SESIÓN ORDINARIA No. 022-2024

Acta de la Sesión Ordinaria número Cero Veintidós dos mil veinticuatro de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, celebrada de manera virtual, mediante la plataforma Microsoft Teams, el martes veintisiete de febrero de dos mil veinticuatro, a las ocho horas y cuatro minutos, con la siguiente asistencia:

- Lic. Jorge Rodríguez Rodríguez, presidente.
- Prof. Errol Pereira Torres, vicepresidente.
- M.Sc. Erick Vega Salas, M.B.A., secretario.
- M.G.P. Seidy Álvarez Bolaños, vocal 1.
- Prof. Ana Isabel Carvajal Montanaro, vocal 2 a.i.
- M.Sc. Hervey Badilla Rojas, vocal 3 a.i.
- M.B.A. Carlos Arias Alvarado, director ejecutivo.

Ausentes con justificación: el M.Sc. José Edgardo Morales Romero, M.B.A., por asuntos personales.

Ausentes sin justificación: no hay.

Invitados: para la discusión del artículo sexto: la Lcda. Marisol Vargas Arias, jefa del Departamento Concesión de Derechos. Para el análisis del artículo sétimo: el M.Sc. Econ. Luis Paulino Gutiérrez Sandí, jefe del Departamento de Inversiones. Para el tratamiento del artículo octavo: el Lic. Diego Vargas Sanabria, jefe del Departamento Legal y el Ing. José Daniel Alpízar Ulloa,

encargado del Área de Seguridad de la Información. Para abordar el artículo décimo: la Lcda. Xinia Wong Solano, auditora Interna.

CAPÍTULO I. AGENDA

El Lic. Jorge Rodríguez Rodríguez, presidente de la Junta Directiva, saluda a las señora y los señores miembros directivos y somete a votación el siguiente orden del día, el cual es aprobado:

ARTÍCULO PRIMERO:

Lectura y aprobación de la agenda.

ARTÍCULO SEGUNDO:

Correspondencia.

ARTÍCULO TERCERO:

Asuntos de los directivos.

ARTÍCULO CUARTO:

Análisis de las actas de Junta Directiva de las sesiones ordinarias Nos. 016 y 017-2024; para resolución final del Cuerpo Colegiado.

ARTÍCULO QUINTO:

Entrega del acta de Junta Directiva de la sesión ordinaria No. 018-2024; para posterior resolución final del Cuerpo Colegiado.

ARTÍCULO SEXTO:

Entrega y análisis del oficio DE-0099-02-2024: aplicación del costo de vida para la población correspondiente de la Ley 2248, propiamente de la Universidad de Costa Rica; para resolución final de la Junta Directiva.

ARTÍCULO SÉTIMO:

Entrega y análisis del acta de la sesión ordinaria No. 03-2023 del Comité de Inversiones; para resolución final de la Junta Directiva.

ARTÍCULO OCTAVO:

Entrega y análisis del acta de la sesión ordinaria No. 010-2023 de la Comisión de Asuntos Jurídicos y Sociales; para resolución final de la Junta Directiva.

ARTÍCULO NOVENO:

Entrega y análisis del oficio SG-P-12-2024 remitido por el Sindicato de Trabajadoras y Trabajadores de la Educación Costarricense (SEC), referente al rechazo de la remoción del M.Sc. José Edgardo Morales Romero; para resolución final de la Junta Directiva.

ARTÍCULO DÉCIMO:

Entrega y análisis de los siguientes estudios de la Auditoría Interna; para resolución final de la Junta Directiva: 1) Estudio No. 44-2023: "Riesgos de seguridad de la información". Oficios AI-1073-12-2023 y AI-1061-12-2023. 2) Estudio No. 45-2023: "Cuentas por pagar proveedores". Oficios AI-1073-12-2023 y AI-1065-12-2023.

ARTÍCULO DÉCIMO PRIMERO:

Mociones.

ARTÍCULO DÉCIMO SEGUNDO:

Asuntos varios.

El **Lic. Jorge Rodríguez Rodríguez** informa: fue necesario agregar el artículo sexto, pues era un tema importante de analizar; sin embargo, no estaba contemplado en la agenda que se les remitió mediante correo electrónico.

El **Prof. Errol Pereira Torres** menciona: hasta ahora se nos está brindando en el orden y quería ver la documentación, pero la Lcda. Ana Lucía Calderón

Calvo, coordinadora de la Unidad Secretarial, lo acaba de enviar; sin embargo, llega hasta ahora y de acuerdo con lo que vaya a salir del análisis sería bueno ver si lo podemos resolver o si se va a dar un primer análisis hoy. Ahora lo veríamos.

El **Lic. Jorge Rodríguez Rodríguez** indica: si le parece, don Errol, vemos el tema y si consideramos que no requiere de mayor análisis, se toma la determinación o el acuerdo que haya que tomar y si es necesario lo volvemos a retomar.

El **Prof. Errol Pereira Torres** externa: sí correcto, en primera instancia era si había documentación, pero ya doña Ana Lucía la envió. Gracias.

El **M.Sc. Hervey Badilla Rojas** señala: para aclarar que la información del tema que se está discutiendo fue entregada en la sesión ordinaria No. 016-2024.

CAPÍTULO II. CORRESPONDENCIA

ARTÍCULO II: Correspondencia.

El **M.Sc. Erick Vega Salas, M.B.A.** lee la siguiente correspondencia la cual se agrega como **anexo No. 1** de esta acta.

Inciso a) Oficio DE-0080-02-2024 remitido por el M.B.A. Carlos Arias Alvarado, director ejecutivo, en el que adjunta el oficio DA-0065-02-2024 que contempla el informe de los activos donados durante el periodo 2023. **SE TOMA NOTA.**

Inciso b) Oficio G.-048-02-2024 suscrito por la Licda. Zianny Morales Guevara, gerente de la Corporación de Servicios Múltiples del Magisterio Nacional, en el que remite los estados financieros de la Corporación, correspondientes a enero de 2024.

El Cuerpo Colegiado conviene remitirlos a la Auditoría Interna, en el plazo de 2 días hábiles, para su análisis y posterior informe a este Cuerpo Colegiado.

Inciso c) Correo electrónico remitido por el M.Sc. José Edgardo Morales Romero, M.B.A., miembro de Junta Directiva, en el que justifica su ausencia a la sesión de hoy, por asuntos personales. **SE TOMA NOTA.**

CAPÍTULO III. ASUNTOS DE LOS DIRECTIVOS

ARTÍCULO III: Asuntos de los Directivos.

Las señoras y señores miembros de la Junta Directiva no presentan asuntos para discusión en esta sesión.

CAPÍTULO IV. ENTREGA Y ANÁLISIS DE ACTAS

ARTÍCULO IV: Análisis de las actas de Junta Directiva de las sesiones ordinarias Nos. 016 y 017-2024; para resolución final del Cuerpo Colegiado.

El **Lic. Jorge Rodríguez Rodríguez** somete a conocimiento y resolución las actas de Junta Directiva correspondientes a las sesiones ordinarias Nos. 016 y 017-2024, las cuales son aprobadas por unanimidad, sin observaciones. **SE TOMA NOTA.**

ARTÍCULO V: Entrega del acta de Junta Directiva de la sesión ordinaria No. 018-2024; para posterior resolución final del Cuerpo Colegiado.

La **Lcda. Ana Lucía Calderón Calvo**, coordinadora de la Unidad Secretarial, remite mediante correo electrónico el acta de Junta Directiva correspondiente a la sesión ordinaria No. 018-2024, para posterior análisis y resolución.

El **Lic. Jorge Rodríguez Rodríguez** indica: esta acta las estaremos analizando en la próxima sesión ordinaria. **SE TOMA NOTA.**

CAPÍTULO V. RESOLUTIVOS

ARTÍCULO VI: Entrega y análisis del oficio DE-0099-02-2024: aplicación del costo de vida para la población correspondiente de la Ley 2248, propiamente de la Universidad de Costa Rica; para resolución final de la Junta Directiva.

Con el aval de la Presidencia se incorpora a la sesión virtual la Lcda. Marisol Vargas Arias, a quien se le brinda una cordial bienvenida.

La **Lcda. Marisol Vargas Arias** expone el oficio DE-0099-02-2024 y sus adjuntos: los oficios JD-US-0042-01-2024, ORH-7437-2023, ORH-7367-2023, la escala salarial administrativa 2021-2023 y la escala salarial docente 2021-2023; que corresponden a la aplicación del costo de vida para la población correspondiente de la Ley 2248, propiamente de la Universidad de Costa Rica. Documentos adjuntos como **anexo No. 2** de esta acta.

Comenta: recordemos que hace unos días habíamos presentado la modificación del tope de catedrático y justamente eso se debió a que la Universidad de Costa Rica (UCR) a finales del año pasado nos comunicó que tenían aumento por costo de vida; entonces, ese aumento lo aplicamos para los pensionados de la Ley 2248 y que la Universidad lo propone escalonado. Mediante el oficio ORH-7367-2023 de fecha 14 de diciembre de 2023, nosotros lo recibimos en enero, lo trabajamos a finales de enero y ahora en febrero se terminó de realizar esa corrida y el incremento que ellos proponen es este y leo lo que indica la nota de la UCR: "*Para los procesos que correspondan, me permito adjuntar las escalas salariales administrativas*

y docentes desde enero de 2021 a la fecha. / Incluyen un incremento salarial del 2.0% para las clases ocupacionales con categoría inferior a 10 y un 1.1% para las clases ocupacionales con categoría igual o superior a 10. Cabe señalar que el incremento salarial para el personal docente corresponde al 1.1%.". De esta manera estamos trabajando con esos 2 porcentajes: el 2% que es para aquellos que tienen una escala salarial inferior a 10 y el 1.1% para los demás y las categorías docentes.

Adiciona: "*Ambos porcentajes se aplican sobre el salario base a diciembre de 2021.",* y es lo que estamos proponiendo en este momento con el acuerdo.

Recordemos el procedimiento para aplicar los costos de vida: en este sentido, ya tenemos la comunicación oficial de la Universidad de Costa Rica, debemos elaborar una resolución, por eso hoy estoy presentando el tema, con este acuerdo ya nosotros procedemos a confeccionar la resolución de Junta Directiva y esa resolución conlleva toda la información de los casos que vamos a pagar y los montos que se van a cancelar. Posteriormente a que ya tengamos la resolución nuestra se la remitimos al Ministerio de Trabajo y Seguridad Social (MTSS), ellos hacen otra resolución dando aprobación a la nuestra y con eso procedemos a realizar el pago. La idea de presentarlo hoy es para que nos dé oportunidad de cancelar el costo de vida en la planilla de marzo, que es la próxima a cancelar. Este costo de vida también lleva períodos fiscales vencidos, entonces, ahí vamos a tener un trabajo similar al que hemos venido realizando desde el año pasado, con el costo de vida de la UCR que habíamos aplicado en diciembre de 2022.

La propuesta de acuerdo indica: "*Propuesta de acuerdo para el ajuste por costos de vida de los pensionados y jubilados de la Universidad de Costa Rica al amparo de la Ley N°2248. / La Junta Directiva de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, con las potestades que le confiere el artículo 29 de la Ley No. 2248, acuerda: Autorizar a la Dirección Ejecutiva, para que proceda con la adecuación de los derechos de pensión o jubilación de la Universidad de Costa Rica, otorgados al amparo de la Ley No. 2248 del 05 de setiembre de 1958; conforme al acuerdo de la Rectoría # R-325-2023 del 07 de diciembre de 2023, que declara el reconocimiento por costo de vida de un incremento salarial del 2% para las clases ocupacionales con categoría inferior a 10 y un 1.1% para las clases ocupacionales con categoría igual o superior a 10. Que el incremento salarial para el personal docente corresponde al 1.1%; calculado sobre el salario base al 31 de diciembre de 2021, aplicación con rige al primero de enero de 2021, lo anterior según comunicado de la Rectoría R-8111-2023 del 12 de diciembre 2023 y de la oficina de Recursos Humanos ORH-7367-2023 del 14 de diciembre 2023 y ORH-7437-2023 del 22 de diciembre de 2023.*".

Como les mencionaba, lleva períodos fiscales vencidos porque el rige que le están dando es a enero de 2021, tendríamos que cancelar por períodos fiscales vencidos el 2021, 2022 y 2023, son 3 años retroactivos, entonces, tendríamos que coordinar para repetir el proceso que actualmente estamos haciendo con el que pagamos en diciembre de 2022 y que a la fecha hemos logrado cancelar casi el 50%, pero todavía falta un poco.

En resumen, esta es la propuesta de acuerdo para cancelar el costo de vida de estos pensionados al amparo de la Ley 2248, que repito, son únicamente aquellos de la Universidad de Costa Rica.

El **Lic. Jorge Rodríguez Rodríguez** consulta: ¿el tema fue bien revisado?, estamos aprobando algo que corresponde a dinero, a un aumento, entonces, me parece que estos temas siempre son de mucho cuidado por la responsabilidad que nos implica como directores aprobar. Quisiera consultarle si, de acuerdo con la normativa ¿todo fue revisado con cuidado?, para aprobarlo con tranquilidad.

La **Lcda. Marisol Vargas Arias** responde: claro que sí, es parte de la responsabilidad que tenemos en el Departamento Concesión de Derechos, nosotros trabajamos con dinero, incluso, otorgar un derecho de pensión estamos manejando plata, por eso en ocasiones que se discuten los perfiles de puesto, cuando me indican en el Departamento Gestión de Talento Humano que nosotros no manejamos plata, pienso que asemejan la plata con los cajeros que están ahí con los billetes y usted los puede ver; todo lo que es otorgamiento de derechos, pago de períodos fiscales vencidos, pago de estos costos de vida que es la materia que manejamos en la Unidad de Pagos y Revaloraciones del Derecho, todo esto implica dinero.

Un dato importante que creo no les di: son 2.948 personas y este pago que se les realiza en marzo da un total de ¢135.883.338,00, esto sin tomar en cuenta el retroactivo. Don Jorge, esto lo realizamos por medio de un sistema, el sistema de costo de vida, porque no es tan sencillo como cuando aplicamos la Ley 7531, que es nada más tomar el monto de pensión y aplicarle 1.1% o 2%, sino que este costo de vida toma en cuenta los componentes salariales. A nivel de sistema ya está estructurada una aplicación que nos permite realizar estos costos de vida. Por supuesto que sí, si aquí hay fallo, le aseguro que soy la primera que me voy.

El **Lic. Jorge Rodríguez Rodríguez** menciona: uno sabe que no solo es dinero, es mucho dinero. En buena hora que estos procesos se llevan a cabo para una justicia salarial, uno se alegra cuando se puede aprobar para los compañeros que representamos en alguna medida una equiparación salarial, alguna revaloración, este tipo de temas. Efectivamente son de mucho cuidado y de mucha responsabilidad; le agradecemos que ampliara un poco en ese sentido.

La **Lcda. Marisol Vargas Arias** indica: esto es parte del procedimiento que nosotros realizamos, lo que sucede es que como en los últimos años no han decretado aumentos por costo de vida, solamente con la Ley 7531, no lo tenemos como algo tan rutinario, pero para el Departamento Concesión de Derechos, lo que fue antes del 2020 aplicamos todos los demás, lo que decretaba las universidades, cada vez que ellos tienen aumentos, nosotros también lo aplicamos. Adicionalmente, sobre esto hay estudios de la Auditoría Interna. ¿Cuáles son las observaciones que nos salen en los estudios de la Auditoría Interna con respecto a pagos de costo de vida?, por ejemplo, que en ocasiones se quedan casos sin cancelar ese costo de vida porque a nivel de sistema están registrados con una Ley que no corresponde, por decir algo, un caso que sea 2248 pero que a nivel de sistema, por error, cuando llega la resolución del Ministerio de Trabajo se incluya con una Ley 7268 o 7531; esos son los casos que posteriormente tenemos que hacerles un estudio integral para cancelarles los costos de vida. También me parece importante acotar eso, que cuando la Auditoría nos ha realizado estudios sobre las aplicaciones de costo de vida en realidad las observaciones que nos han hecho son muy pequeñas, casos aislados como estos que les comentaba que se quedan sin aplicar, pero

nunca nos ha realizado una observación de que pagamos un porcentaje que no era el correcto o que le pagamos a una población que no correspondía; esa parte es un proceso que nosotros ya lo tenemos bastante dominado por decirlo de esa manera, porque son muchísimos los años realizando estos pagos.

Analizada la propuesta, las señoras y señores miembros de la Junta Directiva por unanimidad adoptan el siguiente acuerdo:

ACUERDO No. 1

"La Junta Directiva de la Junta de Pensiones y Jubilaciones del Magisterio Nacional, con las potestades que le confiere el artículo 29 de la Ley No. 2248, acuerda: Autorizar a la Dirección Ejecutiva, para que proceda con la adecuación de los derechos de pensión o jubilación de la Universidad de Costa Rica, otorgados al amparo de la Ley No. 2248 del 05 de setiembre de 1958; conforme al acuerdo de la Rectoría # R-325-2023 del 07 de diciembre de 2023, que declara el reconocimiento por costo de vida de un incremento salarial del 2% para las clases ocupacionales con categoría inferior a 10 y un 1.1% para las clases ocupacionales con categoría igual o superior a 10. Que el incremento salarial para el personal docente corresponde al 1.1%; calculado sobre el salario base al 31 de diciembre de 2021, aplicación con rige al primero de enero de 2021, lo anterior según comunicado de la Rectoría R-8111-2023 del 12 de diciembre 2023 y de la oficina de Recursos Humanos ORH-7367-2023 del 14 de

diciembre 2023 y ORH-7437-2023 del 22 de diciembre de 2023". Acuerdo unánime y en firme con seis votos.

Se le agradece la participación a la Lcda. Marisol Vargas Arias, quien abandona la sesión virtual.

ARTÍCULO VII: Entrega y análisis del acta de la sesión ordinaria No. 03-2023 del Comité de Inversiones; para resolución final de la Junta Directiva.

Con el aval de la Presidencia se incorpora a la sesión virtual el M.Sc. Econ. Luis Paulino Gutiérrez Sandí, a quien se le brinda una cordial bienvenida.

El **M.Sc. Econ. Luis Paulino Gutiérrez Sandí** expone el oficio COM-INV-0003-02-2024 que contempla el acta de la sesión ordinaria No. 03-2023 del Comité de Inversiones. **Anexo No. 3** de esta acta.

Refiere: en el artículo segundo se analizó la presentación de los resultados de las inversiones en el mercado de valores internacionales con corte a enero del 2024, realizada por la empresa Creación de Capitales. Un poco de datos más actualizados a hoy: el portafolio de mercado internacional equivale a US$215 millones, ese es el monto registrado a ayer y presentamos plusvalías de US$15.6 millones, esas plusvalías son ganancias no ejecutadas dado que no se están vendiendo los títulos, pero sí aportan al rendimiento lo cual es importante para nosotros. El portafolio continúa en crecimiento con resultados positivos como las plusvalías y los rendimientos de las inversiones que se están haciendo. Para los próximos días estaremos viendo nuevos productos para aprobación, que son los instrumentos ETF's y Fondos Mutuos que tienen la característica de estar relacionados con criterios ambientales, sociales y de gobernanza, estos productos serían incorporados dentro del

portafolio para agregar diversificación y rendimiento, así como estar ligados al tema de la nueva tendencia de inversiones.

Discutida el acta, el Órgano Colegiado por unanimidad adopta el siguiente acuerdo:

ACUERDO No. 2

"Expuesta el acta de la sesión ordinaria No. 003-2024 del Comité de Inversiones, la Junta Directiva acuerda: Aprobarla y dar por conocida la presentación de los resultados de las inversiones en el mercado de valores internacional con corte a enero del 2024, realizada por la empresa Creación de Capitales". Acuerdo unánime y en firme con seis votos.

Se le agradece la participación al M.Sc. Econ. Luis Paulino Gutiérrez Sandí, quien abandona la sesión virtual.

ARTÍCULO VIII: Entrega y análisis del acta de la sesión ordinaria No. 010-2023 de la Comisión de Asuntos Jurídicos y Sociales; para resolución final de la Junta Directiva.

Con el aval de la Presidencia se incorporan a la sesión virtual el Lic. Diego Vargas Sanabria y el Ing. José Daniel Alpízar Ulloa, a quienes se les brinda una cordial bienvenida.

El **Lic. Diego Vargas Sanabria** inicia con la exposición del oficio COM-AJS-01-01-2024 que contempla el acta de la sesión ordinaria No. 10-2023 de la Comisión de Asuntos Jurídicos y Sociales y el cuadro comparativo titulado: "Reglamento Organización y Funcionamiento", adjuntos como **Anexo No. 4** de esta acta.

Explica: en esta sesión se vieron varios aspectos, entre ellos: el Reglamento de Organización y Funcionamiento, la propuesta de modificación de la Política Marco de Gestión de Seguridad de la Información y la propuesta de modificación de la Política de Seguridad de la Información y Ciberseguridad Institucional.

En cuanto al artículo segundo: "Propuesta de modificación del Reglamento General de Organización y Funcionamiento. Publicación del Diario Oficial La Gaceta No. 201 del 31 de octubre del 2023. Ley 10379. Modificación de la Ley 6227, Ley General de la Administración Pública del 02 de mayo de 1978. Autorización para la celebración de sesiones virtuales a los órganos colegiados de la administración pública."; recordemos que la Junta Directiva podía sesionar virtualmente, pero eso era por una interpretación efectuada por la Procuraduría General de la República; sin embargo, mediante la Ley 10.379 se aprobó autorizar a los Órganos Colegiados a realizar las sesiones ordinarias de esa manera y por se incorpora el último párrafo del artículo No. 18, que precisamente es una traducción o una copia de lo que se establece en la Ley y dice: "*La Junta Directiva, las comisiones y en general cualquier director, podrá sesionar de forma virtual por medio de videoconferencia o cualquier otra tecnología de información idónea para garantizar la simultaneidad, colegialidad, seguridad, autenticidad, integridad y deliberación. / Las sesiones virtuales deben celebrarse sin interrupciones técnicas que afecten el curso ordinario de las discusiones. El miembro de Junta Directiva debe permanecer durante toda la sesión conectado con audio y video. Debe consignarse en actas el nombre del medio tecnológico utilizado para la conducción de la sesión. En las sesiones virtuales se deberá respetar la prohibición de superposición horaria de los*

directores.". Básicamente, repito, lo que se hace mediante este estudio es actualizar la disposición ajustándola a la nueva legislación, de modo que se puedan hacer las sesiones virtuales de manera permanente, común, que era todo lo contrario, era la excepción.

A partir de ahí empezamos con el artículo tercero, que es la "Propuesta de modificación de la Política Marco de Gestión de Seguridad de la Información.", de manera que le cedo la palabra al Ing. José Daniel Alpízar Ulloa, para que les comente los cambios que se están suscitando.

El **Ing. José Daniel Alpízar Ulloa** expone el cuadro comparativo titulado: "P31-RP-002. Política Marco de Gestión de Seguridad de la Información", el cual forma parte del **anexo No. 4** de esta acta.

Señala: efectivamente el Área de Seguridad de la Información realizó cambios en 2 políticas, una de ellas es la Política Marco de Gestión de Seguridad de la Información, que son las pautas o las reglas que el Área de Seguridad de la Información sigue para garantizar que la seguridad de la información se esté llevando a cabo de la mejor manera. Hicimos una actualización de este Marco empezando por la corrección del Código que, si recuerdan hace unos 2 años el Área de Seguridad de la Información dejó de pertenecer al Departamento Tecnología de Información (TI) y pasó a ser un Área independiente, por tanto, nos corresponde un código independiente que no sea de TI, entonces, a partir de ahí realizamos esa actualización, pasamos de "*P17-RP-ISM-11. Política de Gestión de Seguridad de la Información.*", a "*P31-RP-002. Política Marco de Gestión de Seguridad de la Información.*".

Muchas de las actualizaciones que hicimos son meramente de forma, para ajustar al nuevo Marco, en este como tal fueron muy pocas cosas las que se agregaron o las que se corrigieron en el sentido del formato como tal.

En el punto 2 "Alcance del documento", se modifica el último párrafo que indicaba: *"Este sistema es aplicable a todos los trabajadores, miembros de Junta Directiva, consultores, proveedores, terceras partes, que usen y tengan acceso a activos de información que sean propiedad de JUPEMA."*, la redacción propuesta es la siguiente: *"Este sistema es aplicable a todos los trabajadores del área de seguridad de la información, y partes que participen en el sistema de gestión de seguridad de la información."*; vuelvo al mismo punto, el Marco de Gestión de Seguridad de la Información es algo con lo que se mide el Área nada más, no aplica tanto para el resto de la organización.

En el punto 3 "Definiciones" agregamos el término de: "*SGSI: Sistema de Gestión de Seguridad de la Información.*".

En el punto 4 "Documentos de referencia / aplicables", eliminamos el "*EX-026 COBIT V5 (Objetivos de Control para la información y Tecnologías relacionadas).*", que si no me equivoco los compañeros de la Unidad de Gestión y Control de la Calidad removieron este documento de las referencias.

En el punto 5 "Descripción"; antes decía: "*A través de este documento se expresa formalmente las decisiones de la Junta con relación al tratamiento de los riesgos que se realizará en respuesta al análisis de riesgos y diagnóstico de conformidad con la norma ISO 27002:2013.*", la redacción propuesta es la siguiente: "*5.1. Declaración de aplicabilidad. / A través de este documento se expresa formalmente las decisiones de JUPEMA con relación*

al tratamiento de los riesgos que se realizará en respuesta al análisis de riesgos y diagnóstico de conformidad con la norma ISO 27002."; se cambia la palabra "*la Junta*", por "*JUPEMA*", para aclarar que es la organización, si dejamos "la Junta" podría confundirse si es la Junta Directiva o de qué estábamos hablando. También eliminamos el año de la ISO 27002 que se usa y solo dejamos la referencia de la ISO 27002, porque esto se puede estar actualizando año con año y para no estar actualizando la Política todos los años, mejor dejamos el marco general.

Por otra parte, unimos los puntos Nos. 5 y 6, de manera que los nuevos incisos del punto 5 son los siguientes: "*5.2 Marco de Referencia -Sistema de Gestión de Seguridad de la Información – SGSI. / 5.2.1. Seguridad de la Información / La seguridad de la información es la preservación de los pilares básicos de la confidencialidad, integridad y disponibilidad de esta y de los sistemas implicados en su tratamiento. Estos tres pilares se definen como: / Confidencialidad: Acceso a la información por parte, únicamente, de quienes estén autorizados. / Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. / Disponibilidad: Acceso a la información y los sistemas de tratamiento de esta por parte de los usuarios autorizados cuando lo requieran. / En la seguridad de la información, no solo intervienen los aspectos tecnológicos, sino también los procesos, los ambientes (centro de cómputo, ubicación de oficinas) y principalmente las personas.*".

Adicionalmente, como una observación de la Auditoría Interna, agregamos el contexto de la organización, de manera que se adiciona: "*5.2.2. Contexto de la Organización. / 5.2.2.1. Descripción de la Organización: / La Junta de Pensiones y Jubilaciones del Magisterio Nacional (JUPEMA) es un ente*

público no estatal, con personería jurídica y patrimonio propio. Como tal, está sujeta a las normas de la ley que la rigen, así como al ordenamiento jurídico administrativos públicos y particularmente a la fiscalización de la Superintendencia de Pensiones. / Le corresponde a la Junta de Pensiones tramitar y otorgar los derechos de pensión y jubilación del Régimen Transitorio de Reparto (RTR) bajo la supervisión y control de la Dirección Nacional de Pensiones del Ministerio de Trabajo. La administración financiera y pago de las pensiones del RTR corre a cargo del Estado. / A diferencia de lo anterior, a la Junta le compete la administración financiera, actuarial y legal del Régimen de Capitalización Colectiva (RCC) creado al amparo de la Ley 7302 y al que pertenecen todos aquellos trabajadores que empezaron a laborar por primera vez en educación a partir del 15 de julio de 1992. / 5.2.2.2. Naturaleza de la Organización: / JUPEMA es una organización publica no estatal de gran envergadura con múltiples áreas de negocio. Su función principal es el otorgamiento de las pensiones al sector magisterial de Costa Rica. También tiene otras áreas de negocio como el otorgamiento de créditos a los afiliados, así como también inversiones en el mercado tanto a nivel nacional como internacional. / Procesa grandes volúmenes de transacciones financieras en línea y fuera de línea, almacena datos confidenciales de los afiliados y realiza operaciones críticas en los sistemas de información. / 5.2.2.3. Objetivos y Estrategias: / El principal objetivo de JUPEMA es la gestión eficiente del fondo de pensiones de nuestros afiliados del sector magisterial para mejorar su calidad de vida mediante una administración sostenible e innovadora, manteniendo la confianza de los afiliados cumpliendo con las regulaciones existentes y garantizar la continuidad de la gestión de JUPEMA. / Su estrategia se basa en la creación,

mejoramiento y expansión de los servicios en cuanto a sostenibilidad financiera, grupos de interés, procesos internos y aprendizaje y crecimiento, según lo establecido en el Plan Estratégico de JUPEMA. / 5.2.2.4. Partes interesadas: / Las partes interesadas incluyen a: / Afiliados. / Empleados. / Miembros de Junta Directiva. / Superintendencia de Pensiones. / Socios Comerciales. / Proveedores de bienes y servicios. / 5.2.2.5. Requisitos Legales y Regulatorios / JUPEMA está sujeta a una gran variedad de leyes y regulaciones del ámbito de pensiones, como la Ley No. 8968 de protección de la persona frente al tratamiento de sus datos personales, regulaciones y normativas específicas para el sector de pensiones. / Debe cumplir con los requisitos regulatorios nombrados por la Superintendencia de Pensiones, basados en las mejores prácticas de administración, tecnologías de información y seguridad de la información. / 5.2.2.6. Recursos y tecnología. / JUPEMA cuenta con un área de seguridad de la información dedicado a la implementación, monitoreo y mejora continua de la seguridad de la información y la ciberseguridad. / Cuenta con los recursos financieros para invertir en la implementación de controles y medidas de seguridad de la información y ciberseguridad. / Utiliza tecnología avanzada, incluyendo sistemas de seguridad de red, sistemas de detección y prevención de intrusos, entre otros controles especialmente dedicados a la seguridad de la información y la ciberseguridad.". Esto es todo lo relacionado al contexto de la organización, es nuevo, lo tuvimos que agregar y lo tomamos de diferente documentación que encontramos propia de JUPEMA, entonces, de ahí fue donde especificamos el contexto de la organización.

En el punto 5.2.3 "Sistema de Gestión de la Seguridad de la Información" hay unas pequeñas modificaciones más que todo de contexto, para que se lea

como sigue: "*El SGSI es un Sistema de Gestión de la Seguridad de la Información o ISMS por sus siglas en inglés (Information Security Management System), consiste en una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad. / Su propósito es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.*".

En el punto 5.2.4. "Beneficios de la implementación del Sistema de Gestión de Seguridad de la Información", aquí eliminamos las siglas "SGSI" y anotamos el nombre completo para mejor entendimiento. En el primer y segundo párrafo sustituimos la palabra "*implantar*" por "*implementar*", que nos parece va más acorde con el texto, para que se lea como sigue: "*Aplica una arquitectura de Gestión de la Seguridad que identifica y evalúa los riesgos que afectan a la institución, con el objetivo de implementar contramedidas, procesos y procedimientos para su apropiado control, tratamiento y mejora continua. / Ayuda a la institución a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implementar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de*

procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad de la gestión de JUPEMA.".

En el punto 5.2.5. "Justificación de la implementación del Sistema de Gestión de Seguridad de la Información", nuevamente anotamos el nombre completo del Sistema y se sustituye la palabra "*hacking*" por "*hackeo*".

En el punto 5.3 "Componentes principales del Sistema de Gestión de Seguridad de la Información", en los incisos de "*alcance*" y "*procedimientos*" igualmente se eliminan las siglas SGSI y se anota el nombre completo.

En el punto 5.4 "Sistema de gestión de seguridad de la información de JUPEMA", inciso 5.4.1. se agrega "*(…) Sistema de Gestión de Seguridad de la Información*", para que se lea: "*Alcance y límites del Sistema de Gestión de Seguridad de la Información.*". Adicionalmente se agrega el texto: "*(…) Régimen de Capitalización Colectiva del Magisterio (RCC)*", para que se lea: "*Le corresponde a JUPEMA tramitar y otorgar los derechos de pensión y Jubilación del Régimen Transitorio de Reparto (RTR) bajo la supervisión y control de la Dirección Nacional de Pensiones del Ministerio de Trabajo. Por otra parte, le compete la administración financiera, actuarial y legal del Régimen de Capitalización Colectiva (RCC), creado al amparo de la EX-049 Ley 7302 Régimen de Capitalización Colectiva del Magisterio (RCC), al que pertenecen todos aquellos trabajadores que empezaron a laborar por primera vez en educación a partir del 15 de julio de 1992.*".

En el último párrafo se sustituye la palabra "*implantar*" por "*implementar*", para que se lea como sigue: "*El responsable de implementar y mantener el Sistema de Gestión de Seguridad de la información es el Ingeniero de Seguridad Información, encargado del área de Seguridad de Información,*

los recursos y presupuesto asignado a esta área están bajo la gestión de la Dirección Ejecutiva.".

En el punto 5.4.2. "Objetivos del Sistema", se agrega: "*Objetivos del Sistema de gestión de seguridad de la información.".*

En el punto 5.4.4. "Políticas de seguridad de la información", actualizamos los códigos de los documentos, para que se consigne: "*Las políticas y lineamientos en materia de seguridad de la Información de JUPEMA se encuentran contempladas en el documento: P31-RP-001 Políticas de Seguridad de la Información Institucional.".* En el siguiente párrafo se sustituye "de la Unidad" por "del área", para que se lea: "*Al menos una vez al año el encargado del área de Seguridad de Información debe revisarlas y proponer los ajustes que correspondan alineados a la estructura, iniciativas y objetivos estratégicos de la institución.".*

En el punto 5.4.5. "Procedimientos e instructivos que soportan el SGSI", se elimina "*SGSI*" y se anota el nombre completo "*Sistema de Gestión de Seguridad de la Información.".*

En el punto 5.4.6. "Metodología de evaluación de riesgos", se cambia el "*responsable de la Unidad*" por "*encargado del área*". Además, se agrega el párrafo: "*(…) tomando como marco de gestión la ISO 27002 y los controles establecidos en dicho marco de gestión*", para que indique: "*En esta etapa el encargado del área de Seguridad de Información debe realizar una evaluación y revisión de los riesgos, tomando como marco de gestión la ISO 27002 y los controles establecidos en dicho marco de gestión, realizar la propuesta de recomendaciones y controles necesarios, para presentarlo al Comité Estratégico de TI y/o a la Dirección Ejecutiva, cuando corresponda.".*

En el punto 5.4.7. "Informes de seguimiento", se elimina la referencia porque traía como una ubicación en una carpeta compartida, señalaba: *"El formulario para registrar la evidencia necesaria es el P17-FO-ISM-47 Monitoreo de Seguridad. Estos registros son almacenados en la carpeta compartida de Informática_Seguridad_Información /Monitoreo_Seguridad ubicada en el servidor SP-SRVVWDFS03 o servidor de archivos establecido."*, en su lugar se anota: *"El formulario para registrar la evidencia necesaria es el P31-FO-003 Monitoreo de Seguridad."*, esto está publicado en la intranet.

En el punto "5.5.1. Planificación de la gestión del riesgo de la seguridad", se mejora la redacción del último párrafo, para que se lea como sigue: *"Al final de cada año, el encargado del área de seguridad de Información debe realizar un Plan de Trabajo de forma anual, que debe estar firmado por la Dirección Ejecutiva; en el cual debe contemplar la verificación de lo establecido en el procedimiento P31-PR-001 Monitoreo y Seguimiento a cargo del Ingeniero en Seguridad Información, los controles recomendados e implementados por la institución alineado al plan estratégico de TI y el Plan Estratégico Institucional así como el cumplimiento de la normativa en materia de Seguridad de Información."*.

En el punto 5.5.2. se sustituye la palabra *"Implantación"* por *"Implementación"*, para que se consigne: *"Implementación de la gestión del riesgo de la seguridad"*.

En el punto 5.5.3. "Seguimiento de la gestión del riesgo de la seguridad", se sustituye la palabra "implantados" por "implementados", para que se lea de la siguiente manera: *"En esta fase se evalúa la eficacia y el éxito de los controles implementados. Por ello, es muy importante contar con informes que serán dirigidos a la Jefatura de departamento. La cual analizará y*

atenderá las recomendaciones propuestas, así como la prioridad requerida según los resultados de la verificación o revisión.". En el penúltimo párrafo se elimina la periodicidad de "al menos una vez al mes", porque no era necesario especificarla, para que se lea: *"Se debe realizar una reunión de seguimiento con la Jefatura inmediata e informar al Comité Técnico de TI y/o Comité Estratégico de TI cuando corresponda. Con el propósito de analizar y dar seguimiento de los pendientes que se tienen en materia de seguridad, según las recomendaciones e informes que se hayan entregado.".* En el último párrafo se sustituye "de la Unidad" por "del área", para que se consigne: *"El responsable del área de seguridad de Información dará seguimiento y actualizará el informe con las acciones tomadas por la institución. Y presentará un informe de avance al Comité Técnico de TI y/o Comité Estratégico de TI según corresponda, con las acciones realizadas.".*

En el punto 5.5.4. "Mejora de la gestión del riesgo de la seguridad", se incorpora el texto *"(…) de gestión de seguridad de la información"*, para que indique: *"En la fase de mejora se lleva a cabo las labores de mantenimiento del sistema de gestión de seguridad de la información. Si durante la fase anterior de seguimiento se ha detectado algún punto débil, este es el momento de mejorarlo o corregirlo.".*

En el punto 5.6. "Organización de la seguridad", en el segundo párrafo se agrega: *"(…) gestión de seguridad de la información",* para que se lea: *"El Comité Estratégico de TI o la Dirección Ejecutiva en su defecto tendrá las máximas responsabilidades y aprobará las decisiones de alto nivel relativas al sistema de gestión de seguridad de la información.";* esas son cosas que estuvimos agregando para que se especificara y para que se leyera de

mejor manera, tanto en organización de la seguridad, como en el manejo de la gestión de riesgo.

En el punto 5.7. "Concientización y divulgación", se elimina el último párrafo que indicaba: *"El Ingeniero en Seguridad Información debe informar y divulgar de forma periódica, con una regularidad de al menos una vez por mes, temas de seguridad a toda la población de JUPEMA. Utilizando los medios necesarios y disponibles para tal fin."*, y se agrega: *"5.7.3. El área de Seguridad Información debe informar y divulgar de forma periódica, temas de seguridad a toda la población de JUPEMA, utilizando los medios necesarios y disponibles para tal fin."*; esto porque no es una tarea exclusiva mía, sino que el asistente también ayuda bastante con esto, entonces, lo pusimos de manera general como que fuera el Área.

Básicamente estos son los cambios que se realizaron al Marco de Gestión de Seguridad de la Información.

El **Lic. Diego Vargas Sanabria** destaca: después de este, si no tienen observaciones, pasaríamos al artículo cuarto del acta, donde vimos la modificación de la "Política de Seguridad de la Información".

El **Ing. José Daniel Alpízar Ulloa** continúa con la exposición del cuadro comparativo titulado: "P31-RP-001. Política de Seguridad de la Información y Ciberseguridad Institucional", el cual forma parte del **anexo No. 4** de esta acta.

Refiere: nuevamente aquí tenemos un cambio en la nomenclatura, antes le pertenecía al Departamento Tecnología de Información, ahora nos pertenece a nosotros, por así decirlo. Anteriormente decía: *"P17-RP-ISM-01. Política de Seguridad de la Información Institucional"*, la propuesta es: *"P31-RP-001. Política de Seguridad de la Información y Ciberseguridad*

Institucional", es de acatamiento para todos los colaboradores de JUPEMA. Algo muy importante que quisimos agregar, que también es para cumplimiento de Auditorías Internas y Externas, es que le estamos incluyendo el concepto de ciberseguridad, no nos estamos quedando solo en el concepto de seguridad de la Información, sino que le estamos agregando el concepto de ciberseguridad. Adelantándome un poco, todo esto de acuerdo con el cambio de Reglamento del Consejo Nacional de Supervisión del Sistema Financiero (Conassif), que va a pasar de 5-17 a 5-24, inclusive, nos estamos adelantando y vamos a empezar a hacer cumplimiento de ciertas normativas que tienen ellos, al empezar tocar temas de ciberseguridad en nuestras políticas y documentos.

A partir de aquí empezamos a agregar la palabra "ciberseguridad" en varios momentos del documento.

En el punto No. 1 "Propósito" anteriormente indicaba: "*Proveer una guía general sobre las conductas que se esperan del personal usuario en materia de seguridad de la información. / Alertar al personal usuario sobre los riesgos de seguridad y las medidas a tomar para manejar tales riesgos. / Clarificar la responsabilidad y los deberes sobre la protección de los recursos informáticos. / Guiar al personal usuario en cuanto a la toma de decisiones con respecto a la protección de los sistemas de información. / Sensibilizar al personal usuario sobre su papel activo en la estructura de seguridad de la información.*".

La propuesta es la siguiente: "*Proveer una guía general sobre las conductas que se esperan del usuario en materia de seguridad de la información y ciberseguridad. / Alertar a los usuarios sobre los riesgos de seguridad de la información y ciberseguridad, y las medidas a tomar para manejar tales*

riesgos. / Clarificar la responsabilidad y los deberes sobre la protección de los recursos de información que tiene cada uno de los usuarios de JUPEMA. / Guiar a los usuarios en cuanto a la toma de decisiones con respecto a la protección de los sistemas de información. / Sensibilizar a los usuarios sobre su papel activo en la estructura de seguridad de la información y ciberseguridad.".

En el punto 2 "Alcance", se modificó la redacción que decía: "*Las políticas de seguridad de la información Institucional son de carácter obligatorio y deben ser aplicadas sin excepción, por todo el personal de la Institución. / Este documento está fundamentado principalmente en el estándar internacional ISO/IEC 27002:2013 (en lo que a la Institución le es aplicable), y busca fortalecer una cultura en materia de seguridad de la información, donde cada usuario de los recursos informáticos sea elemento activo en la consolidación de la estructura de seguridad de la Institución. / Las políticas de seguridad de la Información Institucional procuran proteger toda la información de interés para la Institución y las personas u organizaciones a las que ésta brinda servicios: (…)".*

La redacción propuesta señala: "*Las políticas de seguridad de la información y ciberseguridad Institucional son de carácter obligatorio y deben ser aplicadas sin excepción, por todos los usuarios de la Institución. / Este documento está fundamentado principalmente en el estándar internacional ISO/IEC 27002 (en lo que a la Institución le es aplicable), y busca fortalecer una cultura en materia de seguridad de la información, donde cada usuario de los recursos de información sea elemento activo en la consolidación de la estructura de seguridad de la Institución.*"; los recursos de información pueden ser informáticos, como no informáticos. / "*Las*

políticas de seguridad de la Información y ciberseguridad Institucional procuran proteger toda la información de interés para la Institución y las personas u organizaciones a las que ésta brinda servicios: (…)", todos estos temas tienen que ver con la ciberseguridad, pues tocamos temas digitales.

El marco legal se eliminó porque el formato del documento cambió, entonces, la Unidad de Gestión y Control de la Calidad eliminó esa sección, pues esto viene en los documentos de referencia, de manera que el punto No. 4 ya no es "Marco Legal", sino que es "Descripción" y cambia la numeración de todo el documento.

En el punto 4 "Descripción" se modifica: en el punto 4.1. se agrega "*Información y ciberseguridad*" para que se lea "*Política Institucional de Seguridad de la Información y ciberseguridad*".

En el punto 4.1.1. al final le adicionamos "*(…) y las mejores prácticas en Ciberseguridad*", para que se lea de la siguiente manera: "*En JUPEMA la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad y las mejores prácticas en Ciberseguridad*".

En el punto 4.1.2., 4.1.3., 4.2 y 4.2.1. se agrega la palabra "*ciberseguridad*", para que se consigne: "*4.1.2. Consciente de sus necesidades actuales, JUPEMA implementa un modelo de gestión de seguridad de la información y ciberseguridad como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y*

garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes. / 4.1.3. El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y ciberseguridad, de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en JUPEMA; este proceso es liderado de manera permanente por el Ingeniero en Seguridad Información.".

"4.2. Política Generales de Seguridad de la Información y Ciberseguridad. / 4.2.1. JUPEMA ha establecido las siguientes Políticas Generales de Seguridad de la Información y ciberseguridad, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información".

En el punto 4.2.1.1. se cambia el número de guía, de manera que la redacción propuesta es: *"El Comité Estratégico de TI (P01-GI-002 Funcionamiento Comité Estratégico de TI) y/o Dirección Ejecutiva, son los responsables del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de JUPEMA".*

En el punto 4.2.1.2. se cambia la palabra *"son"* por *"deben ser";* para que se lea como sigue: *"Los activos de información de JUPEMA, deben ser identificados y clasificados para establecer los mecanismos de protección necesarios".*

En el punto 4.2.1.4. se agrega *"(…) contratistas, proveedores y/o personal externo"*, para que se consigne: *"Todos los trabajadores, contratistas, proveedores y/o personal externo son responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida,*

alteración, destrucción o uso indebido, según se establece en la política P02-RP-001 Política de acceso a la información".

En el punto 4.2.1.6. se agregan los siguientes textos: "*(…) previamente*", "*por el área de seguridad de la información*" y "*Las herramientas que se utilizan a través de Internet o la nube también deben poseer la autorización del área de seguridad de la información previo a su uso*". La redacción propuesta es la siguiente: "*Únicamente se permite el uso de software autorizado que haya sido adquirido legalmente por la Institución, o bien software libre previamente autorizado por el área de seguridad de la información. / Las herramientas que se utilizan a través de Internet o la nube también deben poseer la autorización del área de seguridad de la información previo a su uso.*"; hay softwares que no se instalan en las máquinas, sino que se utilizan a través de los navegadores y esos softwares también tiene que estar autorizados; entonces, esa parte se la agregamos.

En el punto 4.2.1.7. le adicionamos "*(…) contratistas, proveedores y/o personal externo*", para que se lea como sigue: "*Es responsabilidad de todos los trabajadores, contratistas, proveedores y/o personal externo de JUPEMA reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.*". Siempre hay que tomar en consideración esas terceras partes, por eso agregamos bastante la palabra "contratistas y proveedores", porque estos deben cumplir con nuestros requerimientos de ciberseguridad.

En el punto 4.2.1.8. se incluyen las palabras "*(…) y ciberseguridad*" y "*P01-GI-002*", para que se lea: "*Las violaciones a las Políticas y Controles de Seguridad de la Información y ciberseguridad son registradas y reportadas a la Dirección Ejecutiva y/o Comité Estratégico de TI (P01-GI-002*

Funcionamiento Comité Estratégico de TI), para el proceso que corresponda.".

En el punto 4.2.1.9 se corrige el nombre del documento "P02-PR-005 Continuidad de la Gestión de JUPEMA", de manera que indique: "*JUPEMA cuenta con un Plan de Continuidad Institucional que asegura la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales, ver el procedimiento P02-PR-005 Continuidad de la Gestión de JUPEMA*".

En el punto 4.3. se agrega la palabra "*(…) y ciberseguridad*" para que se lea: "*4.3. Organización de la seguridad de la información y ciberseguridad*".

En el punto 4.3.1. "Divulgación y promoción", se mejora la redacción para un mejor entendimiento y se leerá como sigue: "*La Administración debe divulgar y promover el tema de Seguridad de la Información y ciberseguridad, para que en forma clara y breve se describan las políticas, estándares y procedimientos relacionados, con el fin de inculcar en los trabajadores la cultura de la Seguridad de Información. El área de Seguridad de la Información es el responsable de proporcionar a la Administración el material necesario que debe ser divulgado*".

En el punto 4.3.2 se agregan los textos "*(…) y ciberseguridad*", "*y el Área de Seguridad de la Información*" y "*realizarán*", para que indique: "*Definición de las responsabilidades para la seguridad de la información y ciberseguridad. / La Dirección Ejecutiva y el Área de Seguridad de la Información deben dar el seguimiento oportuno sin intervenir en las funciones propias de la Auditoría a todas las transgresiones a esta política que se detecten y comunicar a la jefatura inmediata los hallazgos, para que ésta tome las medidas correctivas correspondientes según el P15-RP-004*

Reglamento Interior de Trabajo. / Cuando sea considerado necesario se realizarán revisiones aleatorias sin previo aviso del cumplimiento de estas políticas".

El **Prof. Errol Pereira Torres** consulta: don José Daniel, siempre lo tenemos a usted en el Comité Estratégico de TI como las Áreas que reportan tanto a la Dirección Ejecutiva, como a Junta Directiva para efectos de seguridad de la información, pero ¿quién es el oficial de ciberseguridad de nuestra institución?

El **Ing. José Daniel Alpízar Ulloa** responde: el oficial de Seguridad de la Información en JUPEMA es el Ingeniero en Seguridad de la Información, que en este caso es este servidor, yo soy el Ingeniero en Seguridad de la Información, que es el equivalente al oficial de Seguridad de la Información.

El **Prof. Errol Pereira Torres** pregunta: ¿de ciberseguridad quién es la persona encargada?

El **Ing. José Daniel Alpízar Ulloa** contesta: es la misma persona, por eso estamos incluyendo los temas de ciberseguridad en la misma figura actualmente.

El **Prof. Errol Pereira Torres** menciona: tal vez usted tiene conocimiento, en algunas organizaciones el encarado de Seguridad de la Información o como se le llame a nivel de otras nomenclaturas, es la persona encargada de absolutamente toda la información, en todas las áreas, pero el de ciberseguridad es seguridad a nivel de tecnología informática y sobre todo lo que tiene que ver con el área del ciberespacio, todo lo que se aloja en los diferentes espacios virtuales y que es como más apegado a esta área específica, tecnológica. Así estamos estructurados nosotros, pero sí es algo que me parece que en algún momento se podría analizar, en el sentido de

que a nivel internacional se ha probado la funcionalidad de esto, con tareas más específicas del encargado de ciberseguridad, que al final sí son supervisadas por el encargado general de Seguridad de la Información. Sería importante analizar un poquito eso en algún momento.

El **Ing. José Daniel Alpízar Ulloa** externa: correcto don Errol, aquí también, tomando en consideración el tamaño de JUPEMA, en realidad la figura cae sobre la misma persona o también por el tamaño del Área, que ahorita no es un Área grande, pero en instituciones un poco más grandes es como usted indica, don Errol, está el oficial de Seguridad de la Información y debajo de él hay varias personas, está: el de ciberseguridad, uno propio de Riesgos y vienen otros, son como 4 o 5 personas más. La misma ISO 27032, que es de seguridad en el ciberespacio da esta figura, de que la mejor organización, por así decirlo, de seguridad de la información es así, un oficial y como 4 o 5 personas debajo de él, inclusive, unidades, hay organizaciones que son tan grandes que crean sus propias unidades supervisadas por el oficial de Seguridad de la Información, pero hay que tomar en cuenta que por el tamaño de JUPEMA actualmente eso recae en una misma persona. Ahora que estamos analizando y creando una comitiva para el Acuerdo 5-24, esto también podría venirse a ver y encontrar la necesidad de que ahora necesitamos una figura exclusiva de ciberseguridad y hacemos ese mismo mapeo, que esté a cargo del oficial de la Seguridad de la Información. Es una muy buena observación y tal vez lo podemos empezar a llevar acotación ahora que estamos examinando el Reglamento del Acuerdo 5-24, para hacer esa separación.

El **Prof. Errol Pereira Torres** señala: sí sobre todo que este reglamento insiste muchísimo en el tema de ciberseguridad. Este encargado de

ciberseguridad se correlaciona con mucha más facilidad con el Área de Tecnología de Información y siempre al final, como es más específico, entra en más en detalle y al final le reporta la generalidad al oficial de Seguridad de la Información. Gracias, don José Daniel, por atender esto, sí me parece importante que en algún momento se pueda entrar a valorar si esta figura puede dar más valor al trabajo de la seguridad y específicamente de ciberseguridad de la información a la institución; si estamos preparados para ello y si a nivel normativo nos podría puntuar mucho mejor, como lo acaba de mencionar, por los requerimientos que actualmente tenemos.

El **Ing. José Daniel Alpízar Ulloa** comenta: perfecto, don Errol, muchas gracias.

Continúa: en el punto 4.4. "Acuerdos de confidencialidad", adicionamos: "*4.4.4. Todos los trabajadores y terceros que utilicen información en el desarrollo de sus funciones deben firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información según se establece en P31-PR-007 Procedimiento Clasificación de la Información; y que cualquier violación con lo establecido en este párrafo es considerada como un "incidente de seguridad.*", lo que quisimos establecer es que literalmente todas las personas que trabajen con información de JUPEMA, deben de tener un acuerdo de confidencialidad, para que no se filtre la información.

En el punto 4.5. "Riesgos relacionados a terceros", se agrega el siguiente punto: "*4.5.3. Todo departamento, área, unidad o dependencia que contrate servicios a terceros es responsable de que el proveedor o tercero*

revise y acepte las buenas prácticas de seguridad que se utilicen en JUPEMA, así como lo dispuesto en esta política.", es responsabilidad de todas aquellas personas que contraten un servicio, que ese proveedor esté al tanto de nuestras prácticas de seguridad y las deben de cumplir.

Eso estaba en el punto 5.6.2 y lo pasamos para el punto 4.5.3 y le cambiamos un poco la sintaxis, de manera que se elimina el texto: "*5.6.2 Todos los trabajadores y terceros que manipulen información en el desarrollo de sus funciones deben firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación con lo establecido en este párrafo es considerada como un "incidente de seguridad".*

En el punto 4.6.2 se agrega el texto "*(…) P02-RP-001 Política de acceso a la información",* para que se lea: "*La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la institución, la información debe estar clasificada según la P02-RP-001 Política de acceso a la información".*

En el punto 4.6.3. se agrega un segundo párrafo que indica: "*Para los medios digitales debe garantizarse su eliminación de los dispositivos de almacenamiento y que la información no pueda ser recuperable bajo ningún método.",* porque aquí estaba hablando solamente de la información en papel y le adicionamos que a nivel digital también debe garantizarse que los dispositivos que almacenan información sensible y que

van a ser desechados, no pueden tener información o que no sea recuperable bajo ningún método.

En el punto 4.6.4. "Acceso a Internet", punto 4.6.4.2, inciso b., se agrega la palabra "*(…) Whatsapp*", para que se lea: "*No está permitido el acceso y el uso de servicios interactivos o mensajería instantánea como Whatsapp, Whatsapp Web, Facebook, Kazaa, MSN Messenger, Yahoo, Net2phone, Skype, Instagram, Myspace, LinkedIn, Twitter y otros similares, que tengan como objetivo crear comunidades para intercambiar información*". Además, se agregan las siguientes 4 reglas que van enfocadas a la inteligencia artificial. No queremos limitar a JUPEMA ante este "*boom*" que existe ahorita de la inteligencia artificial, de hecho, JUPEMA puede aprovechar herramientas de inteligencia artificial, lo único es que hay que regularlas. Se agrega: "*g. Las herramientas o software que utilicen la inteligencia artificial o los algoritmos generados por esta deberán estar al servicio de JUPEMA, generando beneficios identificables para JUPEMA y sus grupos de interés. No se permite la utilización de herramientas de inteligencia artificial con fines personales de los usuarios. / h. Los usuarios que utilicen la inteligencia artificial en beneficio de JUPEMA deberán garantizar la transparencia y trazabilidad que logren identificar que las herramientas fueron utilizadas.*", si utilicé inteligencia artificial, debo especificar que utilicé inteligencia artificial para hacer ese documento, proyecto, etc. "*i. Queda totalmente prohibido utilizar información confidencial, sensible o de uso interno en las herramientas de inteligencia artificial o en herramientas que utilicen algoritmos generados por inteligencia artificial.*", esto porque a veces estas herramientas de inteligencia artificial guardan esos datos que uno incluye y después otra

persona puede consultar o algo por el estilo y esos datos pueden salir a la luz. *"j. Si un usuario utiliza una herramienta o software de inteligencia artificial en beneficio de JUPEMA, deberá garantizar que ninguna propiedad intelectual ha sido violentada o usada sin permiso."*, hay herramientas de inteligencia artificial que cuando usted le pide que arme un proyecto, él toma cosas de propiedad intelectual, entonces, la inteligencia artificial está violando esa propiedad intelectual. Se debe garantizar que no se está violando la propiedad intelectual de nadie o hacer las referencias respectivas, para evitar una demanda. Estas son las 4 regulaciones que estamos usando con la inteligencia artificial, las estamos agregando porque antes no lo tocaba la Política de Seguridad.

En los siguientes puntos se mejora la redacción para un mejor entendimiento, de manera que se leerá como sigue: "4.6.4.3. *JUPEMA realiza un monitoreo automatizado y de forma continua de tiempos de navegación y páginas web visitadas por parte de los trabajadores y/o terceros. Así mismo el personal autorizado, puede inspeccionar y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente para promover el buen uso del servicio".*

"4.6.5. "Correo Electrónico", 4.6.5.2. Los trabajadores y terceros autorizados a quienes JUPEMA les asigne una cuenta de correo deben seguir los siguientes lineamientos: g. Es prohibido utilizar la dirección de correo electrónico de JUPEMA como punto de contacto en comunidades interactivas o redes sociales, tales como Facebook, Instagram, Myspace, LinkedIn, Twitter, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales. / h. No es permitido el envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos debe

ser autorizado por la Dirección Ejecutiva, el Departamento de Tecnología de Información o el Área de Seguridad de la Información. / 4.6.5.3. El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo que JUPEMA proporciona. De igual manera, las cuentas de correo genéricas o de servicio no se deben emplear para uso personal".

En el punto 4.6.5.5. se sustituye la palabra "*computacionales*" por "*informáticos*", para que se lea de la siguiente manera: "*Toda información de JUPEMA generada con los diferentes programas informáticos (Ej. Office, Project, Access, etc.), que requiera ser enviada fuera de JUPEMA, y que por sus características de confidencialidad e integridad debe ser protegida, estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el Departamento de Tecnología de Información. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información*".

En el punto 4.6.5.8. se agregó el siguiente texto por recomendación de la Auditoría Interna: "*Debido a que la cuenta de correo electrónico puede contener información privada personal (colillas de pago, acciones de personal, expediente del médico de empresa), la redirección de correo electrónico debe ser solicitado por el usuario dueño de la cuenta, autorizando el reenvío del correo electrónico a otro buzón de correo. Queda completamente prohibido que otro usuario pueda tener acceso al reenvío de un buzón de correo sin que el dueño del buzón exprese su consentimiento sobre el mismo.*", aquí existía una práctica que tal vez me iba de vacaciones o estaba incapacitado, entonces, nada más pedía que reenviaran mi

buzón a otra persona, pero debe existir una autorización del dueño de ese buzón.

En el punto 4.6.6. "Recursos Tecnológicos" se sustituye la palabra "la Junta" por "JUPEMA", para que se consigne: "*a. La instalación de cualquier tipo de software o hardware en los equipos de cómputo de JUPEMA es responsabilidad del Departamento de Tecnología de Información, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por JUPEMA a través del Departamento de Tecnología de Información*". En los incisos c., f. y g., se agrega el texto: "*(…) el Área de Seguridad de la Información*", para que se lea: "*c. El Departamento de Tecnología de Información en colaboración con el Área de Seguridad de la Información debe definir y actualizar, al menos una vez al año la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas. / f. Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de JUPEMA; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por el Departamento de Tecnología de Información y el Área de Seguridad de la Información. / g. La sincronización de dispositivos móviles, tales como PDAs (Tablet's, Ipads), celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Institución, debe estar debidamente autorizado por la Jefatura del departamento*

juntamente con el Departamento de Tecnología de Información y el Área de Seguridad de la Información y puede llevarse a cabo en dispositivos provistos por la organización para tal fin". Además, se agrega el inciso h., que indica: *"h. Para el uso de los dispositivos móviles, los usuarios deben apegarse a lo estipulado en la guía P17-GI-ISM-031 Buenas Prácticas de Seguridad para el uso de dispositivos móviles"*.

En el punto 4.7. "Control de acceso físico", se adiciona el punto 4.7.2., que señala: *"El ingreso de terceros (proveedores, contratistas, ect.), a las áreas catalogadas como de acceso restringido debe ser junto a personal interno de JUPEMA, quien debe asegurarse de que la información está correctamente protegida."*, hemos notado que no estaba regulado, a veces un proveedor o un contratista andaba solo por ahí y entraba a zonas de acceso restringido sin que nadie lo acompañara, eso es algo que debe cambiarse.

En el punto 4.10. "Protección contra software malicioso", se realizan mejoras en la redacción de los siguientes puntos: *"4.10.1. JUPEMA establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por software malicioso. Es responsabilidad del Departamento de Tecnología de Información en conjunto con el área de Seguridad de la Información autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como de su actualización permanente. / 4.10.2. El*

desarrollo de aplicaciones móviles y/o sitios web, debe seguir las políticas y normas de seguridad definidas y debidamente autorizado por el Departamento de Tecnología de Información y el área de Seguridad de la Información. / 4.10.5. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier software, dispositivo o infraestructura tecnológica".

En el punto 4.11. se sustituye la palabra "*copias*" *por* "*gestión*", para que se lea como sigue: "*Gestión de respaldos*".

En los siguientes puntos se mejora la redacción: "*4.11.1. JUPEMA debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el Departamento de Tecnología de Información, el área de Seguridad de la Información y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se debe establecer un plan de restauración de copias de seguridad que son probados al menos una vez por semestre, con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo acordado. / 4.11.2. El Departamento de Tecnología de Información debe establecer procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y define juntamente con las*

dependencias los períodos de retención de esta. Por otra parte, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada".

Se adiciona el siguiente punto: "*4.11.4. JUPEMA dispone de herramientas en la nube para que los usuarios puedan realizar sus propios respaldos y tener acceso a la información de JUPEMA en cualquier momento. Solo es permitido el uso de la herramienta oficial de JUPEMA para el almacenamiento de información en la nube. Así mismo cada usuario es responsable de realizar sus respaldos en la nube y no debe ser utilizada para almacenar información personal de ningún tipo*".

En el punto 4.12. "Gestión de medios removibles", el punto 4.12.1. se leerá de la siguiente manera: "*El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas, etc.) sobre la infraestructura para el procesamiento de la información de JUPEMA, está autorizado para aquellos trabajadores cuyo perfil del cargo y funciones lo requiera. Para el resto del personal queda totalmente prohibido el uso de medios removibles.*", con las herramientas de la nube, el uso de medios removibles es prácticamente innecesario.

En el punto 4.12.2. se adiciona el texto "*en conjunto con el área de Seguridad de la Información, son (…)*" para que indique: "*El Departamento de Tecnología de Información, en conjunto con el área de Seguridad de la Información, son responsables de implementar los controles necesarios para asegurar que en los sistemas de información de JUPEMA sólo los trabajadores*

autorizados pueden hacer uso de los medios de almacenamiento removibles".

En el punto *4.15.* "Escritorio y pantalla limpia", en los siguientes 2 puntos se agrega el texto: *"Esto también es aplicable para los lugares de trabajo de los usuarios en modalidad Teletrabajo."*, para que se lea como sigue: *"4.15.1. Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los trabajadores de JUPEMA deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata. Esto también es aplicable para los lugares de trabajo de los usuarios en modalidad Teletrabajo. / 4.15.2 Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se puede desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados, excepto los usuarios debidamente autorizados. Esto también es aplicable para los lugares de trabajo de los usuarios en modalidad de Teletrabajo".*

Se adiciona el siguiente punto *"4.15.4 Todos los usuarios deben garantizar que en la pantalla de sus equipos no hay información confidencial o sensible de JUPEMA mostrándose a la hora de recibir un tercero en su puesto de trabajo. Esto también es aplicable para los lugares de trabajo de los usuarios en modalidad de Teletrabajo".* Esto es sencillamente pantalla limpia.

En el punto 4.16.2. "Segregación de las redes", se mejora la redacción de los siguientes puntos: "*4.16.2.2 El Departamento de Tecnología de Información junto con el área de Seguridad de la Información son los encargados de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida. / 4.16.3 No está permitido apoderarse, acceder, modificar, alterar, suprimir, intervenir, interceptar, utilizar, abrir, difundir o desviar de su destino documentos o comunicaciones dirigidas a otra persona sin su autorización. / 4.16.5. Es prohibido para los usuarios, que sin autorización del titular o excediendo la que se le hubiera concedido o instruido, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. / 4.16.6. Es prohibido para los trabajadores suplantar la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información afectando la imagen o interés de JUPEMA*".

En el punto 4.17. "Identificación de requerimientos de seguridad", en los siguientes 2 puntos se agrega el texto: "*(…) Área de Seguridad de la Información*", para que se lea como sigue: "*4.17.1. La inclusión de un nuevo producto de hardware, software, aplicativo, herramienta, plataforma, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en JUPEMA, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad del Área de Seguridad de la Información y las dependencias propietarias del sistema en cuestión. / 4.17.2. Los requerimientos de seguridad de la información*

identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre JUPEMA y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad del Área de Seguridad de la Información y el Departamento de Tecnología de Información garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Dirección Ejecutiva establecer estos aspectos con las obligaciones contractuales específicas".

En el punto 4.19. "Incidentes de seguridad de la información", se agrega el siguiente punto: *"4.19.2. Es responsabilidad de cada trabajador o externo, reportar las sospechas o los incidentes de seguridad al área de Seguridad de la Información o al departamento de TI".*

En el punto 4.20. "Monitoreo de la seguridad" se adiciona el texto: *"El área de Seguridad de la Información"*, en los siguientes puntos: *"4.20.1. El área de Seguridad de la Información es el responsable de valorar y analizar las posibilidades y repercusiones técnicas de seguridad y riesgo, ya sea en la valoración, implementación y mantenimiento de los activos de información. / 4.20.2. Es responsabilidad del área de Seguridad de la información de JUPEMA, implementar y operar de acuerdo con las políticas y procedimientos establecidos. / 4.20.3. El área de Seguridad de la Información debe verificar que la implementación de la seguridad de la información sea probada y monitoreada de forma proactiva".*

Se agrega la parte de sanciones:

"4.21. Sanciones / 4.21.1. Todo trabajador que incumpla lo establecido en la presente política, se expone a las sanciones administrativas aplicables por

parte de JUPEMA. / 4.21.2. Cualquier personal de carácter externo que incumpla lo establecido en la presente política, se expone a las sanciones establecidas en los contratos, a la cancelación del propio contrato e incluso la posibilidad de que JUPEMA tome acciones legales en contra de la persona física o jurídica".

Esta es la modificación que agregamos a la Política de Seguridad de la Información.

El **Lic. Diego Vargas Sanabria** finaliza con la exposición del acta de la sesión ordinaria No. 010-2023 de la Comisión de Asuntos Jurídicos y Sociales.

Aclara: en la página No. 30 se habla del acuerdo No. 2, pero en realidad sería el acuerdo No. 3., hacemos la aclaración y la corrección de una vez.

Discutida el acta, el Cuerpo Colegiado por unanimidad adopta el siguiente acuerdo:

ACUERDO No. 3

"Analizada el acta de la sesión ordinaria No. 010-2023 de la Comisión de Asuntos Jurídicos y Sociales, la Junta Directiva acuerda:

1. ***Aprobarla.***
2. ***Aprobar las modificaciones propuestas a los siguientes documentos:***
   a. ***El Reglamento General de Organización y Funcionamiento (artículo 18 "Generalidades de las sesiones").***
   b. ***La Política Marco de Gestión de Seguridad de la Información.***

c. La Política de Seguridad de la Información y Ciberseguridad Institucional". Acuerdo unánime y en firme con seis votos.

Se le agradece la participación al Lic. Diego Vargas Sanabria y al Ing. José Daniel Alpízar Ulloa, quienes abandonan la sesión virtual.

ARTÍCULO IX: Entrega y análisis del oficio SG-P-12-2024 remitido por el Sindicato de Trabajadoras y Trabajadores de la Educación Costarricense (SEC), referente al rechazo de la remoción del M.Sc. José Edgardo Morales Romero; para resolución final de la Junta Directiva.

El **M.Sc. Erick Vega Salas** lee integralmente el oficio SG-P-12-2024, remitido por el Sindicato de Trabajadoras y Trabajadores de la Educación Costarricense (SEC), referente al rechazo de la remoción del M.Sc. José Edgardo Morales Romero. Documento adjunto como **anexo No. 5** de esta acta.

El **Lic. Jorge Rodríguez Rodríguez** externa: esta es la nota que nos envía nuevamente el SEC, quisiera conocer qué opinan ustedes al respecto.

La **M.G.P. Seidy Álvarez Bolaños** señala: creo que la nota no nos aporta mayores elementos a los que ya teníamos, todos esos puntos ya fueron expuestos, contestados y resueltos en su momento, considero que lo que corresponde de nuevo es hacerle llegar la respuesta que amerita esta nota, en el entendido que de nuevo vamos a analizar los puntos que vienen ahí; encuentro algunos puntos un poco confusos, que no me atrevería a analizar, en virtud de que no tengo una formación jurídica. Me parece que sería importante que contáramos con apoyo y asesoría para este tema, en virtud

de que es prácticamente una repetición de hechos y se agregan algunos elementos como que JUPEMA tiene que hacer el debido proceso, un tema de definir responsables y algunos temas que me parece que deberíamos tener un poco de asesoría para responderlos adecuadamente. Esa es mi posición.

La **Prof. Ana Isabel Carvajal Montanaro** manifiesta: exactamente eso era lo que iba a pedir, que la respuesta sea con la asesoría legal, que el Departamento Legal sea la que analice esto, para que luego nos lo traslade.

El **M.Sc. Hervey Badilla Rojas** indica: totalmente de acuerdo, en la misma línea, me parece que dada la situación que se presenta en el marco de esos 4 puntos que están solicitando o visualizando como "el por tanto" de la nota, se deriva que sí hay necesidad de respuesta. Ante la petición que hace nuevamente la organización, hay por lo menos un par de puntos que considero deben ser aclarados desde un punto de vista legal, dado que es lo más pertinente para un mejor resolver de parte de esta Junta Directiva y bajo ese criterio externo justamente la solicitud de que este documento sea elevado al Departamento Legal para que emita un dictamen, el cumplimiento que correspondería a esta Junta Directiva tomar decisión al respecto.

El **Prof. Errol Pereira Torres** enfatiza: el documento insiste en puntos ya totalmente evacuados por esta Junta Directiva en apego a todo un proceso que se llevó muy responsablemente y que al final condujo a la búsqueda de un criterio de la Procuraduría General de la República, que elevó nuestra anterior presidenta, la M.G.P. Seidy Álvarez Bolaños, a dicho Órgano Consultivo del Estado y que tiene carácter absolutamente vinculante y la vinculancia fue la que nos hizo brindar la última respuesta al SEC, para dar

por cerrado el caso, porque cuando se trata de un criterio con la contundencia, la vinculancia y la jurisprudencia que establece este órgano constituido dentro de todo el marco jurídico de nuestro Estado costarricense, me refiero al PGR-C-184-2023 del 02 de octubre de 2023 (el cual forma parte del **anexo No. 5** de esta acta), uno pensaría que ya se comprende bien que esos alcances deben ser incorporados a la visión jurídica, inclusive de los mismos departamentos legales o asesorías legales que tengan las organizaciones, para el caso de JUPEMA, por su composición, pero parece que así no ha sido y a 14 días de que don Edgardo cumpla su periodo en esta Junta Directiva nos viene esta nota. Pienso que la línea de respuesta debe ir alineada con ese criterio y con lo que acordó la Junta posterior a haber recibido este documento vinculante.

El escrito se refiere a un recurso de amparo que fue rechazado por la Sala Constitucional, hay que decirlo porque no sé cuál es la pretensión de la referencia, dado que fue rechazado desde un principio cuando se estableció desde enero por esta Junta que no veíamos justificación, ni debido proceso para la remoción y que el articulado de la Ley 7531 es claro en cuáles son los postulados para una eventual remoción o interferencia, que venga a truncar el período de 4 años que establece la Ley para las representaciones que aquí se tienen en la Junta Directiva de JUPEMA. Dado que la misma organización fue la que estableció toda la idoneidad para el señor José Edgardo y que luego esta, en enero de 2023, quiere establecer otra condición, tenía que demostrarlo totalmente como lo prevé la Ley 7531 y por eso creímos muy oportuno, así lo hizo saber nuestra presidenta a la Procuraduría General de la República, cuál era la consideración del concepto y cuáles eran los alcances de ese concepto de "causa justa", lo

explicó muy bien la Procuraduría General de la República y esto debía ser totalmente demostrado, sobre todo cuando el Ente Procurador menciona que: *"(…) dicho concepto jurídico indeterminado ha de ser llenado de contenido en cada caso concreto, mediante la aplicación a circunstancias específicas de los factores objetivos y subjetivos que sean congruentes con aquel enunciado genérico. De ahí que la motivación necesaria y adecuada de todo acto que se adopte al respecto, en el que consten las razones de la remoción anticipada, con una indicación precisa de las disposiciones legales y reglamentarias en que se fundamenta y las cualidades específicas del nuevo designado para cumplir la representación de que se trate, es un requisito indispensable en este tipo de conductas administrativas, conforme lo exige el artículo 136 de la LGAP (…)",* en ese y en otro de los párrafos en donde ya brinda su resolución hay suficiente materia para lo que esta Junta determinó. En esa misma línea creo que es conveniente que se traslade a nuestra asesoría legal para que realice un último análisis de esto y se proceda luego con ello a brindar la respuesta como corresponde por porte de esta Junta Directiva. En definitiva, creo que esto ya estaba respondido en todos sus alcances y en todo lo que pretende el documento, uno recomendaría una lectura más profusa por parte de la Organización de esos alcances del criterio de la Procuraduría General de la República.

El **M.Sc. Erick Vega Salas** adiciona: secundar las palabras de los compañeros anteriores, es importante trasladar esta nota a la parte legal para que nos haga un análisis exhaustivo y tener insumos para la toma de decisiones. Esto es un tema álgido, complicado, uno de los mayores desafíos que ha tenido esta Junta en el 2023 y definitivamente se va a requerir esa asesoría legal para poder determinar lo que proceda.

El **Lic. Jorge Rodríguez Rodríguez** plantea: coincido con todos ustedes en que esta nota debe enviarse al Departamento Legal para que nos dé un criterio, nos dé la opinión para poder responder de forma definitiva. Para hoy y como siempre hemos hecho que hemos atendido el tema con esta organización: se ha respondido todo oportunamente, se ha analizado muchísimo este tema, se ha analizado a profundidad, tenemos más de un año de estar en reiteradas ocasiones retomando este tema y me parece que ellos merecen todo nuestro respeto en ese sentido y si tomamos el acuerdo de elevarlo al Departamento Legal, que esto se les comunique de manera inmediata para que ellos vean que el asunto nuevamente está siendo atendido por este Órgano Colegiado. Me parece que el Departamento Legal va a ocupar un plazo, vamos a proponer un plazo para que ellos tampoco le den muchas largas al tema y podamos de manera oportuna brindar una respuesta de fondo acerca de este tema. Quisiera que el Departamento Legal analice lo que se menciona con respecto al recurso de amparo, si hubiese sido acogido y se diera una determinación por parte de la Sala Constitucional, ya nosotros seríamos conocedores de eso, se nos hubiese instruido y dado órdenes de acatamiento de qué deberíamos hacer; entonces, que ese recurso sea revisado para ver en qué proceso está, si fue rechazado, si está en estudio, no sé, eso no se aclara, un recurso lo presenta uno en el momento que quiere y sobre el tema que quiera, pero eso no implica que haya ninguna inobservancia por parte de esta Junta Directiva, con respecto a un recurso del cual no conocemos. Sí creo que nos endosan ahora la responsabilidad de hacer nosotros un debido proceso, es una lástima que después de un año de estar hablando de este tema y la organización no haya hecho lo que desde el primer momento dijimos, que

la Ley 7531 indica que debe hacerse un debido proceso; en fin, no encuentro mucho sentido a lo que expresa la nota, lastimosamente no hay elementos nuevos, me parece que esa organización nos está tratando de endosar responsabilidades, inclusive, atribuciones y cuestiones que no nos corresponden, la Procuraduría General de la República fue muy clara en su dictamen y ese criterio como vinculante que es, fue lo que nosotros acogimos, así que tiene que quedar muy claro que esta Junta siempre ha actuado en apego a la Ley, no somos nosotros los que decimos a quién se pone y a quién se quita de acá, solamente nos hemos apegado a la Ley, por eso en todo momento se han hecho las consultas a los Órganos de alto nivel de este país y es lo que se ha decidido. Creo que es muy sabio también lo que están opinando ustedes de nuevamente hacer la consulta al Departamento Legal y que ellos nos instruyan para un buen proceder por parte de esta Junta Directiva.

La **M.G.P. Seidy Álvarez Bolaños** solicita: a las Organizaciones Laborales de las Instituciones Estatales de Educación Superior (Olies) no las copiaron en la nota, pero sí les hicieron llegar el documento, porque recibí consultas de parte de ellos, entonces, me parece apropiado incluirlas en la respuesta.

El **Lic. Jorge Rodríguez Rodríguez** sugiere: si le parece, doña Seidy, lo dejamos así porque ellos no los copiaron, pero igual usted se encargaría de enviarle la respuesta nuestra a las Olies, ¿o prefiere que lo agreguemos?

La **M.G.P. Seidy Álvarez Bolaños** responde: preferiría agregarlo para hacerlo formal, porque la vía que usaron la desconozco, pero sí fui consultada sobre la nota, entonces, me parece que, para que no llegue por otra vía informal, que sea la vía correcta la que se utilice.

El **Lic. Jorge Rodríguez Rodríguez** resalta: tal vez fue que lo omitieron y no estaría de más.

El **Prof. Errol Pereira Torres** enfatiza: eso mismo, don Jorge, me parece que fue un error material, porque en lo que uno puede deducir ahí es que la intención era que se enterara el resto de las organizaciones representadas aquí, entonces, me parece que lo más adecuado, inclusive, un poco ahí de tomar en cuenta a todas, como debe ser, es brindarle esa información a las Olies.

Sobre el particular, el Órgano Colegiado por unanimidad adopta el siguiente acuerdo:

ACUERDO No. 4

"Analizado el oficio SG-P-12-2024 enviado por el Sindicato de Trabajadoras y Trabajadores de la Educación Costarricense (SEC), referente al rechazo, por parte de JUPEMA, de la remoción del M.Sc. José Edgardo Morales Romero, la Junta Directiva acuerda:

1. Dar por conocido el oficio.

2. Remitir el oficio al Departamento Legal para que realice un análisis y elabore un borrador de respuesta el cual debe ser presentado a este Cuerpo Colegiado en el plazo de ocho días hábiles, para resolución final.

3. Comuníquese este acuerdo a la Superintendencia de Pensiones, al Sindicato de Trabajadoras y Trabajadores de la Educación Costarricense, a la Asociación Nacional de Educadores, a la Asociación de Profesores de Segunda Enseñanza, a la Asociación de Educadores Pensionados, al

Colegio de Licenciados y Profesores en Letras, Filosofía, Ciencias y Artes, a las Organizaciones Laborales de las Instituciones Estatales de Educación Superior y a la Asociación de Funcionarios Universitarios Pensionados".
Acuerdo unánime y en firme con seis votos.

ARTÍCULO X: Entrega y análisis de los siguientes estudios de la Auditoría Interna; para resolución final de la Junta Directiva: 1) Estudio No. 44-2023: "Riesgos de seguridad de la información". Oficios AI-1073-12-2023 y AI-1061-12-2023. 2) Estudio No. 45-2023: "Cuentas por pagar proveedores". Oficios AI-1073-12-2023 y AI-1065-12-2023.

Con el aval de la Presidencia se incorpora a la sesión virtual la Lcda. Xinia Wong Solano, a quien se le brinda una cordial bienvenida.

Inciso a) La **Lcda. Xinia Wong Solano** expone el oficio AI-1073-12-2023 y sus adjuntos: el oficio AI-1061-12-2023 y la presentación del Estudio No. 44-2023: "Riesgos de seguridad de la información". Documentos adjuntos como **anexo No. 6** de esta acta.

Menciona: el alcance del presente estudio procura determinar cómo los riesgos de seguridad de la información son considerados e integrados en la gestión de riesgos de los procesos de JUPEMA.

Los objetivos del estudio son:

1. Verificar cómo los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información son integrados dentro de la gestión del riesgo institucional.

2. Comprobar cuál es el avance realizado por el Área de Seguridad de la Información en relación con la identificación y tratamiento de los riesgos inherentes de su dependencia.

Recordemos que el Área de Seguridad de la Información estaba adscrita antiguamente al Departamento de Tecnología de Información, se hace una separación y comienza su gestión en forma independiente. Nosotros hemos estado siguiéndole el pulso a esto, hemos hecho algunas observaciones y nos interesa saber cómo ellos han ido avanzando en estos procesos de madurez.

Uno de los primeros aspectos que determinamos es: el estado actual de la evaluación de riesgos de seguridad de la información. Señalamos que esta evaluación de riesgos que ejecuta el Área de Seguridad de la Información se encuentra, a criterio nuestro, en un estado inicial, pero se ha avanzado en varios aspectos: la declaración de apetito de riesgos, los escenarios de riesgos, a la fecha de este estudio, que fue el año pasado, había un borrador del Manual de Riesgos, ya de hecho se implementó hasta una segunda versión de ese Manual.

La evaluación de los riesgos de seguridad de la información constituye un proceso necesario, no sólo para el cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI), sino para verificar cómo están siendo gestionados los riesgos menos comunes y sobre los cuales no se tenga detalle de cómo están siendo controlados.

Adicionalmente, las modificaciones en la normativa externa (CONASSIF 5-17, SP-1412-2023) darán énfasis en directrices focalizadas en la gestión de la seguridad de la información y ciberseguridad, por lo cual, el fortalecimiento del SGSI resulta fundamental.

Cuando analizamos esto, nos surgen algunas recomendaciones al Área de Seguridad de la Información y a la Dirección Ejecutiva:

Primero, al Área de Seguridad de la Información: procurar el continuar con los avances en la evaluación de riesgos de seguridad de la información, de forma tal que se logre definir la metodología de gestión y se procure su alineamiento con las mejores prácticas vigentes, por ejemplo, la ISO 27002, versión 2022; lo anterior con el propósito de que el SGSI cuente con dicho insumo para poder proseguir con el tratamiento de riesgos, actualización de la declaración de aplicabilidad, entre otras, lo cual repercute en el fortalecimiento del sistema de gestión, su alcance y eficiencia.

Segundo, se le recomienda a la Dirección Ejecutiva que, para la tercera etapa del mapeo de procesos, valorar la conveniencia de otorgar prioridad al Área de Seguridad de la Información, ya que el mapeo de ese proceso representa un insumo importante para que dicha dependencia pueda proseguir con la evaluación de los riesgos de seguridad de la información, aspecto que es fundamental porque impacta a nivel de toda la institución, además, es un requisito del SGSI. Lo anterior agilizaría el fortalecimiento del SGSI, permitiendo no sólo mejorar la seguridad de la información en la organización, sino también anticiparse a la entrada en vigor del Acuerdo CONASSIF 5-24 (SP-1412-2023), con respecto a las directrices enfocadas en seguridad de la información.

Otro aspecto que revisamos fue la metodología para la evaluación de los riesgos: se observó que el Área de Seguridad de la Información está haciendo uso de la norma ISO 27002 como parte de su metodología para la evaluación de los riesgos; no obstante, la versión de la norma que posee dicha dependencia ya no se encuentra vigente, puesto que en 2022 la ISO

27002 fue actualizada a una nueva versión la cual conlleva modificaciones en la estructura del documento, así como la eliminación, fusión y adición de nuevos controles que buscan mitigar los riesgos de seguridad de la información. Considerando lo anterior, si el Área de Seguridad de la Información se basa en la versión anterior de la norma (no vigente), para realizar la evaluación de riesgos, a futuro implicaría incurrir en un reproceso, dado que dicha dependencia deberá, en algún momento, adaptar la nueva versión de la ISO 27002 en aras de fortalecer el SGSI, tarea que involucraría realizar un nuevo mapeo de los riesgos y de los objetivos de control asociados.

Dentro de las recomendaciones que se le emiten a la Dirección Ejecutiva está: considerar dotar oportunamente al Área de Seguridad de la Información con la nueva versión de la norma ISO 27002, con el objetivo de lograr adoptar dicha norma a la mayor brevedad posible, de forma tal que la evaluación de riesgos y la actualización de la "Declaración de Aplicabilidad" puedan ser ejecutadas basados en la última versión de dicho estándar internacional.

Lo anterior busca los siguientes beneficios:

✓ Mantener un proceso de evaluación de riesgos alineado y actualizado con las mejores prácticas internaciones.

✓ Impedir la omisión de objetivos de control que fueron incluidos en la nueva versión.

✓ Evitar que a futura el Área de Seguridad de la Información incurra en reprocesos necesarios para adaptarse a la nueva versión de la norma.

✓ Fortalecer dos de los principales requisitos: evaluación y tratamiento de riesgos que permitan diseñar, implementar, mantener y mejorar el Sistema

de Gestión de Seguridad de la Información. De hecho, si no me equivoco ayer le di seguimiento a las recomendaciones de este estudio y ya la nueva norma fue adquirida por parte de la institución, eso nos da bastante tranquilidad que el Área de Seguridad de la Información pueda trabajar con una versión actualizada.

Por otra parte, revisamos los Manuales de Gestión de Riesgos y determinamos:

- Actualización del manual de gestión de riesgos: a partir de la inspección del Manual de Riesgos (P20-MA-001), se evidenció la metodología de gestión para diferentes tipos de riesgos, pero no se detalle la gestión del riesgo de seguridad de la información. Cuando le consultamos al Área de Seguridad de la Información cómo les está yendo con esto, nos indican que en este momento se encuentran trabajando en el diseño y ajuste de un Manual de Riesgos específico para seguridad de la información; dicho documento se encuentra en borrador, por lo que resulta oportuno lograr incorporar o referenciar el riesgo de seguridad de la información en la próxima actualización al manual de riesgos.
- Referencias al acuerdo SUGEF 14-17: en el borrador del Manual de Riesgos de Seguridad de la Información (P31-MA-001) se observaron referencias al Acuerdo SUGEF 14-17, el cual fue sustituido por el Acuerdo CONASSIF 5-17 el 29 de abril de 2022 y probablemente sea sustituido próximamente por el Acuerdo CONASSIF 5-24 en el 2024 (SP-1412-2023). Debemos tener mucho cuidado para que nuestro Manual de Riesgos se encuentre actualizado en esas secciones.
- La misma situación se identificó en la sección de Riesgo Tecnológico del Manual de Riesgos.

Las recomendaciones emitas son las siguientes:

a. Una vez que el Manual de Riesgos de Seguridad de la Información (P31-MA-001) se encuentre aprobado y publicado, considerar incluirlo o bien referenciarlo dentro del Manual de Riesgos (P20-MA-001), con el objetivo de que en dicho documento quede constancia de la existencia de una metodología focalizada en la gestión de los riesgos de seguridad de la información, aprovechando que en el P20-MA-001 se centraliza la gestión de los riesgos financieros y no financieros.
b. Verificar las referencias normativas en el Manual de Riesgos (P20-MA-001), con el objetivo de corregir las menciones al Acuerdo SUGEF 14-17 y cualquier otra referencia errónea que pueda ser identificada.

Lo anterior con el propósito de evitar confusiones con referencias a normativa externa no vigente o sustituida; se debe considerar que el Acuerdo CONASSIF 5-17 (anteriormente SUGEF 14-17) recibió una propuesta de modificación durante noviembre del 2023, por lo que eventualmente será publicado como Acuerdo CONASSIF 5-24.

Al Área de Seguridad de la Información se le recomienda verificar las referencias normativas en el Manual de Riesgos de Seguridad de la Información (P31-MA-001), con el objetivo de corregir las menciones al Acuerdo SUGEF 14-17 y cualquier otra referencia errónea que pueda ser identificada.

También revisamos la declaración de aplicabilidad del SGSI:

• Actividad y actualización: la declaración de aplicabilidad es registrada en el formulario P31-FO-014; no obstante, no se observaron directrices sobre el responsable o periodicidad de actualización del documento; esto al inspeccionar la política del "P17-RP-ISM-02, Sistema de Gestión de Seguridad

de la Información" y el procedimiento "P31-PR-001, Monitoreo y seguimiento a cargo del Ingeniero de Seguridad". Estos detalles son importantes, porque si está desactualizado no tenemos a quién solicitarle o a quien responsabilizarlo de esta situación.

- Contenido: se observó que la declaración de aplicabilidad se encuentra basada en una versión anterior de la ISO 27002; la nueva versión de dicha norma incorpora atributos a los controles los cuales permiten filtrar, ordenar y presentar diferentes vistas de los controles para diversos propósitos, por lo que adicionar dichos atributos a la actualización de la declaración de aplicabilidad de JUPEMA puede aportar mayor valor.

De ahí que se le recomienda al Área de Seguridad de la Información: Valorar la posibilidad de consignar directrices en la normativa interna que el Área de Seguridad la Información considere pertinentes, concernientes a la definición y actualización de la declaración de aplicabilidad (P31-FO-014); lo anterior con el propósito de que existan pautas que definan las actividades de control, sus responsables y periodicidad de ejecución, evitando así posibles omisiones en la ejecución de las actividades.

Adicionalmente, evaluar si la incorporación de los atributos de los objetivos de control, adicionados en la nueva versión de la ISO 27002, puede aportar mayor valor al registro de la declaración de aplicabilidad del SGSI, dado que agregarlos no implica mayor esfuerzo (pues viene predefinidos en la norma) y su incorporación podría facilitar la identificación o filtrado de controles según sus atributos, permitiendo determinar, por ejemplo, cuáles controles tienen mayor impacto en la confidencialidad, disponibilidad e integridad de la información.

Finalmente, analizamos el riesgo tecnológico: se verificó la última versión de la matriz de riesgo tecnológico (DE-UR-77-06-2023) y observamos que cuenta con 16 subprocesos y actividades. Estos subprocesos fueron definidos con anterioridad y la actualización de la matriz ocurrió en mayo del 2023; por tanto, no presenta alineación con el mapeo de procesos realizado por la Unidad de Control y Gestión de la Calidad, presentado en setiembre del 2023, mediante la nota DE-GC-0061-0-2023.

Dado lo anterior y considerando que el mapeo de procesos es una herramienta que procura ordenar las actividades de control, eliminando reprocesos y redefiniendo roles y funciones, resulta pertinente que la próxima actualización de la matriz de riesgo tecnológico procure alinear sus subprocesos y actividades con los resultados generados por el mapeo de procesos del Departamento Tecnología de Información.

La recomendación que le realizamos a la jefatura del Departamento de TI es: analizar la necesidad de alinear la matriz de evaluación de riesgo tecnológico (en la próxima actualización) con los resultados del mapeo del proceso de tecnología de información. Lo anterior con el fin de que exista una concordancia entre los procesos mapeados y la evaluación en la gestión del riesgo, minimizando la posibilidad de que puedan omitirse procesos o riesgos en la matriz de evaluación.

Las conclusiones del estudio son las siguientes:

- Se determinó que el proceso de gestión de los riesgos de seguridad de la información se encuentra integrado dentro de la gestión del riesgo institucional, donde la Unidad Integral de Riesgos ha guiado al Área de Seguridad de la Información en la definición de una metodología para

la gestión de dicho riesgo en específico, pero hay aspectos que tienen que irse madurando.

- Además, se constató la existencia de normativa interna asociada, así como la integración de la gestión del riesgo como parte de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).
- Se comprobó que la evaluación de riesgos de seguridad de la información se encuentra en un estadio inicial, pero se han mostrado progresos en aspectos puntuales que contribuyen al avance de la evaluación de los riesgos y el posterior tratamiento de estos.

Como les señalaba, hay aspectos que sí se deben de corregirse y esa es la idea de presentarles este estudio, para que las diferentes unidades y dependencias puedan determinarlos e ir corrigiendo con el apoyo de la Dirección Ejecutiva; hay unos de estos que ya se han ido ejecutando y eso es lo importante para fortalecer el control interno a nivel institucional.

Inciso a) La **Lcda. Xinia Wong Solano** expone el oficio AI-1065-12-2023 y la presentación del Estudio No. 45-2023: "Cuentas por pagar proveedores"; los cuales forman parte del **anexo No. 6** de esta acta.

Señala: el alcance del presente estudio comprende la revisión del control y registro de las cuentas por pagar a proveedores.

El objetivo es verificar que los importes por pagar a proveedores se realizan en tiempo, forma y con los debidos controles.

Uno de los primeros aspectos que revisamos fueron las cuentas por pagar vencidas: al consultar las pantallas FCP30-02; RCP40-08 y RCP-50-06 del sistema de cuentas por pagar, se determinan tres partidas pendientes de pago y nos llamaba mucho la atención, primero, porque no son montos muy significativos, pero la antigüedad oscila entre los 76 y 149 meses.

La recomendación a la jefatura del Departamento Administrativo es: valorar la necesidad de investigar la situación descrita sobre las cuentas por pagar a proveedores antiguas, con el propósito de determinar la veracidad de esas cuentas por pagar y establecer las acciones a implementar: ya sea efectuar los pagos si corresponde o gestionar los ajustes en el sistema de información de cuentas por pagar a proveedores, para que la información consignada sea consistente, veraz y libre de errores.

Por otra parte, analizamos algunas inconsistencias en la información mostrada en la pantalla FCP30-02 "Estado de cuenta detallado" del sistema de cuentas por pagar a proveedores, específicamente en la ventana "Resumen", donde observamos que no hay una uniformidad en los datos que se presentan en estos reportes, por ejemplo:

- En el espacio "Crédito máximo" en algunos casos se consigna ¢1 (un colón) y en otros ¢0 (cero), independientemente si existen o no saldos por pagar.
- En el espacio denominado "Disponible" en algunos casos se muestra el monto pendiente de cancelar como negativo, en otros ¢1 y se desconoce cuál es la razón de ello.

La recomendación a la jefatura del Departamento Administrativo es: analizar la conveniencia de revisar los datos consignados en la pantalla FCP30-02 del reporte "Estado de cuenta detallado" del sistema de cuentas por pagar proveedores, para determinar la pertinencia de seguir contando con esa pantalla, siendo que los sistemas de información deben contemplar procesos requeridos para recopilar, procesar y generar información que responda a las necesidades institucionales, relevante para la toma de decisiones, en cumplimiento del numeral 5.6 de las de las Normas de Control

Interno para el Sector Público. Sería importante valorar si es necesario este tipo de pantallas que pueden llamar a error a la hora de ver los datos que se están consignando.

Además de esto, realizamos la verificación de las conciliaciones de "Cuentas por Pagar Proveedores" de las cuentas contables 03 210 020 000 000-Proveedor de suministros Fondo Especial Operativo y 07 210 020 000 000-Proveedor de activos Fondo Especial Administrativo, de enero a agosto 2023 y se determinó lo siguiente:

Oportuna elaboración: las conciliaciones de cuentas por pagar proveedores no se están efectuando oportunamente, por cuanto, presentan atrasos entre 1 y 5 meses; recordemos que la idea de las conciliaciones es tener una veracidad de los saldos que estamos mostrando en los Estados Financieros, entonces, si estas conciliaciones tienen tantos atrasos, no tenemos esa confianza en los datos que estamos relevando en los Estados Financieras. Adicionalmente, en algunas ocasiones las firmas de control según el orden jerárquico carecen de una secuencia lógica: primero firma el que revisar y luego el que elabora; puedo entender que se pudiera dar un error y se tuviera que firmar nuevamente; sin embargo, sí vimos que es como un patrón que se observa, son varias donde primero firma el que revisa y luego el que elabora.

Partidas conciliatorias: al revisar las partidas conciliatorias de las cuentas por pagar a proveedores, se observó lo siguiente:

- Tres partidas pendientes de pago en los reportes RCP50-06 "Cuentas por pagar de facturas de servicios y gastos" y CON01R051 "Balance de comprobación" del Fondo especial operativo que presentan una antigüedad entre 76 y 149 meses. Recordemos que las conciliaciones son

para ver si hay que ajustar y la idea es que, si lo encuentro hoy en esta conciliación, a más tardar en la siguiente esté ajustando estas partidas; sin embargo, vemos que las partidas pendientes de conciliar se siguen quedando en las conciliaciones y se van aumentado. Entiendo que hay mucho trabajo y muchas cuestiones, pero no podemos seguir manteniendo cuentas por pagar, como lo vimos, de 7 y 12 años; eso no es razonable.

- En la conciliación de agosto 2023, se muestra una cuenta por pagar por ¢300.000,00 pendiente de ajustar desde marzo 2023, consignando que se encuentra pendiente el asiento tipo 65 (Reversión de transferencias). Lo que estamos observando es que se nos van aumentando cada vez más estas partidas por conciliar.

Ajuste menor: en la conciliación de marzo 2023, se presenta un "Ajuste Menor" por un monto de ¢5.084,43; sin embargo, no se consigna detalle o documentación de respaldo para justificar dicha diferencia. Los montos que son poco significativos podría ser la cantidad de decimales, por ejemplo, en las inversiones no contar con un decimal, debido a la partida tan grande, impacta, pero me preocupa cuando veo partidas pequeñas, porque puede ser que sea la suma de varias omisiones; por ejemplo, puedo decir: "*un error de ¢5.000,00*", pero podría ser un débito de ¢11.000.000,00 y un crédito de ¢11.005.000,00 y que se están compensando. A esas partidas hay que ponerles cuidado.

La recomendación a la jefatura del Departamento Financiero Contable es que estamos observando que no es una situación nueva, la estamos viendo en cuentas por pagar, la hemos visto en otras de efectivo, de pólizas y conciliaciones, de manera que se deben implementar medidas para solventar los siguientes aspectos:

- Las conciliaciones de cuentas por pagar a proveedores no se efectúan oportunamente.
- Conciliaciones firmadas por el responsable de revisarlas (encargado de unidad), previo al responsable de su elaboración.
- Oportunidad en las firmas de autorización de las conciliaciones, por cuanto se consignan hasta un mes después del plazo establecido para su elaboración.
- Brindar un seguimiento oportuno a las partidas conciliatorias y consignar las anotaciones pertinentes en las conciliaciones, sobre el origen o razones por las que no se han cancelado o ajustado dichas partidas.

Lo anterior, para que las conciliaciones cumplan con el propósito de su elaboración que es: verificar la razonabilidad de los saldos presentados y poder realizar los ajustes correspondientes con oportunidad; así como dar cumplimiento al Procedimiento Registro contable Fondo Especial de Administración y las Normas de Control Interno para el Sector Público.

Por otra parte, analizar la conveniencia de incorporar en el procedimiento "Registro Contable Fondo Especial de Administración" o en la normativa que considere pertinente:

- El detalle sobre los alcances del asiento tipo 65 - Reversión de transferencias.
- El criterio utilizado en las conciliaciones para determinar cuándo un monto es definido como un "Ajuste menor"; así como documentar las razones de éste en las conciliaciones; ya que los procedimientos son documentos que ayudan en la inducción de personal, contribuyen en la minimización de errores, en la asignación de responsabilidades y en la estandarización de

calidad de las actividades efectuadas. Es importante que lo estemos revisando y lo llevemos cuidadosamente.

Las conclusiones de esta revisión que tenemos como Auditoría: se observaron oportunidades de mejora referente a:

- Partidas pendientes de pago en los reportes RCP50-06 "Cuentas por pagar de facturas de servicios y gastos" y CON01R051 "Balance de comprobación" del Fondo Especial Operativo que presentan una antigüedad significativa.
- Las conciliaciones de cuentas por pagar proveedores no se están efectuando oportunamente, presentan partidas conciliatorias antiguas sin ajustar y en algunas ocasiones las firmas de control según el orden jerárquico carecen de una secuencia lógica.
- El procedimiento Registro contable Fondo Especial de Administración puede ser objeto de mejora, para que ayude en la inducción de personal, en la asignación de responsabilidades, en la estandarización de calidad de las actividades efectuadas y contribuya en la minimización de errores.

Se espera que los resultados de la evaluación puedan servir para la mejora en los aspectos relacionados con el control, registro y elaboración de las conciliaciones de cuentas por pagar proveedores, tanto para el Área de proveeduría, como para la Unidad de contabilidad y presupuesto.

Estas son las observaciones que se están efectuando por parte de esta Auditoría para tratar de fortalecer estos aspectos en la Unidad de Contabilidad y Presupuesto, así como en el Área de Proveeduría.

El **Lic. Jorge Rodríguez Rodríguez** señala: me parece que hay algunos hallazgos de los cuales la Administración debe tomar nota para que

justamente se corrijan esos asuntos. En el estudio anterior es importante ver cómo se tienen fortalezas a nivel institucional en materia del riesgo de la información y temas que sin duda alguna preocupan a todas las organizaciones, dado las amenazas permanentes, entonces, es bueno ver que nos estamos fortaleciendo en tener establecidos esos canales de control, de vigilancia y seguimiento. Por lo demás, doña Xinia, creo que es un excelente trabajo el que se realiza, le agradecemos mucho.

El **Prof. Errol Pereira Torres** agrega: con respecto al informe anterior, es importante ajustarnos a las normativas actuales y a lo que tenemos que asumir con el Acuerdo CONASSIF 5-24 en cuanto a la seguridad de la información, tenemos que apresurar el paso en esto.

En cuanto a las sumas por pagar que se nos acaba de presentar por parte de la Auditoría, tomar esas observaciones muy en serio, uno no cree que haya deudas, inclusive, como lo mencionaba doña Xinia, son proporcionalmente de poco monto para la institución, pero son responsabilidades que se tienen con proveedores, no solo por cuestiones hasta de reputación, sino también que por una cuestión pequeña podemos tener un problema legal, sin necesidad. Creo que definitivamente se debe revisar muy bien dónde está el error y solucionar esto en el menor plazo posible.

Analizados los estudios, el Órgano Colegiado por unanimidad adopta el siguiente acuerdo:

ACUERDO No. 5

"La Junta Directiva de la Junta de Pensiones y Jubilaciones del Magisterio Nacional acuerda: Aprobar los siguientes estudios de la Auditoría Interna:

1. Estudio No. 44-2023: riesgos de seguridad de la información. Oficios AI-1073-12-2023 y AI-1061-12-2023.

2. Estudio No. 45-2023: cuentas por pagar proveedores. Oficios AI-1073-12-2023 y AI-1065-12-2023". Acuerdo unánime y en firme con seis votos.

Se le agradece la participación a la Lcda. Xinia Wong Solano, quien abandona la sesión virtual.

CAPÍTULO VI. MOCIONES

ARTÍCULO XI: Mociones.

Las señoras y señores miembros de la Junta Directiva no presentan mociones en el desarrollo de esta sesión.

CAPÍTULO VII. ASUNTOS VARIOS

ARTÍCULO XII: Asuntos Varios.

Inciso a) El **M.B.A. Carlos Arias Alvarado** comunica: a las 12:00 p.m. tengo una reunión con los representantes de Popular Pensiones, BN Vital, Poder Judicial, Vida Plena OPC y nosotros, para hablar del tema de la SAFI de BCR; para explorar cómo está el tema. Cada uno de ellos y nosotros mismos estaríamos con la asesoría legal para ver los aspectos legales de lo que ha salido recientemente, lo que les he venido conversando, para que ustedes lo tengan ahí en su existencia. Nosotros nos hemos estado moviendo con todos estos temas. **SE TOMA NOTA**

Inciso b) El **M.B.A. Carlos Arias Alvarado** informa: a las 4:00 p.m. tenemos reunión de personal; nosotros hacemos una reunión de personal presencial una vez al mes, entonces, hoy a las 4:00 p.m. estaríamos reuniéndonos, para

que ustedes tengan conocimiento de eso. Esto implica que cerramos las oficinas nuestras antes de las 4:00 p.m.

El **Lic. Jorge Rodríguez Rodríguez** indica: muy importante esos acercamientos con el personal, me parece que sin duda alguna aportan mucho a un buen clima, en buena hora. **SE TOMA NOTA**.

El señor presidente finaliza la sesión al ser las diez horas con veinte minutos.

JORGE EDUARDO RODRIGUEZ RODRIGUEZ (FIRMA)
Firmado digitalmente por JORGE EDUARDO RODRIGUEZ RODRIGUEZ (FIRMA)
Fecha: 2024.03.12 16:31:03 -06'00'

ERICK OLIVER VEGA SALAS (FIRMA)
Firmado digitalmente por ERICK OLIVER VEGA SALAS (FIRMA)
Fecha: 2024.03.12 16:27:58 -06'00'

LIC. JORGE RODRÍGUEZ RODRÍGUEZ
PRESIDENTE

M.SC. ERICK VEGA SALAS, M.B.A.
SECRETARIO

ÍNDICE DE ANEXOS

No. Anexo	Detalle	Numeración del libro
Anexo No. 1	❖ Oficios DE-0080-02-2024 y DA-0065-02-2024: informe de los activos donados durante el periodo 2023. ❖ Oficio G.-048-02-2024 suscrito por la Licda. Zianny Morales Guevara, gerente de la Corporación de Servicios Múltiples del Magisterio Nacional: remite los estados	Folios del 73 al 92

	financieros de la Corporación, correspondientes a enero de 2024. ❖ Correo electrónico remitido por el M.Sc. José Edgardo Morales Romero, M.B.A., miembro de Junta Directiva, en el que justifica su ausencia a la sesión de hoy, por asuntos personales. (20 páginas).	
Anexo No. 2	❖ Oficios DE-0099-02-2024, JD-US-0042-01-2024, ORH-7437-2023, ORH-7367-2023, la escala salarial administrativa 2021-2023 y la escala salarial docente 2021-2023: que corresponden a la aplicación del costo de vida para la población correspondiente de la Ley 2248 de la Universidad de Costa Rica. (6 páginas).	Folios del 93 al 98
Anexo No. 3	❖ Oficio COM-INV-0003-02-2024: acta de la sesión ordinaria No. 03-2023 del Comité de Inversiones. (98 páginas).	Folios del 99 al 196
Anexo No. 4	❖ Oficio COM-AJS-01-01-2024: acta de la sesión ordinaria No. 10-2023 de la Comisión de Asuntos Jurídicos y Sociales.	Folios del 197 al 315

	❖ Cuadro comparativo titulado: "Reglamento Organización y Funcionamiento". ❖ Cuadro comparativo titulado: "P31-RP-002. Política Marco de Gestión de Seguridad de la Información". ❖ Cuadro comparativo titulado: "P31-RP-001. Política de Seguridad de la Información y Ciberseguridad Institucional". (119 páginas).	
Anexo No. 5	❖ Oficio SG-P-12-2024 del SEC, referente al rechazo de la remoción del M.Sc. José Edgardo Morales Romero. ❖ Oficio PGR-C-184-2023 de la PGR: remoción de miembros de Junta Directiva. (25 páginas).	Folios del 316 al 340
Anexo No. 6	❖ Oficios AI-1073-12-2023, AI-1061-12-2023 y la presentación del Estudio No. 44-2023: "Riesgos de seguridad de la información". ❖ Oficio AI-1065-12-2023 y la presentación del Estudio No. 45-2023: "Cuentas por pagar proveedores". (70 páginas).	Folios del 341 al 410
Anexo No. 7	❖ Control de asistencia. (1 página).	Folio 411