AUDITORÍA JUDICIAL
TELÉFONO: 2295-3238
FAX: 2257-05-85
E-MAIL: auditoria@poder-judicial.go.cr
APARTADO: 79-1003 SAN JOSE

N° 59-14-SATI-2020

20 de enero de 2020

Doctor
Franz Vega Zúñiga, Jefatura
Departamento de Medicina Legal

Estimado Señor:

De conformidad con lo dispuesto en el Artículo 36 de la Ley General de Control Interno, le remito informe final correspondiente al Estudio efectuado por la Sección Auditoría Tecnología de Información del Despacho a mi cargo, denominado Evaluación de la seguridad de la información del Sistema Médico Legal.

El estudio tuvo como objetivo, evaluar si la seguridad de la información contenida en el Sistema Médico Legal cumple con los aspectos mínimos necesarios de acuerdo con la normativa vigente.

No omito indicar que con la implementación de las recomendaciones emitidas se pretende minimizar el riesgo de que en el futuro se presenten las debilidades detectadas. Además, es relevante señalar que, de conformidad con lo establecido en la Ley General de Control Interno, esta Auditoría efectuará en su momento un seguimiento, para asegurarse de que las acciones establecidas por las instancias competentes, se hayan implementado eficazmente y dentro de los plazos definidos en cada caso.

Finalmente, en caso de que este documento deba ser facilitado a partes externas del Poder Judicial, deberá preverse lo establecido en la Ley Nº 8968 “Protección de la Persona Frente al tratamiento de sus datos personales”.

Atentamente,

Roy Díaz Chavarría
Subauditor Judicial

c: Consejo Superior
Sección Auditoría Tecnología de Información
Archivo.-(SATI-24-2019)

AUDITORIA JUDICIAL

Informe de auditoría para el mejoramiento del control interno relativo a la seguridad de la información del Sistema Médico Legal (SIMEL)

Sección Auditoría Tecnología de Información

Enero 2020

AUDITORÍA JUDICIAL
TELÉFONO: 2295-3238
FAX: 2257-05-85
E-MAIL: auditoria@poder-judicial.go.cr
APARTADO: 79-1003 SAN JOSE

Tabla de Contenido

RESUMEN EJECUTIVO 4
1 INTRODUCCIÓN 5
1.1 Trámite de los informes de auditoría según la Ley General de Control Interno 5
1.2 Origen del estudio 5
1.3 Objetivo general 5
1.4 Alcance y naturaleza 5
1.5 Equipo de trabajo 5
1.6 Normativa técnica aplicada 5
1.7 Difusión verbal de los resultados 5
2 RESULTADOS DEL ESTUDIO 6
2.1 Importancia de establecer una adecuada asignación de permisos de acceso, formalizar procedimientos para la revisión de cuentas de usuario y de la bitácora del SIMEL 6
2.2 Importancia de documentar y mantener actualizada la información generada del SIMEL 10
2.3 Conveniencia de definir formalmente la ejecución periódica de pruebas de recuperación sobre los respaldos y establecer un plan de contingencia para el SIMEL 11
3 CONCLUSIONES DEL ESTUDIO 13
4 RECOMENDACIONES DEL ESTUDIO 14

AUDITORÍA JUDICIAL
TELÉFONO: 2295-3238
FAX: 2257-05-85
E-MAIL: auditoria@poder-judicial.go.cr
APARTADO: 79-1003 SAN JOSE

RESUMEN EJECUTIVO

El trabajo realizado corresponde a una auditoría cuyo objetivo fue evaluar si la seguridad de la información contenida en el Sistema Médico Legal cumple con los aspectos mínimos necesarios de acuerdo con la normativa vigente. Se consideró la situación encontrada con fecha de corte al 10 de enero del 2020.

El Sistema de Medicina Legal (SIMEL), tiene la finalidad de registrar y ayudar con las labores y procesos de las diferentes secciones o unidades que integran el Departamento de Medicina Legal; además de interactuar con la información generada desde otros sistemas como Ciencias Forenses y Gestión. Esta Auditoría consideró relevante su evaluación debido al nivel de riesgo que representa para la Institución el acceso y uso inadecuado de la información sensible de los procesos judiciales; de conformidad con la Ley de Control Interno y demás normas de la Contraloría General de la República.

Una vez concluido el trabajo de auditoría, se logró identificar algunos aspectos susceptibles de mejora en lo relativo a la administración de cuentas de usuario y las revisiones periódicas de los accesos otorgados, así como de la bitácora del Sistema.

Igualmente se identificaron debilidades en cuanto a la ejecución de pruebas de recuperación de los respaldos generados, falta de un plan de contingencia y omisión o desactualización en la documentación del proyecto, específicamente en lo relacionado a las minutas de las reuniones, manuales del Sistema y algunos procedimientos; aumentando los riesgos operativos de información inaccesible, pérdida de información y atraso en los procesos. Concluyendo de esta forma, que la seguridad de la información contenida en el Sistema Médico Legal no cumple con los aspectos mínimos necesarios de acuerdo con la normativa vigente.

Producto de las debilidades encontradas, esta auditoria emitió recomendaciones a la Dirección de Tecnología de Información, al Departamento de Medicina Legal y la Unidad Tecnológica Informática del OIJ para que se implementen acciones específicas que subsanen los aspectos descritos en este informe.

Evaluación de la seguridad de la información del Sistema Médico Legal

1 INTRODUCCIÓN

1.1 Trámite de los informes de auditoría según la Ley General de Control Interno

El artículo 36 de la Ley General de Control Interno, establece el tratamiento que los titulares subordinados encargados de las áreas evaluadas, deben dar a los informes de fiscalización que emite la Auditoría Interna, el cual incluye, la orden de implementación de las recomendaciones vertidas en el informe o el planteamiento de discrepancia ante el Jerarca, en el plazo de diez días hábiles a partir de la fecha de recibido el documento.

A su vez, el artículo 39 de la citada Ley advierte de la responsabilidad administrativa o civil que puede acarrear sobre los responsables, la inobservancia de las recomendaciones emitidas por la Auditoría Interna.

1.2 Origen del estudio

El presente estudio no programado realizado de conformidad con las competencias que son atinentes a esta Auditoría, señalado en el artículo 22 de la Ley General de Control Interno.

1.3 Objetivo general

Evaluar si la seguridad de la información contenida en el Sistema Médico Legal, cumple con los aspectos mínimos necesarios de acuerdo con la normativa vigente.

1.4 Alcance y naturaleza

La naturaleza del estudio es operativa y comprendió el análisis de la seguridad de la información que se procesa mediante el Sistema Médico Legal. Además, consideró la situación encontrada al momento de la auditoría, con fecha de corte al 10 de enero del 2020.

1.5 Equipo de trabajo

El estudio fue desarrollado por el profesional de esta Auditoría, Luis Diego Madrigal González, en coordinación con la jefatura de esta sección, Alicia Sancho Brenes.

1.6 Normativa técnica aplicada

Para la ejecución de este estudio se observaron las Normas para el Ejercicio de la Auditoría Interna en el Sector Público y las Normas Generales de Auditoría para el Sector Público, ambas promulgadas por la Contraloría General de la República.

1.7 Difusión verbal de los resultados

Este estudio fue puesto en conocimiento de la Dirección de Tecnología de información mediante informe en borrador 1470-124-SATI-2019, con fecha del 10 de diciembre del 2019 y

comentado en conferencia final efectuada el día 7 de enero del 2020, en la cual participaron:

Por parte de la Dirección de Tecnología de Información:
- Victor Julio Conejo Sanabria – Base Tecnológica
- Jonathan Sánchez Hernández – Gobierno y Control
- Jackeline Chaves Mejía – Informática de Heredia

Por parte de la Auditoría:
- Alicia Sancho Brenes, Jefe, Auditoría de TI
- Luis Diego Madrigal González, Auditor de TI

Igualmente, el informe fue puesto en conocimiento del Departamento de Medicina Legal y la Unidad Tecnológica Informática mediante los informes en borrador 1471-124-SATI-2019 y 1472-124-SATI-2019 respectivamente, con fecha del 10 de enero del 2019 y comentado en conferencia final efectuada el día 7 de enero del 2019, en la cual participaron:

Por parte del Departamento de Medicina Legal:
- Franz Vega Zúñiga – Jefatura de Medicina Legal
- Johana Villalobos Berrios – Medicina Legal
- Gabriela Valverde Rojas – Unidad Tecnológica Informática
- Jesús Benavidez Chacón – Unidad Tecnológica Informática
- Roger Martínez Ruiz – Unidad Tecnológica Informática

Por parte de la Auditoría:
- Alicia Sancho Brenes, Jefe, Auditoría de TI
- Luis Diego Madrigal González, Auditor de TI

La discusión de los resultados de auditoría tratados durante esta etapa, permitió considerar las observaciones expuestas por las áreas auditadas y las responsables de implementación de las mejoras propuestas; las cuales se han incorporado al informe en lo pertinente.

2 RESULTADOS DEL ESTUDIO

Como producto de la auditoría realizada en el área bajo estudio, se determinaron los aspectos que se detallan a continuación:

2.1 Importancia de establecer una adecuada asignación de permisos de acceso, formalizar procedimientos para la revisión de cuentas de usuario y de la bitácora del SIMEL

Como parte del trabajo de Auditoría elaborado para verificar el estado de las cuentas de usuario del SIMEL[1] y según las indagaciones efectuadas y el análisis de la información suministrada, se identificaron las siguientes irregularidades al respecto:

[1] SIMEL: Sistema de Medicina Legal

- **Asignación y modificación de permisos de acceso**: Es del conocimiento de esta Auditoría que el Departamento de Medicina Legal, estableció que la administración de cuentas de su Sistema de Información se distribuyera en Administradores locales para dar soporte a sus respectivas secciones o unidades Médico Legal, asignando, modificando o eliminando los permisos de acceso del resto de usuarios; con lo cual se le otorgó permisos de ese tipo a 25 diferentes funcionarios dentro y fuera del Departamento, que al 31 de diciembre del 2019 se encontraban activos.

  Además, se identificaron 8 funcionarios con más de una oficina en la que podían brindar permisos de acceso al Sistema. Inclusive 6 de ellos, contaban con permisos en tantas oficinas que se podrían considerar administradores globales (Usuarios del Sistema con posibilidad de dar acceso a todas las oficinas del país).

  Cabe resaltar que, de los 25 funcionarios mencionados anteriormente, al 10 de enero del presente año, solamente 15 mantenían activos los permisos citados; de los cuales 14 pertenecen al Departamento de Medicina Legal y 1 es personal informático de la Ciudad Judicial de San Joaquín de Flores.

  De acuerdo con lo mencionado por el personal de Medicina Legal, esta situación se da, debido a que poseen oficinas a nivel nacional, las cuales en algunos casos laboran 24/7 los 365 días del año, siendo necesario para cada uno de estos centros, contar con una persona disponible para la activación de usuarios en caso de ser requerido.

  La desconcentración de la Administración del Sistema y específicamente en lo que se refiere al mantenimiento de cuentas de accesos, aumenta el riesgo de permisos otorgados de manera irregular; debido a la complejidad de controlar el buen uso de los privilegios de este perfil, entre más personas les sea asignado.

- **Revisión de cuentas de usuario**: Se comprobó que no se ha definido un procedimiento formal ligado directamente con la revisión periódica de cuentas de acceso al SIMEL; siendo responsabilidad de cada una de las oficinas, el mantener actualizados los permisos y las cuentas de usuario debidamente asignados, garantizando que todos los accesos sean adecuados según las políticas de la Institución y las funciones del personal respectivo.

  Aunque inicialmente a cada una de estas cuentas se le otorgan los permisos necesarios para efectuar sus respectivas funciones, es claro que se dan movimientos en los puestos, ya sea por ausencias debido a vacaciones, permisos, ascensos o incapacidades o por finalizar la relación laboral, entre otras razones; las cuales requieren deshabilitar permisos concedidos para la seguridad de la información.

  El personal de la Unidad Tecnológica Informática del OIJ (UTI), indicó que estas funciones son propias del Departamento de Medicina Legal; mientras que estos últimos mencionan que, por cuestiones de restricción de permisos, es el personal técnico informático el que puede ejecutar estas funciones con autorización previa de la Jefatura de Sección o Unidad Médico Legal interesada; con lo cual se comprueba la confusión existente dentro del personal, por la falta de un procedimiento formal al respecto; a la vez que no se tiene certeza si se mantiene un control, ni como lo hace cada una de las diferentes dependencias.

La ausencia de este procedimiento dificulta corroborar la permanencia de permisos adecuados de acceso al Sistema; posibilitando el ingreso de personas no autorizadas a fuentes de consulta oficiales, lo cual provoca la exposición de información privada para usos indebidos.

- **Revisión de bitácoras del SIMEL**: Se determinó la ausencia de un procedimiento formal relacionado directamente con la revisión periódica de las bitácoras. Por lo cual no se han establecido los aspectos a registrar, los encargados de realizar el control; así como la periodicidad de ejecución y las acciones a tomar en caso de identificar anomalías. Este tipo de revisiones tiene como objetivo garantizar de forma razonable que los accesos y movimientos efectuados en el SIMEL, se encuentran en función a las políticas Institucionales y labores del personal respectivo.

  De acuerdo con lo manifestado por los usuarios consultados, de igual forma que en el punto anterior, el personal de la UTI señaló que estas funciones son propias del Departamento de Medicina Legal; mientras que estos últimos mencionan que, por cuestiones de restricción de permisos, es el personal técnico informático el que puede ejecutar estas funciones con autorización previa de la Jefatura de Sección o Unidad Médico Legal interesada. Igualmente, externaron que las revisiones de este tipo ejecutadas hasta el momento se deben a solicitudes específicas y no obedecen a un procedimiento definido, ya que no ha sido considerado a la fecha.

  La ausencia de una revisión periódica sobre el uso del Sistema podría permitir al personal con acceso a éste, genere acciones no autorizadas, sin ser detectadas de manera oportuna.

Con base en todo lo anterior, el mantener las condiciones descritas aumentan la posibilidad de que se presenten los riesgos operativos relacionados con:

- Pérdida de Información
- Información Inaccesible.

En relación con este tema, las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) de la Contraloría General de la República indican:

> ***"4.2 Requisitos de las actividades de control***
> *Las actividades de control deben reunir los siguientes requisitos:*
> *[...]*
> *e.* ***Documentación****. Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación.*
> *f.* ***Divulgación****. Las actividades de control deben ser de conocimiento general, y comunicarse a los funcionarios que deben aplicarlas en el desempeño de sus cargos. Dicha comunicación debe darse preferiblemente por escrito, en términos claros y específicos."*

Por otro lado, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República, mencionan lo siguiente:

> *"**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*. […]
> *d) Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.*
> *e) Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.*

Por su parte, el estándar ISO/IEC 27002:2013, relacionado con normas de seguridad de la información, en su traducción al español establecen lo siguiente:

> ***"9.2.5 Revisión de derechos de acceso de usuarios.***
>
> *Control*
> *Los propietarios de los activos deben revisar los derechos de acceso de los usuarios en intervalos regulares.*
>
> *Guía de implementación.*
> *La revisión de los derechos de acceso debería considerar lo siguiente:*
>
> *a. Los derechos de acceso de los usuarios deberían ser revisados en intervalos regulares y después de algún cambio, tales como ascensos, cambio de puesto o finalización de relación laboral.*
> *b. Los derechos de acceso de los usuarios deberían ser revisados y re-autorizados aun cuando sea una reubicación de puesto dentro de la misma organización.*
> *c. Las autorizaciones para derechos de acceso especiales deberían ser revisados en intervalos más frecuentes.*
> *d. La asignación de privilegios debe ser revisado en intervalos regulares para evitar que se den privilegios sin autorización.*
> *e. Los cambios en las cuentas especiales deberían ser registradas para ser revisadas periódicamente."*

2.2 Importancia de documentar y mantener actualizada la información generada del SIMEL

Luego de las indagaciones realizadas y la revisión de la documentación suministrada por el Área auditada, se confirmaron algunos aspectos de mejora en cuanto a documentación se refiere, que se detallan a continuación:

- Desde el desarrollo del SIMEL, solamente se generó el Manual de Usuario; el cual no ha sido modificado desde que se creó, a pesar de que el Sistema ya presenta variaciones. Con respecto al Manual Técnico, se mencionó que nunca fue elaborado.

- A pesar de contar con un control de actividades pendientes que se va actualizando con base en las reuniones sostenidas entre el personal de la UTI y la Jefatura del Departamento de Medicina Legal, las minutas de estas reuniones no se han documentado de manera consistente a lo largo de la ejecución del Proyecto, provocando que no se cuente con evidencia formal de los acuerdos de servicio y priorización de actividades a los que han llegado.

En relación con este tema, las Normas de Control Interno para el Sector Público, emitidas por la Contraloría General de la República (N-2-2009-CO-DFOE), indica lo siguiente:

> ***"4.2 Requisitos de las actividades de control***
> *Las actividades de control deben reunir los siguientes requisitos:*
> *[…]*
> *e.* ***Documentación****. Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación."*
>
> ***"5.4 Gestión documental***
> *El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales".*

Por su lado, el marco de referencia "Guía de los fundamentos para la Dirección de Proyectos (PMBOK) 6ta edición" se refiere al respecto, señalando lo siguiente:

> ***"4.5 Monitorear y Controlar el Trabajo del Proyecto***
> *Monitorear y Controlar el Trabajo del Proyecto es el proceso de dar seguimiento, revisar e informar el avance a fin de cumplir con los objetivos de desempeño definidos en el plan para la dirección del proyecto. […] El proceso Monitorear y Controlar el Trabajo del Proyecto se ocupa de:*

- *[…]mantener, durante la ejecución del proyecto, una base de información precisa y oportuna relativa al producto o a los productos del proyecto y a su documentación relacionada."*

De acuerdo con lo señalado por el personal consultado de la UTI, las situaciones descritas se deben a:

- Los manuales debieron ser generados por parte de la Dirección de Tecnología de Información al momento de desarrollar el Sistema; sin embargo, cuando se trasladó a la UTI, solamente se había creado el Manual de usuario y a la fecha no se ha podido actualizar porque se les ha dado prioridad a otras actividades por parte del Departamento de Medicina Legal.

- La falta de formalización de las minutas se debe principalmente a que las labores diarias que se realizan consumen la mayoría del tiempo disponible; aunado a las cargas de trabajo que impiden darle prioridad a la documentación de las labores efectuadas. Igualmente se mencionó que no se le ha dado la importancia del caso, ya que los nuevos requerimientos y la priorización de las actividades se van agregando a la lista de pendientes.

La omisión de documentación formal sobre los manuales del Sistema y las minutas de las reuniones sostenidas, aumentan la probabilidad de que se presenten riesgos operativos, como "Atraso en los procesos" y "Pérdida de Información" debido a que:

- El personal, ya sea técnico o usuario común, no cuente con la documentación soporte que les permita consultar en caso de dudas a la hora de ejecutar alguna labor en el SIMEL, máxime cuando se presenta rotación o ingreso de nuevo personal; lo cual puede incidir en atrasos o errores innecesarios.

- El personal encargado ejerza inadecuadamente las tareas asignadas, al no contar con las minutas formales de las reuniones sostenidas, temas tratados y que las tareas pendientes sean poco claras.

- Las personas que no asistieron a las reuniones o unidades fiscalizadoras carezcan de la manera de enterarse sobre los temas tratados, acuerdos establecidos, responsables y tareas pendientes; impidiendo mantener un adecuado monitoreo y control del desarrollo del Proyecto y de aspectos por mejorar.

2.3 Conveniencia de definir formalmente la ejecución periódica de pruebas de recuperación sobre los respaldos y establecer un plan de contingencia para el SIMEL

Como parte de la evaluación desarrollada por esta Auditoría, se realizó una revisión sobre los procesos de ejecución de respaldos y recuperación de datos del SIMEL; así como de la existencia de un plan de contingencia que permita mantenerse en operación en caso de presentarse alguna eventualidad que afecte el Sistema.

Ante las indagaciones efectuadas, se comprobó que los respaldos se generan de manera periódica, tanto sobre las bitácoras, como de la base de datos; no obstante, se determinó que

no se ha establecido de manera formal la ejecución de pruebas de recuperación sobre los respaldos generados.
Actualmente se ha ejecutado en promedio, una prueba de recuperación por año; sin embargo, no se cuenta con un procedimiento definido sobre las acciones a realizar, la documentación a generar, ni la periodicidad de estas; por lo que no se puede asegurar que todos los respaldos se hayan ejecutado adecuadamente.

Además, no se están documentando los resultados obtenidos, ya que únicamente se menciona la fecha y hora de su ejecución y si fue exitoso o no y quien fue el responsable; sin embargo, se carece de aspectos como el detalle del proceso elaborado, los resultados y errores que se pudieran presentar y servir como guía para futuro.

Igualmente se comprobó con el personal de la Dirección de Tecnología de Información (DTI), que actualmente el Sistema presenta algunas medidas de seguridad en cuanto a recuperación se refiere, como la mencionada anteriormente con respecto a la ejecución de los respaldos; a pesar de ello, no cuenta con un Plan de Contingencia propio, ni se cuenta con mecanismos de continuidad de operaciones como lo es un esquema de alta disponibilidad[2].

Sobre estos temas, las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" (N-2-2007-CO-DFOE) de la Contraloría General de la República, establecen:

> ***"1.4.7 Continuidad de los servicios de TI.***
> *La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.*
>
> *Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura."*

Por su lado, el "Marco de referencia de buenas prácticas para el control de las Tecnologías de Información" COBIT en su versión 5.0 manifiesta:

> ***"DSS04 Gestionar la Continuidad***
> *Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa."*
>
> ***"DSS04.07 Gestionar acuerdos de respaldo.***
> *Mantener la disponibilidad de la información crítica del negocio.*
> *Actividades*

[2] Algunos sistemas institucionales considerados críticos replican los datos en un segundo servidor, por lo que, en caso de interrupción, de inmediato entra en funcionamiento el segundo. En caso de que no sea posible acceder a ambos, se dispone de un sitio alterno.

[…] 5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente".

De acuerdo con lo manifestado por el personal de la Unidad Tecnológica Informática (UTI), las pruebas de recuperación deben ser hechas por el personal de la DTI, sin embargo, al consultarle al personal de dicha Dirección, indicaron que los dueños de la Aplicación son quienes deben solicitarlas y hasta la fecha, no se ha pedido ningún tipo de procedimiento al respecto.

En cuanto a un plan de contingencias para el SIMEL, se indicó que, con el paso de la administración del Sistema de la DTI a la UTI, se definieron algunas responsabilidades como la ejecución de respaldos; sin embargo, no se ha definido responsables para la creación de un plan de contingencia, ni las medidas necesarias para mantenerse en operación ante cualquier eventualidad.

La ausencia de planes de contingencia para sistemas de información, ha sido comunicada anteriormente por parte de esta Auditoria en reiteradas ocasiones; la más reciente por medio del Informe N°1342-116-SATI-2019, del 6 de noviembre del 2019, sobre la "*Evaluación del plan de contingencia en lo competente a la Dirección de Tecnología de Información, Unidad Tecnológica Informática del OIJ"*, el cual entre otros aspectos recomienda, crear un estándar para la elaboración de planes de contingencia en las aplicaciones, con lo cual se espera que todos los sistemas dispongan de su propio documento; además de la calendarización de pruebas de restauración con un enfoque integral, para que no solo contemple respaldos.

Sin pruebas de recuperación sobre los respaldos previamente generados, no se puede garantizar que la información se esté resguardando adecuadamente. Por su lado, con respecto a la falta de un plan de contingencia que muestre los pasos a seguir en caso de presentarse alguna falla en la aplicación o cualquier eventualidad que interrumpa el servicio brindado o el acceso a los datos, limita la posibilidad de contar con mecanismos que permitan la identificación de errores de manera ágil, así como los pasos y tiempos de recuperación.

En ambos casos, de presentarse alguna contingencia, se aumentan los riesgos operativos de "Atraso en los Procesos", "Pérdida de información" e "Información inaccesible", incrementando los tiempos de espera mientras se logran solucionar las fallas presentadas, lo cual afecta directamente los trámites judiciales y la mora judicial; además del riesgo reputacional de generar una afectación en la imagen de la Institución, ya que durante el tiempo que se tarde en la recuperación, no es posible acceder a los servicios asociados.

3 CONCLUSIONES DEL ESTUDIO

De la evaluación desarrollada se puede concluir que la seguridad de la información contenida en el Sistema Médico Legal no cumple con los aspectos mínimos necesarios de acuerdo con la normativa vigente, debido a que se identificaron aspectos de mejora en lo relativo a la administración de cuentas de usuario, revisiones periódicas de los accesos otorgados y de la bitácora del Sistema.

Igualmente se identificaron debilidades en cuanto a la ejecución de pruebas de recuperación de los respaldos generados, falta de un plan de contingencia y omisión o desactualización en la documentación del proyecto, específicamente en lo relacionado a las minutas de las reuniones,

manuales del Sistema y algunos procedimientos.

4 RECOMENDACIONES DEL ESTUDIO

A la Jefatura de la Dirección de Tecnología de Información

4.1. Establecer un procedimiento que defina la ejecución de pruebas de recuperación de manera periódica sobre los respaldos generados; así como la obligatoriedad de documentar sus respectivos resultados. Esto con el fin de garantizar la disponibilidad de la información en el momento que se requiera, ante la posibilidad de que se presente cualquier contingencia o eventualidad.

Cabe indicar que lo anterior, debe estar acorde con los esfuerzos que ya se han definido para atender las recomendaciones del oficio N°1342-116-SATI-2019, mencionado en el este informe.

Plazo de implementación: 3 meses

4.2. Crear un Plan de Contingencia para el SIMEL, que permita a los encargados contar con una guía para la recuperación de las operaciones en el menor tiempo y costo posible.

Lo anterior, de conformidad con el estándar solicitado por medio del oficio N°1342-116-SATI-2019, mencionado en el presente informe.

Plazo de implementación: 6 meses

4.3. Valorar, en conjunto con el personal de la Unidad Tecnológica Informática, la posibilidad de incluir el Sistema en un esquema de alta disponibilidad y documentar el análisis que se realice. Lo anterior, con el fin de dar más seguridad ante una eventual contingencia.

Plazo de implementación: 6 meses

A la Jefatura del Departamento de Medicina Legal

4.4. Realizar una revisión del esquema establecido en cuanto a la cantidad de administradores de usuarios del SIMEL, de tal forma que se efectúen los ajustes necesarios minimizando los riesgos asociados mencionados en el presente informe.

Plazo de implementación: 3 meses

4.5. Establecer un procedimiento formal sobre la obligatoriedad de efectuar revisiones de permisos y cuentas de usuarios al SIMEL de manera periódica, garantizando razonablemente que los accesos al Sistema se encuentren debidamente definidos de acuerdo con las políticas Institucionales y funciones del personal respectivo.

Plazo de implementación: 3 meses

4.6. Efectuar, en coordinación con la Unidad Tecnológica Informática un análisis sobre el diseño actual de las bitácoras del SIMEL, de tal forma que se valore la conveniencia de modificarlas o generar reportes sobre éstas e incluir dicho trabajo dentro del listado de requerimientos pendientes; con el fin de que la información generada, sea de utilidad para la Administración en cuanto al monitoreo de las acciones realizadas en el Sistema.

Plazo de implementación: 3 meses para el análisis, y su modificación según prioridad establecida en el listado de requerimientos pendientes

4.7. Establecer, luego de definir el diseño de las bitácoras o reportes de la recomendación anterior, un procedimiento formal de revisión sobre este mecanismo de control según lo indicado en el presente informe; con el fin de garantizar razonablemente que el Sistema sea utilizado correctamente.

Plazo de implementación: 3 meses para el procedimiento, y la aplicación una vez que se implemente la recomendación anterior.

A la Jefatura de la Unidad Tecnológica Informática

4.8. Crear y mantener actualizados los manuales, técnico y de usuario del SIMEL, de tal forma que el personal que lo requiera cuente con la documentación que le permita realizar las consultas del caso para ejecutar ciertas funciones en el Sistema.

Plazo de implementación: 1 año.

4.9. Documentar y archivar las minutas de las reuniones sostenidas del Proyecto; con el fin de garantizar que la información registrada corresponda con documentos formales en cuanto a los temas tratados, acuerdos establecidos y tareas pendientes, manteniendo el control adecuado respectivo.

Plazo de implementación: Inmediato.