ATIC-83-2018
27-07-2018

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2018 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar el cumplimiento de la Ley No. 8968 *"Protección de la Persona Frente al Tratamiento de sus Datos Personales"* y su reglamento en la Caja Costarricense de Seguro Social (CCSS).

Los resultados del informe permitieron evidenciar la ausencia de un modelo de gestión integral orientado al tratamiento y protección de los datos personales administrados por la Institución, lo anterior ante la ausencia de instancias institucionales formalmente definidas encargadas de abordar el tema, delegación concreta de roles y responsabilidades, mecanismos de coordinación entre Presidencia, las distintas Gerencias y sus unidades adscritas, entre otros. Además, se carece de un inventario institucional unificado sobre las bases de datos con datos personales, así como una diferenciación de cuales son carácter interno y las que deberían formar parte del ámbito de aplicación de la Ley 8968 y su reglamento por no tener fines exclusivamente internos, personales, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas.

Por otra parte, se comprobó la necesidad que tiene la Institución de apegarse al concepto de "Responsable de base de datos" estipulado en la Ley supra citada, lo anterior en virtud que la Administración Activa designa en esta función a Gerentes, Nombres de Direcciones o Áreas, directores, Jefes de Área, Sub Áreas, informáticos, médicos o funcionarios operativos, además, se evidenciaron instancias técnicas que relacionan al "Líder Usuario" de los aplicativos bajo esta función, siendo las tareas de una naturaleza diferente.

Aunado a lo anterior, existen debilidades en los procesos de inscripción de bases de datos institucionales ante la Prodhab, el establecimiento de medidas de seguridad afines con los términos establecidos en la Ley 8968 y su reglamento, así como el marco normativo institucional vigente en esta materia.

Por último, se puede constatar la necesidad de fortalecer los procesos de capacitación a nivel institucional en el tema de protección y tratamiento de datos personales, generando como efecto que a nivel institucional se detecten prácticas no alineadas al marco normativo en esta materia.

En virtud de lo expuesto, este Órgano de Fiscalización ha solicitado a Presidencia Ejecutiva, para que adopten acciones concretas para la atención de las recomendaciones insertas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

ATIC-83-2018
27-07-2018

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN DE CARÁCTER ESPECIAL REFERENTE AL CUMPLIMIENTO DE LA LEY NO. 8968 PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES EN LA CAJA COSTARRICENSE DE SEGURO SOCIAL (CCSS)

PRESIDENCIA EJECUTIVA U.E. 1102
GERENCIA FINANCIERA U.E 1103
GERENCIA ADMINISTRATIVA U.E 1104
GERENCIA LOGÍSTICA U.E 1106
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS U.E. 1107
GERENCIA MÉDICA U.E. 2901
GERENCIA DE PENSIONES U.E 9108

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo del 2018 para el Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar el cumplimiento de la Ley No. 8968 “Protección de la Persona Frente al Tratamiento de sus Datos Personales” y su reglamento en la Caja Costarricense de Seguro Social (CCSS).

OBJETIVOS ESPECÍFICOS

1. Determinar el modelo de gestión a nivel institucional para el tratamiento de datos personales en la Caja.

2. Identificar los mecanismos de control implementados en torno a las bases de datos a nivel institucional que contienen registros personales.

3. Revisar el marco normativo institucional vigente en materia de protección y tratamiento de datos personales, así como su alineamiento con la Ley No. 8968.

4. Verificar la capacitación recibida en torno a la aplicación de la Ley No. 8968, por parte de funcionarios que brindan atención directa al usuario.

5. Determinar la gestión realizada en torno a la inscripción de bases de datos institucionales en la Agencia de Protección de Datos de los Habitantes (Prodhab).

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

6. Comprobar la participación de la Administración en la definición de medidas de seguridad en las bases de datos institucionales que contienen información personal.

7. Constatar si existen prácticas institucionales que incumplan el tratamiento de datos personales.

ALCANCE

El estudio comprende las acciones realizadas por Presidencia Ejecutiva, Gerencias y sus unidades adscritas para garantizar el cumplimiento de la Ley No. 8968 *"Protección de la Persona Frente al Tratamiento de sus Datos Personales"* y su respectivo reglamento. Lo anterior considerando el período comprendido entre enero 2016 y mayo 2018, ampliándose en aquellos casos que se resultó pertinente.

Adicionalmente, se visitaron las siguientes unidades: Área de Salud Catedral Noreste, Hospital San Vicente de Paúl y Hospital Rafael Ángel Calderón Guardia con el objetivo de verificar si existen prácticas institucionales que incumplan lo señalado en la Ley No. 8968 sobre el tratamiento de datos personales.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:

- Identificación de las bases de datos a nivel institucional que contienen registros personales.

- Solicitud y revisión de documentación remitida por la Administración Activa en torno al cumplimiento institucional sobre la Ley No. 8968 y su reglamento.

- Verificación del marco normativo institucional en materia de protección y tratamiento de datos personales y su alineamiento con la Ley 8968 y su reglamento.

- Consulta a funcionarios que participan en la prestación directa de servicios de salud, tales como Enfermería, Laboratorio, Farmacia, Contralorías de Servicios de Salud, Registros y Estadísticas de Salud, así como Sucursales Financieras, en torno a capacitación recibida en el tema de protección de la persona frente al tratamiento de sus datos personales.

MARCO NORMATIVO

- Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, N°8968.
- Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.
- Ley General de Control Interno, N°8292
- Normas de Control Interno para el Sector Público.
- Normas Técnicas para la Gestión y Control de las Tecnologías de la Información (CGR).

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoría, informa y previene al Jerarca y a los titulares subordinados, acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios (…)"*

ANTECEDENTES

Antes de la entrada en vigor de la ley 8968, Costa Rica regulaba el tema de la protección de datos a través normas contenidas en el Código Penal Costarricense, Código Civil, Constitución Política y en otras normas, tales como Ley General de Aduanas, Ley General de Telecomunicaciones, Ley de Administración Financiera de la República y Presupuestos Públicos, el Código de Normas y Procedimientos Tributarios, entre otras.

Adicionalmente, el artículo 196 bis de nuestro Código Penal contiene una pena de cárcel de uno a tres años para quienes vulneren la intimidad de otra persona, es decir, que sin sus consentimientos se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos.

Del mismo modo, otros artículos de marcos normativos nacionales que abarcan aspectos relacionados con el tratamiento de datos personales son los siguientes:

- *Artículo 24 de la Constitución Política. Derecho a intimidad, libertad y secreto de comunicaciones.*
- *Artículo 47 Código Civil. Derecho a la imagen.*
- *Artículo 615 Código de Comercio. "Secreto bancario"*
- *Sala Constitucional-Habeas Data.*

Ante esto, considerando que a nivel comercial y jurídico los datos personales en Costa Rica venían adoptando significativa relevancia, mediante publicación en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011, se promulgó la Ley 8968 *Protección de la Persona frente al Tratamiento de sus Datos Personales*. Además, su primer Reglamento fue creado mediante Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012 y publicado en el Alcance No. 45 del Diario Oficial La Gaceta del 05 de marzo de 2013.

En este sentido, el objetivo y fin de la Ley 8968, estipula lo siguiente:

> *"Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."

En línea con lo anterior, cabe señalar que en el 2016 se determinó la necesidad de reformar varias disposiciones del citado Reglamento, a efecto de esclarecer aspectos, facilitar la debida aplicación de la Ley y coadyuvar con la simplificación de trámites. Así, se realizan las nuevas reformas al Reglamento mediante el Decreto Ejecutivo No. 40008-JP del 19 de julio del 2016 y publicado en el Alcance No. 287 del Diario Oficial La Gaceta del 6 de diciembre del 2016, de esta manera se reconoce legislativamente el derecho a la autodeterminación Informativa.

Así mismo, el derecho antes mencionado el cual, con base en el valor y relevancia actual de los datos personales, establece la facultad de cada persona en proteger su intimidad y decidir qué datos pueden ser o no tratados, almacenados, transferidos, divulgados y comercializados en el territorio de la República de Costa Rica. En virtud de lo anterior, los organismos públicos y privados deben garantizar los derechos especiales enmarcados en la Ley 8968, los cuales a nivel internacional son identificados como los DERECHOS ARCO, los cuales permiten que el ciudadano pueda ejercer el derecho de Acceso, Rectificación, Cancelación y Oposición frente al tratamiento de sus datos personales.

Al respecto, en Costa Rica existe la Agencia de Protección de Datos de los Habitantes (Prodhab), como organismo fiscalizador y regulador de las bases de datos. Dicha institución podrá realizar intervenciones sobre bases de datos, ya sea de oficio o a petición de un interesado, y en caso de verificarse violación al derecho de autodeterminación informativa, podrá imponer sanciones administrativas y de carácter económico.

Con lo expuesto, es relevante tanto para los organismos públicos como privados comprender el concepto de datos personales, su categorización, así como las responsabilidades establecidas para el tratamiento y protección de este tipo de información. En este sentido, dentro de las definiciones que estipula esta Ley y Reglamento, se encuentran las siguientes:

- **Base de datos**: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

- **Responsable de la base de datos**: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán.

- **Encargado**: Toda persona física o jurídica, entidad pública o privada, o cualquier otro organismo que da tratamiento a los datos personales por cuenta del responsable de la base de datos.

- **Intermediario tecnológico o proveedor de servicios**: Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- **Datos Personales:** cualquier dato relativo a una persona física identificada o identificable.

- **Datos Personales de Acceso Restringido:** los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

- **Datos Personales de Acceso Irrestricto:** los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

- **Datos Sensibles:** información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

A continuación, se presentan ejemplos:

Figura 1. Ejemplos de Datos Personales

Fuente: Agencia de Protección de Datos de los Habitantes, abril 2018.

Por otra parte, es relevante indicar que deben inscribirse ante esa Agencia todas las bases, públicas o privadas, con una finalidad de comercialización o distribución o difusión comercial, quedando exentas los repositorios de entidades financieras que se encuentran sujetas al control y regulación de la Superintendencia General de Entidades Financieras (SUGEF), las cuales no requerirán inscribirse ante la Prodhab. Sin perjuicio de esto, la Agencia tiene plena competencia para regular y fiscalizar la protección de los derechos y garantías cubiertas bajo la Ley No. 8968 y ejercer todas las acciones que se concedan al afecto sobre dichas bases.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Datos Personales en la CCSS

Como organismo público, la Caja Costarricense de Seguro Social debe apegarse a los términos de la legislación y gestionar la información de conformidad con lo dispuesto en la Ley 8968 y su Reglamento, lo anterior, considerando la relevancia a nivel país de los datos administrados en materia de salud, recaudación patronal y pensiones, entre otros. Del mismo modo, la CCSS por el uso de tecnologías en sus aplicaciones y redes de telecomunicaciones podría enfrentar riesgos de seguridad en su información con un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo o desastres naturales, asimismo, las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes y sofisticadas, lo anterior comprometiendo directa o indirectamente los registros de carácter personal que administra la Caja.

En ese orden de ideas, la seguridad de la información tiene un papel determinante, dado que la misma puede garantizar razonablemente la protección de los datos a través de medios técnicos, sin embargo, debe ser apoyada con los procedimientos y controles adecuados, garantizando un modelo de gestión que involucre los niveles operativos, tácticos y estratégicos de la organización, para cumplir con lo estipulado en la Ley 8968 sobre tratamiento de los datos personales.

Ante lo expuesto, como parte del presente informe esta Auditoría mediante oficio 6399 del 05 de abril de 2018, solicitó a Presidencia y todas las Gerencias, remitir la información sobre las bases de datos a su cargo que disponen de datos personales. A continuación, se presenta la información remitida por las unidades:

Tabla 1
Bases de datos que contienen registros de carácter personal

N°	*Nombre de la Base(s) de Datos [1]*	*Ubicación Física*	*Sistema de Información utilizado para registrar los datos*	*Nombre y puesto del responsable (s) de la base de datos [2].*	*Estado actual del Sistema de Información*	*Inscrita ante la PRODHAB*
1	*Pensiones*	*Gerencia Pensiones*	*Sistema Integrado de Pensiones*	*Dirección Administración de Pensiones*	*Producción*	*No*
2	*GECREDIT*	*Gerencia Pensiones*	*Sistema de Gestión de Créditos*	*Dirección Financiera Administrativa*	*Producción*	*No*
3	*SIGNOS (Base de datos que forma parte del Expediente Digital Único en Salud (EDUS)*	*Oficentro Tecnológico, Tibás*	*SIAC_ADSCRIPCIÓN, SIAC_AGENDAS, SIAC_CITAS; BENEFICIO_FAMILIAR.*	*Villalta Bonilla María Eugenia*	*Producción*	*En proceso*
4	*ARCA Sistema Integrado de Atención Hospitalaria (SIAH) del egreso hospitalario y módulo quirúrgico*	*Data Center Hospital San Vicente de Paul.*	*Incluye lo relacionado a la admisión y egreso del paciente. Módulo quirúrgico incluye lista de espera y programación, dictado quirúrgico*	*Villalta Bonilla María Eugenia*	*Producción*	*En proceso*
5	*GDO_CORRES*	*Oficentro Tecnológico, Tibás*	*SAYC 2.0*	*N/A*	*Producción*	*No*

1 Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, que sean objeto de tratamiento, automatizado o manual, en el sitio o en la nube, bajo control o dirección de un responsable, cualquiera que sea la modalidad de su elaboración, organización o acceso. Fuente: Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.
2 Persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento se les aplicarán. Fuente: Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (8968)

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

6	*SAYC WEB*	*Oficentro Tecnológico, Tibás*	*SAYC 3.0 WEB*	*N/A*	*Desarrollo*	*No*
7	*BDADMIN*	*Oficentro Tecnológico, Tibás*	*SOCO*	*N/A*	*Producción*	*No*
8	*SIFC*	*Oficentro Tecnológico, Tibás*	*SIFC*	*N/A*	*Producción*	*No*
9	*SFCV (SICERE)*	*Codisa*	*Registro de Facturas por servicios médicos (MIFRE-No asegurados-Validación de Derechos en Línea*	*Lic. Wven Porras Núñez, Jefe Área Gestión de Riesgos Excluidos y Lic. Eduardo Flores Castro, Jefe Área Coberturas del Estado*	*Producción*	*Si está inscrita según expediente 0047-01-2015-INS 15-INS (Se adjunta documento)*
10	*BD_APAS_APORTE_PATRONAL*	*10.1.2.15*	*APAS WEB (Recursos Humanos/APAS PRODUCCIÓN*	*Sub Área de Contabilidad Operativa/Jefatura (Proceso), back up datos CGI Dirección Financiera/Jefatura*	*APAS PRODUCCION /DESARROLLO/ APAS WED, Ambiente SQL*	*No*
11	*BD_SIIF_INTEGRADO _FINANCIERO*	*Oficentro Tecnológico*	*SIIF-Sistema Institucional de Presupuesto*	*Lic. Olger Vargas Pérez Jefe Subárea Gestión de Bases de Datos*	*Producción*	*No lo requiere según oficio APD-11-177-2016*
12	*Base de Datos SICERE (SFCV)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Gerente Financiero a través de la Dir. SICERE (DSCR)*	*Producción*	*Si (GF-2517-15/Exp 0047-01-2015-INS PRODHAB)*
13	*Base de Datos SICERE (SFCV)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Sandra Campos Cubillo (AFCOP)*	*Pruebas*	*Base de Datos SICERE (SFCVC)*
14	*Base de Datos SICERE (SFCVA)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Alexander Angelini (SFA)*	*Desarrollo*	*Base de Datos SICERE (SFCVA)*
15	*Base de Datos SICERE (SFCVB)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Alexander Angelini (SFA)*	*Desarrollo*	*Base de Datos SICERE (SFCVB)*
16	*Base de Datos SICERE (SFCVE)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*		*Pruebas*	*Base de Datos SICERE (SFCVE)*
17	*Base de Datos SICERE (SFCVE)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Alexandra Guzmán (SCO)*	*Pruebas*	*Base de Datos SICERE (SFCVE)*
18	*Base de Datos SICERE (SFCVG)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Alexandra Guzmán (SCO)*	*Pruebas*	*Base de Datos SICERE (SFCVG)*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

19	*Base de Datos SICERE (SFCVF)*	*Data Center Tibás*	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	*Susana Ureña (ARCA)*	*Pruebas*	*Base de Datos SICERE (SFCVF)*
20	*BDADMIN_BDD1213*	*Data center*	*Carrera Profesional*	*Lic. Karla Quintero*	*Producción*	*NO*
			MAPA	*Lic. Ana Gabriela Jiménez*	*Producción*	*NO*
			SESI	*Dra. Cruz Sancho*	*Producción*	*NO*
			SOVT	*Ing. Esmeralda Díaz Navarro*	*Producción*	*NO*
			SOCO	*Ing. Teófilo Peralta*	*Producción*	*NO*
21	*BDADMINA*	*Data center*	*Carrera Profesional*	*Lic. Karla Quintero*	*Desarrollo*	*NO*
			MAPA	*Lic. Ana Gabriela Jiménez*	*Desarrollo*	*NO*
			SESI	*Dra. Cruz Sancho*	*Desarrollo*	*NO*
			SOVT	*Ing. Esmeralda Díaz Navarro*	*Desarrollo*	*NO*
			SOCO	*Ing. Teófilo Peralta*	*Desarrollo*	*NO*
22	*BDADMINB*	*Data center*	*MAPA*	*Lic. Ana Gabriela Jiménez*	*Pruebas*	*NO*
			SESI	*Dra. Cruz Sancho*	*Pruebas*	*NO*
			SOVT	*Ing. Esmeralda Díaz Navarro*	*Pruebas*	*NO*
			SOCO	*Ing. Teófilo Peralta*	*Pruebas*	*NO*
23	*RRHH (base de datos de recursos humanos)*	*Data center*	*Portal RRHH y sus aplicaciones*	*Laura Paz Morales, jefe Subárea de sistema automatizado en RH. Walter Campos Paniagua, subdirector Dirección de Administración y Gestión de Personal.*	*Producción*	*No*
24	*ccss2014 Atrévase a donar, Tabla:* ***t_donar***	*Servidor administrado por la DTIC*	*Mysql, Portal Web CCSS*	*Dr. Marvin Agüero Chinchilla, Coordinador Técnico Programa Institucional de Normalización en Donación y Trasplante de órganos, tejidos y células*	*Producción*	*No*
25	*ccss2014 Boletín de noticias Tabla:* ***t_sec_usuarios***	*Servidor administrado por la DTIC*	*Mysql, Portal Web CCSS*	*Máster María Isabel Solís Ramírez, jefa del Área de Comunicación y Extensión Cultural*	*Producción*	*No*
25	*Ccss2014 Formulario de contacto Tabla:* ***t_contacto***	*Servidor administrado por la DTIC*	*Mysql, Portal Web CCSS*	*Máster Ramsés Román, jefe del Área de Comunicación Digital*	*Producción*	*No*
26	*BD_Gafetes_ Choferes BD_Gafetes_Funcionarios BD_Gafetes_Juntas_Salud BD_Gafetes_Nayuribes BD_Gafetes_Pensionados*	*Centro de monitoreo Oficinas Centrales*	*Sistema Confección de Gafetes*	*Gerardo Salazar González, Jefe Subárea Archivo y Correspondencia*	*Producción*	*No aplica*
27	*Bit3*	*Centro de monitoreo*	*Reloj Marcador*		*Producción*	*No aplica*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

		Oficinas Centrales		*Andrey Salazar Cuadra, Jefe Subárea Radiocomunicación*		
28	*Bit4*	*Centro de monitoreo Oficinas Centrales*	*Reloj Marcador*	*Gerardo Salazar González, Jefe Subárea Archivo y Correspondencia*	*Producción*	*No aplica*
29	*Bit5*	*Centro de monitoreo Oficinas Centrales*	*Reloj Marcador*	*Esmeralda Díaz Navarro, Jefe Subárea Transportes*	*Producción*	*No aplica*
30	*Bit6*	*Centro de monitoreo Oficinas Centrales*	*Reloj Marcador*	*Steve Rojas Zúliga, Jefe Subárea Taller Mecánico*	*Producción*	*No aplica*

Fuente: Oficios CGI-GADMIN 133-2018, GF-1771-2018, GIT-0632-2018, AES-1-236-2018, DAGP-0706-2018, DSI-0155-2018, DCO-0161-2018, AGI-GP-0230-2018.

Adicional a la tabla anterior, en el anexo 1 del presente informe se encuentra el detalle con las bases de datos remitidas por la Dirección de Tecnologías de Información y Comunicaciones.

Oficio de Advertencia AD-ATIC-49757-2016.

En relación con el tema, es significativo mencionar que este Órgano Fiscalizador, mediante el oficio AD-ATIC-49757-2016, del 21 de enero del 2016, en cumplimiento de las funciones de asesoría, capacitación y prevención contempladas en su Plan Anual Operativo, previno a la Administración Activa respecto a lo señalado en la Ley 8968, particularmente a lo indicado en el artículo 21 respecto al registro de archivos y bases de datos, el cual establece lo siguiente:

> *"(…) Toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica el trasbase o la transferencia de los datos.*
>
> *Deberá inscribir cualesquiera otras informaciones que las normas de rango legal le impongan y los protocolos de actuación a que hacen referencia el artículo 12 y el inciso c) del artículo 16 de esta ley (…)".*

Adicionalmente, se indica repositorios de información que no están inscritos, encontrándose al margen de lo establecido en el artículo supra citado, por lo cual se solicitó revisar la situación con el propósito que se coordinaran y adoptaran las medidas según correspondan, en apego a la normativa en mención, y con el fin de verificar los controles de seguridad y los protocolos mínimos de actuación, evitando posibles demandas y problemas legales a futuro que se podrían derivar de la omisión de la aplicación de la norma establecida.

Considerando lo expuesto, se detallan a continuación los hallazgos evidenciados por esta Auditoría en torno a riesgos detectados en el cumplimiento de la Ley No. 8968 y su reglamento en la Caja Costarricense de Seguro Social.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

HALLAZGOS

1. SOBRE UN MODELO DE GESTIÓN ORIENTADO AL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES.

Se determinó la ausencia de un modelo de gestión integral orientado al tratamiento y protección de los datos personales administrados por la Institución, lo anterior a partir de los siguientes aspectos:

- Se carece de instancias institucionales formalmente definidas que aborden el tema en forma integral, además, no se observa una delegación concreta con roles y responsabilidades dentro de las mismas Gerencias y Presidencia Ejecutiva en torno a dicho tema, lo anterior se evidenció con la solicitud de información emitida por esta Auditoría, en la cual se observa una delegación del nivel Gerencial a Áreas, Direcciones o Centros de Gestión Informática, obteniendo respuestas que no contemplaban un alcance representativo de toda la Gerencia, caso contrario, se circunscriben al ámbito operativo de la unidad. A continuación, se presentan ejemplos de lo antes mencionado:

  El oficio AES-1-236-2018 del 14 de mayo del 2018, suscrito por la MSc. Ana Lorena Solís Guevara, Jefe del Área de Estadística, en la cual responde lo siguiente sobre el punto 2 de solicitud de información, lo siguiente:

  "2. Convenios firmados entre la CCSS e instituciones gubernamentales o empresas privadas para el acceso de información contenida en las bases de datos institucionales que contienen datos personales.

  *En la actualidad esta **Área** no realiza convenios con otras instituciones gubernamentales" (Formato subrayado y negrita no pertenece al original)*

  Del mismo modo, se observa en el oficio AGI-GP-0230-2018 del 11 de mayo de 2018, emitido por el Lic. Eithel Corea Baltodano, jefe del Centro de Gestión Informática de la Gerencia de Pensiones, en la cual indica al Lic. Jaime Barrantes Espinoza, Gerente de Pensiones, sobre la respuesta al oficio 6399 de esta Auditoría, lo siguiente:

  *"Es importante aclarar que si bien es cierto el Área de Gestión Informática administra la parte técnica de las bases de datos de los principales sistemas de información de la Gerencia de Pensiones, **la administración de la información contenida en dichas bases de datos y la gestión a través de los sistemas de información, es una función que recae directamente sobre las Direcciones en las que se realizan las actividades sustantivas de la Gerencia de Pensiones** basadas en el procesamiento de la información" (El formato negrita y subrayado no corresponde al original)*

- Ausencia de estrategias institucionales y procedimientos de control interno para garantizar de forma estandarizada y razonable el cumplimiento de la Ley No. 8968.

- Se carece de mecanismos de coordinación entre Presidencia, las distintas Gerencias y sus unidades adscritas para garantizar razonablemente el cumplimiento de la normativa vigente aplicable en esta

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

materia, ejemplo de lo anterior se evidencia en las respuestas emitidas al oficio 6399 de esta Auditoría por parte de Gerencia Médica, mediante oficio AES-1-236-2018 del 14 de mayo del 2018, suscrito por la Msc. Ana Lorena Solís Guevara, jefe del Área de Estadística en Salud y el oficio DTIC-2302-2018 del 18 de abril de 2018 remitido por la Gerencia de Infraestructura y Tecnología a través de la DTIC. A continuación, el detalle:

Tabla 2
Respuestas de Gerencia Médica e Infraestructura y Tecnologías para atención de los puntos 3,4,5,6,7 y 8 del oficio 6399 de Auditoría Interna

Respuesta en Oficio AES-1-236-2018	Respuesta en Oficio DTIC-2302-2018
*"(…) **Respecto a los puntos 3, 4, 5, 6, 7 y 8** cabe mencionar, que la Dirección de Tecnologías de Información y Comunicaciones, es el ente técnico especializado, responsable de la conducción, gestión e integración de las tecnologías de información y comunicaciones en la Institución. (…)*	**"Punto 3.** *No aplica. Los medios y forma de comunicación electrónica lo definen los administradores y dueños de los diferentes sistemas de información, no es competencia de la Dirección de Tecnologías.* ***Punto 4.*** *No aplica. Los usuarios dueños de los sistemas son los responsables para establecer la inclusión, conservación, modificación, bloqueo y supresión de datos personales. La Dirección de Tecnologías únicamente se enfoca a prestar los servicios tecnológicos y los controles que defina* *el usuario.* ***Punto 5.*** *No aplica. Por motivo que esta Dirección brinda un servicio de administración del motor de la base de datos, lo cual, consiste en labores técnicas relacionadas con su adecuado funcionamiento, como parte de los servicios TIC.* ***Punto 6, 7 y 8*** *No aplica dado que le negocio no ha establecido acciones de seguridad concretas en función de la protección de datos personales. La Dirección de Tecnologías de Información y Comunicaciones ha venido desarrollando una serie de esfuerzos relacionados con la seguridad informática sin ninguna vinculación a la ley de protección de datos personales."*

Fuente: AES-1-236-2018 y Oficio DTIC-2302-2018

Como se observa en la tabla anterior, en el oficio AES-1-236-2018, la respuesta a los puntos del 3 al 8, hace referencia a la DTIC como el ente técnico especializado, responsable de la conducción, gestión e integración de las tecnologías de información y comunicaciones en la Institución, sin embargo, en la respuesta de la Gerencia de Infraestructura y Tecnologías mediante oficio DTIC-2302-2018, establece

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

que los puntos no aplican para su unidad debido, dado que son funciones y responsabilidades del área usuario o dueña del proceso.

Referente a lo expuesto por ambas unidades, es criterio de esta Auditoría que lo señalado por la DTIC se apega a los alcances establecidos en la Ley 8968 y su presente reglamento, lo anterior en virtud de que la información solicitada corresponde al *"Responsable de la base de datos"* y no al intermediario tecnológico (en este caso es la DTIC), por ende, la respuesta emitida por Gerencia Médica no corresponde a lo solicitado por este Órgano Fiscalizador. En síntesis, se evidencia la ausencia de coordinación sobre el tema a nivel táctico, operativo y estratégico.

- Según lo indicado por el Sub Gerente de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), unidad encargada de administrar una cantidad de significativa de bases de datos en forma integral (resguarden o no de datos personales), el negocio (haciendo referencia a la parte corporativa) no ha establecido acciones de seguridad concretas en función de la protección de datos personales, repercutiendo en que esa Dirección desarrolle esfuerzos relacionados con la seguridad informática sin ninguna vinculación a la ley 8968.

- Se carece de manual(es) institucional(es) orientados a la capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales y que los mismos sean puestos en práctica.

Por lo anterior, el tema se torna relevante, considerando la cantidad de repositorios de información institucionales que resguardan datos personales de carácter público, restringido y sensible de usuarios, pacientes, patronos, trabajadores, funcionarios, pensionados de los regímenes de Invalidez Vejez y Muerte y No contributivo, entre otros.

La Ley 8968, en su Capítulo I Disposiciones Generales, señala en el artículo 2, lo siguiente:

> *"Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.*
>
> *El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas." (El formato subrayado no corresponde al original)*

La Ley General de Control Interno N° 8292, en sus artículos 12,13 y 15, estipula lo siguiente:

> *"Artículo 12.—**Deberes del jerarca y de los titulares subordinados en el sistema de control interno**. En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:*
> *a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.*
> *b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan.
d) Asegurarse de que los sistemas de control interno cumplan al menos con las características definidas en el artículo 7 de esta Ley.
e) Presentar un informe de fin de gestión y realizar la entrega formal del ente o el órgano a su sucesor, de acuerdo con las directrices emitidas por la Contraloría General de la República y por los entes y órganos competentes de la administración activa.

*Artículo 13.—**Ambiente de control.** En cuanto al ambiente de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*

a) Mantener y demostrar integridad y valores éticos en el ejercicio de sus deberes y obligaciones, así como contribuir con su liderazgo y sus acciones a promoverlos en el resto de la organización, para el cumplimiento efectivo por parte de los demás funcionarios.
b) Desarrollar y mantener una filosofía y un estilo de gestión que permitan administrar un nivel de riesgo determinado, orientados al logro de resultados y a la medición del desempeño, y que promuevan una actitud abierta hacia mecanismos y procesos que mejoren el sistema de control interno.
c) Evaluar el funcionamiento de la estructura organizativa de la institución y tomar las medidas pertinentes para garantizar el cumplimiento de los fines institucionales; todo de conformidad con el ordenamiento jurídico y técnico aplicable.
d) Establecer claramente las relaciones de jerarquía, asignar la autoridad y responsabilidad de los funcionarios y proporcionar los canales adecuados de comunicación, para que los procesos se lleven a cabo; todo de conformidad con el ordenamiento jurídico y técnico aplicable.
e) Establecer políticas y prácticas de gestión de recursos humanos apropiadas, principalmente en cuanto a contratación, vinculación, entrenamiento, evaluación, promoción y acciones disciplinarias; todo de conformidad con el ordenamiento jurídico y técnico aplicable.

*Artículo 15.—**Actividades de control.** Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*

a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.
b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:
i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.
ii. La protección y conservación de todos los activos institucionales.
iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.
v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación."

Las Normas de Control Interno para el Sector Público, en artículo 4.2 Requisitos de las actividades de control, inciso a., indica lo siguiente:

"Las actividades de control deben reunir los siguientes requisitos:

***a. Integración a la gestión**. Las actividades de control diseñadas deben ser parte inherente de la gestión institucional, e incorporarse en ella en forma natural y sin provocar menoscabo a la observancia de los principios constitucionales de eficacia, eficiencia, simplicidad y celeridad, y evitando restricciones, requisitos y trámites que dificulten el disfrute pleno de los derechos fundamentales de los ciudadanos."*

En oficio DTIC-2302-2018 del 18 de abril de 2018, el Máster Robert Picado Mora, Subgerente a.i. de la DTIC, menciona lo siguiente:

"(…) Es importante indicar que la precisión sobre las Bases de Datos que contienen "datos personales", así también, los registros ante la PROHAB, son criterios y acciones que corresponden al negocio, considerando que el contexto de la interpretación y conocimiento de los datos, incluyendo la identificación de los datos que se consideran como "datos personales".

"(…) El negocio no ha establecido acciones de seguridad concretas en función de la protección de datos personales. La Dirección de Tecnologías de Información y Comunicaciones ha venido desarrollando una serie de esfuerzos relacionados con la seguridad informática sin ninguna vinculación a la ley de protección de datos personales.

De manera respetuosa, esta Dirección recomienda a la Alta Gerencia, conocer el modelo de Gobierno y Gestión de las TIC, específicamente lo relacionado con seguridad de la información, para que se comience a habilitar los foros y procesos para abordar estos temas."

El Lic. Eithel Corea Baltodano, Jefe del Centro de Gestión Informática de la Gerencia de Pensiones

"Es importante aclarar que si bien es cierto el Área de Gestión Informática administra la parte técnica de las bases de datos de los principales sistemas de información de la Gerencia de Pensiones, la administración de la información contenida en dichas bases de datos y la gestión a través de los sistemas de información, es una función que recae directamente sobre las Direcciones en las que se realizan las actividades sustantivas de la Gerencia de Pensiones basadas en el procesamiento de la información" (El formato negrita y subrayado no corresponde al original)

La Licda. Giselle Tenorio Chacón, Jefe a.i. del Centro Gestión Informática de la Gerencia Administrativa, indicó en oficio CGI-GADMIN 133-2018 del 17 de abril del año en curso, lo siguiente:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

"(…) Por medio de la Comisión Institucional de Seguridad de la Información, se coordinó con la Agencia de Protección de Datos de los Habitantes (PRODHAB) presentación del proceso a seguir para inscribir las bases ante este organismo, y se explicó lo por parte del Lic. Luis Chinchilla y Lic. Mauricio Garro Guillén lo siguiente:

- *El alcance de la Ley N° 8968 y su Reglamento*
- *Solo se debe inscribir las Base de Datos que tienen datos personales y que dicha información sea compartida con otras instituciones.*
- *Si los datos se mantienen únicamente para uso interno, no deben de inscribirse ante este organismo.*
- *Se indicó que el Reglamento a la Ley de Protección de la Persona frente al tratamiento de sus datos personal, Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012, fue publicado en El Alcance No. 42 a La Gaceta No. 45 del 05 de marzo del 2013.*

Por otra parte, se envía la información solicitada como inventario de Base de Datos, administradas en forma compartida por este Centro de Gestión Informática y la Subárea Gestión de Base de Datos de la DTIC, sin embargo, ***se debe recordar que el usuario dueño es el responsable de la información almacenada y de las modificaciones que solicita por medio de requerimientos y los cuales cuenta con su autorización****. (…)" (El formato negrito y subrayado no corresponde al original)*

En el oficio AES-1-236-2018 del 14 de mayo del 2018, suscrito por la MSc. Ana Lorena Solís Guevara, Jefe del Área de Estadística, menciona en relación al tema lo siguiente:

"(…) El 18 de abril de 2018 el Área de Estadísticas en Salud presentó al Comité Estratégico EDUS-ARCA, la viabilidad de conformar una comisión técnica intergerencial, con el propósito de documentar los aspectos normativos que solicita la ley N° 8968 y afines que permitan la inscripción de las bases de datos de la Institución ante el PRODHAB. Esta propuesta fue avalada por este Comité Estratégico. "

El Lic. Olger Vargas Pérez, Jefe de la Sub Área de Gestión de Bases de Datos, indicó lo siguiente:

"No ha existido participación de responsables de la parte usuaria que soliciten requerimientos de seguridad en función de la protección de datos personales."

La ausencia de un modelo de gestión integral y debidamente articulado entre las diferentes instancias con participación en cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, en etapas que van desde la recolección, registro, organización, conservación, modificación, extracción, entre otros, así como su bloqueo, supresión o destrucción, podría comprometer que la Institución no cumpla con el objetivo y fin de la Ley 8968, el cual refiere a garantizar a cualquier persona, independientemente de su nacionalidad, residencia

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

o domicilio, el respeto a sus derechos fundamentales, concretamente, la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Del mismo modo, dada la cantidad de datos personales administrados por la Caja a nivel país, la ausencia de procedimientos estandarizados sobre los pasos a seguir en la recolección, el almacenamiento y el manejo de los datos personales así como la definición de responsables conforme a las reglas previstas en ley No. 8968, podría materializar riesgos de seguridad, confidencialidad, integridad y privacidad que afecten a los usuarios, pacientes, funcionarios, trabajadores, pensionados y patronos, lo anterior ante la ausencia de garantías que permitan brindar seguridad sobre la información resguardada por la CCSS en sus bases de datos.

Finalmente, la situación descrita podría generar que ante una violación de los principios establecidos en la ley supra citada afecte en primera instancia los derechos de los ciudadanos sobre el tratamiento de sus datos personales, además, institucionalmente comprometería la reputación e imagen y finalmente podría verse sometida al régimen sancionatorio que establece dicho marco normativo.

2. SOBRE EL INVENTARIO INSTITUCIONAL DE BASES DE DATOS QUE CONTIENEN DATOS PERSONALES.

Se evidenció la ausencia de un inventario institucional con las bases de datos que contienen registros de carácter personal, provocando riesgos sobre la identificación, exactitud y totalidad de los repositorios que dispone la CCSS con este tipo de información.

Al respecto, esta Auditoría considera que uno de los principios desde un marco de control interno para una adecuada administración de los datos personales resguardados por la Institución, inicia con la identificación de cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, objeto de tratamiento o procesamiento, ya sea automatizado o manual, independientemente de su modalidad, elaboración, organización o acceso, posterior a este objetivo, se puede gestionar el respectivo cumplimiento de lo estipulado en la Ley 8968 y su reglamento, por ende, la ausencia de un inventario o que el mismo sea limitado, provoca riesgos de control y detección.

En línea con el tema, sobre la información remitida por Gerencia Médica a esta Auditoría con las bases de datos con registros de carácter personal, únicamente se hace referencia a las aplicaciones que conforman el Expediente Digital Único en Salud (EDUS) y el ARCA, omitiendo otros repositorios de información dentro de esa Gerencia que también podrían contener datos personales, tales como:

- Base de datos del Sistema de Vigilancia Epidemiológica (SISVE).
- Base de datos del Sistema de Bancos de Sangre (E-Delphyn).
- Base de datos del Sistema de Laboratorios (LABCORE).
- Base de Datos de la Aplicación de Disponibilidades Médicas (ADIM).
- Base de datos del Sistema Integrado de Farmacias (SIFA)
- Bases de datos del Sistema de Vacunas (SISVAC)

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- Base de Datos de la Oficina Virtual del Centro de Desarrollo Estratégico e Información en Salud y Seguridad Social.
- Base de Datos del Portal Web, en donde se ubica una tabla que resguarda datos personales de la campaña *"Atrévete a donar"***,** misma que al 4 de julio almacena 34912 registros, lo anterior correspondiente al Programa de donación y trasplantes.

Por otra parte, en respuesta emitida por la Presidencia Ejecutiva mediante oficio PE-0751-2018 del 12 de abril del año en curso, suscrito por la MSc. Elena Bogantes Zúñiga, Directora de Despacho, indica que esa unidad no opera una base de datos propia de información personal, sin embargo, esta Auditoría tiene conocimiento que la Dirección Institucional de Contralorías de Servicios de Salud, unidad adscrita a esa instancia, dispone de bases de datos con eventuales registros personales de los usuarios, lo anterior mediante el software *"Sistema Estadístico de la Dirección Institucional de Contralorías de Servicios de Salud",* el cual fue evaluado por este Órgano de Fiscalización en el informe ATIC-28-2017.

En síntesis, lo antes mencionado comprueba que las bases de datos con registros personales reportadas por la Administración Activa y señaladas en los antecedentes del presente estudio podrían carecer de exactitud, lo anterior considerando la omisión de los repositorios de información antes mencionados.

La Ley General de Control Interno No 8292, en su artículo 15, estipula lo siguiente:

> *Artículo 15.—**Actividades de control.** Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
>
> *a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.*
> *b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
> *i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.*
> *ii. La protección y conservación de todos los activos institucionales.*
> *iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.*
> *iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.*
> *v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación.*

Las Normas técnicas para la gestión y el control de las Tecnologías de Información, en el artículo 1.4.1 y 1.4.5, incisos b y c, indica lo siguiente:

> *"**1.4.1 Implementación de un marco de seguridad de la información.***
> *La organización debe implementar un marco de seguridad de la información, para lo cual debe:*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.

b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.

c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados. "

"1.4.5 Control de Acceso
La organización debe proteger la información de accesos no autorizados.
Para dicho propósito debe:

a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI. "

Esas mismas Normas, en el inciso 1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI, menciona que:

"La organización debe identificar y velar por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TI con el propósito de evitar posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza."

El Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, en su artículo 36 Acciones para la seguridad de los datos personales, inciso b, indica lo siguiente:

"A fin de establecer y mantener la seguridad física y lógica de los datos personales, el responsable deberá realizar al menos las siguientes acciones, las cuales podrán ser requeridas en cualquier momento por la Agencia:

*b**)** Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias;"*

Como causa de lo evidenciado en el presente hallazgo, se puede determinar que obedece a lo evidenciado en el punto uno de este informe sobre la ausencia de un modelo de gestión institucional orientado al tratamiento y protección de los datos personales administrados por la Caja, así como la carencia de instancias formalmente definidas que aborden el tema en forma integral y recopilen de manera unificada un inventario de las bases de datos institucionales con información de carácter personal.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

La situación descrita en torno a la ausencia de un inventario unificado de los repositorios de información con datos personales, podría repercutir en que la misma Institución no tenga la certeza razonable de la cantidad de bases existentes a nivel institucional con este tipo de registros, lo anterior se torna relevante considerando que la Caja administra información a nivel país y en diversos ámbitos, es decir, datos personales sobre pacientes, patronos, trabajadores, pensionados y funcionarios, resultando indispensable identificar las fuentes donde son almacenados y alinearlas para cumplir con lo estipulado en la Ley 8968, su reglamento.

3. SOBRE LOS RESPONSABLES[3] DE BASES DE DATOS SEGÚN LOS TERMINOS ESTABLECIDOS EN LA LEY 8968.

De acuerdo con la información suministrada por la Administración Activa sobre las bases de datos que contienen registros personales y sus respectivos responsables, se puede evidenciar que a nivel institucional no existe claridad sobre el concepto (*Responsable*) según lo estipulado en la Ley 8968, lo anterior en virtud de los siguientes aspectos identificados:

- En las respuestas emitidas por la Administración Activa, señalan en esta función a Gerentes, Nombres de Direcciones o Áreas, Directores, Jefes de Área, Sub Áreas, informáticos, médicos o funcionarios operativos, además, en todos los casos anteriores, no se aporta respaldo documental certificando que estos funcionarios o unidades cumplen las tareas estipuladas en la Ley 8968 y su reglamento. Al respecto, tal y como se indica en el hallazgo cuatro del presente informes, no se remitió evidencia que permitiera determinar cuáles de las bases de datos indicadas fueron sometidas a una valoración formal para concluir que son de carácter interno y, por ende, se encuentran fuera del ámbito de aplicación señalado en el marco normativo antes mencionado o, por el contrario, obedece a que no se están ejecutando las responsabilidades pertinentes.

- De igual manera, las respuestas emitidas permiten determinar que no existe una diferenciación entre la definición tipificada en la ley de "*responsable de base de datos"* e "*intermediario tecnológico o proveedor de servicios"*[4], lo anterior en virtud de que se evidencian funcionarios destacados en TIC nombrados como responsables de bases de datos, a continuación, se presenta algunos ejemplos:

Tabla 4
Responsables de Bases de datos con perfil TIC

Nombre de la Base(s) de Datos	***Sistema de Información utilizado para registrar los datos***	***Nombre y puesto del responsable (s) de la base de datos***	***Estado actual del Sistema de Información***
BD_SIIF_INTEGRADO _FINANCIERO	*SIIF-Sistema Institucional de Presupuesto*	***Lic. Olger Vargas Pérez Jefe Subárea Gestión de Bases de Datos***	*Producción*

[3] Toda persona física o jurídica, pública o privada, que administre o, gerencia o, se encargue o, sea propietario, de una o más bases de datos públicas o privadas, competente con arreglo a la Ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento les aplicarán."

[4] Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Base de Datos SICERE (SFCVA)	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	***Alexander Angelini (SFA), Jefe Sub Área de Sistemas Financieros Administrativos***	*Desarrollo*
Base de Datos SICERE (SFCVB)	*SICERE 11g, Oficina Virtual, SISTEMA DE APOYO AL CLIENTE (SAC)*	***Alexander Angelini (SFA), Jefe Sub Área de Sistemas Financieros Administrativos***	*Desarrollo*
RRHH (base de datos de recursos humanos)	*Portal RRHH y sus aplicaciones*	***Laura Paz Morales, jefe Subárea de sistema automatizado en RH.*** *Walter Campos Paniagua, subdirector Dirección de Administración y Gestión de Personal.*	*Producción*

Fuente: Oficios GF-1771-2018, DAGP-0706-2018.

- Existen casos donde se observa la interpretación de que el líder usuario de una aplicación funge como responsable de una base de datos, sin embargo, el primero se aboca a una función sustantiva operativa orientada a la gestión de requerimientos de una solución y no las funciones establecidas en la Ley 8968 y su reglamento, lo anterior de acuerdo con la respuesta emitida por la DTIC, donde figuran líderes usuarios de los diferentes aplicativos que conforman el Expediente Digital Único en Salud (EDUS) como responsables de la base de datos.

- Se observa diferencias en los nombres de responsables señalados por las Gerencias en contraparte a la respuesta emitida por la DTIC sobre todas las bases de datos que administra y sobre quienes considera como sus responsables, evidenciando una discrepancia de criterios entre la parte corporativa (Gerencias y Presidencia) con el intermediario tecnológico (en este caso DTIC). A continuación, se presentan algunos ejemplos:

Tabla 5
Responsables de Bases de datos según negocio y DTIC

Nombre de la Base de datos	***Responsable según Gerencias***	***Responsable según DTIC***
SIGNOS (Base de datos que forma parte del Expediente Digital Único en Salud (EDUS)	*Villalta Bonilla María Eugenia*	*SIES-Eduardo Rodríguez Cubillo* *SIFF-Guiselle Barrantes Brenes* *SIAC-Róger Jován López Espinoza* *SILC-Ana Lorena Torres Rosales* *SIFA-(Bases de datos Locales) Isela Araya Piedra* *SICI-Rodrigo Manuel Álvarez Ramírez*
Base de Datos SICERE (SFCV)	*Gerente Financiero a través de la Dir. SICERE (DSCR)*	*Luis Rivera Cordero*
RRHH (base de datos de recursos humanos)	*Laura Paz Morales, jefe Subárea de sistema automatizado en RH.* *Walter Campos Paniagua, subdirector Dirección de Administración y Gestión de Personal.*	*Laura Paz Morales*

Fuente: Oficios GF-1771-2018, GIT-0632-2018, AES-1-236-2018, DAGP-0706-2018.

Las Normas de Control Interno para el Sector Público, en el apartado 1.4 Responsabilidad del jerarca y los titulares subordinados sobre el SCI, estipulan lo siguiente:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

"La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.

En el cumplimiento de esa responsabilidad las autoridades citadas deben dar especial énfasis a áreas consideradas relevantes con base en criterios tales como su materialidad, el riesgo asociado y su impacto en la consecución de los fines institucionales, incluyendo lo relativo a la desconcentración de competencias y la contratación de servicios de apoyo. Como parte de ello, deben contemplar, entre otros asuntos, los siguientes:

a. La definición de criterios que brinden una orientación básica para la instauración y el funcionamiento de los componentes orgánicos y funcionales del SCI con las características requeridas.
b. El apoyo con acciones concretas, al establecimiento, el funcionamiento y el fortalecimiento de la actividad de auditoría interna, incluyendo la dotación de recursos y las condiciones necesarias para que se desarrolle eficazmente y agregue valor a los procesos de control, riesgo y dirección.
c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y actualizados, y sean divulgados y puestos a disposición para su consulta.
d. La vigilancia del cumplimiento, la validez y la suficiencia de todos los controles que integran el SCI.
e. La comunicación constante y el seguimiento de los asuntos asignados a los distintos miembros de la institución, en relación con el diseño, la ejecución y el seguimiento del SCI.
f. Las acciones pertinentes para el fortalecimiento del SCI, en respuesta a las condiciones institucionales y del entorno."
g. Una pronta atención a las recomendaciones, disposiciones y observaciones que los distintos órganos de control y fiscalización emitan sobre el particular.

Esas mismas Normas, en el apartado 1.7 Rendición de cuentas sobre el SCI, indican lo siguiente:

"El jerarca y los titulares subordinados, según sus competencias, deben disponer y ejecutar un proceso periódico, formal y oportuno de rendición de cuentas sobre el diseño, el funcionamiento, la evaluación y el perfeccionamiento del SCI, ante los diversos sujetos interesados."

El reglamento de la Ley 8968, en su artículo 2 Definiciones, siglas y acrónimos, indica lo siguiente para responsable e intermediario tecnológico o proveedor de servicios:

"Además de las definiciones establecidas en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, para los efectos del presente Reglamento se entenderá por:

***Responsable:** Toda persona física o jurídica, pública o privada, que administre o, gerencia o, se encargue o, sea propietario, de una o más bases de datos públicas o privadas, competente con arreglo a la Ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento les aplicarán."*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

> ***Intermediario tecnológico o proveedor de servicios****: Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios."*

Respecto al tema, la Agencia de Protección de Datos de los Habitantes, indicó mediante correo electrónico el siguiente criterio:

> *"(…)El criterio de la Agencia ha sido siempre que independientemente de si la base de datos está obligada o no a inscribirse ante esta institución, a pesar de lo que indica el artículo 3 del reglamento, todas las bases de datos que administren datos personales deben tener presente que según lo que establece el artículo 1 de la Ley 8968 que indica "Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.". Es decir, independientemente del tipo de base de datos sea interna o doméstica, es importante que el dueño o responsable de la misma mantenga los mecanismos necesarios, las medidas de seguridad y los protocolos mínimos en torno a los datos personales que mantenga en su base de datos.*
>
> *Lo anterior por cuanto en el momento que así lo requiera el titular de los datos ante un mal uso de sus datos personales o recopilados de forma ilícita, podrá interponer ante la Agencia un Procedimiento de Proteccion de Derechos, con tan solo tener un interés legítimo o un derecho subjetivo. De igual manera podría eventualmente la persona titular de los datos acudir a la sede penal e interponer una denuncia por la violación a sus datos personales, según lo que establece el artículo 196 bis del Código Penal. Producto de lo anterior se recomienda tomar en cuenta los artículos 32 referente a los protocolos mínimos de actuación y 35 al 39 atinentes a las medidas de seguridad que establece el Reglamento a la Ley 8968.*

Como causa de lo evidenciado en el presente hallazgo, se puede determinar que obedece a lo evidenciado en el punto uno de este informe sobre la ausencia de un modelo de gestión institucional orientado al tratamiento y protección de los datos personales administrados por la Caja, así como la carencia de instancias formalmente definidas que aborden el tema en forma integral.

En oficio DTIC-2302-2018 del 18 de abril de 2018, el Máster Robert Picado Mora, Subgerente a.i. de la DTIC, menciona lo siguiente:

> *"(…) Es importante indicar que la precisión sobre las Bases de Datos que contienen "datos personales", así también, los registros ante la PROHAB, son criterios y acciones que corresponden al negocio, considerando que el contexto de la interpretación y conocimiento de los datos, incluyendo la identificación de los datos que se consideran como "datos personales (…).*
>
> *(…) Los usuarios dueños de los sistemas, son los responsables para establecer la inclusión, conservación, modificación, bloqueo y supresión de datos personales. La Dirección de*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Tecnologías únicamente se enfoca a prestar los servicios tecnológicos y los controles que defina el usuario. (…)

(…) De manera respetuosa, esta Dirección recomienda a la Alta Gerencia, conocer el modelo de Gobierno y Gestión de las TIC, específicamente lo relacionado con seguridad de la información, para que se comience a habilitar los foros y procesos para abordar estos temas."

El Lic. Eithel Corea Baltodano, Jefe del Centro de Gestión Informática de la Gerencia de Pensiones

"Es importante aclarar que si bien es cierto el Área de Gestión Informática administra la parte técnica de las bases de datos de los principales sistemas de información de la Gerencia de Pensiones, ***la administración de la información contenida en dichas bases de datos y la gestión a través de los sistemas de información, es una función que recae directamente sobre las Direcciones en las que se realizan las actividades sustantivas de la Gerencia de Pensiones*** *basadas en el procesamiento de la información" (El formato negrita y subrayado no corresponde al original)*

La Giselle Tenorio Chacón, Jefe a.i. del Centro Gestión Informática de la Gerencia Administrativa, indicó en oficio CGI-GADMIN 133-2018 del 17 de abril del año en curso, lo siguiente:

"(…) Se envía la información solicitada como inventario de Base de Datos, administradas en forma compartida por este Centro de Gestión Informática y la Subárea Gestión de Base de Datos de la DTIC, sin embargo, ***se debe recordar que el usuario dueño es el responsable de la información almacenada y de las modificaciones que solicita por medio de requerimientos y los cuales cuenta con su autorización****. (…)" (El formato negrito y subrayado no corresponde al original)*

El Lic. Olger Vargas Pérez, Jefe de la Sub Área de Gestión de Bases de Datos, indicó lo siguiente:

"Tenemos identificados usuarios líder para las principales bases de datos que administramos. Sin embargo, no tenemos información acerca de cuál base de datos contiene datos personales."

La situación descrita podría materializar riesgos sobre la Institución referentes al efectivo cumplimiento de la Ley 8968 y su reglamento, teniendo consideración que el responsable de la base de datos tiene funciones indispensables para garantizar los derechos de los titulares y su ejercicio, el tratamiento de los datos personales y las medidas de seguridad pertinentes, por lo anterior, la no definición formal y concreta de responsables sobre los repositorios de información con registros personales, impide establecer procesos de rendición de cuentas sobre los funcionarios que cumplen con las tareas establecidas el marco normativo supra citado.

4. SOBRE LA CLASIFICACIÓN DE LAS BASES DE DATOS QUE RESGUARDAN DATOS PERSONALES.

Sobre las bases de datos institucionales que almacenan datos personales, se evidenció la ausencia de respaldo documental que permita establecer con criterios competentes y pertinentes, una diferenciación sobre los repositorios de información que son de carácter interno y los que deberían formar parte del

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

ámbito de aplicación de la Ley 8968 y su reglamento por no tener "*fines exclusivamente internos, personales, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas",* según lo establece el artículo 2.

Sin embargo, en diversas respuestas brindadas por la Administración Activa, se justifica la aplicación parcial del Reglamento a la ley antes citada, basándose en el criterio indicado en el artículo dos de ese marco regulatorio, sin aportarse las valoraciones y definiciones formales que sustenten esa afirmación.

Al respecto, esta Auditoría contactó con personal de Prodhab, a fin de conocer y compartir criterios generales con relación a la Ley y el alcance establecido el artículo 3 del reglamento, lográndose determinar entre otros aspectos, que las únicas Bases de Datos fuera del ámbito de aplicación de ese marco normativo son las del Sistema Bancario Nacional y las de uso interno, pero estas últimas deben ser debidamente justificadas, cumplir con los protocolos de seguridad, definición de responsables y consentimiento informado en caso de ser requerido, es decir, todas las bases de datos institucionales están sometidas bajo la Ley 8968, lo que hace la excepción es la no inscripción; sin embargo, todas están sujetas o expuestas a denuncias, por casos como fraude o robo de información, entre otros.

La Ley 8968, en sus artículos 1 y 2, establecen lo siguiente:

> *"**ARTÍCULO 1.- Objetivo y fin***
>
> *Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.*
>
> ***ARTÍCULO 2.- Ámbito de aplicación***
>
> *Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.*
>
> *El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas."*

Respecto al tema, la Agencia de Protección de Datos de los Habitantes, indicó mediante correo electrónico el siguiente criterio:

> *"(…)El criterio de la Agencia ha sido siempre que independientemente de si la base de datos está obligada o no a inscribirse ante esta institución, a pesar de lo que indica el artículo 3 del reglamento, todas las bases de datos que administren datos personales deben tener presente*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

que según lo que establece el artículo 1 de la Ley 8968 que indica "Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.". Es decir, independientemente del tipo de base de datos sea interna o doméstica, es importante que el dueño o responsable de la misma mantenga los mecanismos necesarios, las medidas de seguridad y los protocolos mínimos en torno a los datos personales que mantenga en su base de datos.

Lo anterior por cuanto en el momento que así lo requiera el titular de los datos ante un mal uso de sus datos personales o recopilados de forma ilícita, podrá interponer ante la Agencia un Procedimiento de Proteccion de Derechos, con tan solo tener un interés legítimo o un derecho subjetivo. De igual manera podría eventualmente la persona titular de los datos acudir a la sede penal e interponer una denuncia por la violación a sus datos personales, según lo que establece el artículo 196 bis del Código Penal. Producto de lo anterior se recomienda tomar en cuenta los artículos 32 referente a los protocolos mínimos de actuación y 35 al 39 atinentes a las medidas de seguridad que establece el Reglamento a la Ley 8968.

Como causa de lo evidenciado en el presente hallazgo, se puede determinar que responde a la situación detectada en el punto uno y dos de este informe sobre la ausencia de un modelo de gestión institucional orientado al tratamiento y protección de los datos personales administrados por la Caja, así como la carencia de instancias formalmente definidas que aborden el tema en forma integral y recopilen de manera unificada un inventario de las bases de datos institucionales con información de carácter personal, permitiendo establecer una valoración que fundamente si estas forman parte del ámbito de aplicación de la Ley 8968 y su reglamento.

Producto de la situación descrita en el hallazgo, surge como efecto que tanto la Administración Activa como este Órgano de Fiscalización no puede determinar en forma certera los responsables de bases de datos con registros personales cumplen las siguientes funciones estipuladas en la Ley 8968 y su reglamento, tales como:

- Medio y forma de comunicación electrónica definido por el responsable para facilitar a los titulares el ejercicio de sus derechos.

- Procedimientos establecidos por el responsable para la inclusión, conservación, modificación, bloqueo y supresión de datos personales.

- Mecanismos o procedimientos establecidos por el responsable de la base de datos para comunicar a los encargados, las obligaciones en el tratamiento de bases de datos personales.

- Protocolos mínimos de actuación para la recolección, almacenamiento y el manejo de los datos personales.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- El proceso de divulgación efectuado para dichos protocolos, a fin de garantizar el cumplimiento por parte de los encargados en el tratamiento de datos personales.

- Medidas de seguridad, administrativas, físicas y lógicas implementadas por el responsable para la protección de datos personales.

- Mecanismos de control implementados por el responsable para garantizar o velar que los encargados de bases de datos y el intermediario tecnológico cumplen las medidas supra citadas en torno al resguardo de la información.
- Acciones para la seguridad de los datos personales, establecidas en el artículo 36 del Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.

5. SOBRE LA INSCRIPCIÓN DE BASES DE DATOS QUE CONTIENEN DATOS PERSONALES ANTE LA PRODHAB.

Al 30 de mayo del presente año, se evidencia que la única base de datos inscrita ante la Agencia de Protección de Datos (Prodhab) es la del Sistema Centralizado de Recaudación, pese a que esta Auditoría contabilizó 30 repositorios de información a nivel institucional, los cuales podrían estar sometidos a este procedimiento por contener datos personales y no cumplir con fines exclusivamente internos, sin embargo, por lo señalado en el hallazgo 4 de este informe no es posible identificar cuales deben inscribirse.

Como excepción a lo anterior, se evidenció que la Administración Activa se encuentra realizando gestiones para inscribir ante la Agencia la base de datos del EDUS, no obstante, se evidenciaron los siguientes riesgos:

- A la fecha de este estudio la base de datos del EDUS no se encuentra inscrita ante la Prodhab, pese a que la Ley 8968 entró en vigencia desde el año 2011, es decir, han transcurrido cerca de siete años al margen de lo indicado en su artículo 21, lo anterior llama la atención considerando aplicativos como el Sistema de Identificación Agendas y Citas (SIAC), el Sistema Integrado de Expediente en Salud (SIES), Sistema Integrado de Ficha Familiar (SIFF), el Sistema Integrado de Farmacias (SIFA), los cuales eran utilizados por la Institución inclusive antes de que existiera dicha Ley.

- Adicional a lo anterior, se evidenció que la Gerencia Médica hasta abril de 2016, delegó la inscripción de las bases de datos del EDUS al Área de Estadística en Salud, precisamente producto del oficio de advertencia AD-ATIC-49757-2016 emitido por esta Auditoría, sin embargo, han transcurrido más de dos años y esta unidad no ha finalizado el proceso ante la Prodhab.

- Los aplicativos ARCA (Admisión y Egreso, Quirúrgico y Patología) siendo que son bases de datos independientes del aplicativo EDUS pero que se integran y forman parte del Proyecto, a la fecha de este informe tampoco ha sido gestionado su registrado ante la Prodhab.

Ahora bien, considerando que los datos relativos a la salud están clasificados como registros sensibles y que según su ámbito de competencia son administrados por la Gerencia Médica, llama la atención no estén inscritas todas las bases de datos referentes al sector médico, de las cuales esta Auditoría tiene conocimiento existen procesos de transferencia de información a instancias como el Ministerio de Salud,

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

como por ejemplo los sistemas relacionados con la gestión de farmacias, vigilancia epidemiológica o inmunizaciones y que no residen en los aplicativos del proyecto EDUS-ARCA.

Similar a lo anterior, existe software de la Gerencia de Pensiones que almacena información en salud para casos referentes a trámites de pensiones de invalidez, vejez y muerte o del régimen no contributivo, así como datos relativos a registros bancarios y crediticios, sin embargo, estos repositorios tampoco están inscritos ante la Prodhab.

La Ley General de Control Interno N° 8292, en sus artículos 8, punto estipula en los incisos c y d, lo siguiente:

> *"Para efectos de esta Ley, se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:*
>
> *c) Garantizar eficiencia y eficacia de las operaciones.*
> *d) Cumplir con el ordenamiento jurídico y técnico."*

Esa misma Ley, en su artículo 12 Deberes del jerarca y de los titulares subordinados en el sistema de control interno, punto a,b y c, citan que:

> *"En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:*
>
> *a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.*
> *b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades.*
> *c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan. "*

La Ley 8968, en su artículo 21 Registro de archivos y bases de datos, indica lo siguiente:

> *"Toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Prodhab. La inscripción no implica el trasbase o la transferencia de los datos.*
>
> *Deberá inscribir cualesquiera otras informaciones que las normas de rango legal le impongan y los protocolos de actuación a que hacen referencia el artículo 12 y el inciso c) del artículo 16 de esta ley."*

Respecto al tema, la Agencia de Protección de Datos de los Habitantes, indicó mediante correo electrónico el siguiente criterio:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

"(…)El criterio de la Agencia ha sido siempre que independientemente de si la base de datos está obligada o no a inscribirse ante esta institución, a pesar de lo que indica el artículo 3 del reglamento, todas las bases de datos que administren datos personales deben tener presente que según lo que establece el artículo 1 de la Ley 8968 que indica "Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.". Es decir, independientemente del tipo de base de datos sea interna o doméstica, es importante que el dueño o responsable de la misma mantenga los mecanismos necesarios, las medidas de seguridad y los protocolos mínimos en torno a los datos personales que mantenga en su base de datos.

Lo anterior por cuanto en el momento que así lo requiera el titular de los datos ante un mal uso de sus datos personales o recopilados de forma ilícita, podrá interponer ante la Agencia un Procedimiento de Proteccion de Derechos, con tan solo tener un interés legítimo o un derecho subjetivo. De igual manera podría eventualmente la persona titular de los datos acudir a la sede penal e interponer una denuncia por la violación a sus datos personales, según lo que establece el artículo 196 bis del Código Penal. Producto de lo anterior se recomienda tomar en cuenta los artículos 32 referente a los protocolos mínimos de actuación y 35 al 39 atinentes a las medidas de seguridad que establece el Reglamento a la Ley 8968.

Mediante oficio AES-1-236-2018 del 14 de mayo de 2018, la Msc. Ana Lorena Solís Guevara, jefe del Área de Estadística en Salud, remite al Dr. Fernando Llorca Castro, Presidente Ejecutivo, Gerente Médico A/c, indicando lo siguiente:

"En atención a oficio GM-AUDB-5129-2018, cuyo asunto es oficio 6399-2018 Solicitud de información relacionada con el tratamiento de datos personales contenidos en las bases de datos, se hace de su conocimiento las acciones ejecutadas por el Área de Estadística en Salud (AES), desde el año 2016, a la fecha, en el proceso de inscripción de la base de datos SIGNOS, ante la Agencia de Protección de Datos de los Habitantes. (PRODHAB).

***1.** El 6 de abril de 2016 mediante oficio GM-CGI-10099-16, la Dra. María Eugenia Villalta Bonilla, Gerente Médica, instruyó al Área de Estadística en Salud, a realizar el proceso de Inscripción de la base de datos SIGNOS que contiene los siguientes sistemas de información:*

Ambiente	***Base de Datos***	***Usuario Dueño***
Oracle	*SIGNOS (Módulo) SIAC_ADSCRIPCIÓN* *SIGNOS (Módulo) SIAC_AGENDAS* *SIGNOS (Módulo) SIAC_CITAS* *SIGNOS (Módulo) SIAC_BENEFICIO_FAMILIAR*	*Msc. Leslie Vargas Vásquez*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Esto en razón de los oficios TIC-0274-16 y TIC-1039-2016, ambos firmados por el Msc. Robert Picado Mora, Subgerente de la Dirección de Tecnologías de Información y Comunicaciones, donde señaló que esos sistemas pertenecen a la Gerencia Médica.

***2.** El 1 de diciembre de 2016, en oficio GM-SJD-22741-2016 Disposiciones para el cumplimiento de lo establecido en la ley de protección de datos personales. (EDUS), la Dra. María Eugenia Villalta Bonilla, Gerente Médica, solicitó apoyo y colaboración al Área de Estadísticas de Salud, para que se ejecuten las acciones y disposiciones necesarias con el fin de cumplir con lo establecido en la ley de N°8968 de la protección de datos, en atención a lo planteado por el Directivo Rolando Barrantes Muñoz, además, se coordine las acciones que se requiera para disponer de los instruido con la Gerencia Infraestructura y Tecnologías.*

***3.** El 6 de diciembre de 2016, el Área de Estadística en Salud mediante nota AES-1-641-2016, da respuesta al oficio GM-SJD-22741-2016 a la Dra. María Eugenia Villalta Bonilla, Gerente Médica, indicándole que mediante oficio EDUS-16757-2016, TIC-1398-2016 y AES-1-550-2016, se abordó entre otros temas la Seguridad de la Información y Seguridad Informática, señalando lo siguiente:*

"El Área de Estadística en Salud, da acompañamiento y apoyo incondicional en los temas que son de su competencia técnica, que forman parte en el desarrollo del proyecto EDUS y los aspectos relacionados directamente con el manejo de la seguridad de la información (codificación, completitud, calidad e integridad). (…)"

***4.** El 22 de diciembre de 2016 en oficio GM-CGI-23809-16, en atención al oficio GM-CGI-10099-16 del 6 de abril de 2016, la Dra. María Eugenia Villalta Bonilla, Gerente, Gerencia Médica, solicitó los informes de las acciones realizadas sobre los trámites de inscripción de las bases de datos.*

***5.** El 9 de mayo de 2017, en oficio GM-CGI-22467-17, "Solicitud de conclusión trámite de inscripción Base de Datos SIGNOS – sistema EDUS ante Agencia Prodhab", enviada a la Msc. Ana Lorena Solís Guevara, Jefe Área de Estadística en Salud, la Gerente Médica, Dra. María Eugenia Villalta Bonilla, expresó lo siguiente "… agradecerle por lo gestionado hasta el momento, con relación al tema supracitado. Así mismo le solicito proceder a la brevedad con la entrega de la documentación y formularios respectivos para el trámite de la firma por parte de la Señora Presidenta Ejecutiva." Además "… ya se dispone de los requisitos exigidos por la Agencia PRODHAB en apego a la Ley 8968 que aplica a todos aquellos sistemas de información institucionales."*

***6.** El 19 de junio de 2017, en oficio GM-SJD-24491-17, Solicitud de análisis y propuesta de respuesta, cumplimiento ley de la protección de la persona frente al tratamiento de sus datos personales (agencia PRODHAB), enviada a la Msc. Ana Lorena Solís Guevara, Jefe Área de Estadística en Salud, la Gerente Médica, Dra. María Eugenia Villalta Bonilla, indicó lo siguiente "…se debe analizar detalladamente la inscripción o no de la base de datos en la agencia de Protección de Datos a los habitantes (PRODHAB)." Por lo que solicita preparar respuesta al oficio GIT-7983-2017, aclarando que la Gerencia Médica no es responsable de la base de datos como*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

tal, sino de los datos únicamente, ya que la responsabilidad de la base de datos técnicamente corresponde a la Dirección de Tecnologías de Información y Comunicación.

***7.** El 7 de julio de 2017, en oficio GM-SJD-25508-17, Solicitud de informe urgente ley protección de datos personales, enviada a la Msc. Ana Lorena Solís Guevara, Jefe Área de Estadística en Salud, la Gerente Médica, Dra. María Eugenia Villalta Bonilla, solicitó en conjunto con la Dirección de Tecnologías de Información y Comunicaciones con carácter urgente presentar informe, con el fin de que se establezcan y ejecuten las acciones necesarias que garanticen que la base de datos EDUS cumpla con la protección que exige esa ley.*

***8.** El 14 de julio de 2017, mediante oficio del Área de Estadística en Salud AES-1-402-2017, dirigida a la Dra. María Eugenia Villalta Bonilla, Gerente Médica, se da respuesta a oficio GM-SJD-25508-17, donde se indica "De acuerdo a lo solicitado en los oficios GM-CGI-10099-16 y GM-SJD-22741-16, el Área de Estadística en Salud (AES) en conjunto con la Dirección de Tecnologías de Información y Comunicaciones preparó la documentación requerida por la Agencia de Protección de Datos de los Habitantes (PRODHAB) para la inscripción de la base de datos del Expediente Digital Único en Salud (EDUS), ante dicho Órgano según lo estable la Ley N°8968 "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales".*

"Dicha documentación fue remitida, en el segundo semestre del año 2016, al Comité Gestor del EDUS para su revisión y posterior envío a la Presidencia Ejecutiva, con el fin de que se realizara los trámites necesarios para completar el proceso de inscripción de dicha base de datos. Posteriormente, dicho comité remitió este tema a la presidencia Ejecutiva por medio del Dr. Mario Felipe Ruiz Cubillo, como enlace del Comité Gestor ante la Presidencia. No obstante, en la Presidencia Ejecutiva por medio de sus asesores indicaron que el tema debía verse en la Gerencia Médica para su aval. Tal instrucción fue remitida vía correo electrónico al AES."
"En seguimiento al trámite, el AES preparó nuevamente la documentación y remitió a la Gerencia Médica, el 11 de julio de 2017 mediante oficio AES-1-378-2017, para su debida revisión y firma, de manera que se complete los requerimientos para el proceso de inscripción de la base de datos EDUS-SIGNOS ante la PRODHAB, trámite que está en proceso en esa Gerencia."

***9.** El 27 de julio de 2017, en oficio GM-AB-26769-17 "Decreto Ejecutivo N° 40008-JP", enviada a la Msc. Ana Lorena Solís Guevara, Jefe Área de Estadística en Salud, la Gerente Médica, Dra. María Eugenia Villalta Bonilla, manifestó "En relación al tema inscripción de las bases de datos en la Agencia de Protección de Datos de los Habitantes (PRODHAB), en este acto hacemos formal traslado del Decreto Ejecutivo N° 40008-JP, para que manifieste técnicamente, de manera urgente." En este oficio además se adjunta oficio DTIC-2822-2017.*

***10.** El 16 de agosto de 2017, mediante oficio AES-1-451-2017 el Área de Estadística en Salud, dirigida a la Dra. María Eugenia Villalta Bonilla, Gerente Médica, da respuesta a oficio GM-AB-26769-17, señalando que la recomendación técnica del AES es realizar el proceso de inscripción de la base de datos SIGNOS ante PRODHAB.*

***11.** El 2 de octubre de 2017, mediante oficio GM-AB-29832-2017 la Dra. María Eugenia Villalta Bonilla, Gerente Médica, instruyó al máster Roberto Masis Fonseca, Jefe a.i. del Centro de*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Gestión Informática de la Gerencia Médica y a la máster Ana Lorena Solís Guevara, Jefe del Área de Estadísticas en Salud para que en conjunto se atienda lo señalado en el oficio CGICM-259-2017.

***12.** El 30 de noviembre de 2017, como parte del trabajo conjunto solicitado por la Gerente Médica mediante oficio GM-AB-29832-2017, se elaboró la minuta GM-DPSS-AES-MIN-001 en la que participaron el Lic. Leslie Vargas Vásquez, Licda. Arlette Centeno Barrantes y el Ing. Ronald Guzmán Vásquez, todos funcionarios del Área de Estadísticas en Salud y el Ing. Esteban Zúñiga Chacón del Centro de Gestión Informática de la Gerencia Médica.*

Donde se acordó, lo siguiente:
Acuerdos

- *El Ing. Esteban Zúñiga Ch, trasladará al Equipo Gestor la recomendación del punto 3 del oficio CGIGM-259-2017 con sus respectivos incisos b,c,d y e, para su consideración, valoración y aprobación.*

El AES actualizará la información de los oficios de la inscripción de la base de datos SIGNOS, para que la Gerencia Médica proceda con la inscripción ante la Agencia de Protección de los Datos de los Habitantes.

- *El Ing. Esteban Zúñiga Ch, procederá a coordinar reunión con las abogadas asesoras de la Gerencia Médica, para la próxima semana, quedará sujeta a la confirmación de estas profesionales.*
- *La inscripción de la Base de Datos de ARCA, será un proceso independiente, por su diferente modelaje de su estructura a la del EDUS.*
- *Cuando se incorporen otros sistemas de información al modelaje de la base de datos del EDUS, se actualizará la inscripción ante la Agencia PRODHAB.*
- *El Ing. Esteban Zúñiga Ch, procederá a solicitar el acuerdo integral con la Dirección de Tecnologías de Información y Comunicaciones, en cuanto al modelo de seguridad informática que contempla la escalabilidad y evolución de las soluciones de software, como lo indica el punto a) de la recomendación número 3.*

***13.** El 6 de diciembre de 2017, en minuta GM-DPSS-AES-MIN-02, en la que participaron la Licda. María del Rocío Rivas López, abogada de la Gerencia Médica, Licda. Arlette Centeno Barrantes, Ing. Ronald Guzmán Vásquez, ambos del Área de Estadísticas en Salud y el Ing. Esteban Zúñiga Chacón del Centro de Gestión Informática de la Gerencia Médica.*

Donde se acordó, lo siguiente:
Acuerdos

- *Continuar con las recomendaciones técnicas indicadas en ambos oficios.*
- *El AES actualizará la información de los oficios de la inscripción de la base de datos SIGNOS, para que la Gerencia Médica proceda con la inscripción ante la Agencia de Protección de los Datos de los Habitantes.*
- *La Licda. Rivas López, informará a la Gerencia Médica, sobre el acuerdo tomado por ambas instancias técnicas en cuando a las recomendaciones de seguridad.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- *La Licda. Rivas López, informará de la colaboración solicitada por este equipo de trabajo en cuanto a:*
- *La solicitud del propietario físico o jurídico, este debidamente autenticado notarialmente o confrontada la firma.*
- *En caso de persona jurídica presentar personería jurídica vigente con máximo un mes de haber sido expedida.*
- *Remitir por correo electrónico los documentos de Normativa institucional y de Seguridad Informática a la Licda. Rivas López, a cargo del Ing. Ronald Guzmán Vásquez.*
- *El equipo elevará a la Gerencia Médica, además de los documentos del proceso de inscripción, nota indicando que las recomendaciones se ejecutarán en forma conjunta.*

Trasladar a la Msc. Lorena Solís Guevara, Jefe del Área Estadística en Salud, la sugerencia de plantear al equipo Gestor del EDUS la posibilidad de activar la Comisión Institucional de Seguridad Informática, para que revise y actualice la normativa vigente con base a la Ley.

- *Elevar a la instancia respectiva criterio técnico-legal en cuanto al tema del acceso a la información de la base de datos del EDUS por personas que no se encuentran en el país (aérea, marítima o terrestre), ya que la Ley 8968 no es clara sobre al asunto de la transferencia de datos personales.*

***14.** El 5 de abril de 2018, en minuta GM-DPSS-AES-MIN-03-18, en la que participaron la Msc. Ana Lorena Solís Guevara, Odilíe Fernández Ríos, Ronald Guzmán Vásquez, todos del Área de Estadísticas en Salud, el Ing. Esteban Zúñiga Chacón del Centro de Gestión Informática de la Gerencia Médica y la Licda. María del Rocío Rivas López, abogada de la Gerencia Médica*
Donde se acordó, lo siguiente:
Acuerdos

- *Completar el expediente administrativo con los antecedentes del ARCA y oficios actualizados AES.*
- *Borrador de oficio de la solicitud Comisión Inter-gerencial a presentar a la Dra. Villalta. AES y Legal.*
- *Aportar acuerdo de JD donde se hace referencia a la solicitud de inscripción de la base de datos a la Agencia Prodhab.*
- *Aportar acuerdo de JD de la creación de la Unidad Ejecutora Dirección EDUS.*
- *Aportar acuerdo de JD de la integración EDUS/ARCA y el Plan de Implementación, con fecha del 15 mayo.*
- *Aportar circular donde se indica a los Establecimientos de Salud apoyar la implementación del EDUS/ARCA.*
- *Realizar taller de análisis del riesgo en seguridad de los datos, se informará fecha y lugar, hora y participantes.*
- *Solicitar espacio para asistir a la reunión de la Comisión Institucional de Seguridad Informática (SISE), para exponer los requerimientos de la Gerencia Médica en seguridad de los datos.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- *Próxima reunión 16 de abril 10 a.m. en la sala de reuniones del CGI piso cuarto, edificio Laureano Echandi.*

15. *El 18 de abril de 2018 el Área de Estadísticas en Salud presentó al Comité Estratégico EDUS-ARCA, la viabilidad de conformar una comisión técnica intergerencial, con el propósito de documentar los aspectos normativos que solicita la ley N° 8968 y afines que permitan la inscripción de las bases de datos de la Institución ante el PRODHAB. Esta propuesta fue avalada por este Comité Estratégico.*

Conforme a lo anterior se evidencia que el Área de Estadísticas en Salud ejecutó en tiempo y forma lo solicitado por la Gerencia Médica. Así mismo, para el proceso de inscripción de la base de datos SIGNOS y ARCA ante la PRODHAB facilitó la siguiente documentación:

- *Formulario para la inscripción del registro de la base de datos (Organismos Públicos) con los datos debidamente actualizados. Dicho formulario debía ser firmado y autenticado por la Dra. María Eugenia Villalta Bonilla, como representante Jurídico de la CCSS.*
- *Oficio sobre la exoneración al pago de $200 (doscientos dólares americanos) por canon de inscripción de la base de datos SIGNOS-EDUS.*
- *Oficio donde se asigna al Lic. Olger Vargas Pérez, Jefe de la Subárea Gestión Base de Datos de la Dirección de Tecnologías de Información y Comunicaciones, como representante técnico.*

En oficio DTIC-2302-2018 del 18 de abril de 2018, el Máster Robert Picado Mora, Subgerente a.i. de la DTIC, menciona lo siguiente:

"(…) Es importante indicar que la precisión sobre las Bases de Datos que contienen "datos personales", así también, los registros ante la PRODHAB, son criterios y acciones que corresponden al negocio, considerando que el contexto de la interpretación y conocimiento de los datos, incluyendo la identificación de los datos que se consideran como "datos personales".

"(…) El negocio no ha establecido acciones de seguridad concretas en función de la protección de datos personales. La Dirección de Tecnologías de Información y Comunicaciones ha venido desarrollando una serie de esfuerzos relacionados con la seguridad informática sin ninguna vinculación a la ley de protección de datos personales.

De manera respetuosa, esta Dirección recomienda a la Alta Gerencia, conocer el modelo de Gobierno y Gestión de las TIC, específicamente lo relacionado con seguridad de la información, para que se comience a habilitar los foros y procesos para abordar estos temas."

La situación descrita podría materializar riesgos en torno al cumplimiento de lo estipulado en la Ley 8968, debido a que una Base de Datos que requiera ser inscrita, según lo indicado en el artículo 21, y no se inscribe, estaría actuando de forma ilegal, por lo que la agencia Prohab tiene la potestad para actuar ya sea de oficio o visita a la Institución y podría empezar un procedimiento sancionatorio.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Del mismo modo, la duración del proceso de inscripción de la base de datos del EDUS ante la Prodhab, desvirtúa los objetivos de control interno referentes a eficiencia y eficacia de las operaciones, así como garantizar el ordenamiento jurídico y técnico, lo anterior en el entendido de que dicho tema fue delegado al Área de Estadística en Salud desde hace más de dos años y a la fecha el repositorio de información no ha sido registrado ante la Agencia de Protección de Datos de los Habitantes.

6. SOBRE LAS MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES.

Se evidenció que la Institución no ha establecido medidas de seguridad afines con los términos establecidos en la Ley 8968 y su reglamento para la protección de datos personales, caso contrario, según lo indicado por el Sub Gerente de la DTIC, dicha unidad rectora desarrolla esfuerzos relacionados con seguridad informática sin ningún alineamiento a lo señalado en el marco normativo antes mencionado.

En este sentido, esta Auditoría determina riesgos referentes a la ausencia de vinculación entre las instancias corporativas y las unidades encargadas de la administración de las TI a nivel institucional, dado que el intermediario tecnológico, tanto la DTIC como los Centros de Gestión Informática, tienen como principal función sustantiva brindar servicios de infraestructura, plataforma, software u otros, mientras que según los términos de la Ley, recae en la figura del responsable, determinar la precisión sobre los repositorios de información con datos personales, lo anterior considerando el contexto de la automatización de procesos, la interpretación y conocimiento de los datos, incluyendo su identificación, categorización y tratamiento corresponde a los dueños del proceso que se automatiza.

La Ley 8968, en su artículo 10 Seguridad de los datos, indica lo siguiente:

> *"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.*
>
> *Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos."*

Las Normas Técnicas para la Gestión y Control de las Tecnologías de la Información (CGR), en el inciso 1.4.1 y 1.4.2, estipulan que:

> ***"1.4.1 Implementación de un marco de seguridad de la información***

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.
c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.

1.4.2 Compromiso del personal con la seguridad de la información

El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.
Para ello, el jerarca, debe:

a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos."

El Reglamento de la Ley 8968, estipula en sus artículos 34, 35 y 36, lo siguiente:

*"**Artículo 34. De las medidas de seguridad en el tratamiento de datos personales.***

El responsable, deberá establecer y mantener las medidas de seguridad administrativas, físicas y lógicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Reglamento. Se entenderá por medidas de seguridad el control o grupo de controles para proteger los datos personales.

Asimismo, el responsable deberá velar porque el encargado de la base de datos y el intermediario tecnológico cumplan con dichas medidas de seguridad, para el resguardo de la información.

Artículo 35. Factores para determinar las medidas de seguridad.

El responsable determinará las medidas de seguridad, aplicables a los datos personales que trate o almacene, considerando los siguientes factores:

a) La sensibilidad de los datos personales tratados, en los casos que la ley lo permita;
b) El desarrollo tecnológico;
c) Las posibles consecuencias de una vulneración para los titulares de sus datos personales.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

d) El número de titulares de datos personales;
e) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento o almacenamiento;
f) El riesgo por el valor, cuantitativo o cualitativo, que pudieran tener los datos personales; y
g) Demás factores que resulten de otras leyes o regulación aplicable al responsable.

Artículo 36. Acciones para la seguridad de los datos personales.

A fin de establecer y mantener la seguridad física y lógica de los datos personales, el responsable deberá realizar al menos las siguientes acciones, las cuales podrán ser requeridas en cualquier momento por la Agencia:

a) Elaborar una descripción detallada del tipo de datos personales tratados o almacenados;
b) Crear y mantener actualizado un inventario de la infraestructura tecnológica, incluyendo los equipos y programas de cómputo y sus licencias;
c) Señalar el tipo de sistema, programa, método o proceso utilizado en el tratamiento o almacenamiento de los datos; igualmente, indicarse el nombre y la versión de la base de datos utilizada cuando proceda.
d) Contar con un análisis de riesgos, que consiste en identificar peligros y estimar los riesgos que podrían afectar los datos personales;
e) Establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva;
f) Calcular el riesgo residual existente basado en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
g) Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivados del resultado del cálculo del riesgo residual."

En oficio DTIC-2302-2018 del 18 de abril de 2018, el Máster Robert Picado Mora, Subgerente a.i. de la DTIC, menciona lo siguiente:

"(…) Es importante indicar que la precisión sobre las Bases de Datos que contienen "datos personales", así también, los registros ante la PROHAB, son criterios y acciones que corresponden al negocio, considerando que el contexto de la interpretación y conocimiento de los datos, incluyendo la identificación de los datos que se consideran como "datos personales".

"(…) El negocio no ha establecido acciones de seguridad concretas en función de la protección de datos personales. La Dirección de Tecnologías de Información y Comunicaciones ha venido desarrollando una serie de esfuerzos relacionados con la seguridad informática sin ninguna vinculación a la ley de protección de datos personales.

De manera respetuosa, esta Dirección recomienda a la Alta Gerencia, conocer el modelo de Gobierno y Gestión de las TIC, específicamente lo relacionado con seguridad de la información, para que se comience a habilitar los foros y procesos para abordar estos temas."

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

El Lic. Olger Vargas Pérez, Jefe de la Sub Área de Gestión de Bases de Datos, indicó lo siguiente:

> *"No ha existido participación de responsables de la parte usuaria que soliciten requerimientos de seguridad en función de la protección de datos personales."*

Como causa de lo evidenciado en el presente hallazgo, responde a la situación detectada los puntos unos, dos, tres, cuatro y cinco de este informe sobre la ausencia de un modelo de gestión institucional orientado al tratamiento y protección de los datos personales administrados por la Caja, la carencia de instancias formalmente definidas que aborden el tema en forma integral y recopilen de manera unificada un inventario de las bases de datos institucionales con información de carácter personal, su respectiva clasificación y su pertinente inscripción ante la Agencia de Protección de Datos de los Habitantes, permitiendo establecer cuales bases de datos forman parte del ámbito de aplicación de la Ley 8968 y por ende, identificar las que deben apegarse a las artículos relacionados con seguridad de los datos.

La situación descrita podría materializar riesgos en torno a la seguridad de los datos personales almacenados en las diferentes bases de datos institucionales, provocando que los usuarios no tengan una certeza razonable de que los responsables establecen las medidas correspondientes considerando aspectos como la sensibilidad de los registros personales tratados, las posibles consecuencias de una vulneración para los titulares de sus registros así como acciones enfocadas en calcular el riesgo residual existente basado en la diferencia de las medidas existentes y aquellas faltantes que resultan necesarias para la protección de la información o en el establecimiento de planes de planes de trabajo para la implementación de las medidas de seguridad faltantes, derivados del resultado del cálculo del riesgo antes indicado.

7. SOBRE EL MARCO NORMATIVO INSTITUCIONAL RELACIONADO CON EL TRATAMIENTO DE DATOS PERSONALES.

Se determinaron oportunidades de mejora relacionadas con la norma institucional vigente referente al tratamiento de datos personales. A continuación, el detalle:

- El marco normativo institucional carece alineamiento con lo estipulado en los artículos de la Ley 8968 y su reglamento, lo anterior en virtud de que las Políticas de Seguridad Informática y Normas Institucionales de Seguridad Informática vigentes, fueron creadas en octubre 2007 y abril 2008 respectivamente, y las mismas no han sido sometidas a actualizaciones según su historial de revisiones desde esas fechas, lo anterior a pesar que la Ley supra citada y su respectivo reglamento fueron publicados en el año 2011 y 2013, esto evidencia la ausencia de actualizaciones o incorporaciones que permitan una vinculación más directa entre ambos.

  Respecto al tema, preocupa a esta Auditoría que desde el año 2014 mediante el informe ATIC-049-2014, fueron emitidas observaciones en torno al tema de actualización del marco normativo de seguridad informática generando una recomendación a la Gerencia Infraestructura y Tecnologías, sin embargo, en el transcurso del tiempo este Órgano Fiscalizador ha elaborado cinco seguimientos sobre la gestiones efectuadas y dicha recomendación continúa en proceso.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- Las Políticas de Seguridad Informática únicamente hacen mención al principio de confidencialidad de la información y trato con terceros, referenciando las Normas Institucionales de Seguridad, misma que expone lineamientos para la Política supra citada. En este punto, sobre el tema de datos personales estipula lo siguiente:

  *"**Uso de datos personales.** Los datos personales de los usuarios no deben ser entregados por la CCSS a terceros, esto debido a la confidencialidad que estos esperan de la CCSS de la información que esta administra. En caso de que sea necesario para la ejecución de pruebas o alguna otra razón se deberá mantener la confidencialidad de la información suministrada. "*

  En virtud de lo anterior, esta Norma solamente indica que los datos personales no deben ser entregados por la Caja a terceros, debido a la confidencialidad esperada de la Institución sobre la información que administra, sin embargo, se carece de lineamientos generales o específicos que establezcan lo relacionado con el tratamiento de estos datos, desde las etapas de recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción.

- Desde el año 2014, esta Auditoría mediante informe ATIC-049-2014 evidenció la ausencia mecanismos o estrategia orientado(a) a informar, capacitar y vigilar la seguridad informática y seguridad de la información a nivel institucional y que permita articular los procesos efectuados por las Gerencias y la Dirección de Tecnologías de Información y Comunicaciones, por ende, si existen referencias en estas normas sobre el uso de datos personales, las mismas se encuentran inmersas dentro de la problemática mencionada.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de la Información (CGR), en el inciso 1.4.1 y 1.4.2, estipulan que:

*"**1.4.1 Implementación de un marco de seguridad de la información***

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.
c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.

1.4.2 Compromiso del personal con la seguridad de la información

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.
Para ello, el jerarca, debe:

a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos."

Como causa de lo evidenciado en el presente hallazgo, se puede determinar que responde a la situación detectada en el punto uno de este informe, referente a la ausencia de un modelo de gestión institucional orientado al tratamiento y protección de los datos personales administrados por la Caja, la carencia de instancias formalmente definidas que aborden el tema en forma integral y que estén al tanto de promulgar e implementar normativa alineada con la Ley 8968 y su reglamento.

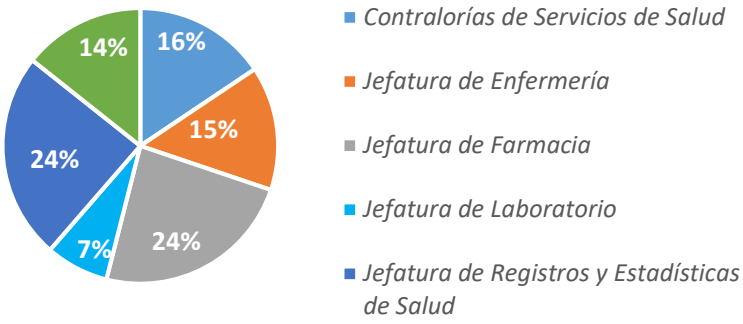
La situación descrita podría materializar riesgos referentes a una eficiente gestión institucional en torno al tema de protección de datos personales, lo anterior considerando que existe una tendiente necesidad de alinear el marco normativo de seguridad informática institucional con lo dispuesto en la ley 8968 y su reglamento, por ende, provocaría brechas de seguridad en cuanto al conocimiento de los funcionarios de la Caja sobre el marco normativo interno así como por la Ley supra citada, lo cual eventualmente podría repercutir en acciones sancionatorias de carácter administrativo y legal que impactarían la imagen institucional.

8. SOBRE LA CAPACITACIÓN EN PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

Se evidenciaron debilidades concernientes a la capacitación a nivel institucional en el tema de protección y tratamiento de datos personales según lo indicado en la ley 8968 y su reglamento, lo anterior a partir de los resultados obtenidos en consulta realizada a 391 funcionarios destacados en el I, II y III nivel de atención, así como Sucursales Financieras y Contralores de Servicios de Salud. Por consiguiente, se efectuaron preguntas relacionadas con la Ley supra citada. A continuación, se presentan gráficos con las respuestas de los participantes:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Gráfico 1
Participación de funcionarios según servicio



Fuente: Auditoría Interna. Elaboración propia con base en respuestas emitidas por funcionarios de la Administración Activa, mayo 2018.

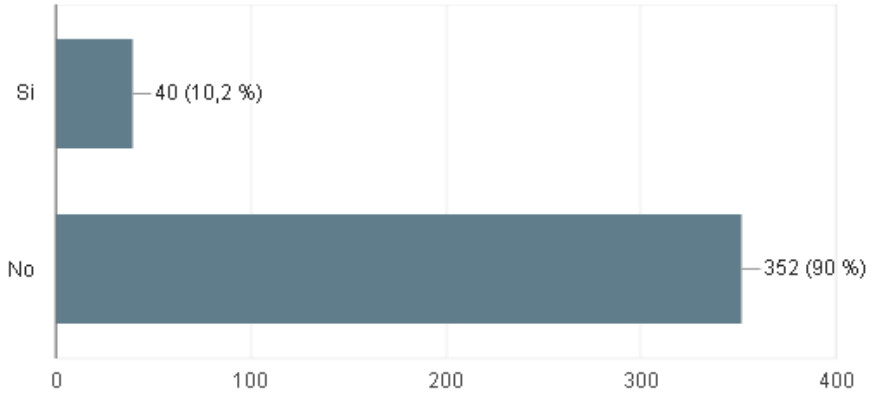
Como se observa, existió una participación significativa de colaboradores destacados en los servicios de Farmacia, Registros y Estadística en Salud, Laboratorio, Enfermería, Farmacia, Contralorías y Sucursales Financieras, lo anterior considerando que estas unidades tienen atención directa en la prestación de servicios de salud, los cuales dentro de sus funciones diarias utilizan sistemas informáticos para recopilar datos personales de los ciudadanos, tales como:

- Aplicativos del EDUS (SIAC, SIFF, SILC y SIES)
- Soluciones ARCA (Admisión y egreso Hospitalario, Módulo Quirúrgico)
- Sistema Integrado de Farmacias (SIFA)
- Sistema Centralizado de Recaudación (SICERE y sus aplicativos dependientes tales como: Sistema Integrado de Comprobantes (SICO), Sistema Institucional para la Gestión de Inspección (SIGI), Registro Control y Pago de Incapacidades (RCPI), entre otros)
- Sistema de Vigilancia Epidemiológica (SISVE).
- Sistema de Bancos de Sangre (E-Delphyn).
- Sistema de Laboratorios (LABCORE).
- Sistema de Vacunas (SISVAC)
- Sistema Estadístico de la Dirección Institucional de Contralorías de Servicios de Salud

Adicionalmente, se consultó a las Jefaturas, si ellos o sus funcionarios a cargo habían recibido capacitación referente a la Ley 8968. A continuación, el detalle:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Gráfico 2
¿Han recibido sus funcionarios a cargo o usted, capacitación específica referente a la Ley 8968 "Protección de la Persona frente al tratamiento de sus datos personales" y su reglamento?

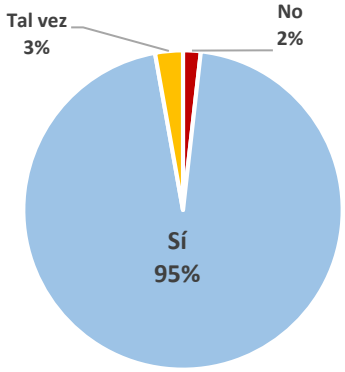


Fuente: Auditoría Interna. Elaboración propia con base en respuestas emitidas por funcionarios de la Administración Activa, mayo 2018.

Como se observa en el gráfico anterior, el 90% de los consultados, afirma no haber recibido ningún tipo de capacitación en torno a la ley supra citada, lo cual se torna relevante considerando que son funcionarios de atención directa en la prestación de servicios de salud y utilizan soluciones informáticas como las mencionadas anteriormente.

Finalmente, se consultó si considera conveniente que exista capacitación periódica a nivel institucional en torno a la protección y tratamiento de datos personales, de lo cual se obtuvieron los siguientes resultados:

Gráfico 3
Respuestas de pregunta: ¿Considera que debe existir capacitación periódica a nivel institucional en torno al tema de protección y tratamiento de datos personales?



Fuente: Auditoría Interna. Elaboración propia con base en respuestas emitidas por funcionarios de la Administración Activa, mayo 2018.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Como se observa en el gráfico 3, el 95% indica la necesidad de capacitación periódica a nivel institucional en torno al tema de protección y tratamiento de datos personales, evidenciando la necesidad que tienen los funcionarios que utilizan aplicaciones informáticas y recopilan registros de carácter personal de conocer el marco normativo que regula esta materia.

Lo antes mencionado, también se logra determinar cuándo se les consultó a los funcionarios si deseaban agregar algún comentario en torno al tema. A continuación, se presentan algunas de las respuestas recopiladas:

Tabla 5
¿Algún comentario que desee agregar en torno al tema?

Como funcionarios públicos somos depositarios de las Leyes y por ende es importante la capacitación para su correcta aplicación.
CON QUIEN SE COORDINA DICHAS CAPACITACIONES
Considero el tema de gran relevancia, debido a la discrecionalidad que hay que tener con respecto a diagnósticos y tratamientos, y el impacto que puede tener en los usuarios un mal manejo de la información.
Deberían mantenerse capacitaciones no solo a las jefaturas sino a funcionarios del área de pensiones e inspección.
Es un tema que existe cero divulgaciones.
Sinceramente no he leído sobre esta ley.
El funcionario desconoce las restricciones y limitaciones en el acceso a los datos personales.
Es importante conocer esta temática para estar saber los alcances legales y hasta qué punto se puede manejar los datos personales de un usuario.
Es muy importante conocer de este tema ya que a diario nos hacen consultas y no lo tenemos muy claro y la legalidad del asunto o no.
Es muy importante saber sobre la protección de nuestros datos. Como, por ejemplo, a qué datos tienen derecho al acceso y a qué información no tienen derecho. ¿Ya que a veces lo hacen firmar a uno una boleta aceptando eso, pero hasta dónde pueden revisar?
Es necesaria la capacitación de la Ley 8968, principalmente ahora con en el manejo de la información en el EDUS
Es necesario la capacitación y el conocimiento de estos temas tanto para el servicio de Laboratorio Clínico como también para el personal médico en situaciones tales como la solicitud de copias de exámenes.
Es requerido capacitar al personal en esa materia siendo que a nivel de sucursales la demanda de información es constante
Es un tema de mucha relevancia, principalmente por el tipo de información que se maneja en el Laboratorio, para el cual no estamos capacitados ni entendemos las dimensiones de nuestro accionar.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

ESTA CAPACITACIÓN DEBE SER ESTABLECIDA COMO REQUISITO
Estos temas deben de estar constantemente capacitando a los funcionarios involucrados, pues son muy sensibles a nivel de los Servicios de la Institución y si se desconoce del tema se puede incurrir en errores graves que afecten la Caja
Se debería valorar la posibilidad de incluir esta capacitación en el curso de inducción, que realizan los funcionarios de nuevo ingreso.
Sería muy importante recibir este tipo de capacitación, por cuanto en las Sucursal los funcionarios tienen accesos a mucha información, y es bueno que sepan de qué forma se debe manejar estar, que se puede brindar que no, a que estarían expuestos por un mal manejo de dicha información.

Fuente: Auditoría Interna. Elaboración propia con base en respuestas emitidas por funcionarios de la Administración Activa, mayo 2018.

La Ley 8968, en su Capítulo I Disposiciones Generales, señala en el artículo 1 objetivo y fin, lo siguiente:

> *"Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."*

Las Normas técnicas para la Gestión y el Control de las Tecnologías de Información, en el artículo 1.4.1 y 1.4.2, señalan que:

> ***"1.4.1 Implementación de un marco de seguridad de la información***
> *La organización debe implementar un marco de seguridad de la información, para lo cual debe:*
>
> *a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.*
>
> *b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.*
>
> *c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.*
>
> ***1.4.2 Compromiso del personal con la seguridad de la información***
>
> *El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Para ello, el jerarca, debe:

a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.

b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.

c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.

Como causa de lo evidenciado en el presente hallazgo, responde a la situación detectada en el punto uno este informe sobre la ausencia de un modelo de gestión institucional orientado al tratamiento y protección de los datos personales administrados por la Caja, así como la carencia de instancias formalmente definidas que aborden el tema en forma integral, permitiendo identificar, planificar y gestionar las necesidades de capacitación del personal que interactúan con aplicaciones informáticas o mecanismos manuales para recopilar datos personales.

La situación descrita, podría generar riesgos en torno a los diversos funcionarios que dentro de sus labores les corresponde ejecutar cualquier operación mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, conservación, modificación, utilización, entre otros, no se apeguen a los términos estipulados en la ley 8968 y su reglamento, lo anterior producto de la ausencia de capacitación periódica sobre el tema.

Del mismo modo, el desconocimiento de la ley antes mencionada y su respectivo reglamento, materializaría riesgos en aspectos como principios de la calidad de la información, seguridad, así como el deber de confidencialidad y el cumplimiento de protocolos de actuación según los términos establecidos el marco normativo, situación que afectaría los derechos de los ciudadanos sobre el tratamiento de sus datos personales, poniendo en compromiso la reputación e imagen de la Institución ante posibles sanciones por parte de la Agencia de Protección de Datos de los Habitantes.

9. SOBRE PRÁCTICAS DE INCUMPLIMIENTO A LA NORMA DE PROTECCIÓN DE DATOS PERSONALES.

Se evidenció prácticas institucionales que incumplen lo estipulado en la Ley 8968 y su reglamento en torno a la protección y tratamiento de datos personales. A continuación, el detalle:

9.1 Publicación de cédulas de identificación en las ventanillas o mostradores sin el consentimiento del ciudadano.

Como se indicó en los antecedentes de este informe, datos como la foto, imagen, voz, raza o etnia son categorizados como *"Datos Sensibles"*. Ante esto, la cédula costarricense posee este tipo de información, dado que en la parte frontal se muestra la foto del ciudadano en la esquina superior izquierda, así como una disminuida (parte inferior izquierda), por ende, la exposición de esta en una ventanilla o mostrador se coteja como un incumplimiento sobre la protección de datos personales, lo anterior debido a su exposición sin el consentimiento del ciudadano.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

En este sentido, cuando una persona extravía una cédula en los centros médicos o administrativos de la Caja, se evidencia dicha práctica, lo cual generalmente se realiza con el fin de que el ciudadano pueda recuperarla si regresa a la unidad, no obstante, también podría presentarse el caso, donde el usuario alegue una violación a los datos personales por publicar el documento sin su consentimiento. A continuación, se presenta ejemplos detectados en tres centros médicos señalados en el alcance del presente informe:

Imagen 1
Sección Rayos X
Hospital Nacional Calderón Guardia

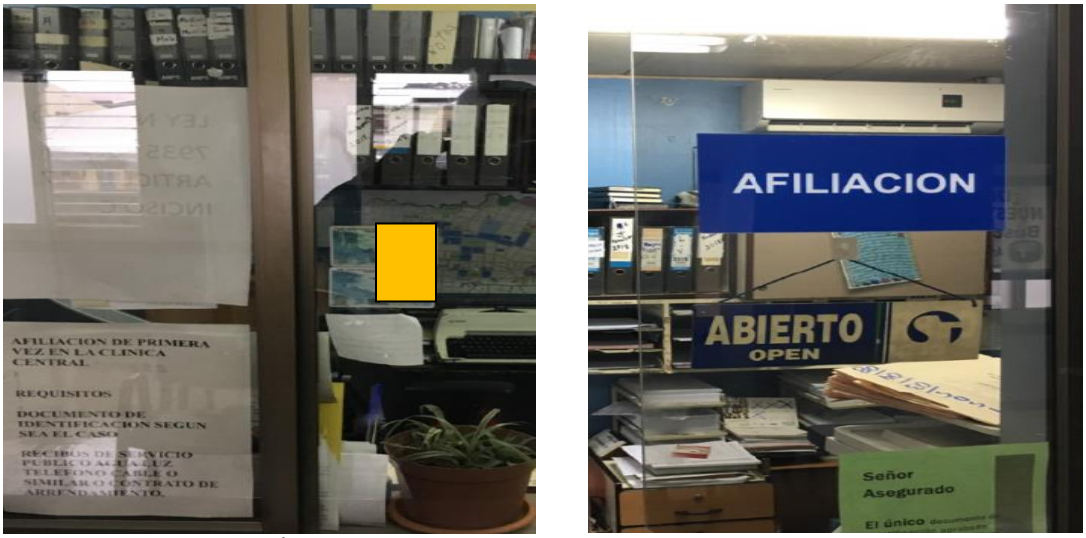
Fuente: Sección Rayos X, Hospital Nacional Calderón Guardia, mayo 2018.

Imagen 2
Sección Vascular Periférico
Hospital Nacional Calderón Guardia

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Fuente: Sección Vascular Periférico, Hospital Nacional Calderón Guardia, mayo 2018.

Imagen 3
Sección Afiliación
Área de Salud Central Noreste



Fuente: Sección Afiliación, Área de Salud Central Noreste, mayo 2018.

Imagen 4
Sección Farmacia.
Hospital San Vicente de Paúl

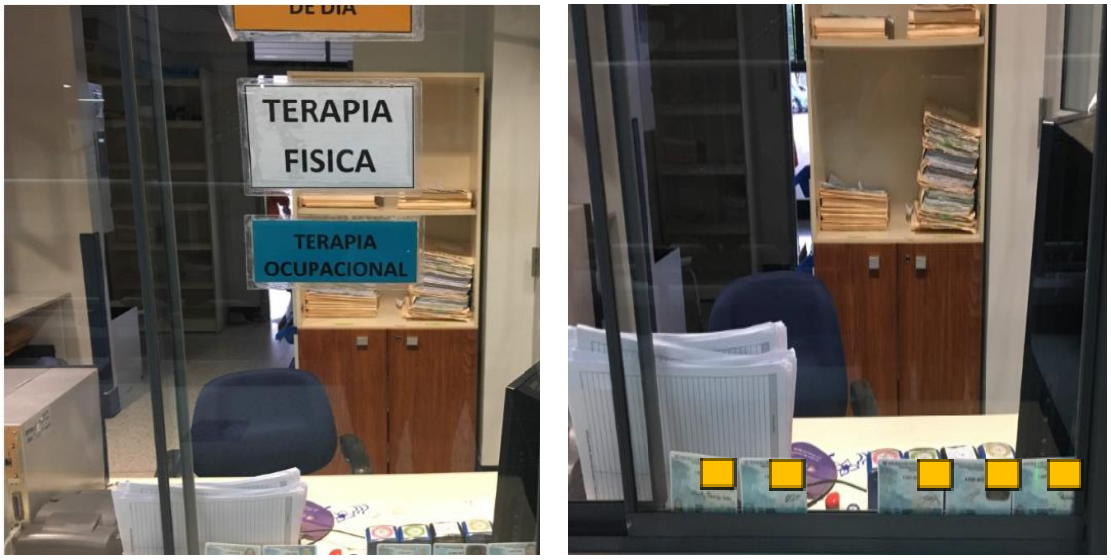
Fuente: Sección Farmacia, Hospital San Vicente de Paúl (HSVP), mayo 2018.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Imagen 5
Sección Urología
Hospital San Vicente de Paúl

Fuente: Sección Urología, HSVP, junio 2018.

Imagen 6
Sección Terapia Física/Ocupacional – Hospital de Día
Hospital San Vicente de Paúl



San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Fuente: Sección terapia Física/Ocupacional, Hospital de Día, HSVP, junio 2018.

Imagen 7
Sección Ortopedia
Hospital San Vicente de Paúl

Fuente: Sección Ortopedia, Hospital San Vicente de Paúl, junio 2018.

9.2 Publicación de imágenes con datos personales de pacientes mediante aplicaciones móviles.

Se detectó el uso de un mecanismo no oficial donde se reportan incidencias, consultas y otros temas relacionados con el funcionamiento de los aplicativos EDUS, particularmente SIES en su versión 1.0 y 2.0 y superiores, en este sentido, se recurre a la práctica de compartir imágenes o videos del aplicativo para evidenciar un problema en particular, incurriendo que en ocasiones se reflejen datos sensibles de los pacientes, lo cual implica la publicación de datos personales fuera del ámbito y resguardo del Expediente Digital en Salud, lo anterior se realiza mediante la aplicación móvil llamada Whatsapp[5], en un grupo bajo el nombre de *"Módulo Urgencias EDUS"*, creado desde el 29 de mayo del 2015 y conformado por funcionarios de diversas Áreas de Salud, Hospitales, Dirección Proyecto EDUS y DTIC.

En este sentido, si bien la evolución de las tecnologías ha permitido la adopción de herramientas ágiles de mensajería instantánea, también se debe considerar que la utilización de esta aplicación para fines relacionados con la gestión institucional provoca riesgos en aspectos como el debido tratamiento de los datos personales, su seguridad y la confidencialidad, misma que debe prevalecer exclusivamente en los aplicativos EDUS-ARCA, además, otro punto a tener en cuenta es el uso de dispositivos móviles personales (celulares) en horas laborales, aspecto regulado a nivel institucional.

Al respecto, esta Auditoría mediante informe ATIC-221-2017 *"Evaluación de carácter especial sobre la gestión automatizada de los servicios de urgencias a través los aplicativos Sistema Integrado de Agendas*

[5] WhatsApp es gratuito y ofrece mensajería, llamadas de una manera simple, segura y confiable disponible en teléfonos alrededor mundo. Fuente: https://www.whatsapp.com/about/

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

y Citas (SIAC) y Sistema Integrado Expediente en Salud (SIES)" había destacado las observaciones correspondientes en torno a dicho tema, asimismo, mediante oficio GM-AUDC-31997-2017 del 13 de noviembre del 2017 publicado en WebMaster el 21 de noviembre de ese mismo año, la Dra. María Eugenia Villalta Bonilla, Gerente Médica en ese momento, emitió directrices en torno al tema, sin embargo, se evidencia que a la fecha, continúa siendo utilizado con los fines antes expuestos.

La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Ley 8968), en el Artículo 3 Definiciones, inciso i., indica lo siguiente:

> *"**Tratamiento de datos personales:** cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros."*

Del mismo modo, dicha Ley en su artículo 4 Autodeterminación informativa, estipula que:

> *"Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.*
>
> *Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias."*

Además, la Ley 8968 en su Artículo 9, Categorías particulares de los datos, indica lo siguiente:

> *"Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán, se regirán por las siguientes disposiciones:*
>
> ***1.- Datos sensibles***
> *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. (…)"*

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información y Comunicaciones, en el apartado 1.4. Gestión de la seguridad de la información, indica lo siguiente:

> *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones. (…)"

Esas mismas Normas, en el punto 1.4.2. Compromiso del personal con la seguridad de la información, estipula que:

"El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.
Para ello, el jerarca, debe:
a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos".

El Reglamento de la ley 8968, en su artículo 2 Definiciones, siglas y acrónimos, indica lo siguiente:

"Consentimiento del titular de los datos personales: Toda manifestación de voluntad expresa, libre, inequívoca, informada y específica que se otorgue por escrito o en medio digital para un fin determinado, mediante la cual el titular de los datos personales o su representante consienta el tratamiento de sus datos personales. Si el consentimiento se otorga en el marco de un contrato para otros fines, dicho contrato deberá contar con una cláusula específica e independiente sobre consentimiento del tratamiento de datos personales."

Ese mismo Reglamento en su artículo 4, Requisitos del Consentimiento, mencionan:

"La obtención del consentimiento deberá ser:
a) Libre: no debe mediar error, mala fe, violencia física o psicológica o dolo,
que puedan afectar la manifestación de voluntad del titular;
b) Específico: referido a una o varias finalidades determinadas y definidas que justifiquen el tratamiento;
c) Informado: que el titular tenga conocimiento previo al tratamiento, a qué serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento. Asimismo, de saber quién es el responsable que interviene en el tratamiento de sus datos personales, y su lugar o medio de contacto;

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

d) Inequívoco: debe otorgarse por cualquier medio o mediante conductas inequívocas del titular de forma tal que pueda demostrarse de manera indubitable su otorgamiento y que permita su consulta posterior.
e) Individualizado: debe existir mínimo un otorgamiento del consentimiento por parte de cada titular de los datos personales."

El Código de Ética del servidor del Seguro Social, en su artículo 12 Deber de confidencialidad, indica lo siguiente:

"El servidor de la Caja está obligado a guardar discreción y reserva sobre los documentos, hechos e informaciones a las cuales tenga acceso y conocimiento como consecuencia del ejercicio o con motivo del ejercicio de las funciones, independientemente de que el asunto haya sido calificado o no como confidencial por el superior, salvo que esté autorizado para dar información sin perjuicio del derecho de información del administrado, ejercido conforme al ordenamiento jurídico vigente o bien, cuando el contenido del documento e información no implique ocultamiento de un hecho ilegítimo que pueda acarrear responsabilidad administrativa, penal y/o civil."

La Circular 000920 Política para el uso de teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la C.C.S.S. del 19 de enero del 2005, indica lo siguiente:

"Me permito informarles, con el ruego de que lo hagan del conocimiento de sus colaboradores, que la Junta Directiva, en Artículo 10º de la sesión Nº 7921, celebrada el 6 de enero del año 2005 acordó aprobar la siguiente ***POLÍTICA PARA EL USO DE TELÉFONOS CELULARES, RADIOS LOCALIZADORES, RADIOS PORTÁTILES Y OTROS EN DEPENDENCIAS DE LA C.C.S.S.:***
"*Considerando que:*

1. el Reglamento del Seguro de Salud, dentro de los principios y derechos de los asegurados (as), señala el derecho de ser atendidos con el máximo respeto y bajo una relación que destaque su condición de ser humano,

2. el Artículo 53 del Reglamento Interior de Trabajo establece absolutamente la prohibición a los (as) trabajadores (as) de realizar actividades particulares, de cualquier naturaleza, así como también atender visitas y efectuar llamadas telefónicas de carácter personal, durante las horas de trabajo, sin permiso o autorización del jefe inmediato,

3. el Artículo 26 denominado "Durante la jornada laboral", Capítulo III "Prohibiciones" del Código de Ética del Servidor (a) de la CCSS, prohíbe al funcionario (a) atender visitas o llamadas personales o bien hacerlas en horas de trabajo para asuntos privados, salvo situaciones de urgencia o emergencia y dentro de los límites que la prudencia y el servicio imponen,
4. las Políticas y Normas Institucionales 2005 - 2006, aprobadas por la Junta Directiva, en el Artículo 1º de la sesión Nº 7865, celebrada el 17 de junio 2004, establecen en su aparte "servicio al usuario", que la prestación de los servicios se debe efectuar con calidad técnica y social, como producto de múltiples interrelaciones entre equidad, eficiencia, eficacia, oportunidad, humanización, continuidad, seguridad, información y respeto a los derechos humanos,

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

5. mediante la "Política sobre la contratación y promoción de los funcionarios de la CCSS con cualidades para prestar un servicio con calidad y calidez humana", aprobada por la Junta Directiva en el Artículo 8º de la sesión Nº 7798, celebrada el 09 de octubre de 2003, se indica que la Dirección de Recursos Humanos debe adecuar los instrumentos, lineamientos y procedimientos técnicos utilizados para contratar y promover al recurso humano, dando énfasis a cualidades de afectividad, cordialidad y buen trato hacia el usuario interno y externo, con el fin de propiciar un ambiente laboral más cálido en el centro de trabajo,

Y, en función de la atención que debe prevalecer y el respeto a los derechos, dignidad humana, consideración, cuidado y amabilidad hacia el paciente, usuarios y público en general, en los servicios de la institución,

La Junta Directiva acuerda aprobar la siguiente ***Política para el uso de teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la C.C.S.S.****, que restringe el uso de los teléfonos celulares -entre otros medios de comunicación de uso personal- durante la jornada laboral ordinaria y extraordinaria, en los siguientes términos:*
Queda totalmente prohibido el uso de teléfonos celulares, radios localizadores, radios portátiles y otros artefactos en aquellas áreas en donde por aspectos de equipo médico o de alcance tecnológico, su uso puede interferir en los resultados de los diferentes exámenes o procesos diagnóstico.

En todos los centros de la institución, y durante la prestación de los servicios que se brinden, deberá prevalecer y destacarse el respeto a los derechos, dignidad humana, consideración, cuidado y amabilidad al paciente, usuario o público en general. El cumplimiento de este principio, será de acatamiento obligatorio por todos (as) los (as) funcionarios (as) de la C.C.S.S.

Por tal motivo, queda restringido a los (as) funcionarios (as) de la CAJA, durante su jornada de trabajo, sea esta ordinaria o extraordinaria, el uso de teléfonos celulares, radios localizadores, radios portátiles y otros artefactos que interfieran en la adecuada prestación de los servicios, especialmente durante la atención a los pacientes, usuarios o público en general.

Únicamente podrán hacer uso de esos medios aquellos funcionarios (as) a quienes, por sus labores, la CAJA se los haya proporcionado, o así lo requieran, para atender asuntos exclusivos de sus funciones.

Para la aplicación de la política anterior, se deberá tomar en cuenta las normas que a continuación se detallan:

Normas para el uso de teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la C.C.S.S.

1. *Según los términos de la Ley General de Control Interno Nº 8292 y sus respectivas normas, quedará bajo la responsabilidad de la Jefatura Inmediata de cada servicio en los diferentes centros de trabajo de la Institución velar por el cumplimiento constante de las presentes disposiciones.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

2. En caso de que un trabajador (a) incumpla con lo dispuesto, la jefatura inmediata deberá de aplicar la respectiva sanción, según las medidas disciplinarias señaladas en el Artículo 79 y subsiguientes del Reglamento Interior de Trabajo, aplicando el debido proceso.
3. En caso de que alguna denuncia, por esta causa, sea interpuesta en la Contraloría de Servicios del centro de trabajo, por algún paciente, usuario o público en general, el Contralor (a) deberá notificar lo sucedido a la jefatura inmediata del trabajador (a) denunciado (a), o en su defecto, a la instancia jerárquica correspondiente, iniciando paralelamente la respectiva investigación y proceso.

Normas para la divulgación y comunicación de la presente política:
1. Será obligatorio para los directores o instancias superiores de cada centro, velar para que en los diferentes servicios, salas, consultorios, oficinas y zonas de los centros de trabajo, en donde se presta la atención a pacientes, usuarios o público en general, se mantenga un afiche en donde se indique la prohibición en esa zona, del uso de teléfonos celulares, radios localizadores, radios portátiles y otros.
2. La Administración de cada centro de trabajo, se encargará de distribuir y colocar en un lugar visible dicho afiche, el cual será distribuido o puede ser solicitado a la Dirección de Recursos Humanos.
3. La Oficina de Recursos Humanos de cada centro de trabajo, será la responsable de colocar la circular mediante la cual se comunica el presente acuerdo, en las vitrinas y lugares visibles, así como también deberá hacer del conocimiento de manera formal a todos (as) los (as) funcionarios (as), las presentes disposiciones:
Rige a partir de su aprobación".
Asimismo, en esa oportunidad quedó clara la excepción para los médicos que hacen disponibilidad, así como informar adecuadamente a los familiares de los pacientes sobre esta disposición."

El oficio GM-AUDC-31997-2017 del 13 de noviembre del 2017, suscrito por la Dra. María Eugenia Villalta Bonilla, Gerente Médica en ese momento, indica lo siguiente:

"(…) La Auditoria Interna, realizó una evaluación de la gestión automatizada de los servicios de urgencias, la cual evidencio el uso de un mecanismo no oficial, mediante la utilización de la aplicación Whatsapp, en donde fue creado un grupo llamado "Módulo Urgencias EDUS", conformado por funcionarios de diversas Áreas de Salud, Hospitales, Dirección Proyecto EDUS y DTIC, para el reporte de incidencias relacionadas con el funcionamiento de los aplicativos SIAC-SIES Urgencias.

El uso de este instrumento tecnológico provoca riesgos en aspectos como seguridad y confidencialidad en la información de los pacientes que acuden a los servicios de urgencias, así como el uso de dispositivos móviles (celulares) en horas laborales; particularmente por funcionarios que están en atención directa con el paciente, entre otros.

Es importante señalar que con anterioridad la Institución ha emitido directrices que restringen el uso teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la C.C.S.S., durante la jornada laboral. Asimismo, en cuanto a la seguridad y confidencialidad de la

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

información de los pacientes la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales señala:

Artículo 3 Definiciones, inciso i:

"Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros."

Artículo 9, Categorías particulares de los datos:
"Además de las reglas generales establecidas en esta ley, para el tratamiento de los datos personales, las categorías particulares de los datos que se mencionarán, se regirán por las siguientes disposiciones:
1.- Datos sensibles
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. (…)"

Asimismo la Junta Directiva en el artículo 1 de la sesión 7979 celebrada el 28 de julio de 2005, con la aprobación de las políticas institucionales en el campo de la comunicación, la información pública, la educación en salud y seguridad social, reguló la restricción del uso de artefactos que pueden interferir en una adecuada prestación del servicio, limitando su uso.

En este sentido se señaló que en jornadas ordinarias y extraordinarias queda totalmente restringido a los funcionarios de la institución el uso de aparatos o artefactos que puedan interferir con el derecho de los asegurados de ser atendidos con el máximo respeto y bajo una relación que destaque su condición de ser humano. Asimismo, se destaca lo regulado en el artículo 53 del Reglamento Interior de Trabajo que establece la prohibición a los trabajadores de realizar actividades particulares, de cualquier naturaleza, estas disposiciones que son de acatamiento obligatorio para todos los servidores de la institución.

En este sentido el día 01 de febrero de 2013, se realizó un recordatorio vía web master en torno al uso de aparatos de comunicación en horas de trabajo, al respecto se señaló:

"El uso de teléfonos celulares, radio localizadores, radios portátiles, televisores u otros artefactos que interfieran en la adecuada prestación de los servicios que brinda la Caja Costarricense de Seguro Social (CCSS), queda totalmente restringido en jornadas ordinarias y extraordinarias, desde el año 2005 y el cumplimiento de este principio es de acatamiento obligatorio para todos los servidores.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

La "Política para el uso de teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la CCSS" que rige desde enero de ese año, considera entre otros aspectos que: el Reglamento del Seguro de Salud, dentro de los principios y derechos de los asegurados (as), señala el derecho de ser atendidos con el máximo respeto y bajo una relación que destaque su condición de ser humano.
Además, el artículo 53 del Reglamento Interior de Trabajo establece absolutamente la prohibición a los trabajadores de realizar actividades particulares, de cualquier naturaleza, así como también atender visitas y efectuar llamadas telefónicas de carácter personal, durante las horas de trabajo, sin permiso o autorización del jefe inmediato.

Queda, además totalmente prohibido el uso de teléfonos celulares, radios localizadores, radios portátiles y otros artefactos en aquellas áreas en donde por aspectos de equipo médico o de alcance tecnológico, su uso puede interferir en los resultados de los diferentes exámenes o procesos diagnóstico.

En todos los centros de la institución y durante la prestación de los servicios que se brinden, deberá prevalecer y destacarse el respeto a los derechos, dignidad humana, consideración, cuidado y amabilidad al paciente, usuario o público en general.

Únicamente podrán hacer uso de esos medios aquellos funcionarios (as) a quienes por sus labores, la Institución se los haya proporcionado, o así lo requieran, para atender asuntos exclusivos de sus funciones.

Para la aplicación de la política anterior, se deberá tomar en cuenta las normas que a continuación se detallan:

Normas para el uso de teléfonos celulares, radios localizadores, radios portátiles y otros en dependencias de la CCSS
1. Según los términos de la Ley General de Control Interno Nº 8292 y sus respectivas normas, quedará bajo la responsabilidad de la Jefatura Inmediata de cada servicio en los diferentes centros de trabajo de la Institución velar por el cumplimiento constante de las presentes disposiciones.
2. En caso de que un trabajador (a) incumpla con lo dispuesto, la jefatura inmediata deberá de aplicar la respectiva sanción, según las medidas disciplinarias señaladas en el artículo 79 y subsiguientes del Reglamento Interior de Trabajo, aplicando el debido proceso.
3. En caso de que alguna denuncia, por esta causa, sea interpuesta en la Contraloría de Servicios del centro de trabajo, por algún paciente, usuario o público en general, el Contralor (a) deberá notificar lo sucedido a la jefatura inmediata del trabajador (a) denunciado (a), o en su defecto, a la instancia jerárquica correspondiente, iniciando paralelamente la respectiva investigación y proceso.

Normas para la divulgación y comunicación de la presente política:
1. Será obligatorio para los Directores o instancias superiores de cada centro, velar para que en los diferentes servicios, salas, consultorios, oficinas y zonas de los centros de trabajo, en donde se presta la atención a pacientes, usuarios o público en general, se mantenga un afiche en donde

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

se indique la prohibición en esa zona, del uso de teléfonos celulares, radios localizadores, radios portátiles y otros.
2. La Administración de cada centro de trabajo, se encargará de distribuir y colocar en un lugar visible dicho afiche, el cual será distribuido o puede ser solicitado a la Dirección de Recursos Humanos.
3. La Oficina de Recursos Humanos de cada centro de trabajo, será la responsable de colocar la circular mediante la cual se comunica el presente acuerdo, en las vitrinas y lugares visibles, así como también deberá hacer del conocimiento de manera formal a todos (as) los (as) funcionarios (as), las presentes disposiciones.

Por lo anterior, indicado se insta a emitir un recordatorio a los funcionarios sobre las directrices que restringen el uso teléfonos celulares, radios localizadores, radios portátiles y otros en instalaciones de la CCSS, durante la jornada laboral y se instruya a la no utilización del Whatsapp como medio para reportar incidencias u otro relacionado con la prestación de servicios de salud, hasta tanto la institución no regule su uso. Además, se recuerda que el medio oficial para reportar incidencias generadas en relación al funcionamiento de los aplicativos EDUS, es a través de la Mesa de Servicios TIC. "

Como causa de lo evidenciado se puede determinar que responde a la situación detectada en el hallazgo ocho de la presentación evaluación, relacionado con las debilidades concernientes a la capacitación a nivel institucional en el tema de protección y tratamiento de datos personales según lo indicado en la ley 8968 y su reglamento.

Por otra parte, respecto al uso de aplicaciones móviles como Whatsapp para reportar temas relacionados con los aplicativos institucionales, podría obedecer a la ausencia de mecanismos y protocolos eficientes, efectivos y ágiles que les permita a los usuarios reportar incidencias u otros aspectos relacionados con el funcionamiento del EDUS, lo anterior bajo un esquema de seguridad institucional y mediante la implementación de acuerdos de servicio que le permita a los usuarios tener una certeza razonable de que sus inquietudes son resueltas en tiempo y forma por las instancias técnicas y usuarias responsables.

La situación descrita, podría generar una violación a los datos personales catalogados como sensibles y dentro de los cuales se encuentra las fotos, por ende, la publicación en ventanillas o mostradores de una identificación sin el consentimiento de la persona materializa riesgos referentes sanciones administrativas o legales que podría sufrir la Institución por un desconocimiento de sus funcionarios sobre lo estipulado en la ley 8968 y su respectivo reglamento.

Así mismo, acciones como compartir, publicar, difundir, entre otros, información que tiene inmersa datos de carácter personal sin la debida autorización de sus titulares, podría incurrir que tanto la Institución como sus funcionarios puedan ser sometidos a sanciones en la vía administrativa, legal e inclusive penal, por incumplimiento de normativa interna, de lo estipulado en la Ley 8968 y su reglamento, así como lo señalado en el Código Penal en su artículo 196 sobre la violación de datos personales.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

CONCLUSIONES

Actualmente, en diversos sectores como bancos, gobierno, educación, salud, la automatización exponencial de los procesos de negocio están ampliando el entorno tanto del análisis como del consumo de datos, emergiendo una necesidad urgente de disponer de información para tomar decisiones, ante esto, se establece un escenario donde dichos datos deben ser instantáneos y accesibles a las diferentes áreas que conforman las organizaciones.

En este contexto, tratar de contener la información que debe ser reservada, bien por condiciones de negocio o cumplimiento normativo, representa un reto de alta exigencia, pues todo alrededor nos sugiere una conexión o transmisión de información, siendo una decisión final sujeta a los individuos con acceso a ella, a su criterio de seguridad y control, así como a su entendimiento, sobre la protección de los datos personales.

Así mismo, los flujos de información que se generan permiten una mayor identificación de los individuos, donde la privacidad establece un reto para los usuarios y las organizaciones. En este sentido, la Ley 8968 y su reglamento pretende incentivar en el país, un adecuado tratamiento de los datos personales partiendo del objetivo de garantizar a cualquier persona el respeto a sus derechos fundamentales, concretamente, la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad en esta temática.

Bajo estos parámetros, se evalúa las acciones ejecutadas por la Caja para garantizar el cumplimiento razonable de lo estipulado en la Ley 8968 y su respectivo reglamento, determinando la ausencia de un modelo de gestión integral orientado al tratamiento y protección de los datos personales administrados por la Institución, lo anterior ante la ausencia de instancias formalmente definidas que aborden el tema en forma global, delegación concreta con roles y responsabilidades, mecanismos de coordinación entre Presidencia, las distintas Gerencias y sus unidades adscritas, manuales institucionales de capacitación, actualización y concientización del personal sobre las obligaciones relacionados con el marco normativo mencionado.

Adicionalmente, se determinaron debilidades como la falta de un inventario institucional unificado sobre las bases de datos con datos personales, así como la diferenciación de los repositorios de información entre los de carácter interno y los que forman parte del ámbito de aplicación de la Ley 8968 y su reglamento.

Del mismo modo, se evidencia que a nivel institucional no existe claridad sobre el concepto de *"Responsable"* estipulado en la normativa supra citada, lo anterior con base en las respuestas emitidas por la Administración Activa, las cuales señalan en esta función a Gerentes, Nombres de Direcciones o Áreas, informática, directores, Jefes de Área, Sub Áreas, médicos o funcionarios operativos, asimismo, se produce una tendencia de relacionar al *"Líder Usuario"* de los aplicativos bajo este rol, siendo que la naturaleza de sus funciones podría ser diferente.

Por otra parte, se constatan oportunidades de mejora en los procesos de inscripción de bases de datos institucionales ante la Prodhab, el establecimiento de medidas de seguridad afines con los términos

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

establecidos en la Ley 8968 y su reglamento, así como el alineamiento y vigencia del marco normativo institucional vigente con lo estipulado en esa ley.

Finalmente, se determinó una tendiente necesidad de fortalecer los procesos de capacitación a nivel institucional en el tema de protección y tratamiento de datos personales, generando como efecto que a nivel institucional se detecten prácticas que podrían estar violentando el marco normativo en esta materia.

En virtud de lo anterior, esta Auditoría propone una serie de recomendaciones a la administración activa, con el fin de solventar las oportunidades de mejora identificadas.

RECOMENDACIONES

AL DOCTOR FERNANDO LLORCA CASTRO, EN SU CALIDAD DE PRESIDENTE EJECUTIVO, O QUIEN EN SU LUGAR OCUPEN EL CARGO.

1. Basados en los hallazgos identificados en el presente informe, la relevancia de los datos personales administrados por la Caja en sus diversos ámbitos y considerando las debilidades en la gestión integral sobre el tratamiento y protección de este tipo de información, así como el rol de coordinación de las instancias estratégicas en materia de TIC a cargo de esa Presidencia; conformar una Comisión Institucional integrada por representantes de ese nivel jerárquico, las gerencias institucionales, Dirección de Tecnologías de Información y Comunicaciones en su función de asesoría técnica, y demás instancias que se estime pertinente, la cual se encargue de establecer un modelo de gestión integral orientado a garantizar el cumplimiento de lo establecido en la Ley 8968 y su reglamento en la CCSS.

En este sentido, es oportuno que dicha Comisión establezca un plan de trabajo con plazos, actividades, estrategias y responsables en aras de brindar un abordaje y cobertura integral sobre todas las bases de datos con información personal que resguarda la institución. Al respecto, es pertinente valorar los siguientes aspectos:

a. Definición de unidades institucionales a cargo del tema.
b. Definición de roles y responsabilidades concretas según el ámbito de competencia.
c. Mecanismos de coordinación entre los diferentes niveles de la organización.
d. Elaboración y actualización de marcos normativos institucionales asociados a la Ley 8968 y su reglamento.
e. Establecimiento de instancias y/o funcionarios encargados del monitoreo y seguimiento integral al cumplimiento de las acciones indicadas en la recomendación 3 del presente informe.
f. Capacitación a nivel Institucional para los usuarios que participan en el tratamiento de datos personales, en torno a la aplicación de la Ley 8969 y su reglamento.
g. Alineamiento con las iniciativas ejecutadas por la DTIC a través de la Licitación Abreviada No. 2016LA-000003-1150 “Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS”, lo anterior en lo que respecta a seguridad de la información en cumplimiento del marco normativo analizado en el presente informe.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

h. Revisión y actualización de los convenios firmados entre la CCSS e instituciones gubernamentales o empresas privadas para el acceso de información contenida en las bases de datos institucionales que contienen datos personales.
i. Otros aspectos que la Comisión considere necesario.

Esta Auditoría considera conveniente se valore que dicha Comisión sea coordinada por la Gerencia Administrativa, lo anterior en virtud que esa instancia ha ejecutado iniciativas de direccionamiento estratégico en líneas de acción tales como el desarrollo de una arquitectura empresarial, así como la implementación de un Sistema de Gestión de Calidad y una Oficina de Administración de Proyectos. Además, ha participado en el análisis y actualización de la Política de Calidad Institucional, restructuración del nivel central, simplificación de trámites, procedimiento para la Gestión documental en la Institución, entre otros.

Finalmente, es conveniente el patrocinio de esa Presidencia, la cual es necesario establezca mecanismos de control a través de los cuales se brinde seguimiento a la definición del modelo solicitado considerando la asesoría en caso de ser requerida, de la Agencia de Protección de Datos de los Habitantes (Prodhab).

Es importante que el modelo definido disponga del aval del Consejo de Presidencia y Gerentes, en aras de ser divulgado a nivel institucional para la atención obligatoria de las regulaciones y disposiciones que se generen al respecto.

Para acreditar el cumplimiento de esta recomendación, debe remitirse a este Órgano de Fiscalización, en un plazo de 6 meses posterior al recibo del presente estudio, el respaldo documental de la conformación de la Comisión, el plan de trabajo y la valoración de los aspectos señalados mencionados por esta Auditoría para establecer el modelo de gestión orientado al tratamiento y protección de datos personales en la CCSS.

2. Una vez establecido el modelo producto de la recomendación uno de este informe, ejecutar las acciones correspondientes para elaborar un inventario institucional de todas las bases de datos que resguardan datos personales, considerando que las mismas sean por mecanismos automatizados o manuales. Posteriormente, efectuar las gestiones correspondientes para garantizar sobre dichas bases, lo siguiente:

a. Definición formal de los indicadores que deben considerarse en la clasificación de bases de datos según lo dispuesto en la Ley No. 8968.

b. Categorización de las bases de datos que son internas y las que pertenecen al ámbito de aplicación de la Ley 8968, de acuerdo con lo establecido en atención del punto anterior. Al respecto, debe existir justificación suficiente, competente y pertinente sobre las bases de datos que resguardan datos personales y no forman parte del alcance del marco normativo analizado en el presente informe.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

c. Designación formal del responsable de cada base de datos, los encargados y el intermediario tecnológico, lo anterior en concordancia con las definiciones estipuladas en el reglamento a la Ley 8968.

Al respecto, es necesario definir un funcionario y/o instancia institucional encargado de gestionar el inventario establecido en atención de esta recomendación.

Para acreditar el cumplimiento de esta recomendación, debe remitirse a este Órgano de Fiscalización, en un plazo de 9 meses posterior al recibo del presente estudio, el respaldo documental de la elaboración del inventario de las bases de datos institucionales, así como las gestiones para atender lo señalado en los puntos a, b, c, y la designación del responsable de gestionar dicho inventario.

3. Una vez designado los responsables en atención del punto c de la recomendación dos del presente informe, instruir a cada uno de ellos en alineamiento al modelo de gestión establecido en atención de la disposición uno, la ejecución de las acciones correspondientes, coordinando con las instancias que considere pertinente, en aras de garantizar el cumplimiento de todas las funciones descritas en los artículos del Reglamento a la Ley 8968, a saber:

a. Medio y forma de comunicación electrónica para facilitar a los titulares el ejercicio de sus derechos (artículo 16).
b. Procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de datos personales (artículo 27).
c. Mecanismos o procedimientos establecidos para comunicar a los encargados, las obligaciones en el tratamiento de bases de datos personales (artículo 31).
d. Protocolos mínimos de actuación elaborados para la recolección, almacenamiento y el manejo de los datos personales. (artículo 32).
e. Medidas de seguridad, administrativas, físicas y lógicas implementadas por el responsable para la protección de datos personales (artículo 34)
f. Entre otros que se estime pertinente.

Es necesario considerar que, si bien la aplicación de los artículos mencionados anteriormente corresponde para las bases de datos que están sujetas a la ley 8968 y su reglamento, se debe valorar la atención de estos en los repositorios de información de carácter interno, máxime al corresponder a buenas prácticas de seguridad en el manejo de datos institucionales.

Para acreditar el cumplimiento de esta recomendación, debe remitirse a este Órgano de Fiscalización, en un plazo de 12 meses posterior al recibo del presente estudio, el respaldo documental en torno al cumplimiento de las funciones descritas en los puntos de la presente disposición, así como la valoración sobre bases de datos catalogadas de carácter interno.

4. Una vez identificadas las bases de datos que se encuentran dentro del ámbito de aplicación de la Ley 8968, instruir a los responsables para ejecutar las gestiones correspondientes a fin de inscribir dichos repositorios ante la Agencia de Protección de los Habitantes según los términos solicitados.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Para acreditar el cumplimiento de esta recomendación, debe remitirse a este Órgano de Fiscalización, en un plazo de 12 meses posterior al recibo del presente estudio, la instrucción a los responsables de las bases de datos para inscribir los repositorios de información ante la Agencia de Protección de los Habitantes, así como las gestiones que éstos realizaron en la Prodhab para iniciar el proceso de inscripción.

5. Instruir a la Comisión conformada en atención de la recomendación uno del presente informe, defina un plan que establezca las acciones a ejecutar para mitigar los riesgos señalados por esta Auditoría en relación con las prácticas institucionales identificadas en el hallazgo 9 del presente informe.

Una vez definido el plan, deberán emitirse las directrices y mecanismos pertinentes, con el fin de evitar que las situaciones mencionadas se presenten en el futuro. Así mismo, debe considerarse la regulación en el establecimiento de las acciones que conforme derecho corresponda ante el incumplimiento de las normas y medidas definidas en torno a la protección de datos personales.

Para acreditar el cumplimiento de esta recomendación, debe remitirse a este Órgano de Fiscalización, en un plazo de 3 meses posterior al recibo del presente estudio, el plan de acción definido para mitigar los riesgos identificados en el hallazgo nueve, así como las directrices y mecanismos establecidos para evitar la materialización de estos en el futuro.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 26 de julio del 2018 con la Licda. María Elena Matamoros Jiménez, Funcionaria de Presidencia Ejecutiva.

A continuación, se indican las observaciones realizadas en torno a los hallazgos y recomendaciones:

Sobre los Hallazgos y recomendaciones:

No hay observaciones.

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ESTEBAN ZAMORA CHAVES (FIRMA)
Firmado digitalmente por ESTEBAN ZAMORA CHAVES (FIRMA)
Fecha: 2018.07.30 16:12:14 -06'00'

Lic. Esteban Zamora Chaves
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2018.07.30 16:32:31 -06'00'

Lic. Rafael Ángel Herrera Mora
JEFE DE ÁREA

RAHM/EZCH/trg

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

ANEXO 1
Bases de datos Administradas por la Dirección de Tecnologías de Información y Comunicaciones

Nombre de la Base(s) de Datos [6]	***Ubicación Física***	***Sistema de Información utilizado para registrar los datos***	***Nombre y puesto del responsable (s) de la base de datos*** [7].	***Estado actual del Sistema de Información***	***Inscrita ante la PRODHAB***
SFCV	*Oficentro Tecnológico, Tibás*	*SICERE Oficina Virtual del SICERE Autogestión de Planilla en Línea Facturación por Servicios Médicos, Consulta Morosidad Web, Registro Control y Pago de Incapacidades, Sistema Integrado de Comprobantes, Sistema Institucional de la Gestión de Inspección, Sistema de Compras Exentas, Call Center de Cobros, Socket de Conectividad con Entidades Financieras, Socket de la Plataforma Institucional de Cajas Socket de Conectividad Institucional, EDUS (SIAC),Discoverer,Webservices*	*Luis Rivera Cordero*	*Producción*	*SI*
SCBM	*Oficentro Tecnológico, Tibás*	*SCBM*	*Lic. Marco Antonio Agüero Fernández*	*Producción*	*NO*
SICS	*Oficentro Tecnológico, Tibás*	*Sistema Informático Contabilidad y Suministros*	*Lic. Marco Antonio Agüero Fernández*	*Producción*	*NO*
SIFF	*Oficentro Tecnológico, Tibás*	*Base de datos Signos (Módulos) SIFF*	*LOAIZA MADRIZ CARMEN MA.*	*Producción*	*NO*
SIGNOS	*Oficentro Tecnológico, Tibás*	*Expediente Único en Salud (EDUS)-SIES*	*Eduardo Rodríguez Cubillo*	*Producción*	*NO*
	Oficentro Tecnológico, Tibás	*Expediente Único en Salud (EDUS)-SIFF*	*Guiselle Barrantes Brenes*	*Producción*	*NO*
	Oficentro Tecnológico, Tibás	*Expediente Unico en Salud (EDUS)-SIAC*	*Róger Jován López Espinoza*	*Producción*	*NO*
	Oficentro Tecnológico, Tibás	*Expediente Único en Salud (EDUS)-SILC*	*Ana Lorena Torres Rosales*	*Producción*	*NO*
	Oficentro Tecnológico, Tibás	*Expediente Unico en Salud (EDUS)-SIFA (Bases de datos Locales)*	*Isela Araya Piedra*	*Producción*	*NO*

6 Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, que sean objeto de tratamiento, automatizado o manual, en el sitio o en la nube, bajo control o dirección de un responsable, cualquiera que sea la modalidad de su elaboración, organización o acceso. Fuente: Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.

7 Persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrarse y qué tipo de tratamiento se les aplicarán. Fuente: Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (8968)

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

	Oficentro Tecnológico, Tibás	*Expediente Unico en Salud (EDUS) (SICI)*	*Rodrigo Manuel Álvarez Ramírez*	*Producción*	*NO*
CARRERAPROD	*Oficentro Tecnológico, Tibás*	*RRHH*	*Laura Paz Morales*	*Producción*	*NO*
BDADMIN	*Oficentro Tecnológico, Tibás*	*BDADMIN*	*Esmeralda Díaz Navarro*	*Producción*	*NO*
SCBM	*Oficentro Tecnológico, Tibás*	*Sistema Contable de Bienes Muebles*	*Lic. Róger Vallejos Apú*	*Producción*	*NO*
SICS	*Oficentro Tecnológico, Tibás*	*Sistema Informático de Contabilidad de Suministros*	*Marvin Porras Fernández*	*Producción*	*NO*
SGEO	*Oficentro Tecnológico, Tibás*	*SGEO*	*Marcel Ortiz*	*Producción*	*NO*
Catálogo de Teléfonos	*Oficentro Tecnológico, Tibás*	*Catálogo de Teléfonos*	*Pamela Rojas*	*Producción*	*NO*
Sistema de Matrícula de CENDEISSS	*Oficentro Tecnológico, Tibás*	*Sistema de Matrícula de CENDEISSS*	*Marianne Carballo*	*Producción*	*NO*
Control de Transportes	*Oficentro Tecnológico, Tibás*	*Control de Transportes*	*Esteban Vega*	*Producción*	*NO*
Datos de Registro IRAG	*Oficentro Tecnológico, Tibás*	*Datos de Registro IRAG*	*Roy Wong*	*Producción*	*NO*
SOVT	*Oficentro Tecnológico, Tibás*	*Sistema Operación de Vales de Transporte*	*Área Servicios Generale*	*Producción*	*NO*
SIGES	*Oficentro Tecnológico, Tibás*	*Sistema de Gestión de Suministros*	*Lic. Manrique Cascante Naranjo*	*Producción*	*NO*
FRAP	*Oficentro Tecnológico, Tibás*	*Fondo de Retiro Ahorro y Préstamo*	*Andrés Arrieta Barrantes.*	*Producción*	*NO*
SOCO SOVT	*Oficentro Tecnológico, Tibás*	*Sistema Operación de Vales de Transporte*	*Esmeralda Díaz Navarr*	*Producción*	*NO*
SIGC	*Oficentro Tecnológico, Tibás*	*Sistema de Información Gerencial CENDEISSS*	*Jorge Peñaranda Guerrero*	*Producción*	*NO*
SIIP	*Oficentro Tecnológico, Tibás*	*Sistema Integrado Institucional de Presupuesto*	*Lic. Carlos Alberto Ampié Gutiérrez,Licda. Leylin Méndez Esquivel*	*Producción*	*NO*
SPLA	*Oficentro Tecnológico, Tibás*	*Sistema de Planilla Ampliada*	*Lic. Carlos Alberto Ampié Gutiérrez,Licda. Leylin Méndez Esquivel*	*Producción*	*NO*
SIPO	*Oficentro Tecnológico, Tibás*	*Sistema de Operación Presupuestaria*	*Lic. Carlos Alberto Ampié Gutiérrez,Licda. Leylin Méndez Esquivel*	*Producción*	*NO*
PORTALRH_TA	*Oficentro Tecnológico, Tibás*	*Recursos Humano*	*Laura Paz Morales*	*Producción*	*NO*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

CARRERAPROD	*Oficentro Tecnológico, Tibás*	*Sistema de Carrera Profesional*	*Guillermo Abarca*	*Producción*	*NO*
ESEP	*Oficentro Tecnológico, Tibás*	*Encuesta Salida de Pensionados*	*Cruz Sancho*	*Producción*	*NO*
FRAP	*Oficentro Tecnológico, Tibás*	*Fondo Retiro Ahorro y Préstamo*	*Víctor Fernández Badilla*	*Producción*	*NO*
SAPC	*Oficentro Tecnológico, Tibás*	*Sistema Administración Planes de Continuidad y Resguardos*	*ASCI - Lic. Leonardo Fernández Mora*	*Producción*	*NO*
SOCO	*Oficentro Tecnológico, Tibás*	*Sistema Operación Control y Mantenimiento*	*Teófilo Peralta*	*Producción*	*NO*
SOVT	*Oficentro Tecnológico, Tibás*	*Sistema de Vales de Transporte*	*Giorgianella Araya Araya*	*Producción*	*NO*
SPCA	*Oficentro Tecnológico, Tibás*	*SCIP*	*Giorgianella Araya Araya*	*Producción*	*NO*
BD_SIDJ_DIRECCION_JURIDICA	*Edificio Jenaro Valverde piso 11*	*Dirección Jurídica*	*Sofía Calderón Jurídica*	*Producción*	*NO*
FM_CCSS	*Edificio Jenaro Valverde piso 11*	*FileMaster Dirección Jurídica*	*Sofía Calderón Jurídica*	*Producción*	*NO*
DB_CANCER	*Oficentro Tecnológico, Tibás*	*App. De Vigilancia Epidemiológica*	*Dr. Roy Wong de Vigilancia Epidemiológica*	*Producción*	*NO*
DB_CITOLOGIAS	*Oficentro Tecnológico, Tibás*	*App. De Vigilancia Epidemiológica*	*Dr. Roy Wong de Vigilancia Epidemiológica*	*Producción*	*NO*
DB_ERC	*Oficentro Tecnológico, Tibás*	*App. De Vigilancia Epidemiológica*	*Dr. Roy Wong de Vigilancia Epidemiológica*	*Producción*	*NO*
Egreso_Hospitalario	*Oficentro Tecnológico, Tibás*	*App. De Vigilancia Epidemiológica*	*Dr. Roy Wong de Vigilancia Epidemiológica*	*Producción*	*NO*
SISVE	*Oficentro Tecnológico, Tibás*	*App. De Vigilancia Epidemiológica*	*Dr. Roy Wong de Vigilancia Epidemiológica*	*Producción*	*NO*

Fuente: Dirección de Tecnologías de Información y Comunicaciones, mayo 2015.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888