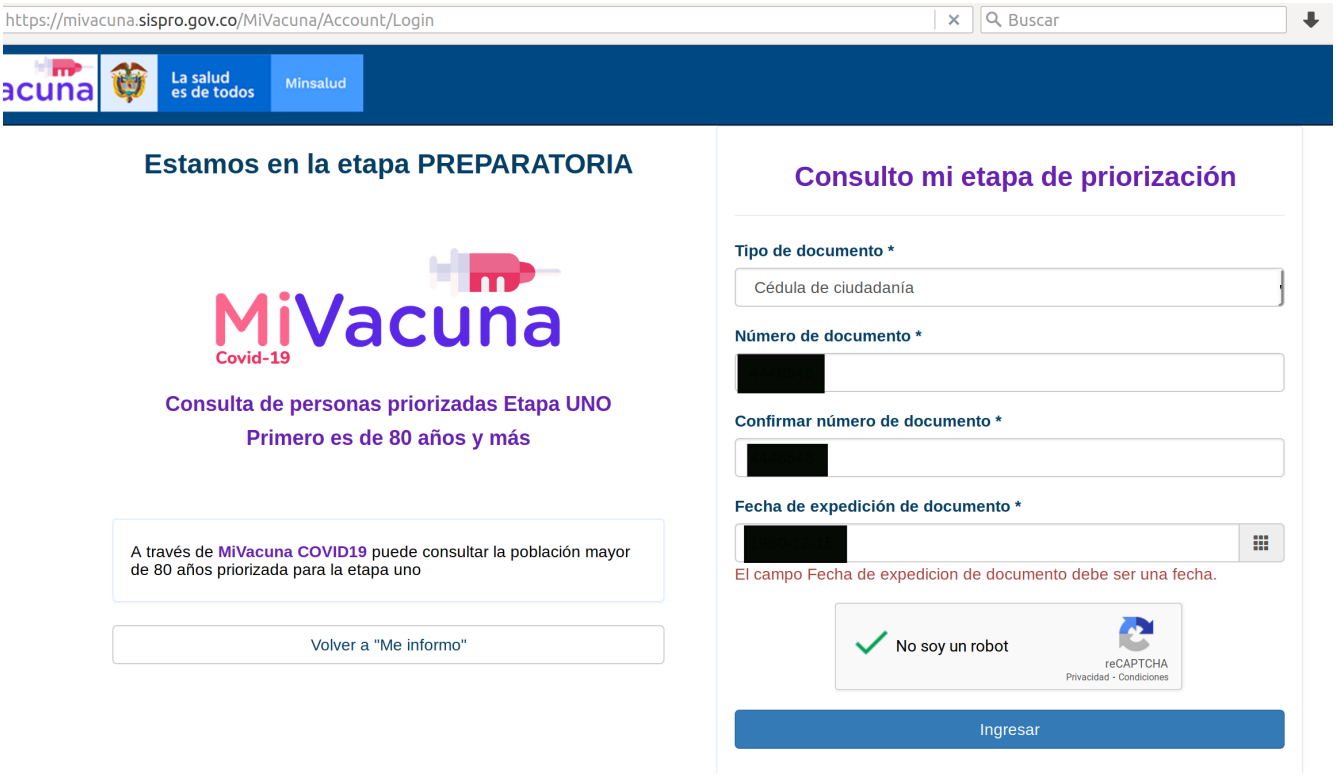
País	US
Organización	DigiCert Inc
Nombre común	DigiCert TLS RSA SHA256 2020 CA1

Validez

No antes	24/1/2021, 7:00:00 p. m. (hora de Ecuador)
No después	1/2/2022, 6:59:59 p. m. (hora de Ecuador)

[2] Transmisión de datos personales y autenticación

Cuando se completa el primer formulario[3]:



Se genera la siguiente solicitud HTTP(S) siguiente:

https://mivacuna.sispro.gov.co/MiVacuna/Account/Login

```
POST /MiVacuna/Account/Login HTTP/1.1
Host: mivacuna.sispro.gov.co
[…]
Content-Length: 783
Cookie:
f=MPt7m30nIXh5Ocx564uBifFAT3u5SQ3qt9vywF5FFb5Dbp1waUyQ6My2Od9IgfA2rVTDak7
hDNYNGpR4VW56_49YkL8XzcVP8l9LCcIXHxE1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__RequestVerificationToken=uau8-W48Nd8YcY-
ZZhTWR5Pm49tHwrUTfj4BXyF4eA58vty0PxGcTzrHCEpWwl1ZGwcsiCf-si5kBT5OjbjjF-
_LYvXjRTlWipzdV3XV2UU1&tipoIdentificacion=CC&numeroIdentificacion=XXXXX&n
umeroIdentificacionConfirmacion=XXXXXX&fechaExpDocumento=XXXXX&g-
recaptcha-response=[...]
```

[3] Aquí los datos personales están ofuscados, pero hicimos la prueba con datos reales de una persona conocida, con su consentimiento.

En su respuesta, el servidor instala una cookie de sesión llamada “a” y que contiene un token de autenticación:

```
Set-Cookie:                    a=nD9XpnPXIF_QsUka-vY-RAErqiEAojCkfU2Fb_rkdxRhzd-
8YMbdnr76hf1x0JfTS3sKUdM546WIo93AZPnXm5FCQp9ZiGYw9Y5zb-YCnI62lJih-
s0VHx6GpQJ7kEKwoqb_qjjhmmtyYhlwqT5KLAEvSmxZb-
Y2sDfQaTfW1xkliqRah4SIa9itrGT78dznLKoUCHImzKraIKi6ByKSWJ7TYAWycpyqCrGuxJG
h9GRBoWkiAxVMtaPthasElczAiFJAzbRJ54MXvgVrr568wbPKxCdte9cLL4dZBqMoEFdEHgeJ
gsFs33_51AlMzEsOklKiRPmRjLHmC8M8FdwyjNvv7yCBjYqJrEQxKlU7sJxW0yZd-
elDFRQ__BHfQXXiDSQEmlinNAPX6teLuaxV5m2LGb6y5sJWwQDZNwH3Xut9tGtvYv6Y8denUW
eFGqfKP-dFoe_rXmw-qBx9CeKF1Q; path=/; secure; HttpOnly
```

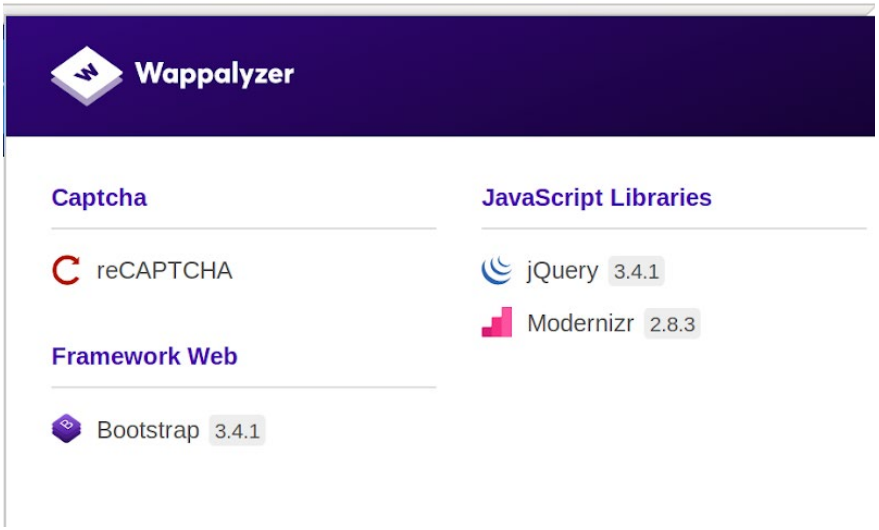
Esta cookie incluye los parámetros (flag) “secure” y “HttpOnly”. El primero garantiza que sea transmitido sólo con el protocolo HTTPS (protección en las transmisiones) y el segundo que sea accedido sólo del lado del servidor web, impidiendo por ejemplo que sea accedido por un javascript de tercero (protección en el acceso).

[3] Tecnologías usadas

El hecho de que el servidor web sea un servidor Micosoft IIS se puede observar en ciertas respuestas HTTP del servidor:

```
HTTP/1.1 200 OK
[...]
Server: Microsoft-IIS/10.0
```

El uso del framework de código abierto Bootstrap, junto con ciertas bibliotecas javascript, se puede observar por ejemplo con la herramienta Wappalyzer[4] o directamente en el código fuente HTML de la página:




```
<script
src="/MiVacuna/bundles/bootstrap?v=M4Nk6kIOwMFflsEKET0iPL9i5YBqbzMzvUOrd8
gyCnw1"></script>

<script src="/MiVacuna/Scripts/bootstrap-datepicker.min.js"></script>
```

[4] https://www.wappalyzer.com/

[4] Implementación de protecciones adicionales

Se pueden observar en las respuestas del servidor web, por ejemplo en esta, que sigue el envío de datos personales:

```
HTTP/1.1 302 Found
Cache-Control: public, no-store, max-age=0
[...]
Set-Cookie: a=nD9XpnPXIF_QsUka-vY-RAErqiEAojCkfU2Fb_rkdxRhzd-
8YMbdnr76hf1x0JfTS3sKUdM546WIo93AZPnXm5FCQp9ZiGYw9Y5zb-YCnI62lJih-
s0VHx6GpQJ7kEKwoqb_qjjhmmtyYhlwqT5KLAEvSmxZb-
Y2sDfQaTfW1xkliqRah4SIa9itrGT78dznLKoUCHImzKraIKi6ByKSWJ7TYAWycpyqCrGuxJG
h9GRBoWkiAxVMtaPthasElczAiFJAzbRJ54MXvgVrr568wbPKxCdte9cLL4dZBqMoEFdEHgeJ
gsFs33_51AlMzEsOklKiRPmRjLHmC8M8FdwyjNvv7yCBjYqJrEQxKlU7sJxW0yZd-
elDFRQ__BHfQXXiDSQEmlinNAPX6teLuaxV5m2LGb6y5sJWwQDZNwH3Xut9tGtvYv6Y8denUW
eFGqfKP-dFoe_rXmw-qBx9CeKF1Q; path=/; secure; HttpOnly
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Date: Sun, 07 Feb 2021 22:36:35 GMT
Content-Length: 145
Strict-Transport-Security: max-age=15552000
```

[5] Cookies instaladas

Las siguientes cookies se instalan en durante el proceso de consulta en MiVacuna:

Domain	Name	Content	HTTP Only	Secure	Expires
mivacuna.sispro.gov.co	a	nD9XpnPXIF_QsUka-vY-RAErqiEAojCkfU2Fb_rkdxRhzd-8YMb...	Yes	Yes	Al terminar la sesión
.google.com	_GRECAPTCHA	09AGjLO1ysaryekDm7ZQWRQM5pQR3qmsAr8wMsXLg4DZi...	Yes	Yes	7 de febrero de 2022 17:36:07 GMT-5
mivacuna.sispro.gov.co	f	MPt7m30nIXh5Ocx564uBifFAT3u5SQ3qt9vywF5FFb5Dbp1...	Yes	Yes	Al terminar la sesión

La cookie externa "_GRECAPTCHA", con dominio "google.com" contiene un número de identificación (a priori en Base64) y tiene una fecha de expiración de un año, que es mucho mas de lo necesario para su finalidad inicial (protección contra los robots durante la sesión). Tiene las características de una cookie de rastreo y puede ser usada por Google con este fin, más allá de la finalidad de seguridad.

<K+LAB>