

ÍNDICE

SESIÓN ORDINARIA N.º 2512

Lunes 7 de octubre del 2024

CAPÍTULO I	APROBACIÓN DEL ACTA
1.º	Aprobación del acta de la sesión ordinaria número 2511 del lunes 30 de setiembre del 2024.
CAPÍTULO II	ASUNTOS DE LA GERENCIA GENERAL
2.º	Sistema de Planificación de Recursos Empresariales ERP y Proyecto Sistema Integrado de Planificación SIP. Informe trimestral.
3.º	Actualización del informe sobre contrataciones que RACSA ha adjudicado y en las que resultó adjudicataria y figuras de contratación.
4.º	Estrategia Corporativa Grupo ICE 2023-2027. Cuadro de Mando Integral Corporativo. Informe para el Comité de Estrategia y el Consejo Directivo del ICE. Confidencial.
5.º	Cumplimiento metas establecidas en Plan Financiero 2024. ICE Consejo Directivo 6643 0012-536-2024. Confidencial.
6.º	Resumen de las principales actividades realizadas por la Auditoría Interna al I Semestre 2024 y estado de las recomendaciones emitidas por la Auditoría Interna y Entes Externos. Informe sobre el estado de los hechos relevantes. Confidencial.
7.º	Reglamento de Uso de Recursos Informáticos de RACSA.
8.º	Presupuesto Empresarial 2024 (Contraloría General de la República. Improbación del presupuesto extraordinario número 1-2024. Oficio 13490 DFOE-CIU-0351-2024. Confidencial.
CAPÍTULO III	ASUNTOS DE LA JUNTA DIRECTIVA
9.º	Política de Transparencia y Acceso de la Información Pública del Grupo ICE. Informe de cumplimiento.
CAPÍTULO IV	COMENTARIOS Y PROPOSICIONES
10.º	Programa General 5G Alianza Estratégica ICE-RACSA. Solicitud de ampliación de plazo sobre la actualización del caso de negocio. Confidencial.

ACTA DE LA SESIÓN ORDINARIA N.º 2512

Antes de iniciar la sesión, la Presidencia y la Secretaría de la Junta Directiva hacen constar que dicha sesión se realizará mediante la utilización de la plataforma tecnológica Zoom, la cual permite cumplir con las condiciones esenciales de simultaneidad, interactividad e integralidad en la comunicación de todos los participantes. Lo anterior en acatamiento de lo que establece la Directriz DPJ-001-2020 de la Dirección Registro de Personas Jurídicas sobre la celebración de asambleas y sesiones, la Ley General de Administración Pública N.º6227 y la Norma Técnica NTN-006.

Acta de la sesión ordinaria número dos mil quinientos doce celebrada por la Junta Directiva de Radiográfica Costarricense, Sociedad Anónima, a partir de las diecisiete horas con veintisiete minutos del lunes siete de octubre del año dos mil veinticuatro.

Presentes; el presidente, señor Rodolfo Enrique Corrales Herrera, ubicado en su oficina; la vicepresidenta, señora Laura María Paniagua Solís, ubicada en su domicilio; el tesorero, señor Erick Mauricio Brenes Mata, ubicado en su domicilio; la secretaria, Natuska Traña Porras, ubicada en su domicilio; y el vocal, señor Luis Fernando Ramírez Loría, ubicado en su domicilio.

Como invitados, por la Administración: el gerente general, señor Mauricio Barrantes Quesada; el director administrativo – financiero, señor José Mario Murillo Meléndez; el director de operaciones a.i., señor Daniel Valverde Ramírez; el director del proyecto SIP ERP, señor Gustavo Montero Zúñiga; la directora jurídica y regulatoria, señora Illiana Rodríguez Quirós, todos ubicados en su domicilio.

El señor Rodolfo Corrales, en su condición de presidente, inicia la sesión e indica: *“Buenas tardes, espero que se encuentren muy bien. Vamos a dar inicio, a la sesión ordinaria número 2512, a celebrar hoy lunes 7 de octubre del 2024, al ser las diecisiete horas con veintisiete minutos”*.

CAPÍTULO I APROBACIÓN DEL ACTA

Artículo 1. ° Aprobación del acta de la sesión ordinaria número 2511 del lunes 30 de octubre del 2024

El señor Rodolfo Corrales, indica: *“Como primer punto de nuestra agenda tenemos la aprobación del acta anterior, que corresponde a la sesión número 2511, celebrada el pasado lunes 30 de setiembre del 2024.*

La cual someto a votación.”

El presidente, señor Rodolfo Enrique Corrales Herrera; la vicepresidenta, señora Laura María Paniagua Solís; el tesorero, señor Erick Mauricio Brenes Mata; la secretaria, señora Natuska Traña Porras; y el vocal, señor Luis Fernando Ramírez Loría, se manifiestan de acuerdo con el contenido del acta y la dan por aprobada.

CAPÍTULO II ASUNTOS DE LA GERENCIA GENERAL

Artículo 2. ° Sistema de Planificación de Recursos Empresariales ERP y Proyecto Sistema Integrado de Planificación SIP. Informe trimestral.

El señor Rodolfo Corrales, indica: *“En razón del seguimiento que se ha dado a la implementación del Sistema de Planificación de Recursos Empresariales ERP – Talento Humano y Costo, denominado: Proyecto Sistema Integrado de Planificación – SIP, según consta en las sesiones números: 2311, 2314, 2324, 2335, 2338, 2341, 2367, 2381, 2397, 2410, 2425, 2438, 2451, 2464, 2476, 2485, 2490, 2496, 2500 y 2508, la Gerencia General, mediante los oficios de referencia GG-1601-2024 del 27 de setiembre del 2024 y GG-1630-2024 del 1° de octubre del 2024, presenta a esta Junta Directiva y al Comité de Vigilancia el informe trimestral con el estado del proyecto y señala que dado su complejidad autorizó la entrada en operación a partir de diciembre del 2024.*

En cuanto a la atención de las recomendaciones que ha emitido las auditorías sobre este tema, la Administración mediante el oficio de referencia DIAF-547-2024 del 30 de setiembre, señala que la mayoría de ellas están contempladas; no obstante, no se pueden dar por atendidas hasta que el sistema entre en producción.

Con el propósito de conocer en detalle la situación de este proyecto, este tema será expuesto por los representantes de la Administración, a quienes les damos la bienvenida.

Buenas tardes don Mauricio, don José Mario, don Gustavo y don Daniel”.

Ingresan a la sesión de forma virtual, el gerente general, señor Mauricio Barrantes Quesada, el director administrativo financiero, señor José Mario Murillo Meléndez; el director de operaciones a.i., señor Daniel Valverde Ramírez; y el director del proyecto SIP ERP, señor Gustavo Montero Zúñiga.

El señor Gustavo Montero, inicia la exposición e indica: *“Buenas tardes, perfecto, bueno, vamos a empezar entonces con lo que corresponde al informe número 12, el resumen correspondiente al corte al 16 de setiembre del 2024.*

En esta primera diapositiva, lo que encontramos es el estatus del proyecto en cada uno de los diferentes módulos con respecto a las diferentes etapas del ciclo de vida de los sistemas.

En términos globales, podemos ver que el avance es de un 90, 27 % y aquí viene cada uno de los diferentes sistemas en sus etapas. Igualmente aquí vienen los diferentes valores, en la parte de abajo viene cuál es el avance, pero en la siguiente diapositiva, se puede ver aún mejor este avance.

Bien, entonces en este caso lo que sí podemos ver es que de la totalidad de módulos que se tienen están siendo atendidos 21 de ellos, del 22 al 24 ya también están siendo atendidos, como ya se han empezado a liberar recursos ya se están atendiendo los mismos, y lo que es el módulo 28, digamos, a RACSA a no tener deuda, pues entonces habría quedado por fuera, y los otros tres que están aquí del 25 al 27 están o en espera de definición de requerimientos o una solicitud expresa, como es el caso de la parte de gerencia y de gobierno corporativo.

En esta diapositiva, lo que resume son los diferentes estados, cuáles son los módulos o funcionalidades que están en producción, pues los ya conocidos a nivel de salud y bienestar, expediente y capacitación, la parte de seguridad que abarca todos y presupuesto en lo que corresponde a la modalidad de formulación.

En los módulos que estaban en pruebas funcionales integrales estaba la parte de nómina. Que en realidad nómina está funcionando con un paralelo, tratando de cerrar una de las quincenas para poder detectar una serie de errores y poder con ello ya tomar decisiones con respecto a lo que corresponde.

Los resultados han sido bastante satisfactorios, de hecho, aquí me voy a adelantar un poquitito con algo, dentro de lo que son los hallazgos, y es que al haber una serie de cosas o de inconsistencias en el sistema que se está usando hoy en día y que se tienen que hacer muchos ajustes en las diferentes quincenas, más bien lo que se ha logrado determinar es que el sistema nuevo claramente resuelve todo ese problema de inconsistencias. Provocando que el comparativo que se está haciendo con respecto a las quincenas no cierre.

Por una razón muy sencilla, el sistema está haciendo las cosas bien y el otro más bien es el que tenía las diferencias que se ajustan en la quincena posterior. Entonces lo último que estábamos encontrando eran pequeños movimientos que tal vez no estaban aplicados y en los próximos días más bien va a venir una resolución, pero que es prácticamente un hecho que va a ir en la línea de empezar de una sola vez con el sistema en producción completo, ya teniendo cargados todas las diferentes deducciones y todos los diferentes incidentes, puesto que no es posible llegar a obtener que el paralelo dé igual, cuando ya sabemos que el sistema que estamos utilizando actualmente, digamos, que no está dando los resultados correctamente, y más bien el sistema nuevo elimina toda esa problemática, porque todo lo está procesando completamente en línea.

Contabilidad, se está trabajando en lo que es la obtención de los saldos, para poder empezar a hacer un paralelo en un ambiente controlado.

Cuentas por pagar, registro de facturas también estaba como parte de estos avances a nivel de lo que eran los pendientes para cerrarlo, pero también entraría dentro de lo que es ese ambiente controlado a partir del próximo mes.

Y se está trabajando en los desarrollos, bueno, en la parte de lo que es la nómina, en lo que es cuentas por pagar, contabilidad y evaluación de desempeño. También ya se están atendiendo otros módulos como es la parte de gestión del tiempo, como formación, capacitación y desarrollo.

También estamos trabajando en lo que es la parte de compensación y beneficios que esos, digamos, acaban apenas de empezarse.

Aquí es donde viene el resumen ya completo de cada uno de los módulos con su respectivo avance individual, en donde podemos ver, digamos, ya lo que sería, por ejemplo, conciliaciones bancarias, movimientos bancarios, lo mismo que contabilidad y cuentas por cobrar, son los módulos que estaríamos empezando ahorita una vez que tengamos los saldos contables correspondientes al corte del mes de agosto, son los que estarían entrando en producción en un ambiente controlado y cuando ya tengamos los resultados de estos modos estaríamos empezando con el grueso de los módulos, que serían prácticamente todos los demás, a excepción de compras, recepción de materiales y otros que estaban por ahí, que más adelante se exponen; sin embargo, aquí vienen los avances individuales de cada uno de los diferentes módulos para dar el 90,27 %.

En cuanto a lo que era el avance de las pruebas y certificación, ya en lo que era nómina, digamos, estaba en un 85 %; sin embargo, aquí ya más bien estamos corriendo paralelo, de tal forma que ese 15 % restante no lo vamos a ver tal cual en el avance acá, sino que prácticamente va a ser en los mismos resultados que se están obteniendo con respecto al paralelo efectuado.

En el caso de la contabilidad prácticamente que va a ser igual, puesto que ya inclusive si están revisando los diferentes estados financieros, y lo que está pendiente únicamente es el poder cuadrar los saldos con los cuales vamos a empezar, dado que el catálogo contable con el que se está trabajando actualmente, para el nuevo sistema se reduce sustancialmente. Y el trabajo de poder obtener los saldos iniciales a partir del catálogo nuevo, pues es un trabajo bastante complejo que todavía se sigue atacando y que hasta que no esté listo, en realidad no podemos empezar con todos los demás.

Sin embargo, ya lo llevamos bastante adelantado, y esperamos en los próximos días que ya podamos tener esos saldos iniciales con los cuales ya pueden empezar a ejecutarse o a correr los diferentes

módulos que están previstos para la primera etapa de entrada en producción, en un ambiente controlado.

Cuentas por pagar, registro de facturas, en realidad estaba pendiente más bien que la contabilidad obtuviera esos saldos iniciales para poder liberar el espacio como tal y que le pueden empezar a probar asientos contables, porque lo que queda pendiente solamente son aprobación de asientos y validar que los mismos estén ahí listos.

En evaluación de desempeño, es un módulo que no pertenece al CORE, o sea, no es un módulo central y se había detenido en un momento dado porque se habían cambiado una serie de requerimientos asociados al mismo; sin embargo, ya se retomaron lo que son las pruebas de este módulo y en los próximos días ya más bien estaría dándose por certificado.

En lo que corresponde a la capitalización del proyecto, el monto capitalizado por lo menos a la fecha corte era de 1 100 millones. En el informe propiamente en la descripción también hacemos una acotación con respecto a este monto, y es que este monto incluye tanto lo que es la parte del desarrollo como tal, como el tiempo de toda la gente que de una u otra manera ha participado en todo el proceso de definición de requerimientos, llevar a cabo las diferentes pruebas funcionales, pruebas técnicas, en fin todo ese proceso es lo que lleva ese acumulado a nivel de la capitalización.

Y hacemos una diferenciación con respecto a lo que igualmente se había puesto en el proyecto, en la definición original del proyecto que fue aprobado, porque en apariencia hace verse una diferencia muy amplia en cuanto a la variación de los costos; sin embargo, los que se definieron originalmente solo incluían lo que normalmente ofrecen los proveedores y contra lo que se comparó originalmente también que era los costos del desarrollo y la implementación como tal, más no el tiempo de toda la gente que participa, en reuniones, en definición y en todo ese tipo de elementos.

Eso sí, cuando hacemos una comparación ya más realista de los montos, en realidad lo que nos hemos pasado con respecto al monto original anda alrededor de un 5 %.

Esta en realidad, lo que viene es a mostrar una serie de fechas que se habían propuesto, que es finalizar las pruebas en el transcurso de este mes, las de CxP cuentas por pagar, registro de facturas y la parte de contabilidad.

Y aquí en lo que viene en el tiempo límite de migración de datos es que, como estaríamos entrando en producción en un ambiente controlado con los diferentes módulos, entonces el primer grupo tenía un tiempo límite para lo que era la migración de datos al 25 de setiembre, esto era conciliaciones bancarias, movimientos bancarios, y cuentas por cobrar.

Después entra en el otro grupo, los del 11 de octubre, entrarían ya por ejemplo, los que tienen que ver con cuentas por pagar, lo que tiene que ver con la parte de recepción de materiales, el manejo de las órdenes de compra, en fin, los que están definidos en el segundo grupo, que también creo que es en el mismo informe se expone.

Después finalmente, viene la parte del inicio productivo, que es en el paralelo, que en realidad, bueno, ya este primer grupo el corte estaba al 31 de agosto para obtener los saldos de contabilidad; sin embargo, como todavía no los hemos obtenido, entonces no han podido iniciar los demás y esos son los que se van a correr un poquito.

Sin embargo, lo que sí tenemos previsto es en que lo que resta del año los módulos van a ir entrando en producción en un ambiente controlado para certificar que efectivamente están funcionando bien entre sí, que los saldos y que están funcionando también perfectamente, los movimientos que se están dando entre ellos, para finalmente en diciembre dar garantía de que todo funciona correctamente, que tenemos todo pegado al centrado, por lo menos en cuanto en la forma en que está funcionando, hacer un borrado y empezar año nuevo con saldos nuevos, y a sabiendas de que todos los módulos estaban funcionando perfectamente para no afectar el ciclo como tal que corresponde al año. Que todo se empiece con un histórico único.

Esto corresponde a lo que es el informe de gestión del cambio, en donde se viene dando el apoyo de los compañeros de gestión del cambio, en donde nos acompañan en lo que son las reuniones de seguimiento, el apoyo en la gestión de las reuniones del proyecto, campañas de comunicación, actividades de capacitación, comunicación general del proyecto, realización de las entrevistas ADKAR, y aquí falta inclusive agregar algunos elementos que nos están apoyando hoy en día, como son las coordinaciones de las capacitaciones, el llevar los controles de asistencia. Luego todo lo que son los comunicados a lo interno de los avances y de las cosas que están entrando en producción.

Básicamente, eso es lo que corresponde a la presentación que nosotros tenemos con respecto al avance del proyecto.

¿No sé si alguien quiere agregar algo más? Sino quedo a las órdenes”.

El señor Rodolfo Corrales, señala: *“Muchas gracias, don Gustavo. Don José Mario, adelante”.*

El señor José Mario Murillo, responde: *“Muchas gracias, don Rodolfo, si quisiera hacer un par de comentarios.*

Las decisiones que se han tomado con respecto al tema del ERP y su prolongación en el tiempo que nos ha llevado, son decisiones que hemos pensado y actuado en consecuencia a intentar cumplir con tres requisitos que son muy importantes para nosotros, el tema de la confiabilidad de la información y eso enfáticamente, Gustavo dice que lo que necesitamos ahora es que todo...”.

La señora Laura Paniagua, interrumpe: *“No se escucha don José Mario”.*

El señor José Mario Murillo explica: *“Algo pasó me “mutearon” por ahí.*

Les repito perdón, que son tres requisitos que hemos estado pensándolos y siendo muy consecuentes en el tema de poder asegurarnos los tres, uno la confiabilidad de la información para que los diferentes módulos se hablen entre sí, que la información corra de un lado a otro de manera transparente y verificable a nivel de cada uno de los módulos.

Porque lo que hemos hecho es muchas piezas de un lego, verdad, es un lego bastante grande, es un lego que no es pequeño y lo que necesitamos es que encajen muy bien, verdad, y que no tengan ninguna fricción una con otra.

El otro tema es la reducción, evidentemente de que en ese momento, cuando echamos a caminar con la máquina encendida, que tengamos la menor cantidad de errores o fallos, porque eso en la implementación es muy complejo. Porque si desanima al usuario, lo pone a dudar, hace un ambiente

bastante complicado y entonces para nosotros es fundamental que cuando echemos a correr todo mundo con el aplicativo completo, esa cantidad de fallos sea la mínima posible.

Y el tema, evidentemente, de la carga de trabajo de los usuarios es algo que hemos pensado, que hemos trabajado, que hemos considerado, porque llevar un paralelo es pesado, verdad, es trabajar con lo que estoy haciendo hoy actualmente en los sistemas, que hoy hago actualmente y tener que replicarlo en el sistema nuevo.

Ahí hay un factor que también es importante y que hemos valorado en otros momentos, porque hemos planteado poder echar a andar el sistema en otros meses durante el año. Contablemente, evidentemente, el mejor mes para echar a andar un sistema es en enero.

¿Por qué? Porque yo arranco solo teniendo que trasladar ciertos saldos que van al estado de situación, pero lo que tiene que ver con ingresos y con gastos siempre arranco desde cero. Entonces esa información no tengo que transmitirla, no tengo que llevarla, no tengo que migrarla, la empiezo desde cero en enero.

Entonces, eso es parte de lo que hemos venido valorando y que para nosotros es muy importante.

En el Comité de Vigilancia se hace una observación con el tema del seguimiento que vimos en un informe en la última sesión, con respecto a los hallazgos de auditoría externa que mencionan temas del SIP-ERP, parte de lo que se planteaba es que si los íbamos a tener nuevamente con la auditoría que está iniciando operación este año para todo el Grupo ICE, que es la empresa Crow, probablemente sí, creemos desde la parte financiera ellos estén analizando lo que viene en las cartas anteriores y analizando el desarrollo que tenemos en este momento, que por cierto, hace unos días se les hizo una presentación de todo lo que era el tema del SIP-ERP, puede ser que ellos perfectamente lo vuelvan a mencionar, pero eso no es un hallazgo grave en el entendido de lo tenemos identificado, pero son las limitaciones del sistema.

Ellos, al ver que estamos desarrollando, probablemente van a ver el respaldo de hacia dónde vamos y posteriormente en las diferentes revisiones que ellos realicen, van a ver que eso se complementa perfectamente en el desarrollo del sistema, con lo que son las observaciones de limitaciones que tenemos actualmente.

Eso es, digamos, lo más relevante que quisiera mencionarles, porque es un tema que probablemente no vamos a poder, que podemos tal vez negociar con ellos, pero que probablemente ellos pueden incluirlo como una observación nuevamente o un hallazgo de auditoría, que lo que hace es revelar de la situación de lo que tenemos actualmente, pero que sabemos que estamos en camino de resolverlo a través del SIP-ERP.

Eso era lo que quería mencionarles don Rodolfo”.

El señor Rodolfo Corrales, indica: “Gracias, alguno otro tiene una consulta o comentario al respecto”.

La señora Laura Paniagua, consulta: “¿Y cómo lo ven con respecto a los tiempos? Sí lo vamos a poder cumplir, para no incrementar más, digamos, el tema de los imprevistos, los costos, no sé si don José Mario”.

El señor José Mario Murillo, responde: *“Yo soy el más interesado, doña Laura, Gustavo no me deja mentir, soy el más estresado al respecto, Daniel mismo que está aquí, nosotros somos el cliente número uno porque sabemos que vamos a un mejor mundo de lo que tenemos hoy actualmente.*

Y a partir de lo que tengamos y de lo que se cierre en esta primera fase del proyecto, todavía tenemos que construir más, porque hay un tema de riqueza ya de la plataforma como tal, que tenemos que potenciar todavía muchísimo más. Pero bueno, esas serán otras etapas.

Lo que vamos a recibir es muchísimo más de lo que tenemos, entonces para nosotros es fundamental.

Vamos a ver esta aproximación que estamos haciendo en este momento, que es un cambio lo que habíamos dicho anteriormente, lo que intenta es eso, un poquito equilibrar cargas de trabajo, equilibrar a los equipos. La gente ya está cansada, es evidente que el desarrollo propio interno es pesado, verdad, porque es el mismo usuario haciendo el esfuerzo de hacer las cosas mejor en un sistema nuevo, pero sin dejar de hacer lo que estoy haciendo todos los días en los sistemas viejos”.

La señora Laura Paniagua, agrega: *“Ya la operación.”.*

El señor José Mario Murillo responde: *“Exacto, es la operación del día a día.*

Creemos que con los márgenes de tiempo que estamos planteando podemos salir. Esa es la conclusión que tenemos”.

El señor Gustavo Montero, agrega: *“Yo igualmente creo lo mismo, que sí vamos a salir con esto, y que cómo se llama, que más bien precisamente este lapso que nos está quedando, es más bien no para pegar y terminar pruebas, sino para llegar y ver que todas las pruebas que hicimos estamos haciéndolas bien, que lo que vamos a correr, llamémosle un paralelo, pero es para que la gente vea funcionando el sistema, cómo se va alimentando y todo, pero ese paralelo en realidad se va a materializar en el mes de enero, cuando hagamos el borrado completo, empecemos desde cero con los saldos que indicó don José Mario, y que ya más bien estos tres meses que tenemos, en el que estamos ahorita y los dos siguientes, únicamente son para garantizar que lo que la gente está metiendo, los cálculos que se están haciendo son correctos y podemos hacer el borrado a finales de diciembre, para empezar con los saldos del corte al 31 de diciembre, metidos en el sistema en los primeros días de enero, y a partir de ahí, adiós sistema anterior, bienvenido al sistema nuevo”.*

La señora Laura Paniagua, indica: *“Muy bien. Muchas gracias don Gustavo y don José Mario”.*

El señor Rodolfo Corrales, señala: *“Natuska, adelante”.*

La señora Natuska Traña consulta: *“Buenas tardes, yo tengo una pregunta, estaba revisando que en la sesión ordinaria del 7 de julio de 2021, la número 2335 se dio el plan de trabajo de ERP Costeo y Talento Humano, para julio 2021 se había establecido el plazo para concluirlo de 18 meses.*

Entonces no me queda claro de la presentación y el informe registrado, si no se cumple el plazo de los 18 meses, de cuánto eran las prórrogas establecidas y las justificaciones para que estemos en este momento viendo estos puntos del informe, considerando, verdad, que el monto actualmente ha superado en un 53 % el presupuesto inicial del proyecto.

Entonces, quisiera saber, verdad, de esos 18 meses, cuánto se estableció al inicio de proyecto que se podían extender en prórrogas y cuál es el plazo de finalización que va a tener este proyecto, gracias”.

El señor Gustavo Montero explica: *“Ok, sobre ese particular, en realidad bueno, eso que está ahí, es en lo que es la definición del proyecto y es correcto lo que ahí se había establecido.*

Sin embargo, a lo largo del tiempo hay una serie de informes en los cuales nosotros venimos presentando qué era lo que iba sucediendo, y una de las cosas más importantes es que todas las premisas iniciales del proyecto no necesariamente se cumplieron.

No se cumplieron en varios aspectos, bueno, primero que todo, la cantidad de recursos que se definieron para lo que era el desarrollo del proyecto, o sea, cuando se parte de que se dura 18 meses, se parte de un conjunto de recursos, los cuales iban a tener ciertas características por definición. ¿Qué sucede?, cuando nosotros nos damos a la tarea de contratar los recursos, con lo que nosotros estábamos ofreciendo para contratar los recursos, en lugar de poder contratar profesionales que fueran ya que vinieran a producir de manera inmediata, tuvimos la mala suerte de que no logramos contratar prácticamente a nadie que tuviera las habilidades ya desarrolladas, a excepción de una o dos personas, que de alguna manera en conjunto con los recursos que ya teníamos, entonces tuvimos que hacer una mezcla entre recursos novatos con recursos capacitados, entonces, primera razón. Ya eso, obviamente, iba a demorar lo que era el desarrollo.

Segunda razón, lo que era la parte a nivel de lo que es la definición de los requerimientos, el tiempo de la misma gente, todo esto que está mencionando don José Mario, donde habla de que la gente tiene que convivir con su día a día, no hay un “pool” de recursos adicionales, en ningún momento a lo largo de todo el proyecto, nunca hubo un “pool” aparte de recursos para que vinieran e hicieran las tareas de ese día a día y que la gente se dedicara completamente a lo que era el desarrollo. Entonces eso también fue otra de las cosas.

Ahora con respecto que si en algún momento en el proyecto se indicaba que había plazos para prórrogas, no, lo que sí hay son informes en donde en cada uno de ellos nosotros solicitamos prórroga de “x” tiempo, las cuales fueron del conocimiento tanto de la Gerencia como de la Junta Directiva, y en cada uno de esos informes también se expusieron las razones del porqué era que se iban extendiendo los plazos.

Ahora si lo vemos también desde el punto de vista de lo que se presentó ahorita, ya podríamos decir que estos tres meses que restan serían lo último y ya no son ni siquiera una prórroga porque nosotros estamos atrasados con respecto a un desarrollo, sino más bien son una prórroga para garantizar lo que dijo don José Mario, hace pocos minutos, que es garantizar la confiabilidad de los datos, garantizar de que efectivamente todos los procesos están funcionando correctamente y más bien ganarnos la confianza de los usuarios y evitar esa posibilidad de que empiecen a fallar las cosas y que luego los mismos usuarios sean los decepcionados con respecto a todo este proceso.

Ahora la diferencia que también menciona, posiblemente usted está refiriéndose al informe anterior con respecto al informe financiero que apareció, en donde se hace una comparación con respecto a lo que estaba estipulado originalmente con respecto a lo que se llevaba gastado en su momento, pues como lo indiqué, hay que tener mucho cuidado con respecto a los números, porque los números que indican a nivel de capitalización no necesariamente coinciden con la misma forma en que se calcularon los números con respecto a la definición.

Cuando nosotros hicimos la definición de los cálculos del proyecto, dijimos cuesta 733 millones de colones, con base a qué, con base al desarrollo, eso fue lo que se comparó contra las ofertas de SOIN, contra las ofertas de Oracle, contra las ofertas de los diferentes oferentes y qué es lo que ofertan ellos, su software, su implementación y nada más.

Qué es lo que pasa con la capitalización, la capitalización incluye, además de esos mismos costos, también incluye el tiempo de la gente, las reuniones, la preparación de requerimientos, la asistencia a todas las reuniones, el desarrollo de las pruebas, certificación, etcétera. Esa es básicamente la diferencia, por eso, aunque en el informe financiero se dice se habla del 53 %, pero es crudo si se comparan a valores iguales que serían contra los desarrollos, la diferencia es de un 5 %, dentro de 5 % y 10 %”.

La señora Natuska Traña, agrega: *“Gracias don Gustavo. Entonces de lo que usted menciona a este informe y a esta fecha, ¿ya tenemos la información suficiente para establecer la fecha de finalización del proyecto?”*

El señor Gustavo Montero explica: *“Sí, claro”.*

La señora Natuska Traña, agrega: *“Si sería importante también mencionarnos cuándo se prevé en si la finalización, justifica implementar lo que nos han expuesto en este informe”.*

El señor Gustavo Montero explica: *“Ok, precisamente es lo que ahorita que acabamos de mencionar, en donde más bien la idea es hacer el paralelo en este tiempo que nos está restando el año, para empezar en enero del 2025 y cuando hablo de enero del 2025, no es cerrando el mes de enero, no cerrando el mes de diciembre, que eso sí va a significar por ahí del 15 enero más o menos, entrar en producción ya con todo, y eso significa abandonar el sistema anterior y empezar ya todos los módulos en el sistema nuevo.*

Ese es el inicio productivo real del sistema, y en estos meses que restan van a ser inicios, nosotros le llamamos un paralelo controlado, pero es probando la funcionalidad de los diferentes módulos”.

La señora Natuska Traña, responde: *“Gracias”.*

El señor Rodolfo Corrales, agrega: *“Luis, adelante”.*

El señor Luis Ramírez, expresa: *“Muchas gracias, don Rodolfo.*

En mi caso eran dos preguntas, tal vez una un poco más técnica y una más administrativa, verdad, digamos a nivel técnico don Gustavo, entonces de aquí a final de año o bueno no sé si parte del proceso hay algún asunto sobre migración de información, es que, digamos, usted nos indica que los sistemas viejitos los vamos a apagar”.

El señor Gustavo Montero explica: *“No, no se van a apagar, ellos van a permanecer como historia. Como historia, porque en el nuevo va borrón y cuenta nueva de que todos van a tener su inicio de históricos a partir de aquí, los viejos no se van a apagar, ahí van a estar y van a estar disponibles para que se consulten y ahí van a poder sacar los comparativos de todo el año ahí para atrás y el nuevo va a ir a generar su propia historia.*

En los casos que sea necesario, sí se va a arrastrar un poco más de historia, porque por ejemplo, para conciliaciones bancarias se necesitan movimientos bancarios, estados de cuenta y otro montón de cosas hacia atrás, pero en realidad conciliamos hacia adelante”.

El señor Luis Ramírez, responde: *“Correcto, sí, perfecto.*

Entonces aquí el proceso de aquí a fin de año y al arrancar el otro año no considera ningún movimiento de información histórica, sino más la información operativa, es así”.

El señor Gustavo Montero, agrega: *“La que sea necesaria para cada módulo”.*

El señor Luis Ramírez, indica: *“Ok perfecto.*

La segunda pregunta es si, digamos, también en ese tiempo, vamos, entonces a completar temas como capacitación a los funcionarios en la nueva funcionalidad. Si vamos a completar la recopilación de todo el tema de perfiles, accesos, verdad, digamos, todo lo que se necesite para tener, verdad, el registro y los datos y la creación de usuarios, designación de perfiles, segregación de funciones, todo lo que, verdad, nos pidió un proyecto de esta naturaleza y que también está en varios de los estudios de auditoría, verdad, que quieren que se haga.

Entonces, si todo eso estaría contemplado entre esos plazos, ya para ese eventual 15 de enero tendríamos este tema los registros básicos que tenga el sistema, pero también todo el tema de usuarios y ya creados y capacitados”.

El señor Gustavo Montero responde: *“Sí, es correcto. De hecho, ya estamos trabajando en eso, hoy por ejemplo iniciamos una capacitación a nivel de movimientos bancarios. También empezamos en una capacitación con cuentas por cobrar hoy, mañana y el miércoles.*

También están previstas otras capacitaciones en las subsiguientes semanas y conforme van ingresando los respectivos módulos.

Junto con eso viene la definición de los usuarios y obviamente la parte de la asignación de roles, porque alentar cada módulo de esos en producción hacíamos de una vez la definición de usuarios, asignación de roles con sus responsabilidades, quiénes son los cuadros de reemplazo.

Porque hasta eso ya los sistemas lo van a tener controlado, y es que a nivel de talento humano, una de las cosas que tenemos es que eso es una novedad, porque antes ni siquiera estaba integrado, a nivel de talento humano ya tenemos inclusive quién es reemplazo de quién, quién labora para quién o quién autoriza a quién, porque entonces todo ese tipo de cosas, cuando una persona esté de vacaciones, igual no se va a quedar un trabajo sin hacer, porque ya sabemos quién es el segundo a bordo.

Entonces todo ese tipo de cosas ya no solamente está la definición de roles y responsabilidades en un módulo en particular, sino además su relación con talento humano para saber quién es el que lo va a reemplazar y que continúe la tarea, y que la empresa no se detenga porque un usuario no estaba definido, pero eso lo estamos haciendo desde ya”.

El señor Luis Ramírez agrega: *“La última pregunta que decía que es un poco más administrativa, digamos, aquí se presentan varios de los módulos, digamos, en cada módulo tiene que haber un área rectora en la materia, digamos, no necesariamente es el equipo de TI, verdad.*

Entonces eso también está definido, es que son las cosas que apoyan en la implementación de un ERP, verdad, que digamos quiénes son los responsables de la materia de bienestar, por ejemplo, de ese módulo, entonces eso también está claramente identificado.

Porque ahí es donde las áreas de TI se deberían de apoyar cuando entren todo el sistema ERP en operación, esas áreas rectoras son las primeras que tienen que apoyar, verdad, tanto en las pruebas en la implementación o si hubiesen consultas de otras áreas.

Entonces si por cada módulo ya tenemos definidas áreas rectora, que es la que después tiene que apoyar, tanto en la evolución, en la madurez del módulo y que probablemente también tenga algunos retos porque tiene algunos asuntos de auditoría y otros pendientes por ahí. Entonces ¿si esa definición ya la tenemos?”

El señor Gustavo Montero explica: *“Sí, es más, más bien esa respuesta, bueno, aquí tenemos presente al rector número uno, que es don José Mario, que es el que a partir de ahí, bueno, prácticamente, que como él lo dijo, él es el interesado número uno, ¿Por qué? Porque precisamente el ERP está hecho para todos los departamentos que él tiene a su cargo.*

Estamos hablando que empieza desde la Dirección Administrativa Financiera, pasa por talento humano, sigue con aseguramiento financiero y también está en la parte de proveeduría, y a partir de ahí inclusive se desglosa hacia diferentes áreas como presupuesto, cuentas por cobrar, cuentas por pagar, etcétera. Así en cada una de ellas, y precisamente bajo esa misma estructura, es que se construyó todo el ERP.

Entonces quiere decir que toda la gente, es más, el ERP que está aquí, no es una construcción de TI, eso es algo muy valioso que en realidad deberíamos entender.

Este ERP se construyó por parte de TI, con la ayuda de cada una de todas las diferentes áreas funcionales y en las cuales se les asignó un líder de TI, sobre lo cual de manera conjunta a lo que le iba indicando uno, iba desarrollando el otro y así fue como se le dio forma a toda esta pirámide que hoy le podríamos llamar ERP”.

El señor Luis Ramírez, responde: *“Muchas gracias. Don Gustavo”.*

El señor Gustavo Montero indica: *“Con gusto a la orden”.*

A partir de este momento se retira de la sesión el Presidente, debido que tiene un asunto propio de RACSA que atender.

La señora Laura Paniagua, manifiesta: *“Bueno, buenas tardes, don Rodolfo se tuvo que retirar, entonces voy a continuar yo con la sesión en mi rol de vicepresidenta.*

Don José Mario, adelante”.

El señor José Mario Murillo explica: *“Muchas gracias, doña Laura.*

Rápidamente también para complementar la respuesta de Natuska, el tema también del alcance de los módulos, lo que en el mapa original se había establecido en el desarrollo del sistema varió un poquito en el camino.

Por poner un ejemplo, llegó un director administrativo financiero nuevo y se le ocurrió preguntar de dónde estaba el tema de las cuentas por pagar, verdad, porque normalmente en las empresas afuera hay una sección solo de cuentas por pagar.

Bueno, eso en el mapeo que había original no estaba tan claro y tuvimos que hacer unas modificaciones ahí en el camino. Ese tipo de cambios, de modificaciones y de ajustes que se fueron dando en el tema del sistema, evidentemente amplían el alcance de lo que se pretendía originalmente, pero también ampliar un poco el plazo del desarrollo que había.

Entonces, esa es una de las razones del por qué, digamos, se han corrido de las fechas en ese tema, es muy importante lo que mencionaba Gustavo, en la administración original del proyecto no se cumplió la meta que se tenía de tener la suficiente o un número de capacidad técnica de desarrolladores que originalmente se había planteado, verdad, entonces, hay un desfase ahí de tiempo en el desarrollo que también nos pasó factura finalmente en el desarrollo.

Y sí, es importante también el tema del presupuesto, yo lo he comentado con Gustavo y lo hemos visto. En realidad seguimos dentro de la línea de lo que se había planificado en términos del costo original, el costo incremental que tenía para la empresa, porque a la hora que nosotros presentamos el número de capitalización, ahí estamos incluyendo todo el recurso humano que ya está en la empresa, que no se va a ir, que son los funcionales, digamos, de las diferentes áreas, la gente de contabilidad, la gente de presupuesto, la gente proveeduría, que son quienes hacen el trabajo normal, pero que son los que participaron, como bien lo dice Gustavo, en la elaboración del sistema.

Y bueno, esos eran, digamos, como los puntos a Natuska.

Y sí, tal vez contestarle a don Luis, los sistemas actuales permanecen completamente funcionales, van a ser la historia de RACSA y ahí está plasmada para cualquier requerimiento de información futura. Tienen que seguir, digamos, existiendo y demás, porque van a guardar esa historia.

Cuando hacemos el traspaso nos vamos a llevar pequeñas partes de esa historia, las que estén vigentes y la que sea necesaria trasladar, en términos de saldos de algunas de las cuentas, no necesariamente, y como les decía, por ejemplo, para empezar el primero de enero, yo lo que hago es un borrón y cuenta nueva en parte de ingresos y gastos, y empiezo a elaborar esa historia a partir de ahí, pero para ciertas cuentas y tengo que trasladar aquello que no tenga resuelto.

En eso estamos haciendo un esfuerzo muy importante también para limpiar todo aquello que haya en nuestro sistema hoy, que son cosas muy viejas, o sea, estamos hablando de cosas y registros de los ochentas, en algunos casos, que hemos venido limpiando, sacando para que no sean parte de esa transferencia que tenemos que hacer, porque tenga alguna vigencia alguno de esos estos datos.

Y evidentemente sí, como bien lo explica Gustavo, cada módulo tiene un líder técnico de la parte de TI, pero tiene un líder funcional, que es la parte quien ejecuta las labores del sistema o quien ejecuta las labores en este momento en la parte administrativa o financiera, y ese es el que tiene el liderazgo en términos de las respuestas o de las inquietudes que hay de cómo se hacen las cosas en los sistemas”.

El señor Luis Ramírez agrega: “Muchas gracias”.

La señora Laura Paniagua, indica: *“Muy bien, muchas gracias. Bueno, ¿no sé si alguno tiene otra consulta al respecto?”*

El señor Erick Brenes, consulta: *“No, doña Laura, yo tenía una consulta del proceso de transición, pero ya quedó respondida gracias a las preguntas de don Luis, gracias”.*

La señora Laura Paniagua, indica: *“Muchísimas gracias, don Erick.*

Bueno, entonces si es así, le agradecemos a don José Mario, a don Gustavo, verdad, y a don Mauricio también está con nosotros. Muchas gracias”.

A partir de este momento se retiran los representantes de la administración.

La señora Laura Paniagua, en su condición de Presidenta en ejercicio, concluye: *“Propongo dar por recibido el informe y solicitar a la Administración dar un seguimiento puntual a este tema para finalizar en la fecha planteada, en razón del impacto que tiene para la empresa la implementación de este proyecto.”*

La presidenta en ejercicio, señora Laura María Paniagua Solís; el tesorero, señor Erick Mauricio Brenes Mata; la secretaria, señora Natuska Traña Porras; y el vocal, señor Luis Fernando Ramírez Loría, resuelven dar por recibido el informe y solicitan a la Gerencia General dar un seguimiento puntual a este tema para finalizar en la fecha planteada, en razón del impacto que tiene para la empresa la implementación de este proyecto. Asimismo para efectos de seguimiento se programa el informe trimestral para la sesión de la tercera semana de enero del 2025.

Artículo 3. ° Actualización del informe sobre contrataciones que RACSA ha adjudicado y en las que resultó adjudicataria y figuras de contratación.

La señora Laura Paniagua Solís, en condición de Presidenta en ejercicio: *“La Gerencia General con el propósito de atender una solicitud planteada por el Comité de Vigilancia y lo dispuesto por esta Junta Directiva en la sesión número 2507, mediante el oficio de referencia GG-1591-2024 del 24 de setiembre del 2024, presenta un informe sobre las contrataciones que RACSA ha adjudicado o en las que ha resultado adjudicataria, así como las acciones que ha emprendido la Administración para mitigar el riesgo de exposición mediática.*

Este tema estuvo en la agenda del Comité de Vigilancia de la semana pasada; no obstante, pospuso el conocimiento hasta que el mismo fuese presentado en este órgano colegiado.

A partir de este momento cedo la palabra a los representantes de la Administración para que nos haga la presentación. Muchas gracias.”

Ingresa a la sesión el gerente general, señor Mauricio Barrantes Quesada y el director administrativo financiero, señor José Mario Murillo Meléndez.

El señor Mauricio Barrantes, inicia la presentación e indica: *“Sí, antes de iniciar, ahí me disculpan un poco, estoy medio resfriado, entonces me cambia la voz.*

Ese tema, digamos, inclusive sobre cada uno de los proyectos que se han adjudicado, desde que hemos arrancado con ese tema, la gerencia ha brindado varios informes, inclusive de la misma Proveeduría sobre los tipos de contrataciones, para determinar, digamos, que todo sea ejecutado según derecho.

Hasta la fecha todos los informes que nos han remitido, digamos, cumplen con ese principio, digamos, verdad, inclusive se pidió de todas las contrataciones, orden de inicio y todo eso, desde diciembre del año pasado.

Bueno, a lo largo del periodo hemos visto algunos requerimientos adicionales de información para tener certeza, igualmente. todos estos informes cuentan con estudios y proyectos, los cuales ya han sido contratados y llevan sus estudios técnicos, sus estudios financieros, sus estudios jurídicos.

Recientemente también solicité, digamos, a la Dirección de Operaciones un informe todavía aún más profundo para llevar un seguimiento mensual en el Comité Gerencial sobre todos los proyectos de inversión que la empresa tiene, y sobre las acciones que han ejecutado, las decisiones en el marco de las competencias conferidas, tanto en la organización como en la delegación de responsabilidades, digamos, que ha hecho la Junta, así con los poderes generalísimos que ellos ostentan.

Eso como para tener certeza de que todo se está trabajando de buena manera y pues cualquier cosa que se están tomando las medidas adecuadas para este encauzar los proyectos que tengan así desviaciones.

Entonces José Mario, si gusta continuar usted”.

El señor José Mario Murillo, continua con la exposición e indica: “*Gracias Mauricio.*

Sí, en contexto, como bien lo decía Mauricio, este es un tema de seguimiento a otros informes que ya se han presentado, que originalmente establecían el levantamiento de todas aquellas contrataciones que RACSA había adjudicado y en los que resultó adjudicataria a partir de diciembre del 2022 y durante el 2023, que fue el periodo que se dieron algunas consultas por parte de externos, dígase, diputados o información por parte de la Contraloría y demás, entonces esto es un seguimiento y es una ampliación de información.

Como verán, viene un detalle adicional, son muchos los procedimientos o los contratos y las adjudicaciones que están establecidas, en donde lo que se hace es un detalle más amplio del tema de cómo fue adjudicado RACSA, cómo se seleccionó, el tipo de servicio qué es, si es un servicio nuevo, era una renovación, etcétera, el monto que fue adjudicado con impuestos, el plazo, el modelo del negocio, cuál fue el aliado en cada caso, la participación que tenía RACSA en cada uno de estos en los casos que aplicara, el método de la selección del aliado, se establecía el tema del ahorro que esto generaba a nivel de lo que era la entidad contratante.

En algunos casos, se puede identificar, en otros no, por ser una contratación individual o que no venía, digamos, de un proceso de licitación anterior, y ese ahorro, digamos, en términos porcentuales.

Entonces verán que el detalle establece todo el inventario de contrataciones que se tuvo durante el 2023.

No voy a entrar en el detalle, ustedes lo tienen ahí, en la ampliación del informe. Vamos a la última que tiene el texto, si tienen alguna duda de alguna de esas, me indican.

Si es importante y recalcando lo que Mauricio mencionaba, la Administración de RACSA ha aplicado la Ley de Contratación Administrativa en todas estas contrataciones, en todas sus versiones, verdad, porque algunas de ellas vienen de procesos previos al último cambio que tuvo la Ley.

Igual se ha enfatizado en todos los involucrados el tema de la actuación ética, que tiene que ver no sólo con los principios de control interno que tiene la empresa, sino con el cumplimiento de la normativa que nos regía o por la que nos regimos en cada una de estas contrataciones.

Evidentemente, debido al fallo de la sala constitucional, en este momento se está en una elaboración, de una actualización de lo que tiene que ver con el Reglamento, que va a regular nuevamente la forma de hacer negocios, pero aplicando siempre los mismos principios fundamentales en términos de contratación, por ser RACSA una institución pública, verdad, y en el resguardo de, principalmente el tema de los bienes públicos, verdad, que tiene todo una connotación de cómo hacer los negocios desde nuestra naturaleza.

Acciones que se han emprendido desde la administración para mitigar el riesgo de exposición mediática, que es complemento también a lo que nos consultaron en términos de lo que había sucedido en su momento, por las consultas que venían de la prensa o de diferentes participantes.

Se ha iniciado una exploratoria de mercado para la contratación de una asesoría especializada en el manejo de crisis en comunicación e imagen empresarial, esto como una herramienta adicional de cómo responder a los públicos de interés, sobre las actuaciones de RACSA.

Se incentivó la participación de negocio, en la cual RACSA aporta el 100 % de los componentes necesarios para brindar los servicios. Si ustedes ven en las últimas contrataciones, en los últimos negocios en donde RACSA ha interactuado va con una intención de ser RACSA quien aporta el 100 %.

Ha variado muchísimo el tema de hacer negocios a lo interno de la empresa, procurando de buscar mejores márgenes inclusive, de la participación que tenemos y se ha procedido, evidentemente con la revisión, como bien lo mencionaba Mauricio, de todos los procesos que intervienen, ya sea en la contratación de bienes y servicios para uso de la empresa, en la selección de socios cuando corresponda y en los procesos de elaboración de ofertas, tanto en las contrataciones directas entre entes de derecho público, así como cuando se oferta bajo la figura de consorcio.

Se ha venido brindando respuesta oportuna a todos los requerimientos planteados por los diferentes actores, dígase, entidades de control, los medios de comunicación, para que al fin y al cabo, podamos demostrar que RACSA se ha pegado a toda la normativa bajo la cual se rige y que nos había aplicado o que nos estaba aplicando en cada momento en que hicimos cada uno de estos negocios.

Se busca un acercamiento con las fracciones legislativas, don Mauricio les ha comentado al respecto anteriormente, con el fin de aclarar el rol de RACSA de explicar qué hace la empresa y cuáles son las competencias que tiene por Ley.

Se ha mantenido un seguimiento periódico de todas las noticias, de todas las referencias que se generan de la empresa, para que se pueda atender oportunamente.

¿No sé si tienen alguna consulta?, creo que por aquí termina la intervención”.

El señor Mauricio Barrantes, acota: *“También es importante indicar que en este punto, la asesoría jurídica ha dado una capacitación adicional, sobre todo el tema de contratación pública a nivel interno, entonces, doña Illiana nos puede ampliar un poco también de ese tipo, creo que no lo mencionamos acá, pero que es importante.*

Nos decía que casi que ha tocado toda la gente que tiene, ya sea contrataciones o con procesos, digamos, de desarrollo y propuestas para los clientes, entonces creo que también es importante mencionarlo, verdad, y donde hay duda, hemos hecho todavía inclusive investigaciones más profundas para determinar si hay algún tema de gestión que requiera oportunidad o que requiera un tema de mejora, como les digo a la fecha, sin tener todavía ningún tema que, digamos, vaya a poner en riesgo con relación a estos procesos”.

La señora Illiana Rodríguez interviene: *“Sí, efectivamente, digamos, cuando hay una contratación que hay duda porque empezó con una normativa y terminó con otra o algo así, nosotros brindamos la asesoría y después, usualmente, siempre, digamos, hemos capacitado en relación con este tema.*

Cuando venía el régimen nuevo y ahora vamos a hacer una para repasar el régimen actual, porque hay gente que hace rato no lo usa o es gente nueva, entonces ya eso nos lo encargaron de parte de la Gerencia General en el Comité Director.

Entonces estamos trabajando en eso, porque la idea es que la gente esté familiarizada, porque a veces hay una confusión, porque dice, “Ah, bueno, tengo la ley nueva, entonces voy a usar solo la ley el 8660”, no señor, pero si usted le va a vender a la Junta de Protección Social, usted tiene que aplicar la ley que la aplica a ellos, que es la Ley General de Contratación Pública.

Entonces tienen que saber que los requisitos que hay que cumplir son los del cliente y nosotros aplicamos los nuestros para las compras que hacemos nosotros y las contrataciones, porque ahora hay que hacer esa diferencia, entonces por eso tienen que conocer los dos tipos de procedimiento.

Pero con mucho gusto, siempre hemos estado en esa mejor disposición y en coordinación con la Proveeduría, pronto vamos a dar una capacitación sobre el régimen de la 8660 y el Reglamento de las empresas y también estamos trabajando en una versión de reforma de ese Reglamento.

La señora Laura Paniagua, responde: *“Muy bien, muchísimas gracias doña Illiana.*

¿No sé si algún compañero tiene alguna consulta adicional? Entonces vamos a dar continuidad con el siguiente tema”.

A partir de este momento abandonan la sesión los representantes de la Administración.

La señora Laura Paniagua Solís: *“En virtud de lo anterior, propongo dar por recibido el informe y solicitar a la Gerencia General, para que con el apoyo de la Directora Jurídica y Regulatoria, programe un espacio de formación para esta Junta Directiva y sus Comités de Apoyo, así como para los miembros de la Comisión de Adquisiciones, sobre la formas de hacer negocio que tiene la empresa, el alcance de la Ley General de Contratación Pública y la Política corporativa para la prevención de la corrupción y gestión de conflicto de intereses y en un plazo de un mes presente la propuesta, la cual deberá ser de forma virtual, por un espacio de dos horas como máximo”.*

La presidenta en ejercicio, señora Laura María Paniagua Solís; el tesorero, señor Erick Mauricio Brenes Mata; la secretaria, señora Natuska Traña Porras; y el vocal, señor Luis Fernando Ramírez Loría, resuelve dar por recibido el informe y solicitar a la Gerencia General, para que con el apoyo de la Directora Jurídica y Regulatoria, programe un espacio de formación para esta Junta Directiva y sus Comités de Apoyo, así como para los miembros de la Comisión de Adquisiciones, sobre la formas de hacer negocio que tiene la empresa, el alcance de la Ley General de Contratación Pública y la Política corporativa para la prevención de la corrupción y gestión de conflicto de intereses y en un plazo de un mes presente la propuesta, la cual deberá ser de forma virtual, por un espacio de dos horas como máximo.

Artículo 4. ° Estrategia Corporativa Grupo ICE 2023-2027- Cuadro de Mando Integral Corporativo. Informe para el Comité de Estrategia y el Consejo Directivo del ICE. Confidencial.

Confidencialidad otorgada por el Consejo Directivo del ICE en el artículo 4 del Capítulo II de la sesión 6581 del 04 de julio del 2023, según oficio 0012-478-2023, por un plazo de cinco años, visto en la sesión de Junta Directiva N°2455 artículo 6.03 del 10 de julio del 2023, de conformidad a lo que establece la Política Corporativa de Confidencialidad de la Información en el numeral 6.3.3 inciso 2.

Artículo 5. ° Cumplimiento metas establecidas en Plan Financiero 2024. ICE Consejo Directivo 6643 0012-536-2024. Confidencial

Este tema se encuentra protegido por la declaratoria de confidencialidad de los Estados Financieros en Libros del ICE Separado período 2024, aprobada en el artículo 1 del Capítulo III de la Sesión 6614 del 27 de febrero de 2024.

Artículo 6. ° Resumen de las principales actividades realizadas por la Auditoría Interna al I Semestre 2024 y estado de las recomendaciones emitidas por la Auditoría Interna y Entes Externos. Informe sobre el estado de los hechos relevantes. Confidencial

Este artículo contempla las siguientes confidencialidades, según los siguientes temas:

- Servicio Preventivo de Advertencia sobre la Incidencia acontecida el 6 de noviembre de 2023 en el IDC del ICE: Confidencialidad otorgada por el Consejo Directivo del ICE en el artículo 2 del Capítulo II de la sesión 6614 del 27 de febrero del 2024, según oficio 0012-128-2024, por un plazo de cuatro años, visto en la sesión de Junta Directiva nro. 2482 artículo 6.01 del 04 de marzo del 2024.
- Evaluación del Servicio IaaS Infraestructura Convergente ofrecido al Tribunal Supremo de Elecciones: Confidencialidad otorgada por el Consejo Directivo del ICE en el artículo 2 del Capítulo II de la sesión 6581 del 4 de julio del 2023, según oficio 0012-476-2023, por un plazo de cuatro años, visto en la sesión de Junta Directiva nro. 2455 artículo 6.01 del 10 de julio del 2024.

Artículo 7. ° Reglamento de Uso de Recursos Informáticos de RACSA. Propuesta

La señora Laura Paniagua, indica: “*La Gerencia General, por medio del oficio de referencia GG-1622-2024 del 30 de setiembre del 2024, somete a conocimiento y resolución de esta Junta Directiva, una propuesta de reglamento de uso de recursos informáticos de la empresa, que tiene como objetivo establecer las reglas, límites, obligaciones y restricciones para el uso apropiado y requerido de las plataformas, sistemas y recursos de tecnologías de información y comunicaciones de RACSA.*”

Esta gestión cuenta con el criterio jurídico que indica que la aprobación de este instrumento corresponde a esta Junta Directiva y el visto bueno del Departamento de Estrategia e Innovación, en lo que refiere a la estandarización respecto con la normativa vigente.

En virtud de lo anterior, propongo acoger la propuesta de acuerdo en los términos planteados por la Administración”.

La presidenta en ejercicio, señora Laura María Paniagua Solís; el tesorero, señor Erick Mauricio Brenes Mata; la secretaria, señora Natuska Traña Porras; y el vocal, señor Luis Fernando Ramírez Loría, resuelven acoger la propuesta planteada por la Administración para resolver este tema.

La Junta Directiva basada en la documentación aportada, resuelve:

Considerando:

- a) **La Política de Seguridad de la Información de RACSA establece en su artículo primero el compromiso de RACSA en reconocer la información como un activo vital y estratégico para la Empresa y se compromete a establecer las acciones que apoyen la Gestión de la Seguridad de la Información con el fin salvaguardar la confidencialidad, integridad y disponibilidad de la información, mediante estrategias orientadas a la continuidad del negocio, la administración de riesgos informáticos y de información y la consolidación de una cultura de seguridad.**
- b) **El Reglamento de Uso de Recursos Informáticos es establecer las reglas, límites, obligaciones y restricciones para el uso apropiado y requerido de las plataformas, sistemas y recursos de Tecnologías de Información y Comunicaciones de RACSA.**
- c) **El Reglamento en estudio cuenta con el visto bueno de la Dirección Jurídica Regulatoria, por medio del oficio DJR-452-2024 de fecha 13 de agosto del 2024.**
- d) **El Departamento de Estrategia e Innovación, mediante oficio de referencia DEI-396-2024 del 16 de agosto del 2024, otorgó visto bueno al Reglamento de Uso de Recursos Informáticos de RACSA.**
- e) **La Dirección de Operaciones, mediante oficio de referencia DOP-440-2024 de fecha 20 de setiembre del 2024, remite a la Gerencia General para su conocimiento y remisión a la Junta Directiva el Reglamento de Uso de Recursos Informáticos.**

- f) La Gerencia General, mediante oficio de referencia GG-1622-2024 del 30 de setiembre del 2024, eleva a conocimiento de esta Junta Directiva el Reglamento de Uso de Recursos Informáticos de RACSA
- g) La Junta Directiva, según lo dispone el artículo 188 del Código de Comercio, en concordancia con el artículo 8.19 del Reglamento de la Junta Directiva de RACSA, es el Órgano Colegiado responsable de la aprobación de la normativa empresarial.

Por tanto, acuerda:

- 1) Aprobar el Reglamento de Uso de Recursos Informáticos de RACSA, de acuerdo con el siguiente texto:

Reglamento de Uso de Recursos Informáticos de RACSA

1. OBJETIVO

Establecer las reglas, límites, obligaciones y restricciones para el uso apropiado y requerido de las plataformas, sistemas y recursos de Tecnologías de Información y Comunicaciones de RACSA.

2. ALCANCE

El presente reglamento es de acatamiento obligatorio para toda persona que por sus funciones sea habilitada para utilizar equipos, software o para acceder a los recursos y servicios de comunicación propiedad de la Empresa, tanto dentro de las instalaciones como de forma remota.

Cubre la gestión integral de todos los recursos y servicios de Tecnologías de Información y Comunicaciones puestos a disposición del usuario. Además, define las reglas sobre el acceso a las plataformas tecnológicas empresariales por parte de las personas que utilicen equipos o dispositivos que no son propiedad de RACSA.

3. ABREVIATURAS

- **COBIT:** Control Objectives for Information and related Technology (Objetivos de Control para la Información y Tecnologías Relacionadas).
- **DLP:** Data Loss Prevention (Prevención de Pérdida de Datos).
- **FTP:** File Transfer Protocol (Protocolo de Transferencia de Archivos).
- **MFA:** Multi Factor Authentication (Autenticación de Múltiples Factores).
- **P2P:** Peer to Peer (De Persona a Persona).
- **RACSA:** Radiográfica Costarricense Sociedad Anónima.
- **TIC:** Tecnologías de Información y Comunicación.
- **VPN:** Virtual Private Network (Red Privada Virtual).

4. DEFINICIONES

Administrador: rol que desempeña una persona o área para el control y supervisión de uso de los recursos de Tecnologías de Información y Comunicaciones.

Amenaza Calificada: evento que pone en riesgo la operación de los servicios o la continuidad del negocio.

Ataque: es una explotación deliberada de una debilidad detectada en sistemas de información de la computadora, ya sea como objetivos específicos o simplemente como objetivos de la oportunidad.

Cifrado: mecanismo de seguridad que permite almacenar datos utilizando algoritmos matemáticos de codificación, con el fin de ocultar y proteger los datos contra accesos no autorizados. Este mecanismo requiere del uso de un software de encriptación para proteger los datos y una contraseña para tener acceso a la misma.

Colaborador: toda persona que presta a RACSA sus servicios en virtud de un contrato remunerado.

Comunicación Electrónica: los servicios provistos mediante la red institucional, cuyo propósito es la comunicación, tales como mensajería con correo electrónico (interno o externo / e-mail), foros de discusión, mensajería instantánea (Chat), acceso a internet, Red Interna, extranet, servicios de telefonía IP, tableros informativos electrónicos (bulletin boards), aplicaciones para transferencia archivos mediante el protocolo FTP, los dispositivos para vídeos y los sistemas que formen parte de la red institucional con conexión directa o indirecta sea permanente o eventual.

Contraseña: código de identidad secreto, de uso exclusivo y confidencial para los usuarios, complementario a los mecanismos de autenticación de los sistemas informáticos y de comunicaciones.

Correo Electrónico (e-mail) Masivo No Autorizado: es aquel mensaje no autorizado que es enviado a la población de usuarios de correo interno de RACSA, ya sea de forma general, por segmentos o grupos.

Dispositivo Bluetooth: es una especificación industrial para redes inalámbricas de área personal, que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2.4 GHz.

Dispositivo de Almacenamiento Externo: medios de almacenamiento físico empleados para almacenamiento y/o transferencia de datos tales como discos ópticos (CD, DVD,

Blu-ray, HD-DVD), disquetes, discos externos, memorias externas (memoria USB, memory stick, MMD, otros).

Dispositivos de Usuario Personal: todo lo relacionado con el uso de equipos personales portátiles o no, que se conecten a la red institucional y/o hagan uso de los recursos empresariales.

DLP: Data Loss Prevention o Prevención de Pérdida de Datos es una estrategia para asegurar controles para los usuarios sobre el riesgo de pérdida o fuga de información sensible o crítica fuera de la red corporativa.

Equipo Periférico: dispositivos o accesorios complementarios a una computadora de escritorio o laptop que son parte de su conjunto de hardware esencial para operar. En esta categoría se ubican, entre otros similares, impresoras, parlantes externos, ratón, micrófonos externos, headsets o diademas, auriculares, entre otros.

Hardware: conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un ordenador, incluidos sus periféricos: maquinaria y equipos (CPU, discos, cintas, módem, cables, etc.).

Identificación de Acceso: mecanismo para la autenticación y reconocimiento de un usuario en los sistemas y redes de RACSA. El mismo puede corresponder a un dispositivo físico, acceso lógico y las contraseñas asociadas.

Lector Tarjeta Inteligente: una tarjeta inteligente, o tarjeta con circuito integrado, es cualquier tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada.

MFA: es un proceso de registro en varios pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña.

Perfil de Usuario: clasificación que se establece para identificar a un usuario(a) o grupo de usuarios(a) y asociarlos a los privilegios o roles de acceso y la utilización de los sistemas informáticos, servicios de comunicación e infraestructura de TIC.

Phishing: técnica de ingeniería social que consiste en el envío de correos electrónicos que suplantán la identidad del remitente y solicitan información de interés para el atacante.

Plataforma: conjunto de elementos informáticos de hardware y software que funcionan de forma integrada para prestar un servicio y que se ponen a disposición de los usuarios(a) de acuerdo con su perfil.

Recursos Informáticos: todo dispositivo de hardware, herramienta de software o servicios de comunicación que se pongan a disposición del trabajador de RACSA para el desempeño de sus funciones o a disposición de terceros para la realización de un trabajo en particular.

Red Interna: es la red privada de una empresa. El principal propósito de una Red Interna es compartir información propia de la Empresa, así como recursos computacionales entre los empleados.

Red Oscura: conocida también como darknet, es una colección de redes distribuidas no indexadas por los motores de búsqueda, diseñadas para preservar el anonimato de identidades que intercambian información.

Servicio de Red: servicios que se brindan sobre la Red Interna de RACSA.

Software Ilegal: software por el que no se ha pagado un derecho de uso y que no es de uso libre según lo haya determinado su propietario.

Software: es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.

SPAM: también denominado correo basura o mensaje basura, se identifica como spam al conjunto de mensajes enviados de forma individual o masiva sin que medie una autorización previa y que no han sido solicitados por los destinatarios.

Streaming: se refiere a cualquier contenido de medios, ya sea en vivo o grabado, que se puede visualizar en computadoras y aparatos móviles a través de internet y en tiempo real. Los podcasts, webcasts, las películas, los programas de TV y los videos musicales son tipos comunes de contenido de streaming.

Telefonía IP: servicio telefónico o de voz en forma digital que permite el establecimiento de comunicaciones basado en la tecnología IP.

Usuario: persona expresamente autorizada para utilizar equipos de trabajo y acceder a los sistemas informáticos relacionados con sus funciones. Esta persona únicamente podrá utilizar los sistemas de RACSA, dentro de los límites que el Departamento de Gestión de Infraestructura de Tecnologías de Información ha autorizado y los que se establecen en este reglamento.

VPN: la Red Virtual Privada (del inglés Virtual Private Network) es un servicio de red que permite al usuario autorizado establecer una conexión segura de forma remota a la red institucional a través de una red pública o Internet.

5. RESPONSABILIDAD

Junta Directiva:

- **Aprobar el Reglamento de Uso de Recursos Informáticos de RACSA, así como sus actualizaciones.**

Gerencia General:

- **Revisar y elevar para aprobación de la Junta Directiva el Reglamento de Uso de Recursos Informáticos de RACSA.**
- **Velar por el control y seguimiento de la implementación de presente Reglamento de Uso de Recursos Informáticos de RACSA.**

Dirección de Operaciones:

- **Revisar el Reglamento de Uso de Recursos Informáticos de RACSA y proponer actualizaciones a la Gerencia General para que ésta las eleve ante la Junta Directiva para conocimiento y aprobación correspondiente.**
- **Ejercer la rectoría sobre la utilización de recursos de Tecnologías de Información y Comunicaciones de RACSA.**
- **Aplicar e implementar los mecanismos de control necesarios para garantizar la seguridad de los recursos informáticos de RACSA.**
- **Velar y dar seguimiento al cumplimiento por la correcta aplicación del Reglamento de Uso de Recursos Informáticos de RACSA.**

Direcciones y Jefaturas de RACSA:

- **Velar porque los colaboradores a su cargo cumplan y apliquen de manera correcta este reglamento.**
- **Aplicar lo establecido en el Proceso DSS05 – Gestionar los Servicios de Seguridad.**

Colaboradores:

- **Acatar e implementar lo establecido en el presente reglamento.**

Departamento de Estrategia e Innovación:

- **Custodiar la última versión oficial aprobada del documento e incluirla en el repositorio del Sistema de Gestión Integral de RACSA.**

6. DOCUMENTOS DE REFERENCIA

- Código de Ética para los Colaboradores de RACSA.
- Estatuto de Personal de Radiográfica Costarricense S.A.
- Ley N°2, Código de Trabajo.
- Ley N°4573, Código Penal de Costa Rica, Sección VIII – Delitos informáticos y conexos.
- Ley N°8660, Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones.
- Ley N°8968, Ley de Protección de la Persona frente al tratamiento de sus datos personales.
- Ley N°9048, Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.
- Marco de Referencia COBIT 2019.
- Política de Seguridad de la Información de RACSA.
- Proceso DSS05 – Gestionar los Servicios de Seguridad.
- Proceso SOP10 – Gestión Integral de la Seguridad.

7. REGLAMENTO DE USO DE LOS RECURSOS INFORMÁTICOS DE RACSA

CAPÍTULO I – DISPOSICIONES GENERALES

SECCIÓN I - Propiedad de las Plataformas de TIC

Artículo 1. Propiedad y Derechos. RACSA ostenta la propiedad y/o derechos de uso de todo hardware y software puesto a disposición del usuario y tendrá pleno derecho de ejecutar las labores de monitoreo, auditoría, mantenimiento y control que sea requerido en virtud de proteger los intereses empresariales y garantizar la disponibilidad, confidencialidad e integridad de la información empresarial.

Artículo 2. Recursos. RACSA suministrará al usuario autorizado los recursos de TIC necesarios, estrictamente para el desempeño de sus funciones.

Artículo 3. Administración de Recursos. La Dirección de Operaciones a través de sus departamentos técnicos ostenta la rectoría sobre la administración de todos los recursos informáticos y de comunicaciones propiedad de RACSA o propiedad de terceros que se utilicen para un servicio específico, y es responsable de la correcta operación de estos, así como del establecimiento de las medidas de seguridad apropiadas para garantizar el cumplimiento de la Política de Seguridad de Información de RACSA.

CAPÍTULO II – DISPOSICIONES REGLAMENTARIAS

SECCIÓN I – Generalidades

Artículo 4. Equipos. Todos los recursos informáticos (incluyendo equipo periférico) y equipos de trabajo puestos a disposición del usuario serán para uso exclusivo en el cumplimiento de sus funciones y serán responsables de su uso y protección. Es deber de todo usuario de la Empresa al cual se le asigne un equipo de cómputo y/o acceso a sistemas de información, la custodia y protección de los datos, incluida su cuenta, contraseña e información de RACSA y sus clientes.

Artículo 5. Protección de Recursos. Todos los usuarios deben asegurar la protección de los recursos informáticos (incluyendo equipo periférico) y equipos de trabajo puestos a su disposición con el fin de evitar daño físico, alteración, robo o hurto, siempre y cuando no ponga en peligro sus derechos superiores fundamentales.

Artículo 6. Negligencia o Descuido. La negligencia o descuido en el uso de los equipos asignados, que deteriore o dañe los mismos podrá ocasionar sanciones disciplinarias que correspondan, para lo cual se seguirá el respectivo procedimiento administrativo, además del cobro respectivo del activo afectado.

Artículo 7. Sobre los Mecanismos de Control. La Dirección de Operaciones podrá utilizar herramientas de control que posibiliten detectar, analizar y bloquear accesos a sitios restringidos, que pongan en riesgo la seguridad de los recursos informáticos o que atenten contra su eficiencia y desempeño.

Artículo 8. Equipos Autorizados. Solamente aquellos equipos autorizados por el Departamento de Gestión de Infraestructura de Tecnologías de Información que estén configurados con los requerimientos definidos de seguridad podrán acceder a los recursos informáticos de RACSA.

Artículo 9. Fiscalización. La Dirección de Operaciones se reserva para sí, el derecho de actuar como contralor del uso de los recursos informáticos, dentro de los límites permitidos por la Constitución Política, la legislación vigente y la jurisprudencia pertinente y en coordinación con otras dependencias según corresponda, en los aspectos que así lo ameriten.

Artículo 10. Información a las Autoridades Competentes. En caso de tener indicios de cualquier actividad ilegal, RACSA aplicará el debido proceso e informará a las autoridades competentes para la aplicación de las medidas legales aplicables correspondientes.

Artículo 11. Recursos de Impresión. Los recursos de impresión deben ser utilizados de manera razonable y ética procurando un uso optimizado de los consumibles. Dichos recursos pueden ser sujetos a controles técnicos por parte del Departamento de Gestión de Sistemas de Tecnologías de Información.

Artículo 12. Contraseñas. Es responsabilidad del usuario establecer contraseñas fuertes y únicas para cada cuenta. Se recomienda que dicha contraseña debe incluir una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales con una longitud mínima de 10 caracteres.

SECCIÓN II – Prohibiciones

Artículo 13. Material. Se prohíbe la transmisión, distribución o almacenamiento de cualquier material que viole cualquier ley o regulación nacional o internacional incluyendo y sin limitación a: material protegido por derechos de autor, marcas registradas, secretos comerciales u otros derechos de propiedad intelectual, material obsceno o difamatorio.

Artículo 14. Software o Código. Se prohíbe transmitir o distribuir cualquier tipo de software o código que esté diseñado para ejecutar acciones ilegales de acuerdo con las leyes y normativa aplicable de Costa Rica y los Acuerdos Internacionales a los que el país esté suscrito. Así como, cualquier acción de propagación tendiente a violar esta reglamentación o la de cualquier otro Proveedor de Servicios de Internet, lo cual incluye, pero no se limita a, envío de spam, propagación e/o instalación de programa maligno, phishing, ataques de cualquier tipo o cualquier evento similar.

Artículo 15. Accesos No Autorizados. Se prohíben los intentos no autorizados, por cualquier medio, de obtener acceso a cuentas o recursos informáticos de cualquier servicio suministrado o propiedad de RACSA. El acceso no autorizado a cuentas o recursos informáticos de RACSA se constituye en una falta grave que puede desencadenar procesos disciplinarios correspondientes para lo cual se seguirá el respectivo procedimiento administrativo.

Artículo 16. Prohibición de los Servicios. Se prohíbe obtener o intentar obtener cualquier servicio brindado por RACSA de forma ilegal por cualquier medio o dispositivo.

Artículo 17. Información. Se prohíbe el acceso, alteración o destrucción, no autorizados de información de clientes, usuarios o propiedad de RACSA.

Artículo 18. Conexiones Prohibidas. Se prohíbe ejecutar o participar en cualquier actividad cuyo objetivo sea interferir, intervenir con la conexión de redes o servicios de telecomunicaciones a cualquier usuario, en la red de RACSA o en la red de cualquier otro proveedor, incluyendo sin limitación a: ataques de negación al servicio, saturación de red, sobrecargar servicios, aprovechar deshonestamente o abusar de privilegios como usuario.

Artículo 19. Suplantación. Se prohíbe el uso de técnicas de suplantación de identidad física o digital para usos maliciosos, por ejemplo y no limitado a: IP Spoofing, ARP Spoofing, DNS Spoofing, Web Spoofing, Vishing o Email Spoofing entre otros, y la identificación de acceso (usuario y contraseña) de otro usuario para acceder a las distintas plataformas de recursos informáticos. El incumplimiento de lo anterior puede ser considerado suplantación de identidad y es un delito según el Código Penal vigente. Todos los usuarios son responsables de cuidar diligentemente la confidencialidad de sus identidades digitales, por tanto, se considerará falta grave divulgar o compartir dichas credenciales

Artículo 20. Almacenamiento. Se prohíbe recolectar o almacenar sin autorización del propietario datos personales. Se exceptúan los procesos autorizados para la recolección de información del personal en virtud de las funciones asignadas.

Artículo 21. Bases de Datos. Se prohíbe acceder, recolectar, transferir o almacenar sin autorización información de las bases de datos de RACSA o administradas por RACSA. Todo de conformidad con lo establecido en la Ley N°8968.

Artículo 22. Direcciones IP. Se prohíbe la asignación manual no autorizada de direcciones IP en los equipos de usuario o cualquier otro dispositivo que sea conectado a las diferentes redes empresariales.

Artículo 23. Dispositivos No Autorizados. Se prohíbe el acceso no autorizado a cualquier recurso informático empresarial con dispositivos no autorizados por RACSA para su uso, como por ejemplo: computadoras, tabletas u otros dispositivos de índole personal. RACSA se reserva el derecho de evitar por cualquier medio necesario, dicho comportamiento cuando no exista la respectiva autorización.

SECCIÓN III – Correo Electrónico y Medios de Comunicación Empresarial

Artículo 24. Uso Razonable. Los usuarios son responsables de dar un uso razonable a los servicios de correo electrónico y comunicación empresarial como herramientas de trabajo y en ningún momento pueden ser utilizados para realizar prácticas ilícitas o mal intencionadas que atenten contra la Política de Seguridad de la Información de RACSA, contra terceros o la legislación y normativas internas o externas vigentes.

Artículo 25. Herramientas de Comunicación Empresarial. El acceso al correo electrónico y otras herramientas de comunicación empresarial, de acuerdo con el requerimiento de roles y puestos de trabajo, se le brindará al personal de la Empresa y se le asignará una cuenta para la realización de sus funciones. Esta disposición solo es limitada por circunstancias de tipo técnico, económico, o por otras razones debidamente justificadas. La solicitud de un servicio de una cuenta de correo electrónico y demás servicios se realizará de acuerdo con el flujo establecido en el Proceso DSS05 – Gestionar los Servicios de Seguridad vigente.

Artículo 26. Herramientas Oficiales. La herramienta oficial definida por RACSA para la mensajería interna, videollamadas y reuniones es Microsoft Teams y Cisco Webex, cualquier otro software quedará sujeto a su estudio y aprobación por parte del Departamento de Gestión de Infraestructura de Tecnologías de Información.

Artículo 27. Resguardo de Seguridad. Es responsabilidad de los colaboradores resguardar la seguridad de las sesiones o reuniones en Teams o Cisco Webex, por lo que deben asegurarse de que los presentes estén autorizados y bloquear o eliminar a terceros desconocidos.

Artículo 28. Mensajería Personal. Toda la mensajería de tipo personal que se maneje en la plataforma de correo y comunicación empresarial por parte de los usuarios deberá estar contenida en una carpeta separada e identificada, a fin de salvaguardar el acceso confidencial a dicha información ante posibles procesos de auditoría, mantenimientos

o controles. Dicha carpeta y lo ahí contenido será responsabilidad del usuario, eximiendo a RACSA de cualquier efecto civil o penal ante actos ilícitos o información ilegal que se almacene.

Artículo 29. Tamaño de Archivos. En caso de envío o recepción de información adjunta hacia o desde fuera de la red RACSA, los archivos adjuntos no deberán superar los 35 MB de tamaño máximo total.

Artículo 30. Sobre los Adjuntos Autorizados. El Departamento de Gestión de Infraestructura de Tecnologías de Información determinará por razones de seguridad los tipos de archivos que serán permitidos incluir como adjuntos en los correos electrónicos o transferir en las plataformas de comunicación empresarial.

Artículo 31. Almacenamiento de Mensajes. Es responsabilidad del usuario administrar los mensajes almacenados en su buzón de correo electrónico, a fin de mantener el espacio suficiente de acuerdo con la capacidad otorgada.

Artículo 32. Reporte de Elementos No Permitidos. Los colaboradores que reciban algún correo electrónico, mensaje o archivo proveniente de otro colaborador de RACSA a través de las plataformas de comunicación empresarial y que contenga alguno de los elementos no permitidos de acuerdo con las restricciones indicadas, deberá reportarlo a su superior inmediato y este a su vez deberá reportarlo al Departamento de Gestión de Infraestructura de Tecnologías de Información.

Artículo 33. Prohibiciones sobre Correo Electrónico. El correo electrónico y demás medios de comunicación empresarial deberán ser utilizados acatando las disposiciones indicadas en este reglamento, por lo tanto, las siguientes actividades son prohibidas:

- a. **Transferencia del usuario y/o contraseña a otros colaboradores o terceras personas.**
- b. **Creación o distribución de cualquier tipo de mensajes de naturaleza destructiva, difamatoria u ofensiva, incluyendo comentarios ofensivos acerca de raza, género, discapacidades, edad, orientación sexual, pornografía, creencias religiosas, políticas o de naturaleza xenofóbica.**
- c. **Envío de correos electrónicos o mensajes de las siguientes clasificaciones: spam, mail bombing, phishing, escrow fraud, scam 419, pharming, difusión de virus y software malicioso, entre otros, o cualquier otro tipo de actividad realizada con ánimo de sabotear o afectar la imagen empresarial o económica de RACSA y/o a terceros.**
- d. **Envío de mensajes con peticiones de caridad, firmas, o cualquier tipo de mensaje catalogado como cadena, chistes, entre otros.**
- e. **Recopilación de información acerca de otros usuarios, incluyendo direcciones de correo electrónico.**
- f. **Modificación de encabezados de correo electrónico de modo tal que impidan o dificulten el análisis de su origen y ruta.**
- g. **Envío o almacenamiento de archivos que contengan software u otro material protegido por las leyes sobre propiedad intelectual, a menos que se posea o controle los derechos sobre el mismo o se hayan recibido todos los consentimientos necesarios para hacerlo.**

- h. Reenvío automático de mensajes a una dirección externa de RACSA, exceptuando los casos debidamente autorizados por el Departamento de Gestión de Infraestructura de Tecnologías de Información.**
- i. Utilización del correo electrónico o de otros medios de comunicación empresarial para llevar a cabo negocios personales.**

Artículo 34. Facilidades de Telefonía. Las facilidades de telefonía asignadas a los usuarios de telefonía empresarial deberán ser utilizadas de manera racional acorde a su puesto de trabajo.

Artículo 35. Daños a Terminales de Telefonía. Los usuarios serán responsables por los daños provocados a los equipos terminales de telefonía si se estima que se ha dado un uso indebido.

Artículo 36. Uso Racional. Las Direcciones y Jefaturas deberán asegurar el uso racional del servicio de telefonía, a través de la supervisión y control adecuados.

Artículo 37. Prohibición en la Transferencia. Se prohíbe transferir el usuario y/o contraseña de acceso al servicio de telefonía IP a otros colaboradores o terceras personas.

SECCIÓN IV – Acceso a Internet

Artículo 38. Sitios Web Prohibidos. Con el fin de garantizar un entorno de trabajo productivo, seguro y profesional, se prohíbe el acceso a ciertas categorías de sitios web. A continuación, se brinda un listado básico, pero no limitado a, tipos de sitios web los cuales están estrictamente prohibidos:

- a. Redes Sociales:** sitios como Facebook, Twitter, Instagram, LinkedIn, TikTok y otros similares, a menos que se utilicen para actividades específicas relacionadas con el trabajo y cuenten con la aprobación pertinente.
- b. Entretenimiento y Medios:** plataformas como YouTube, Netflix, Hulu y otros servicios de streaming de entretenimiento.
- c. Juegos en Línea:** páginas de juegos en línea, casinos virtuales y sitios de apuestas deportivas.
- d. Contenido para Adultos:** sitios web que contienen material pornográfico, erótico o de citas para adultos.
- e. P2P y Compartición de Archivos:** sitios web de intercambio de archivos como, pero no limitado a, BitTorrent y otros servicios de descarga P2P.
- f. Compras en Línea:** páginas de comercio electrónico como Amazon, eBay, tiendas de moda y otros sitios de compras.
- g. Chats y Mensajería Instantánea:** servicios de mensajería instantánea como WhatsApp Web, Messenger, Telegram y otros, a menos que sean herramientas aprobadas para la comunicación laboral.
- h. Blogs y Foros:** plataformas de blogging y foros de discusión, incluyendo Reddit y otros sitios similares.
- i. Noticias y Medios de Comunicación:** portales de noticias tales como CNN, BBC y periódicos locales o internacionales.
- j. Humor y Satíricos:** sitios web de memes, humor, sátira y contenido cómico.

- k. **Viajes y Turismo:** agencias de viajes, comparadores de vuelos, sitios de reserva de hoteles y otros servicios relacionados con viajes.
- l. **Streaming de Audio y Video:** plataformas de música y video en streaming no relacionadas con actividades laborales.
- m. **Contenido Violento u Odioso:** sitios web que promueven la violencia, el odio, el terrorismo o cualquier forma de discriminación.
- n. **Piratería y Hacking:** páginas que ofrecen software pirata, hacking, cracking y cualquier actividad ilegal relacionada.
- o. **Redes Privadas Virtuales (VPN):** servicios de VPN utilizados para evadir restricciones del presente reglamento.
- p. **Correo Web:** servicios de correo electrónico personales como Gmail, Yahoo Mail, Outlook.com y otros, salvo que sean necesarios por motivos laborales y cuenten con la aprobación pertinente.

No se permitirá el acceso a páginas relacionadas con actividades ilícitas, pornografía, drogas ilegales a nivel nacional e internacional, páginas con contenido que resulte violento, obsceno, abusivo, xenófobo o difamatorio y otras que puedan atentar contra la operatividad de la Empresa, páginas de juegos en línea, contra la dignidad de las personas, la seguridad nacional, las regulaciones y leyes vigentes. Para lo anterior RACSA se reserva el derecho de utilizar filtros de contenido en línea y otras herramientas que permitan llevar un control adecuado.

No se permitirá la descarga, uso, intercambio o instalación de juegos, música, vídeos, películas, imágenes, protectores y fondos de pantalla, software ilegal, información o productos, que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros, tampoco se permitirá el acceso a sitios ubicados en la red oscura (darknet) o cualquier sitio que tenga terminación.

Artículo 39. Excepciones de Acceso. Cualquier excepción de acceso a los sitios web prohibidos por motivos laborales, debe ser autorizado previamente por el Departamento de Gestión de Infraestructura de Tecnologías de Información. La jefatura inmediata deberá solicitar el permiso respectivo por escrito y firmado digitalmente, documento que deberá ser adjunto a la apertura de un caso en la Herramienta de Gestión de TI (Aranda), indicando los usuarios a los cuales se solicita la excepción y explicando la necesidad de dicho acceso. Si producto de dicho análisis se determina que la excepción puede implicar una vulnerabilidad a la seguridad empresarial se denegará la solicitud automáticamente.

Artículo 40. Uso del Nombre de RACSA. Los colaboradores y usuarios no podrán asumir en nombre de RACSA posiciones personales en encuestas de opinión, foros, redes sociales u otros medios similares.

SECCIÓN V – Sobre el Uso del Software

Artículo 41. Instalación de Software Ilegal. Se prohíbe la instalación de software ilegal, también llamado “pirateado” y de aplicaciones punto a punto como del tipo, pero no limitado a: Kazaa, eMule, eDonkey, Shareaza, BitTorrent, Bitcoin o similares, así como

minería de cripto monedas tanto en la plataforma tecnológica de la Empresa como en los dispositivos de usuario.

Artículo 42. Instalación de Software. Se prohíbe la instalación de software de cualquier índole sin la autorización del Departamento de Gestión de Infraestructura de Tecnologías de Información. Para efecto de instalación de software en equipos de usuario se debe abrir un caso en la Mesa de Servicio Interna y contar con la aprobación de la Jefatura respectiva.

Artículo 43. Descargas Prohibidas. Se prohíbe descargar, obtener, almacenar o distribuir material o programas informáticos, archivos o códigos maliciosos con la finalidad de dañar, interferir, alterar, espiar o destruir algún sistema o equipo de RACSA o de un tercero.

Artículo 44. Soluciones de Software. El Departamento de Gestión de Sistemas de Tecnologías de Información proveerá las soluciones de software necesarias para la ejecución de las labores de trabajo de los usuarios, en los equipos asignados, según los requerimientos generados por las Jefaturas de Departamento según el procedimiento de solicitud respectivo.

Artículo 45. Plataformas de Autenticación. El Departamento de Gestión de Infraestructura de Tecnologías de Información proveerá y tendrá el control de las plataformas de autenticación, mismas que son necesarias para el acceso a cada sistema asignado al usuario.

Artículo 46. Software Libre. Para la utilización e instalación de software legal o libre (free o shareware) no oficializado, pero que sea requerido para el desempeño de las funciones, debe contarse con la autorización del Departamento de Gestión de Sistemas de Tecnologías de Información y el Departamento de Gestión de Infraestructura de Tecnologías de Información. Para este fin la Jefatura inmediata correspondiente debe enviar la solicitud vía la Mesa de Servicio.

Artículo 47. Soporte a Software. El Departamento de Gestión de Sistemas de Tecnologías de Información únicamente dará soporte al software que haya sido adquirido para uso Empresarial y que esté bajo su administración.

Artículo 48. Licenciamiento Microsoft 365. Para los colaboradores con licenciamiento Microsoft 365 asignado que incluya el derecho de uso a sus aplicaciones y que son las únicas autorizadas a utilizar para realizar los procesos normales de colaboración y productividad entre colaboradores de RACSA. Todos los colaboradores cuya licencia de Office 365 dé derecho de uso de la aplicación Microsoft OneDrive deberán utilizar esta herramienta para respaldar todos los archivos de interés empresarial.

Se prohíbe el uso de otras herramientas de respaldo tipo Google Drive, Dropbox, o cualquier otra herramienta que hospede archivos de datos empresariales en plataformas de otros proveedores o ambientes diferentes al dominio corporativo de RACSA. Es responsabilidad del colaborador asegurarse que los archivos de datos de su computadora corporativa se hospedan en una ruta cubierta (archivos sincronizados)

por el servicio de OneDrive con el objetivo de garantizar el respaldo de los archivos empresariales.

Artículo 49. Dispositivos Personales. RACSA se reserva el derecho de aprobar el uso o no de dispositivos personales para acceder a las plataformas empresariales de acuerdo con criterios de seguridad y conveniencia empresarial debidamente justificados.

Artículo 50. VPN. Se prohíbe la utilización de cualquier servicio VPN en cualquier dispositivo, personal o corporativo, que no haya sido brindado y/o aprobado por el Departamento de Gestión de Infraestructura de Tecnologías de Información, a través del cual se pretenda acceder a recursos informáticos empresariales.

Artículo 51. Asistencia Remota. Se prohíbe el uso de programas para asistencia remota tales como Anydesk, TeamViewer, VNC Connect u otro similar. Las únicas herramientas autorizadas por RACSA para ser utilizadas por el personal de soporte y tomar control remoto de una computadora y brindar el servicio requerido a los usuarios son Aranda (Virtual Support) y Microsoft Quick Assist.

SECCIÓN VI – Sobre los Equipos de Usuario

Artículo 52. Acceso de Administración. Cuando las funciones asignadas a un usuario ameriten contar con el acceso de administración al computador respectivo, el Jefe de Departamento correspondiente presentará al Departamento de Gestión de Infraestructura de Tecnologías de Información la debida solicitud y justificación en un caso por la Mesa de Servicio. Los colaboradores que cuenten con privilegio de administrador no podrán eliminar ni modificar el software ni las reglas de seguridad instaladas en el computador.

Artículo 53. Monitoreo. El Departamento de Gestión de Infraestructura de Tecnologías de Información para efectos de seguridad de la información y calidad de los servicios ofrecidos, implementará los mecanismos necesarios para controlar y monitorear el uso que se esté dando a las computadoras de trabajo tales como: instalación de software nuevo, modificaciones en la configuración del equipo o del software instalado, o la eliminación del software, entre otros. Lo anterior siempre en apego a las leyes, reglamentos y normas aplicables correspondientes.

Artículo 54. Gestión de Acceso por Uso Inadecuado. Si se detecta un manejo inadecuado de los recursos informáticos, el Departamento de Gestión de Infraestructura de Tecnologías de Información podrá modificar o restringir el rol que posea el usuario, e informar al usuario y a la Jefatura respectiva, de acuerdo con los intereses de RACSA.

Artículo 55. Acceso a Equipos en Caso de Amenazas. En caso de amenazas informáticas debidamente calificadas u otros incidentes de seguridad de la información, el Departamento de Gestión de Infraestructura de Tecnologías de Información podrá ingresar a los equipos de usuario siguiendo el debido proceso. En caso de mediar posibles delitos, el proceso será puesto a conocimiento de las autoridades judiciales respectivas de acuerdo con el Proceso SOP10 - Gestión Integral de la Seguridad.

Artículo 56. Retiro Autorizado de Equipos de Cómputo. El retiro de las instalaciones de equipos de cómputo no asignado a un colaborador debe ser autorizado por la Jefatura del colaborador que tenga asignado el activo. Dicha autorización deberá ser tramitada con el Proceso de Seguridad Física, según los formularios que se tengan vigentes. En caso de que el activo pertenezca al usuario que lo está retirando, pero aún esté registrado a otro usuario (por falta de asignación o asignación incorrecta), deberá notificar al Área de Servicios Generales del Departamento de Proveeduría que el activo debe registrarse o asignarse a su nombre.

Artículo 57. Sanciones por Salida No Autorizada de Equipo. La salida no autorizada de equipo se considera falta grave por lo que la persona que ejecute dicha acción se expone a procesos disciplinarios correspondientes para lo cual se seguirá el respectivo procedimiento administrativo.

Artículo 58. Devolución de Equipos. En caso de que un Colaborador se retire de la Empresa, libere equipo de cómputo y/o sea desvinculado de la Empresa, previo a la salida del colaborador desvinculado la Jefatura a cargo de dicho colaborador, debe velar por la devolución de los equipos de cómputo respectivos al Departamento de Gestión de Infraestructura de Tecnologías de Información – Área de Soporte de TI y además; dicha Jefatura le solicitará al colaborador y velará por el llenado y firma del documento llamado Declaración Jurada Entrega de Activos (solicitado al Departamento de Gestión de Infraestructura de Tecnologías de Información – Área de Soporte de TI); en donde, además de hacer la devolución de activos, se da fe de que al entregar los equipos de cómputo con los activos descritos se ha extraído de éstos, cualquier contenido digital e información de carácter personal y que toda la información que se encuentra almacenada en estos activos es de carácter empresarial y RACSA puede disponer de ellos.

Artículo 59. Extracción de Datos Personales. En el caso de desvinculación de algún colaborador, el interesado podrá solicitar al Departamento de Gestión de Infraestructura de Tecnologías de Información las facilidades tecnológicas para la extracción de sus datos personales, previo a la firma de la Declaración Jurada Entrega de Activos.

Artículo 60. Dispositivos Periféricos No Autorizados. En general, el uso de los siguientes dispositivos periféricos para equipos de usuario en la institución no está autorizado:

- a. Dispositivos de Almacenamiento vía bluetooth, USB.
- b. Unidades de CD/DVD.
- c. Impresoras USB.
- d. Almacenamiento Firewire.
- e. Lector Tarjeta Inteligente para fines distintos a la firma digital.
- f. Dispositivo de Imagen.
- g. Modem.
- h. Puerto LPT.
- i. Puerto COM.
- j. Dispositivos Portables.

Por razones de seguridad, las interfaces USB de los puertos de usuario estarán deshabilitados tanto en equipos de escritorio como en portátiles, excepto para funciones estándar previamente autorizadas por el Departamento de Gestión de Infraestructura de Tecnologías de Información.

Artículo 61. Excepciones para Dispositivos Periféricos. Según el perfil del usuario que requiera el uso de dispositivos periféricos no autorizados se brindarán las siguientes excepciones:

- a. Todo colaborador que para el desempeño de sus funciones requiera la apertura de permisos para uso de dispositivos de almacenamiento externo u otros y con la debida autorización de la jefatura correspondiente, solicitará la habilitación del acceso a dichos dispositivos con un caso en la Mesa de Servicio con el número de serie del dispositivo.
- b. En el caso de que a un usuario se le autorice el uso de la interfaz USB de su terminal de trabajo, las memorias USB utilizadas serán las proporcionadas por RACSA, que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario de RACSA, no debiendo ser utilizadas para otros fines. En caso de que RACSA no pueda proporcionarle al usuario un dispositivo USB, el usuario deberá aportar dicho dispositivo, siempre y cuando cumpla con las disposiciones de seguridad establecidas por el Departamento de Gestión de Infraestructura de Tecnologías de Información.
- c. Las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de archivos, no como herramienta de almacenamiento de archivos personales.
- d. La Dirección de Operaciones podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas de RACSA unidades de almacenamiento en red, que podrán usarse para tal propósito.

La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento e informarse al Departamento de Gestión de Infraestructura de Tecnologías de Información, de forma inmediata mediante la apertura de un caso a través de la Mesa de Servicio.

SECCIÓN VII – Acceso a Redes Internas y Otras Plataformas Digitales

Artículo 62. Acceso a Redes Internas. El Departamento de Gestión de Infraestructura de Tecnologías de Información ejecutará labores de control y monitoreo al acceso de la red interna a través de infraestructura especializada destinada para tal fin, con el objetivo de mitigar riesgos de ciberseguridad y seguridad de la información.

Artículo 63. Conexión de Equipos a Redes Internas. El Departamento de Gestión de Infraestructura de Tecnologías de Información es el único facultado para autorizar y conectar dispositivos a la red interna, por lo que se prohíbe a colaboradores o terceros conectar equipos sin la debida autorización.

Artículo 64. Hacking. Se prohíbe toda actividad de recopilación de datos, espionaje o ingeniería social, escaneo de puertos y cualquier otra actividad de hacking, así como pruebas de vulnerabilidad o de penetración no autorizadas en las redes internas.

Artículo 65. Proyectos en Red Interna. Cualquier proyecto o plan piloto que utilice como transporte la red interna, ya sea de forma total o parcial, debe solicitarse por medio de la jefatura correspondiente al Departamento de Gestión de Infraestructura de Tecnologías de Información vía caso en la Mesa de Servicio, para efectos de análisis y aprobación.

Artículo 66. Ciberseguridad. En caso de presentarse un incidente de ciberseguridad calificado, la Dirección de Operaciones está en la facultad de revocar inmediatamente los permisos de acceso de cualquier usuario, a la vez que realizará las investigaciones respectivas con el apoyo del personal especialista necesario de las distintas dependencias y efectuará el debido proceso.

Artículo 67. Autenticación de Dos Factores. Con el fin de aumentar el nivel de seguridad de acceso a las plataformas digitales, la Dirección de Operaciones podrá facilitar y quedará a su discreción la implementación de herramientas de segundo factor de autenticación, mismas que serán de uso obligatorio por parte de los usuarios una vez se hagan las comunicaciones respectivas.

SECCIÓN VIII – Datos, Respaldo y Almacenamiento

Artículo 68. Uso Exclusivo de OneDrive y SharePoint. Las herramientas oficiales definidas por RACSA para el almacenamiento o respaldo de datos y colaboración son Microsoft OneDrive y Microsoft SharePoint por lo que se prohíbe cualquier otra no autorizada.

Artículo 69. Asignación de Cuentas. De acuerdo con el perfil de usuario RACSA asignará una cuenta de Microsoft OneDrive y/o Microsoft SharePoint para crear un lugar en la nube para acceder, almacenar o respaldar documentos e información empresarial desde internet.

Artículo 70. Prácticas Permitidas en OneDrive y SharePoint. Las prácticas permitidas en el uso de Microsoft OneDrive / SharePoint son:

- a. Utilizar carpetas para compartir grupos de archivos con otros usuarios en línea.
- b. Compartir archivos con individuos específicos, nunca con “todos” o el “público”.
- c. Se permite subir archivos categorizados como confidenciales a OneDrive; sin embargo, deben darle el tratamiento correspondiente con el debido cuidado y debida diligencia.

Artículo 71. Actividades Prohibidas en OneDrive y SharePoint. Las actividades prohibidas en el uso de Microsoft OneDrive / SharePoint son:

- a. Almacenamiento de datos para llevar a cabo negocios personales.
- b. Transmisión no autorizada de material confidencial relativo a las actividades de RACSA.
- c. Proporcionar uso no autorizado de servicios de OneDrive / SharePoint a terceros.

- d. Almacenamiento y transmisión deliberados de material comercial o publicitario no solicitado, u otro de cualquier tipo que no tenga relación laboral o infrinja los derechos de autor y conexos.

SECCIÓN IX – Perfiles de Usuario

Artículo 72. Perfiles de Usuario. Todos los colaboradores tendrán un perfil de usuario asignado que dependerá de la naturaleza de sus funciones. Cada jefatura será responsable de brindar los insumos necesarios al Departamento de Gestión de Infraestructura de Tecnologías de Información para el establecimiento de dichos perfiles.

Artículo 73. Autorizaciones de Acceso. Cualquier cambio en la autorización de accesos debe ser debidamente solicitado al Departamento de Gestión de Infraestructura de Tecnologías de Información para la correspondiente actualización del perfil.

Artículo 74. Salida de la Empresa. El Departamento de Talento Humano y Cultura es responsable de aplicar lo establecido en el Proceso DSS05 – Gestionar los Servicios de Seguridad, ante el Departamento de Gestión de Infraestructura de Tecnologías de Información, sobre la salida o traslado de un usuario (personal fijo o temporal) a su cargo. Esto con el fin de que se inhabiliten o eliminen los privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes.

Artículo 75. Modificación de Usuarios. Las Jefaturas son responsables de aplicar lo establecido en el Proceso DSS05 – Gestionar los Servicios de Seguridad, ante el Departamento de Gestión de Infraestructura de Tecnologías de Información, sobre la modificación de usuarios por cambios de personal fijo o contratado a su cargo.

Artículo 76. Perfiles de Terceros. Los Administradores de Contrato, donde medie la asignación de perfiles de acceso a terceros a las redes y sistemas de la Empresa, deben solicitar vía Mesa de Servicio la creación, modificación o eliminación de los perfiles de usuario de acuerdo con las necesidades específicas del contrato. Es responsabilidad de los Administradores de Contrato solicitar la suspensión definitiva de perfiles de usuario inmediatamente después del cese contractual con terceros por la vía de la Mesa de Servicio.

SECCIÓN X – Seguridad, Confidencialidad y Protecciones

Artículo 77. Control de Acceso. Con la finalidad de brindar protección a la información y a los sistemas, el Departamento de Gestión de Infraestructura de Tecnologías de Información utilizará los mecanismos idóneos para controlar que el acceso a los recursos se permita solamente para los usuarios autorizados.

Artículo 78. Protección de Equipos de Trabajo. Todo usuario debe proteger su equipo de trabajo de accesos no autorizados por lo que debe bloquear el acceso al equipo o apagarlo en caso de que requiera apartarse del mismo.

Artículo 79. Cierre de Sesiones. Todo usuario debe proteger el correo electrónico o cualquier otro aplicativo de accesos no autorizados, por lo que deben cerrarse las

sesiones de trabajo (aplicaciones, accesos remotos, correo, sistema operativo, etc.) cuando por alguna razón requiera apartarse de su puesto de trabajo, de manera que ninguna otra persona pueda hacer uso de los servicios o sistemas en su nombre.

Artículo 80. Prevención y Cifrado. RACSA podrá requerir en equipos de usuario la instalación de software de prevención de fuga de datos y cifrado de archivos, suministrado por el Departamento de Gestión de Infraestructura de Tecnologías de Información, esto con el fin de evitar filtración de datos, divulgación de información a personal no autorizado ya sea con intenciones maliciosas o por un error inadvertido u otras acciones no autorizadas que atenten contra la confidencialidad de la información.

Artículo 81. Cambio de Contraseña y MFA. Es obligación de todo colaborador de RACSA atender las políticas, directrices o cualquier indicación relacionada con el proceso de cambio de contraseña de dominio, así como de doble autenticación (MFA). El Departamento de Gestión de Infraestructura de Tecnologías de Información tiene la rectoría en este tema y cualquier acción orientada a evitar cualquier control en tema de políticas de cambio de contraseña o de uso de mecanismos de doble autenticación (MFA) será considerada como falta grave. Cualquier indicación relacionada a cambio de contraseña de dominio o de MFA debe ser atendida de manera pronta y oportuna por parte del colaborador. Los administradores de servicios deberán trasladar a los socios comerciales y/o proveedores, cuando así se requiera, el acatamiento a cualquier medida de seguridad que RACSA implemente en relación con este tema.

Artículo 82. Contraseña de Dominio. El colaborador debe tener presente que la contraseña de dominio se debe cambiar cada 45 días naturales y luego de esto, si no se cambia, la cuenta se bloquea. Faltando una semana para el bloqueo, se envía una notificación diaria a la dirección de correo corporativa del colaborador y es su deber realizar el cambio en forma inmediata, dado que una vez cumplida la fecha la cuenta de dominio es bloqueada y para garantizar la operación normal del colaborador y su equipo de cómputo deberá llevar el equipo de cómputo para ser atendido por el Equipo de Soporte Técnico del Área de Soporte TI e Infraestructura Interna del Departamento de Gestión de Infraestructura de Tecnologías de Información al Edificio Central de RACSA en horario de lunes a viernes de 7:00 am a 4:00 pm.

Los colaboradores que opten por el teletrabajo fuera del territorio Nacional, cuando administrativamente así proceda, deberán tener muy presente la importancia de cambio de contraseña y evitar el bloqueo de su cuenta de dominio. Al optar por la modalidad de teletrabajo (sea en Costa Rica o fuera del país cuando así se autorice) el colaborador acepta y entiende que la desatención al aviso de cambio de contraseña de dominio podría afectar el desempeño de sus funciones y la disponibilidad de servicios, liberando a su patrono de toda responsabilidad en caso de demostrarse desatención al aviso de cambio de contraseña de dominio.

Artículo 83. Teletrabajo Fuera del Territorio Nacional. Los colaboradores que opten por la modalidad de teletrabajo fuera del territorio Nacional, además de cumplir con los requisitos administrativos que correspondan, al menos 5 días hábiles previo al inicio de las labores desde fuera del territorio Nacional deberán llevar el equipo de cómputo a revisión por parte del Equipo de Soporte Técnico, al Edificio Central de RACSA, en horario de lunes a viernes de 7:00 am a 2:00 pm.

Entre los aspectos a revisar se encuentran:

- a. **Habilitación de herramientas de ciberseguridad.**
- b. **Herramientas aplicables al teletrabajo según el puesto y responsabilidades del colaborador.**
- c. **Herramientas de soporte remoto, revisión física del equipo de cómputo.**
- d. **Cambio de contraseña de dominio.**
- e. **Actualización de software del Sistema Operativo y del fabricante del equipo.**
- f. **Cuenta de dominio.**
- g. **Espacio utilizado en disco, sincronización y respaldo de archivos mediante herramienta Microsoft OneDrive (para los usuarios con licenciamiento de Office 365 que incluya el derecho a Microsoft OneDrive).**

Esta revisión deberá ser documentada en un formulario elaborado para tales efectos que deberá ser firmado tanto por el personal de Soporte Técnico como por el colaborador candidato a realizar el teletrabajo fuera del territorio Nacional y este documento, con su respectiva factibilidad positiva es requisito indispensable para que el colaborador pueda trabajar desde fuera del territorio Nacional. Es obligación del colaborador atender todas las instrucciones brindadas por parte del Equipo de Soporte Técnico, así como brindar toda la información necesaria para garantizar que el equipo de cómputo cuente con todas las facilidades para desempeñar las funciones del colaborador.

Artículo 84. Prohibición de Divulgación No Autorizada. Se prohíbe la divulgación no autorizada de información concerniente a la Empresa, su operación, sus clientes, sus trabajadores o terceros, a través de cualquier medio de comunicación electrónica (incluidas redes sociales) o el uso de dispositivos de almacenamiento externo para los fines antes descritos, de acuerdo con lo establecido en el artículo 71 inciso g. del Código de Trabajo y lo establecido en el Estatuto de Personal de Radiográfica Costarricense S.A.

Artículo 85. Declaración de Información Confidencial. Cualquier información referente a los sistemas, equipos y comunicaciones de la Empresa, procedimientos de recuperación, estrategias de mitigación ante incidentes, planes de continuidad de negocio y evaluaciones de riesgos de continuidad de negocio o de ciberseguridad, deberá ser declarada como confidencial por la Administración conforme a lo establecido en la reforma al artículo 35 de la Ley N°8660, una vez que esto se realice se podrá catalogar como confidencial y, por lo tanto, no debe ser compartida con terceros ni con empleados cuya función no ameritan el conocimiento de esta información.

CAPÍTULO III – DISPOSICIONES FINALES

Artículo 86. Sanciones. En caso de detectarse una conducta contraria a las disposiciones aquí consignadas, la misma será analizada conforme el artículo 72 del Código de Trabajo y el Capítulo VIII, Sección III sobre Orden y Disciplina del Estatuto de Personal de Radiográfica Costarricense S.A, norma que regula la relación laboral en RACSA.

Artículo 87. Consecuencias del Incumplimiento. Las faltas cometidas al tenor de lo dispuesto en este reglamento serán sancionadas de conformidad con las disposiciones legales vigentes y aplicables, sin perjuicio de las responsabilidades civiles y penales que deba asumir el usuario infractor. Además, cualquier permiso previamente concedido para hacer excepciones a los artículos de este reglamento podrá ser revocado sin previo aviso.

Artículo 88. Revisión y Actualización. Este reglamento será revisado periódicamente para asegurar su vigencia y adecuación a las necesidades de la Empresa y las tecnologías emergentes. Cualquier modificación será comunicada oportunamente a todos los colaboradores.

Artículo 89. Vigencia. Este Reglamento deja sin efecto los Lineamientos de Uso de Recursos Informáticos de RACSA aprobados por la Gerencia General el 19 de mayo del 2021 y rige a partir del día de su publicación en el Sistema de Gestión Integral de RACSA.

2) La implementación y comunicación de este acuerdo es responsabilidad de la Gerencia General.

Artículo 8.º Presupuesto Empresarial 2024 (Contraloría General de la República. Improbación del presupuesto extraordinario número 1-2024. Oficio 13490 DFOE-CIU-0351-2024. Confidencial

Confidencialidad otorgada por el Consejo Directivo del ICE en el artículo 2 del Capítulo II de la sesión 6642 del 20 de agosto del 2024, según oficio 0012-508-2024, por un plazo de cuatro años, visto en la sesión de Junta Directiva nro. 2506 artículo 12.01 del 26 de agosto del 2024.

CAPÍTULO III ASUNTOS DE LA JUNTA DIRECTIVA

Artículo 9.º Política de Transparencia y Acceso de la Información Pública del Grupo ICE. Informe de cumplimiento

La señora Laura Paniagua comenta: *“En este punto identificamos un oficio del Comité de Auditoría de esta Junta Directiva, referencia JD-CAU-26-2024 del 30 de setiembre, relacionado con el cumplimiento de la Política de Transparencia y Acceso de la Información Pública del Grupo ICE.*

Don Erick, en su condición de Presidente de ese Comité explicará la solicitud”.

El señor Erick Brenes, comenta: *“Sí, doña Laura.*

La Política de Transparencia y Acceso a la Información Pública del Grupo ICE, tiene como propósito establecer: 1) los principios generales en materia de transparencia y acceso a la información, 2) la información obligatoria que debe publicar de manera proactiva el ICE y sus empresas, 3) las responsabilidades que se derivan dentro de la organización en materia de transparencia y acceso a la

información, y 4) los mecanismos para garantizar el derecho de acceso a la información pública a todas las personas, de manera activa y pasiva.

En virtud de lo anterior y como parte de las funciones establecidas en el Reglamento que regula el Comité de Auditoría, en el artículo 5° inciso f), incida que se debe velar porque los inversionistas y el mercado en general, tengan acceso de manera completa, veraz y oportuna a la información pública que debe revelarse y verificar el adecuado funcionamiento de la página web de Transparencia de RACSA, así como los demás mecanismos de difusión y de reporte normativo de la información financiera, y considerando que es responsabilidad de la Junta Directiva fiscalizar el cumplimiento de dicha Política, se recomienda solicitar a la Gerencia General un informe de seguimiento para el mes de febrero del 2025, cuyo resultado será presentado posteriormente a este órgano colegiado”

La señora Laura Paniagua, concluye: “Muchas gracias don Erick.

De mi parte estoy de acuerdo con la propuesta, por lo que propongo acoger la recomendación planteada por el Comité de Auditoría y trasladarla a la Gerencia General para su implementación, es importante indicar que ante la identificación de aspectos de mejora, se incorpore el plan de acción con los responsables y plazos.

Asimismo, se instruye a la Oficialía de Cumplimiento de Gobierno Corporativo, para que proceda a incluir este informe en la planificación anual de los Comités, la cual deberá formar parte del plan de trabajo anual para el período 2025, así como la actualización de los respectivos charters”.

La presidenta en ejercicio, señora Laura María Paniagua Solís; el tesorero, señor Erick Mauricio Brenes Mata; la secretaria, señora Natuska Traña Porras; y el vocal, señor Luis Fernando Ramírez Loría, resuelve acoger la recomendación planteada por el Comité de Auditoría e instruir a la Gerencia General para que presente en la segunda semana del mes de febrero del 2025 un informe que detalle el nivel de cumplimiento de RACSA a lo que establece la Política de Transparencia y Acceso a la Información Pública del Grupo ICE, y en el caso de que se identifiquen oportunidades de mejora, se aporte el respectivo plan de acción con plazos y responsables.

Asimismo, se instruye a la Oficialía de Cumplimiento de Gobierno Corporativo, para que proceda a incluir de inmediato este informe en la planificación anual de los Comités, instrumento que deberá formar parte del Plan de Trabajo Anual para el período 2025 y proceda con la actualización respectiva de los charters.

CAPÍTULO IV COMENTARIOS Y PROPOSICIONES

Artículo 10. ° Programa General 5G Alianza Estratégica ICE-RACSA. Solicitud de ampliación de plazo sobre la actualización del caso de negocio. Confidencial

Confidencialidad otorgada por el Consejo Directivo del ICE en el inciso C del artículo 1 y en el artículo 1.1 ambos del Capítulo II de la sesión 6535 del 04 de agosto del 2022, según oficio 0012-692-2022, por un plazo de siete años, visto en la sesión de Junta Directiva N°2404 artículo 18 del 08 de agosto del 2022, de conformidad con lo dispuesto en el artículo 6.3.3, inciso 2 de la Política de Confidencialidad del Grupo ICE.

La señora Laura Paniagua concluye: *“De esta manera estamos dando por finalizada nuestra sesión al ser las dieciocho horas con treinta y ocho minutos. Agradezco a todos la participación. Muy buenas noches a todos.”*