Auditoría Interna

CONSEJO DE SEGURIDAD VIAL

AUDITORIA INTERNA

INFORME AI-INF-ATI-2020-12

Evaluación del Sistema biométrica de Marcas

Junio – 2020

Teléfonos: 2522-0915
Fax: 2522-0869
www.csv.go.cr

Auditoría Interna

INDICE

Evaluación del Sistema biométrica de Marcas

1. INTRODUCCIÓN

1.1. Origen del estudio

Este informe corresponde a un estudio especial que fue incorporado en el Plan Anual de Trabajo de la Auditoría Interna para el año 2020.

1.2. Objetivo del estudio

Analizar los controles establecidos en el Sistema biométrica de Marcas.

1.3. Alcance

La evaluación se enfocó en el uso, los controles y los procedimientos del Sistema biométrica de Marcas, en el periodo 2020 y cumplimiento normativo.

El estudio se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público (R-DC-064-2014) y Normas para el Ejercicio de la Auditoría Interna en el Sector Público (R-DC-119-2009) emitidas por la Contraloría General de la República (en adelante CGR) y la normativa aplicable al objeto de estudio.

1.4. Conferencia final

La conferencia final se llevó a cabo el 25-06-2020 y con el consentimiento de los asistentes, consta en un archivo digital. En la misma no se hicieron observaciones.

1.5. Disposiciones de la Ley General de Control Interno, a considerar

➢ Sobre la implantación de recomendaciones

Artículo 36. —Informes dirigidos a los titulares subordinados. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:

a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.

b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.

Artículo 37. —Informes dirigidos al jerarca. Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.

Artículo 38. —Planteamiento de conflictos ante la Contraloría General de la República. Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

- Sobre responsabilidad

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.

El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable.

Asimismo, cabrá responsabilidad administrativa contra el jerarca que injustificadamente no asigne los recursos a la auditoría interna en los términos del artículo 27 de esta Ley.

Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente.

El jerarca, los titulares subordinados y los demás funcionarios públicos también incurrirán en responsabilidad administrativa y civil, cuando corresponda, por obstaculizar o retrasar el cumplimiento de las potestades del auditor, el sub auditor y los demás funcionarios de la auditoría interna, establecidas en esta Ley.

Cuando se trate de actos u omisiones de órganos colegiados, la responsabilidad será atribuida a todos sus integrantes, salvo que conste, de manera expresa, el voto negativo.

1.6. Antecedentes

La Asesoría en Tecnología de la Información, remitió el 08-01-2018 al Departamento de Proveeduría, el Oficio No. ATI-2018-0007, donde adjunta la Solicitud de Materiales, Suministros y Servicios No. ATI-2018-002 para la compra de un Sistema de Control de Acceso mediante tecnología IP denominado Proyecto: "Sistema de control de accesos a las oficinas del COSEVI mediante la aplicación de tecnología IP a nivel institucional". Se indicó que parte del equipo se dividía en:

- Contraparte Administrativa
Sra. AGM, Unidad de Control y Salud Ocupacional.
Sr. GVP, Oficial de Seguridad Institucional.

- Contraparte Técnica:
Sr. DAH, Área de Telemática y Redes.
Sra. SMCh, Área de Telemática y Redes.

El objetivo de la contratación, según la justificación planteada al inicio de la misma era "Administrar, organizar y controlar el flujo de personas que ingresan y salen de las diferentes oficinas del COSEVI, minimizando los riesgos de ingreso de aquellas no acreditadas para ello, mediante la instalación de un Sistema de Control de Accesos con Tecnología IP a Nivel Institucional."

El trámite de la contratación se formalizó con la Licitación Abreviada No. 2018LA000006-0058700001 "Implementación de solución de Sistema de Control de Acceso mediante tecnología IP", por medio del cual se adquirieron 28 Lectoras faciales.

El proyecto al ser llave en mano incluía todos los componentes, materiales, reforzamiento de estructuras, circuitos eléctricos independientes a los actuales y cualquier otro material o componente necesarios para que el mismo sea exitoso. El monto adjudicado ascendió a ¢111,622,931.90.

Los Administradores del contrato, responsables del seguimiento, coordinación, supervisión, recibido conforme contraparte administrativa del servicio/bienes, aprobar mejoras tecnológicas, conceder prórrogas de los plazos de entrega, entre

otros era la **Sra. AGM de la Unidad de Control y Salud Ocupacional** (Sistema de Registro Marcas) y **el Sr GVP Oficial de Seguridad Institucional**, y según el Contrato debían otorgar el recibido conforme posterior a la aprobación técnica por parte de los compañeros de ATI.

El **Sr. DAH y Sra. SMCh de la Asesoría en Tecnología de la información**, fueron los responsables de dar el recibido conforme técnico de dicha contratación.

Mediante esta contratación se pretendía mejorar el desempeño de los recursos informáticos, lo que incluye una mejor seguridad física y lógica del acceso a los Edificios u Oficinas del Consejo de Seguridad Vial.

Las Lectoras cuentan con una garantía activa de 36 meses, contados a partir del recibo conforme de los equipos y una Garantía del equipo pasivo que será de 25 años a partir del recibido conforme.

Cuadro N° 1

Tipo de Garantías sobre las lectoras faciales
Licitación Abreviada No. 2018LA-000006-005870000

Garantía del Equipo Activo	Garantía del Equipo Pasivo
Derecho a Actualización del sistema operativo, que incluya mantenimiento y versiones menores y mayores del software IOS.	La garantía contempla toda la instalación del cableado estructurado efectuado y los materiales y/o equipo pasivo empleados.
b. Derecho a herramientas en línea y recursos de transferencia de conocimiento en la página del fabricante.	Los equipos y todos los productos a utilizar serán nuevos.
c. Acceso a centros de soporte telefónico (TAC): Acceso directo mundial 24x7x365, soporte para la solución de problemas y escalación de problemas críticos.	El contratista se comprometió a suministrar repuestos originales, nuevos y vigentes a partir de la puesta en operación de la solución ofrecida.
d. Reemplazo de partes por adelantados en la modalidad de 8x5x365.	Cualquier inconveniente con el cableado estructurado en relación con conectividad, pérdida de paquetes de datos u otro que sea imputable al cableado deberá ser corregido por el CONTRATISTA sin que esto represente un costo adicional al COSEVI.

Fuente: Contrato N° 0432018001100243-00.

Mediante el Acta de recepción definitiva N° ATI-ATR-2019-004 del 30-04-2019 se otorgó el recibido conforme de dicha contratación por lo tanto las garantías empiezan a regir a partir del día 30-04-2019.

El Sistema de Control de Acceso mediante tecnología IP cuenta con dos herramientas:

- C-Cure es la herramienta que nos sirve para parametrizar horarios, personal y las diferentes autorizaciones que una persona colaboradora pueda tener según el perfil y la asignación que se le brinde por parte de la respectiva jefatura, el sistema se pueden crear eventos determinados con relación a las puertas

- Bio-Star es una herramienta para administrar los dispositivos mediante tecnología IP las lectoras faciales, como permisos de administración, carga de usuarios, carga de lectura biométrica de un usuario.

  Ambas se encuentran implícitamente relacionadas con los dispositivos que se encuentran en cada unidad o departamento.

Aunado a lo anterior se creó un Módulo web de tiempo y asistencia, para poder contar con un control de la entrada y salida de los funcionarios administrados entre el Departamento de Gestión y Desarrollo Humano y la Asesoría en Tecnología de la Información.

2. RESULTADOS DEL ESTUDIO

Ausencia de un Manual sobre el módulo web de tiempo y asistencia mediante tecnología IP

No existe un Manual sobre el módulo web de tiempo y asistencias con el Sistema de Control de Acceso mediante tecnología IP, para que se regule dicha actividad, que se ajuste en cuanto a los requisitos mínimos que se establecen en la “Guía de manuales administrativos” del MIDEPLAN, tal como el diagrama de flujo, glosario de términos, formularios, entre otros y que se contemple como mínimo lo siguiente:

- Sobre los deberes y responsabilidades de los distintos roles establecidos (Colaborador, Jefatura, Recursos Humanos, Director, Súper Usuario).
- Sobre la actividad de control de asistencia mediante el Sistema de Control de Acceso.
- Sobre las acciones en caso de mantenimiento o fallas del equipo.
- Sobre las acciones en caso de modificación (bloquear y habilitar) de accesos a una oficina en el Sistema.
- Sobre los horarios y modificación de los horarios en el Sistema.

- Sobre la creación o bloqueo de accesos al control de la asistencia en la página web (clave y usuario).

Mediante entrevista realizada a la encargada de la Unidad de Control del Departamento de Gestión y Desarrollo Humano, firmada digitalmente el 21-04-2020, indicó lo siguiente:

> *"Se adjunta manuales facilitados por la empresa contratada, sin embargo, debido a los ajustes realizados en el sistema, se deben actualizar."*

En dicha entrevista se adjuntaron tres documentos, que cuentan con un formato de diapositivas que guían al Usuario como acceder al Sistema, sin embargo, no se muestra toda la información básica que debería contener este tipo de documentos o manuales establecidos en la "Guía de manuales administrativos" del MIDEPLAN.

Mediante el Oficio DGDH-2020-0657 del 09-03-2020 el Sr. EEM del Departamento de Gestión y Desarrollo Humano, en conjunto con el Sr. EHA, indicaron que a partir del 10-03-2020, las lectoras biométricas de rostro, son el mecanismo oficial para el registro de la Jornada Laboral, sin contar con un manual o herramienta que apoye dicha gestión, dicho documento cita lo siguiente:

> *"Se les informa que **a partir de mañana 10 de marzo** de los corrientes, el mecanismo oficial para el registro de la jornada laboral (marca de entrada y salida) en las oficinas de la sede central de la Institución, será por medio de las lectoras biométricas de rostro."*
>
> **Nota**: Subrayado y negrita no son del original.

Posterior a las consultas realizadas por esta Auditoría Interna se emite la Circular DGDH-2020-1092 del 07-05-2020, en el cual se realizada un recordatorio y se emiten algunos lineamientos sobre el registro asistencia mediante la lectora facial.

Las inconsistencias descritas, contravienen las siguientes Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), específicamente las que se detallan a continuación:

> *"1.4- Responsabilidad del jerarca y los titulares subordinados sobre el SCI. **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.** (…) d. La vigilancia del cumplimiento, la validez y la suficiencia de todos los controles que integran el SCI."*
>
> *"1.9 Vinculación del SCI con la calidad. El jerarca y los titulares subordinados, según sus competencias, deben promover un compromiso institucional con la calidad y apoyarse en el SCI para propiciar la materialización de ese compromiso en todas las actividades y actuaciones de la*

organización. A los efectos, deben establecer las políticas y las actividades de control pertinentes para gestionar y verificar la calidad de la gestión, para asegurar su conformidad con las necesidades institucionales, a la luz de los objetivos, y con base en un enfoque de mejoramiento continuo."

Nota: El subrayado y la negrita no corresponden al original.

La ausencia de dicho manual, genera que no esté claramente definida, la efectiva intervención de cada una de las partes, afectándose el objeto de este instrumento de control de acceso y asistencia de los funcionarios mediante tecnología IP.

2.1. Ausencia de consentimientos informados

El Consejo de Seguridad Vial, solicitó a cada uno de los funcionarios firmar un documento de consentimiento informado, en amparo en las garantías y obligaciones derivadas de la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 8968, permita que se acceda mediante el sistema adquirido por la Administración, a obtener de su persona la información necesaria a integrarse exclusivamente en una base de datos de único uso institucional, para el acceso de reconocimiento facial y la expedición de tarjetas, para el control de acceso a las dependencias institucionales.

Se determinó que en la Base de Datos de Sistema de Control de Acceso mediante tecnología IP, facilitada por la Asesoría en Tecnología de la Información, existen 384 usuarios registrados al 07-05-2020 y en la Unidad de Control del Departamento de Gestión y Desarrollo Humano solamente cuentan con 328 consentimientos informados (no se determinaron usuarios repetidos en la base de datos).

En la entrevista realizada a la Sra. AGM, de la Unidad de Control del Departamento de Gestión y Desarrollo Humano, firmada digitalmente el 21-04-2020, indicó lo siguiente:

"Mediante oficio ATI-2019-2355 de fecha 22 de julio de 2019 ATI procedió a trasladar a este Departamento los contratos firmados, los cuales mediante Solicitud de Ingreso de Documentos a Expedientes DGDH-2019-2075 fueron ingresados a los expedientes personales de los funcionarios, en total 328 consentimientos."

Por lo tanto, existen 56 funcionarios que están en la base del Sistema de Control de Acceso mediante tecnología IP y la administración no cuenta con el consentimiento firmado para la utilización de sus de datos biométricos o algoritmo matemático de la estructura ósea, incumpliéndose lo que se indica en la Ley No 8968, sobre la

Protección de la persona frente al tratamiento de sus datos personales, que reza en su Artículo No 5, lo siguiente:

> *"ARTÍCULO 5.- Principio de consentimiento informado (…)*
> *2.- Otorgamiento del consentimiento Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. (…) Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos."*

La ausencia de consentimientos se debe a la carencia de mecanismos de control o lineamientos establecidos formalmente por parte de las áreas involucradas (Asesoría en Tecnología de la Información y el Departamento de Gestión y Desarrollo Humano) y una supervisión efectiva, por lo que refleja la falta de organización de la actividad, generándose un debilitamiento del control interno y un incumplimiento normativo.

2.2. Sobre el Manual Integral de Políticas de Seguridad de la Información

El Consejo de Seguridad Vial cuenta con un Manual Integral de Políticas de Seguridad de la Información (Versión No. 1), que fue comunicado a todo el personal, mediante correo electrónico institución del 17-10-2017, como se muestra en la siguiente imagen:

Imagen No 1
Comunicación del Manual Integral de Políticas de Seguridad de la Información

{En el archivado} Manual Integral de Políticas de Seguridad de la Información
Consejo de Seguridad Vial COSEVI 17/10/2017 07:02 a. m.
Para:
cco: [redacted]
Archivar: Este mensaje se está viendo desde el archivado.

Buenos días

El Consejo de Seguridad Vial, se ha caracterizado por ser una Institución que además de buscar la excelencia en sus procesos a fin de brindar servicios de primera calidad a los Administrados, se preocupa por maximizar el rendimiento de todos sus recursos, para así cumplir plenamente tanto con los objetivos propios que se ha trazado, como con las obligaciones que le impone la legislación vigente.

Consecuentemente y en el entendido de que el nivel de seguridad a que se puede aspirar con el uso de la tecnología únicamente, es insuficiente, el COSEVI se dio a la tarea de formular el Manual de Políticas de Seguridad de la Información, el cual además de tener como premisa básica la protección de la información perteneciente a este Consejo y/o en su custodia, constituye realmente la base de la cultura que en materia de seguridad de la información, desea establecer, reforzar, implementar e incorporar en su diario quehacer, con miras no sólo a lograr un manejo eficiente, acorde con el interés público y en estricta concordancia con el ordenamiento jurídico costarricense de sus Recursos Informáticos, sino por sobre todo, a propiciar la eficiencia en las labores y el mejoramiento constante de los servicios que le dan fundamento.

Atentamente

Asesoría en Tecnología de la Información

Manual Integral de Politicas de Seguridad de la Informacion.pdf

Fuente: Correo Electrónico Institucional

En el periodo 2018, fue modificado para generar un Marco Integral de Seguridad y Privacidad de la Información, que guíe y siente las bases para la gestión institucional en la materia. Dicho documento fue aprobado por la Junta Directiva del Consejo con el Oficio No. JD-2018-0497 de la Sesión Ordinaria: 2931-18 del 28-11-2018 que indica lo siguiente:

"Acuerdo: 7.1.1 Se da por recibido el informe de "Políticas de Seguridad de la Información", conforme a las disposiciones de la Contraloría General de la República, con el fin de proteger los recursos de información y las tecnologías utilizadas para su procesamiento frente a las amenazas internas o externas deliberadas o accidentales, con el asegurar el cumplimiento de sus objetivos; integridad, disponibilidad, legalidad y confiabilidad de la información y ***se aprueba el documento Manual de Políticas de Seguridad, las cuales son de acatamiento obligatorio para todos los funcionarios del Cosevi, terceras personas que se involucren con la contratación de bienes y servicios y usuarios de los entes que tengan que ver con la seguridad vial.****"*

Fuente: Oficio JD-2018-0497 del 28-11.2019.
Nota: Subrayado y negrita no son del original.

Sin embargo, dicho documento actualizado no fue <u>debidamente divulgado</u> para acatamiento de todos los funcionarios del Cosevi.

Como se observó en el acuerdo de Junta Directiva se indicó, que el Manual es de acatamiento obligatorio para todos los funcionarios del Cosevi y terceras personas que se involucren con la contratación de bienes y servicios, así como usuarios de los entes que tengan que ver con la seguridad vial, aunado a que no existieron capacitaciones oficiales en el cual se analizara toda la información contenida en este documento.

El Jefe del Área de Seguridad Informática, en la Asesoría en Tecnología de la Información, a la consulta ¿Cuál fue la última capacitación que se desarrolló sobre el Manual Integral de Políticas de Seguridad de la información?, indicó mediante correo electrónico del 04-05-2020, lo siguiente:

"La capacitación general de todo el manual de políticas de seguridad de la información estuvo a cargo del compañero GV de la Unidad de Control Interno la misma se realizó a finales del 2018, ellos le podrían suministrarle el oficio donde se invitó a todo el personal, capsulas informativas y listas de asistencia"

La Jefe de la Unidad de Capacitación del Departamento de Gestión y Desarrollo Humano, indicó mediante correo electrónico del 05-05-2020, lo siguiente:

"Así mismo, la convocatoria para dichas mesas de trabajo se dio mediante Circular de la Dirección Ejecutiva quien nos informa de la realización de las mismas, ya que no fueron capacitaciones reitero, que se efectuaron a todo el personal de COSEVI, ya que en acatamiento a la Resolución DG-165-2017 no se podía establecer una capacitación en tiempo y forma.

Aclarado el hecho de que esto no fue una capacitación, los listados responden a la cantidad de funcionarios que asistieron a las mesas de trabajo de igual manera."

Con lo anterior, se incumplen las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), específicamente en las normas 1.4 y 1.9 anteriormente citadas y las que se detallan a continuación:

*"4.1 Actividades de control. "El Jerarca y los titulares subordinados, según sus competencias, deben diseñar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que **<u>comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SIC y el logro de los objetivos institucionales</u>** (…)"*

"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. **<u>Esa</u>***

***documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación**."*

Nota: Subrayado y negrita no son del original.

La ausencia de una comunicación adecuada de las políticas institucionales, generan que cada una de las partes, no tengan claro cuál es su intervención y se genera un riesgo al no conocer las políticas, afectándose el fortalecimiento de la Seguridad de la Información y el logro de los objetivos institucionales.

2.3. Sobre el nombramiento del Oficial de la Seguridad Administrativa

Se determinó que la Dirección Ejecutiva cambio la persona que funge como Oficial de la Seguridad Administrativa y no se comunicó a toda la Institución, incumpliendo lo establecido en la Ley No. 8968.

Mediante la Circular Institucional No. DE-2019-1649 del 26-06-19, se informó a todo el personal, que la persona responsable de la base de datos y que ocupa el cargo de Oficial de la Seguridad Administrativa (OSA) era el Sr. HRA.

El 02-12-2019, la Dirección Ejecutiva mediante Oficio No. DE-2019-4783, le informó directamente al Sr. HRA, que se deja sin efecto su nombramiento como Oficial de Seguridad Administrativo a partir del 20-12-2019.

Aunado a lo anterior, con el Oficio DE-2019-4785 del 02-12-2019 se informa al Sr. GCR, de la Unidad de Control Interno, que fue designado como Oficial de Seguridad Administrativo a partir del 20-12-2019, dicho documento solo cuenta con copia a Directores del Cosevi, no así a todo el personal.

El Oficial de la Seguridad Administrativa es el responsable de la base de datos en el que se almacena los datos personales de los funcionarios y debe contar con los medios para el ejercicio de sus derechos frente al Sistema de Control de Accesos, Asistencia y Puntualidad mediante Tecnología IP.

Por lo tanto, se incumple lo indicado en la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley No 8968), en su Artículo No. 5 sobre el Principio de consentimiento informado, donde la Administración se ve obligada a informar cuando se solicite datos de carácter personal, la identidad y dirección del responsable de la base de datos según se expone en el inciso h).

Aunado a lo anterior el Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 37554-JP en el Articulo No 4, inciso c) se indica lo siguiente:

> *"(…) 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** (…)"*
>
> **Nota**: Subrayado y negrita no son del original.

La ausencia de una Circular dirigida a todo el personal del Consejo de Seguridad Vial comunicando el nuevo nombramiento del Oficial de Seguridad Administrativo (OSA), refleja el incumplimiento de la Administración en la aplicación de la Ley No 8968 y la falta de interés de los involucrados, generando un riesgo para la Institución e incumplimiento normativo.

2.4. Sobre políticas y procedimientos en la página web del Cosevi

Se determinó que, en la página web del Consejo de Seguridad Vial, existen Políticas y procedimientos para la Gestión Tecnológica, que no cumplen con los requisitos de formalidad de un documento oficial o no son oficiales, ubicados en el apartado de Red Interinstitucional de Transparencia, en la Asesoría en Tecnología de la Información.

2.4.1. Sobre las políticas para la Gestión Tecnológica

Se determinaron 15 políticas para la Gestión Tecnológica que no cuenta con las aprobaciones de las direcciones y aprobación de la Junta Directiva, y fechas correspondientes como vigencia y última actualización, tal y como se muestra a continuación:

Imagen No 2

Política: Privacidad y protección de la Información

cosevi Seguridad Vial

ASESORÍA EN TECNOLOGÍA DE LA INFORMACIÓN
Teléfono: (506) 2257-7280 FAX: (506) 2257-5129 / 2257-5460
Apdo.: 745-1150 La Uruca, SAN JOSÉ, COSTA RICA

Política: Privacidad y protección de la Información	
Código: PL-DTI-006	Fecha de vigencia: dd/mm/aaaa
Versión: 1.0	Fecha de última actualización: dd/mm/aaaa

1. Objetivo

Garantizar la privacidad y proteger la integridad de la información suministrada, creada, adquirida y almacenada por los funcionarios de COSEVI y terceros.

6. Aprobación

6.1 Aprobación y dictamen de conformidad técnica de la DTI

Nombre	Puesto	Firma
	Dirección de TI	

6.2 Aprobación por la Junta Directiva

Acuerdo de aprobación por Junta Directiva	

7. Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión

Fuente: Página web del Consejo de Seguridad Vial

Las políticas que cuentan con estas mismas omisiones, se enlistan a continuación:

Cuadro N° 2

Lista de Políticas en el apartado de
Red Interinstitucional de Transparencia

Políticas para la Gestión Tecnológica	Formalidad	
	SI	NO
PL-DTI-001- Planeación estratégica de TI.		X
PL-DTI-002- Administración de proyectos de TI.		X
PL-DTI-003- Segregación de Funciones y Responsabilidades de TI.		X
PL-DTI-004- Manipulación y Destrucción de Datos		X
PL-DTI-005- Clasificación de la información.		X
PL-DTI-006- Privacidad y Protección de la Información.		**X**
PL-DTI-007- Seguridad de Recurso Humano.		X
PL-DTI-008- Administración de la Capacidad y Disponibilidad.		X
PL-DTI-009- Administración de Cambios y Liberaciones.		X
PL-DTI-010- Administración de Terceros de TI.		X
PL-DTI-011- Administración de la Infraestructura de Software.		X
PL-DTI-012- Administración de la Infraestructura de Hardware.		X
PL-DTI-013- Control de Accesos a los Recursos de TI.		X
PL-DTI-014- Administración de Niveles de Servicio.		X
PL-DTI-015- Administración de Incidentes y Problemas.		X

Fuente: Pagina web del Consejo de Seguridad Vial

2.4.2. Sobre los procedimientos para la Gestión Tecnológica

Existen 14 procedimientos que no están debidamente formalizados (sin la firma digital del encargado del proceso y el visto bueno de la Dirección), se enlistan a continuación

Cuadro N° 3
Lista de Procedimientos en el apartado de
Red Interinstitucional de Transparencia

Procedimientos para la Gestión Tecnológica	Formalidad	
	SI	NO
PRC-DTI-001 Administración de la capacidad.		X
PRC-DTI-002 Administración de Servicios de TI Prestados por Terceros.		X
PRC-DTI-003 Evaluación de Ofertas de TI.		X
PRC-DTI-004 Transferencia Tecnológica.		X
PRC-DTI-005 Administración y Liberación de Cambios.		X
PRC-DTI-006 Administración de Roles de los Sistemas de Información de la DTI.		X
PRC-DTI-007 Administración Cuentas de Usuario.		X
PRC-DTI-008 Administración de la Configuración.		X
PRC-DTI-009 Seguimiento y Monitoreo de la Plataforma Tecnológica.		X
PRC-DTI-010 Creación y control del ambiente de desarrollo y producción.		X
PRC-DTI-011 Mantenimiento y soporte de equipos y dispositivos periféricos.		X
PRC-DTI-012 Respaldos y Recuperación v2.		X
PRC-DTI-013 Administración de Niveles de Servicio.		X
PRC-DTI-014 Atención de Solicitudes Incidentes o Problemas.		X

Fuente: Pagina web del Consejo de Seguridad Vial

Ante las situaciones presentadas se estaría incumpliendo lo establecido en las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), Norma 4.2, Inciso e) antes mencionada y la Norma 4.4 que indican lo siguiente:

*"**4.4 Exigencia de confiabilidad y oportunidad de la información**. El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional, así como que esa información se comunique con la prontitud requerida a las instancias internas y externas respectivas. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas, así como los requisitos indicados en la norma 4.2.*

Lo expuesto refleja la falta de mecanismos de revisión y supervisión sobre el manejo de datos y de documentación oficial, en la página web del Consejo de Seguridad, lo que no provee un sistema de información eficiente.

2.5. Sobre la valoración de riesgos y la identificación de procesos

El Departamento de Gestión y Desarrollo Humano en materia de riesgos, no cuenta aún con un avance en el proceso, que le genere al menos la calificación de los riesgos, sin embargo, si ha incorporado 12 procesos dentro del CSV-02-001 Manual de Procesos del Consejo de Seguridad Vial (cuarta versión aprobada por la Dirección Ejecutiva mediante el Oficio DE-2019-3418 del 12-09-2019, documento que es un insumo para posteriormente realizar la **identificación de los riesgos**.

Cuadro No 4
Clasificación de Procesos en el Departamento de Gestión y Desarrollo Humano

Código del Proceso	Nombre del Proceso
CSV-10-121	Elaboración y seguimiento de acciones de servicio de gestión humana
CSV-10-053	Aprobación de actividades de capacitación
CSV-10-054	Reconocimiento del incentivo de Carrera Profesional
CSV-10-060	Evaluación del Desempeño del Recurso Humano Institucional
CSV-10-055	Revisión, control y pago de Tiempo extraordinario de la institución
CSV-10-072	Elaboración y seguimiento de la nómina salarial institucional
CSV-10-073	Elaboración y análisis de estudios técnicos relativos a material salarial
CSV-10-057	Análisis, inclusión y asesoramiento para la presentación de las declaraciones juradas de bienes ante la Contraloría General de la República.
CSV-10-058	Control de Asistencia institucional.
CSV-10-074	Confección, aprobación y distribución de acciones de personal
CSV-10-075	Gestión de las solicitudes de movimiento de recursos humanos
CSV-10-059	Reclutamiento y Selección de personal

Fuente: Anexo III. Clasificación de Procesos por Área Organizacional (CSV-02-001).

Aunado a que no se ha realizado los ajustes o la nueva ficha de procesos en conjunto con la Asesoría en Tecnología de la información, en donde se tome en cuenta el Módulo web de tiempo y asistencia con el Sistema de Control de Acceso mediante tecnología IP y la administración de la base de datos.

Mediante entrevista realizada a la encargada de la Unidad de Control del Departamento de Gestión y Desarrollo Humano, firmada digitalmente el 21-04-2020, indicó lo siguiente:

"¿Se ha realizado una valoración de riesgos asociado a la utilización del Sistema y la administración de los datos? Ninguna"

Al respecto, el enlace de la Asesoría en Tecnología de la Información en el Área en Telemática y Redes, indicó lo siguiente:

"Se realizó un análisis jurídico de la solución de control de acceso, puntualidad y presencia basada en tecnología IP, a la luz de los requerimientos y principios de la normativa de protección de datos personales costarricense"

Ante dichas ausencias, se contraviene lo estipulado en la Ley General de Control Interno No 8292, que indica lo siguiente:

*"**Artículo No 14.- Valoración del riesgo.** En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:*

a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos

b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.

c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.

d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar. (…)

***Artículo No 19.- Responsabilidad por el funcionamiento del sistema**. El jerarca y los respectivos titulares subordinados de los entes y órganos sujetos a esta Ley, en los que la Contraloría General de la República disponga que debe implementarse el Sistema Específico de Valoración de Riesgo Institucional, adoptarán las medidas necesarias para el adecuado funcionamiento del Sistema y para ubicarse al menos en un nivel de riesgo institucional aceptable."*

Lo anterior se genera ante la inobservancia de la normativa descrita, vulnerándose a la Administración, debido a que podría afectarse la consecución los objetivos planteados, que van de la mano de la misión y visión Institucional.

3. CONCLUSIONES

- El Consejo de Seguridad Vial no cuenta aún con un Manual sobre el Módulo web de tiempo y asistencias con el Sistema de Control de Acceso mediante tecnología IP, en el cual se regule dicha actividad y que cumpla con los requisitos mínimos establecidos por el MIDEPLAN (**Resultado 2.1**).

- Se determinó, que existe una diferencia de 56 consentimientos informados en la Unidad de Control del Departamento de Gestión y Desarrollo Humano con

relación a la Base de Datos de Sistema de Control de Acceso mediante tecnología IP (**Resultado 2.2**).

- El Manual Integral de Políticas de Seguridad de la Información, fue actualizado y aprobado el 28-11-2018, sin embargo, dicho documento nunca fue comunicado a todos los funcionarios del Consejo de Seguridad Vial (**Resultado 2.3**).

- No se hizo partícipe a todo el personal del Consejo de Seguridad Vial, del cambio y nombramiento del nuevo Oficial de Seguridad Administrativo, lo que muestra un incumplimiento por parte de la Administración en la aplicación de la Ley No 8968 (Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales) (**Resultado 2.4**).

- En la página web del Consejo de Seguridad Vial, existen Políticas y procedimientos para la Gestión Tecnológica, que no cumple con los requisitos de formalidad de un documento oficial no cuentan con las debidas aprobaciones (firmas), ubicados en el apartado de Red Interinstitucional de Transparencia, en la Asesoría en Tecnología de la Información (**Resultado 2.5**).

- El Departamento de Gestión y Desarrollo Humano en materia de riesgos, no cuenta aún con un avance en el proceso, que le genere al menos la calificación de los riesgos y aunado a que no se han realizado los ajustes o nueva ficha de procesos en conjunto con la Asesoría en Tecnología de la información, en donde se tome en cuenta el Módulo web de tiempo y asistencia con el Sistema de Control de Acceso mediante tecnología IP y la administración de los datos (**Resultado 2.6**).

4. RECOMENDACIONES

4.1. A la Junta Directiva

A. Girar instrucciones al Director Ejecutivo para que:

A-1 Solicite a la Dirección de Logística, Departamento de Gestión y Desarrollo Humano y la Asesoría en Tecnología de la Información, elaborar un manual o procedimiento que regule la actividad de tiempo y asistencia por medio del módulo web y el Sistema de Control de Acceso mediante

tecnología IP, para que esté debidamente formalizado y publicado para que sea de conocimiento de todo el personal en un corto plazo **(Resultado 2.1-).**

A-2 Solicite a la Dirección de Logística, Departamento de Gestión y Desarrollo Humano y la Asesoría en Tecnología de la Información, una evaluación de quienes cuentan y quienes no cuentan con el Consentimiento Informado para la utilización de sus de datos biométricos o algoritmo matemático de la estructura ósea y sean solicitados para que de ésta manera se cumpla con lo que se indica en la Ley No 8968 y se tomen las medidas para que no se incumpla con dicha Ley **(Resultado 2.2-).**

A-3 Se comunique a todos los funcionarios del Consejo de Seguridad Vial, el Manual Integral de Políticas de Seguridad de la Información actualizado, en acatamiento del Acuerdo 7.1.1 de Junta Directiva de la Sesión Ordinaria: 2931-18 del 28-11-2018 (Oficio No. JD-2018-0497) **(Resultado 2.3-).**

A-4 Sea comunicado a todos los funcionarios del Consejo de Seguridad Vial, de quien es el nuevo Oficial de Seguridad Administrativo, el cual funge como responsable de la base de datos en el que se almacenan los datos personales e indique los medios de comunicación para el ejercicio de sus derechos frente al Sistema de Control de Accesos, Asistencia y Puntualidad mediante Tecnología IP **(Resultado 2.4-).**

A-5 Solicite a la Asesoría en Tecnología de la Información para que en la página Web del Consejo de Seguridad Vial solo se cuente con documentos oficiales y debidamente aprobados, además se realice una revisión de las políticas y procedimientos para la gestión tecnológica que están actualmente para que cumplan con los requisitos de formalidad y confiabilidad de un documento **(Resultado 2.5-).**

A-6 Solicite a la Dirección de Logística, Departamento de Gestión y Desarrollo Humano en conjunto con la Asesoría en Tecnología de la Información, se analice y actualice o genere una nueva ficha de procesos, en donde se tome en cuenta el Módulo web de tiempo y asistencia con el Sistema de Control de Acceso mediante tecnología IP y la administración de la base de datos, para que sea un insumo más en la Valoración de los Riesgos **(Resultado 2.6-).**