CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

AS-AATIC-124-2022
30 de junio de 2022

Doctor
Randal Álvarez Juárez, gerente
GERENCIA MÉDICA - 2901

Estimado señor:

ASUNTO:	**Oficio de Asesoría en relación con riesgos identificados en materia de protección de datos por la implementación de mecanismos contingentes en la atención de pacientes.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno, específicamente en su rol de asesor, esta Auditoría informa sobre los riesgos identificados en materia de protección de datos ante la implementación de mecanismos contingentes en la atención de pacientes en diferentes centros de salud producto del hackeo sufrido en la Institución.

Al respecto, las diferentes unidades de la Institución se han visto obligadas a implementar mecanismos de contingencia para continuar con las actividades sustantivas correspondientes a sus labores en la debida gestión institucional, producto del ataque cibernético sufrido el pasado 31 de mayo del presente año, que requirió a la Caja la desconexión de los sistemas de información, así como de la plataforma tecnológica. Por esta razón los niveles locales y operativos han desarrollado diferentes estrategias para dar continuidad a la atención de usuarios, especialmente en los centros de salud, de tal forma que la afectación en la prestación de los servicios sea la menor posible, no obstante, se han identificado posibles riesgos en dichas estrategias que podrían llevar a la Caja a tener problemas de índole legal con los administrados.

Como ejemplo de lo anterior, esta Auditoría tuvo conocimiento que, en el área de salud de Curridabat como medida contingente para minimizar la afectación sufrida por los ataques cibernéticos en el servicio de Farmacia, se implementó un formulario[1] mediante la plataforma Google Forms, para que los pacientes soliciten la prescripción de medicamentos para los padecimientos regulares, donde mediante un enlace o código QR, deben llenar la información correspondiente, 5 días antes de la fecha del váucher para posteriormente hacer el retiro de los medicamentos, no obstante este mecanismo podría presentar riesgos en materia de protección de datos, ya que la información recopilada en este instrumento externo a la institución, puede ser considerada información sensible, sin existir además, el mecanismo de aceptación por parte del paciente sobre el consentimiento expreso del tratamiento de sus datos en esta plataforma.

Respecto al mecanismo electrónico utilizado, Google Forms, es un software de administración de encuestas y sondeos que forma parte del conjunto Google Docs Editors de la empresa Google, que le permite a los usuarios crear y editar encuestas en línea y en tiempo real, para que otros usuarios las respondan y posteriormente efectuar análisis de los resultados obtenidos, dicha herramienta aplica medidas de seguridad para protección de datos contra software malicioso y cifrado de datos en tránsito y reposo.

[1] Ver Anexo

De lo anterior se identificó, que aparte de datos de acceso irrestricto como nombre completo, número de identificación, y fecha de nacimiento también se solicita información sensible como número de teléfono, correo electrónico, centro de adscripción, tipo de tratamiento médico que consume, dosis de medicamentos, fotografía de la cédula y demás información médica que el paciente desee incluir, gestionando esto mediante una plataforma externa a la Institución que podría materializar riesgos tanto del uso de datos personales como de seguridad de la información violentando aspectos definidos en la Ley 8968 "Protección de la Persona frente al tratamiento de sus datos personales".

Si bien como se mencionó, esta herramienta dispone de mecanismos de seguridad para la protección de la información, se debe hacer la valoración correspondiente de los riesgos legales que podría enfrentar la Institución al gestionar información con datos sensibles en una plataforma externa a la Caja y donde no existe la opción de aceptación de la política de privacidad y los términos y condiciones para el tratamiento de los datos por parte del usuario, asimismo analizar la seguridad en el acceso de la información recopilada y que esta sea gestionada únicamente por las personas competentes y responsables del tratamiento de dichos datos.

Al respecto la Ley 8969 "Protección de la Persona frente al tratamiento de sus datos personales" en el artículo 2 "Otorgamiento del consentimiento" señala:

> *"Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.*
>
> *No será necesario el consentimiento expreso cuando:*
>
> *a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.*
>
> *b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.*
>
> *c) Los datos deban ser entregados por disposición constitucional o legal.*
>
> *Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos."*

Asimismo, en el artículo 9 inciso 1 "Datos Sensibles" establece:

> *"Ninguna persona estará obligada a suministrar datos sensibles. Se prohíbe el tratamiento de datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros.*
>
> *Esta prohibición no se aplicará cuando:*
>
> *(…) d) El tratamiento de los datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios,* ***siempre que dicho tratamiento de datos sea realizado por un funcionario o funcionaria del área de la salud, sujeto al secreto profesional o propio de su función, o por otra persona sujeta****, asimismo, a una obligación equivalente de secreto." (la negrita no es del original)*

Ademán en el artículo 10 "Seguridad de los datos" de la cita norma señala:

> *"El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.*

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. (…)".

En virtud de lo expuesto, se da conocer la información descrita, con el propósito de ser sometidas a valoración y revisión por esa Administración y así coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional, así como del cumplimiento de la normativa legal y técnica especialmente en el tratamiento de datos personales, que puedan generar a la Institución inconvenientes ante la materialización de los riesgos señalados, por esta razón considera esta Auditoría es importante se efectúe un análisis y se adopten las medidas correspondientes para garantizar que las medidas de contingencia utilizadas por las unidades locales en medio de la emergencia por el ataque cibernético, colaboren con la continuidad en la prestación de los servicios sin que se vulneren los derechos de los usuarios.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.06 11:28:53 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

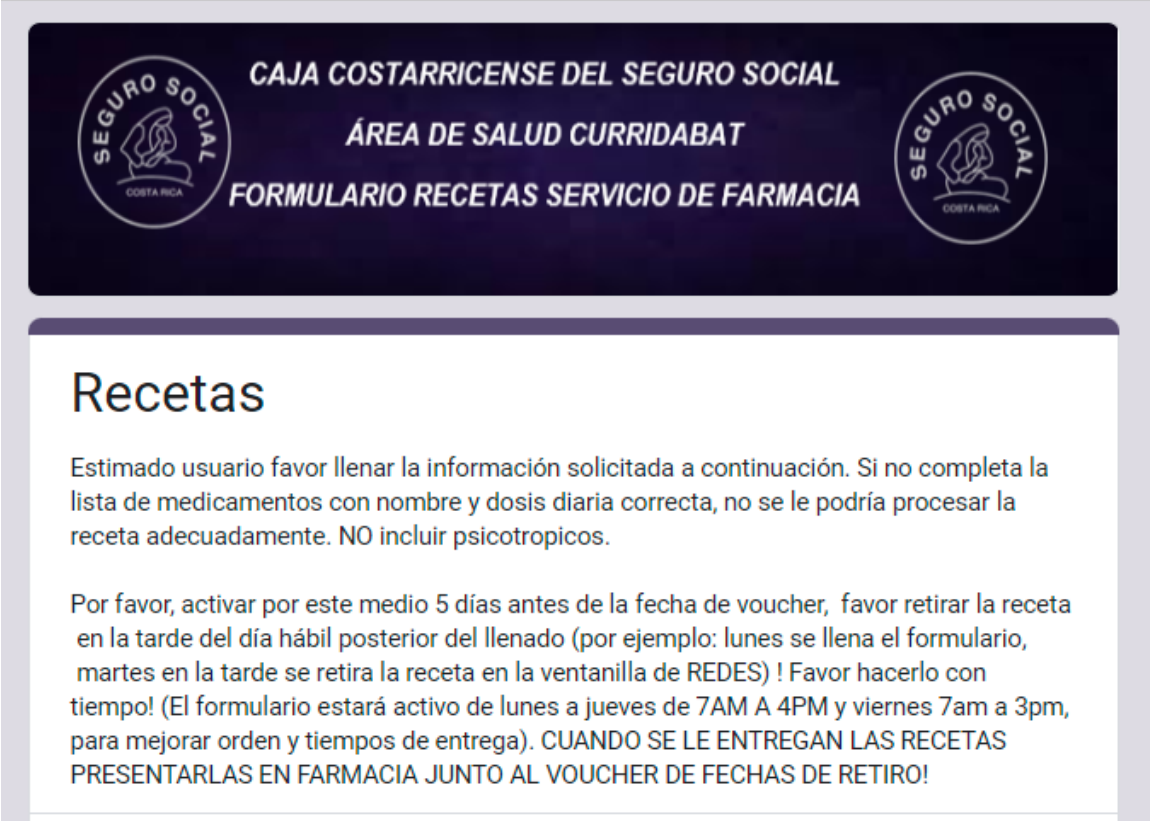
Anexo (1)

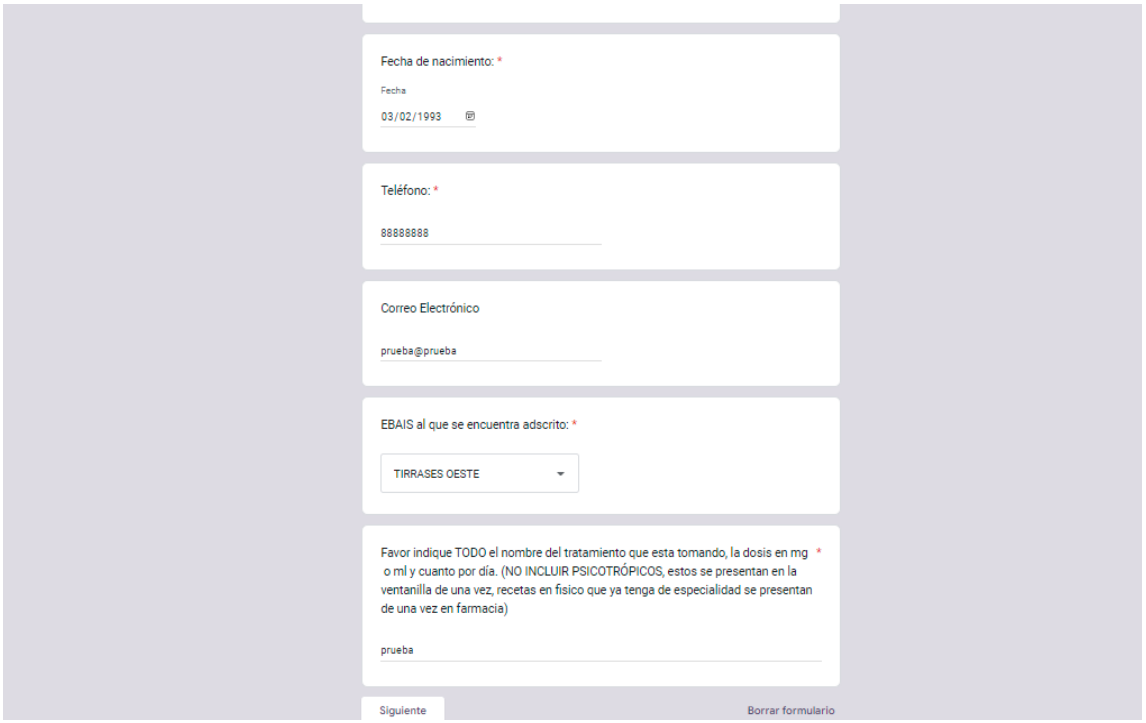
1. Formulario para el trámite de recetas en el servicio de Farmacia del área de Salud de Curridabat

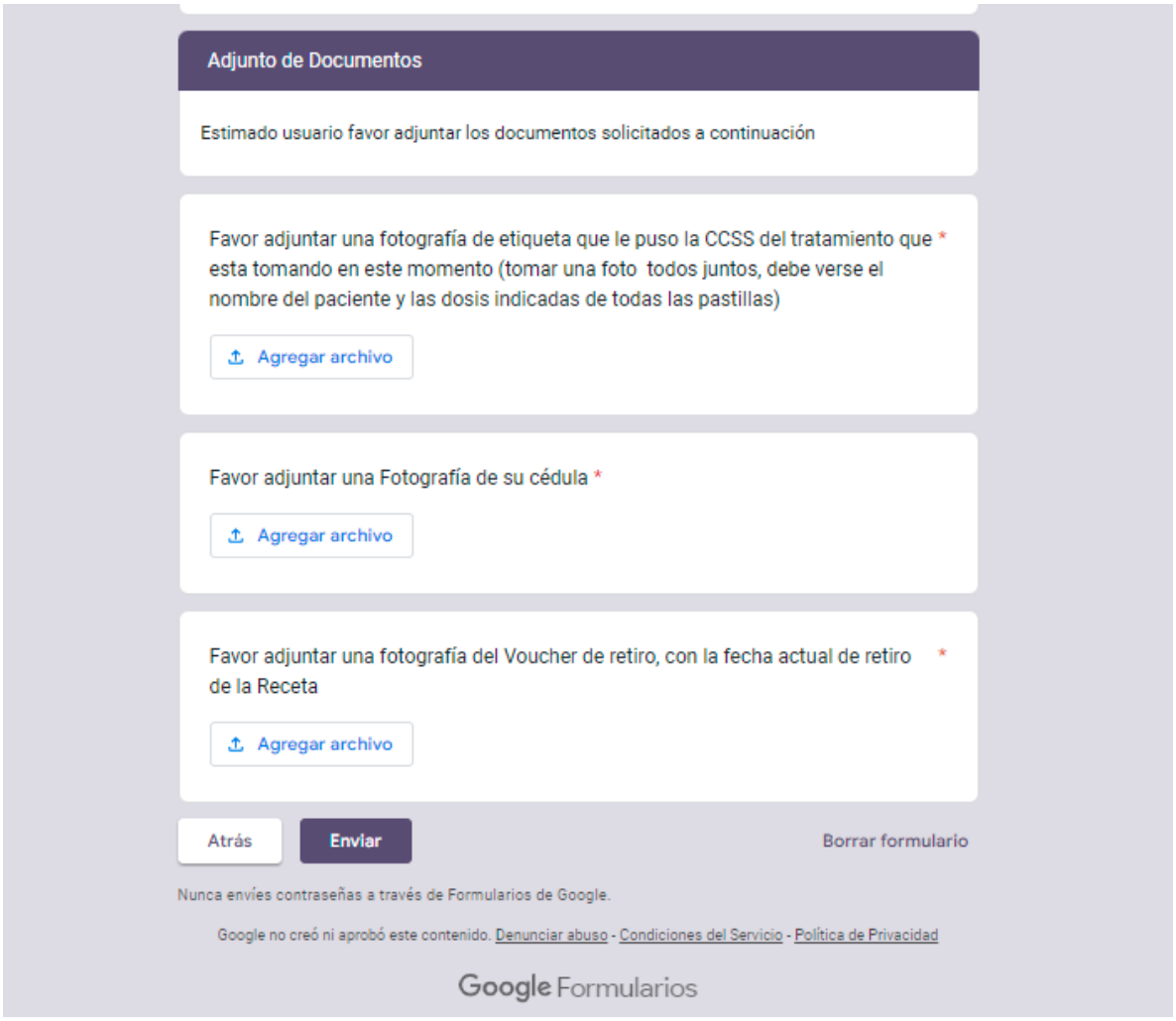
C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General -1100.
Máster Idannia Mata Serrano, subgerente a.i. Dirección de Tecnologías de Información y Comunicaciones-1150
Auditoría

ANEXO

"Formulario para el trámite de recetas en el servicio de Farmacia del área de Salud de Curridabat"




Fecha de nacimiento: *
Fecha
03/02/1993
Teléfono: *
88888888
Correo Electrónico
prueba@prueba
EBAIS al que se encuentra adscrito: *
TIRRASES OESTE
Favor indique TODO el nombre del tratamiento que esta tomando, la dosis en mg o ml y cuanto por día. (NO INCLUIR PSICOTRÓPICOS, estos se presentan en la ventanilla de una vez, recetas en fisico que ya tenga de especialidad se presentan de una vez en farmacia) *
prueba
Siguiente
Borrar formulario


Adjunto de Documentos
Estimado usuario favor adjuntar los documentos solicitados a continuación
Favor adjuntar una fotografía de etiqueta que le puso la CCSS del tratamiento que esta tomando en este momento (tomar una foto todos juntos, debe verse el nombre del paciente y las dosis indicadas de todas las pastillas) *
Agregar archivo
Favor adjuntar una Fotografía de su cédula *
Agregar archivo
Favor adjuntar una fotografía del Voucher de retiro, con la fecha actual de retiro de la Receta *
Agregar archivo
Atrás
Enviar
Borrar formulario
Nunca envíes contraseñas a través de Formularios de Google.
Google no creó ni aprobó este contenido. Denunciar abuso - Condiciones del Servicio - Política de Privacidad
Google Formularios