5.2 Auditoria Interna (Calificación Riesgo Bajo)

Este aspecto obtuvo una calificación promedio de **1,22** puntos sobre 4,00.

El Auditor Interno es nombrado y removido exclusivamente por el Presidente del Directorio de la entidad. Cumple funciones exclusivas propias de su cargo.

La ubicación de la AI en la estructura orgánica es adecuada y demuestra su independencia operativa. No se cuenta con un Comité de Auditoría.

Cuenta con un Plan Anual de Trabajo. Para el ejercicio 2014 fue aprobado en fecha 19 de marzo de 2014 por Resolución del Directorio N° 207/2014, el cual es monitoreado en su cumplimiento.

El personal integrante del área está capacitado para realizar la tarea asignada Recibe sin restricción toda la información que requiere. Emite reportes escritos periódicos con copia al Síndico sobre sus labores y eleva al Directorio para su conocimiento y regularización.

A partir de la toma del cargo del nuevo Auditor Interno, en noviembre de 2013, los papeles de trabajo son guardados en forma ordenada y por el lapso necesario. El archivo anterior a esta fecha está desordenado e incompleto.

La AI cuenta con un personal especializado en auditoría informática y en impacto ambiental.

La AI participa como observador en los inventarios detallados (arqueos físicos) de los bienes del Activo Físico, como así también como testigo en el proceso de ingresos o baja de activos y/o quema de inventarios.

5.3 Auditoria Externa (Calificación Riesgo Bajo)

Este aspecto obtuvo una calificación promedio de **1,57** puntos sobre 4,00.

Se realizan anualmente Auditorías Externas a los Estados Financieros de cada cierre de ejercicio. La AE es designada por el Directorio, en base a una Licitación Pública.

En la última revisión de Auditores Independientes sobre los Estados Financieros de la **ESSAP SA** al 31 de diciembre de 2013, se obtuvo un dictamen con salvedades, emitido en fecha 22 de abril de 2014.

5.4 Junta Directiva (Calificación Riesgo Bajo)

Este aspecto obtuvo una calificación promedio de **1,63** puntos sobre 4,00.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

El Directorio se integra por un mínimo de uno y un máximo de ocho miembros electos por la Asamblea Ordinaria de Accionistas. Actualmente el Directorio está conformado por el Presidente y dos Miembros Titulares.

Tienen definidas sus atribuciones en los Estatutos Sociales de la entidad. No se evidencia que exista un Reglamento Interno del Directorio.

El Directorio rinde cuentas de su gestión y resultados anualmente a la Asamblea Ordinaria de Accionistas.

Los Estados Financieros de ESSAP SA correspondientes al Ejercicio 2013, hasta la fecha de cierre de los trabajos de campo de esta auditoría, aún no fueron debidamente aprobados por la Asamblea Ordinaria de Accionistas, quedando en cuarto intermedio el tratamiento de este punto en particular.

Ha sido informada al Directorio, en su sesión del lunes 16 de marzo de 2015, la propuesta de convocar la Asamblea General Ordinaria para el 30 de marzo de 2015 para tratar la aprobación de los Estados Financieros del Ejercicio 2013 y para el 27 de abril de 2015 para tratar la aprobación de los Estados Financieros del Ejercicio 2014.

El Directorio recibe periódicamente los informes y reportes de las distintas áreas operativas y de control, los analiza, pide las justificaciones e instruye las regularizaciones que correspondan.

No está aprobado el Código de Ética ni de Buen Gobierno (MECIP).

El Directorio se encuentra informado de la situación institucional y sus políticas administrativas. Los riesgos no son evaluados en forma previa por un Comité de Evaluación de Riesgos, quienes en forma específica y periódica deben hacer un análisis, seguimiento y brindar las recomendaciones para la administración y mitigación de los riesgos presentes y potenciales.

Consideraciones finales a la evaluación del Sistema de Control Interno

El Control Interno es un proceso permanente que deriva en generar una actitud activa y de autocontrol de los niveles organizacionales, con el objetivo de asegurar el cumplimiento de los requisitos y procedimientos establecidos para la apropiada ejecución de los procesos y operaciones institucionales.

Las actividades de la organización deben estar sujetas a un proceso de monitoreo continuo que permita conocer oportunamente si la **ESSAP SA** marcha efectivamente hacia la consecución de sus objetivos institucionales, si encauza las labores hacia tales objetivos y si toma las acciones correctivas pertinentes, si se necesitaren.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

Cuando el Presidente, los Miembros del Directorio, los Gerentes y los funcionarios competentes de la entidad, detecten alguna deficiencia y/o desviación en la gestión o en el control interno institucional, o bien, sean informados de ello, deberán determinar sus causas y las opciones de solución disponibles, adoptando en el breve plazo, las acciones que resulten más adecuadas y definitivas con vista a conseguir los objetivos propuestos, dados los recursos institucionales, financieros y técnicos.

La presente evaluación del **Sistema de Control Interno (SCI)** implementado en la **ESSAP SA** utilizando el **Enfoque COSO**, como ya hemos indicado, obtuvo un resultado promedio final de 225,26 puntos, calificando un SCI Confiable de Riesgo Moderado sobre la integridad de los bienes patrimoniales y cumplimiento efectivo de las funciones y objetivos estratégicos institucionales.

Se registró una disminución en la calificación de la efectividad y confiabilidad del Sistema de Control Interno de 5,63 puntos con respecto al resultado obtenido en la misma evaluación de Control Interno realizada en el mes de setiembre de 2014. Esta nueva calificación ya se halla cercana al siguiente rango de SCI no Confiable, que se determina a partir de 251 puntos.

Se observa que el Componente de Información y Comunicación obtuvo una Señal de Alerta de SCI No Confiable, debido a los altos riesgos existentes en el mismo, principalmente en el Area de Tecnología Informática, en la cual, casi no hubo mejoras significativas con respecto a la observación anterior, más bien, la situación tiende a empeorar con la perspectiva de la próxima jubilación del principal responsable y del área y conocedor de la herramienta informática utilizada.

La Dirección de la entidad dispuso a partir de la evaluación de los aspectos de control interno realizada en abril 2014, el seguimiento y regularización de las observaciones realizadas bajo un **Plan de Mejoramiento del SCI Institucional**, a través de un Comité dedicado a dicha tarea.

Al momento de la presente evaluación, se han observado algunas mejoras ya concretadas recientemente, como el ajuste de los porcentajes de previsiones de la cartera de créditos vencida a cobrar, la emisión en duplicado de las facturas, el reconocimiento como Resultados de los Aportes y Contribuciones, el calendario de visitas al interior del país para la realización de inventarios y capacitación sobre el uso del Sistema de Control de Stock de Materiales y la Adecuación del Cuadro de Revaluo y Depreciación según la Ley 125/91 y el Anexo de la Resolución 1346/05.

Si bien ya existen logros concretos de mejoramientos operativos y administrativos, falta encarar y mejorar en el corto plazo en los aspectos de riesgos de Tecnología Informática, de Talentos Humanos, de implementación del MECIP, de identificación preventiva, análisis, administración y mitigación de riesgos presentes y potenciales, contratación de la cobertura de seguros sobre bienes patrimoniales y adicionales de la entidad, de la mejora de la gestión de recuperación de créditos a cobrar en vista de su muy alta morosidad, de la regularización de partidas pendientes de muy larga data,

de registración del Pasivo Laboral, de la aplicación integral de la Ley 3864/08 vía un Decreto Reglamentario y su correspondiente regularización patrimonial, entre otros.

Recomendamos insistir con los trabajos del Comité de Mejoramiento y el cumplimiento del plan trazado, así como encarar para su regularización los aspectos de mayor riesgo detectados en el Sistema de Control Interno, que ponen en peligro el cumplimiento de los objetivos institucionales.

Asunción, 07 de abril de 2015.

DR. NELSON DÍAZ ROJAS
CYCA – CONTADORES Y CONSULTORES ASOC.
MATRÍCULA PROFESIONAL CCPN° F-3

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

3- INFORME SOBRE LA REVISIÓN DEL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN

INFORME SOBRE LA REVISIÓN DEL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN

SEÑORES
PRESIDENTE Y MIEMBROS DEL DIRECTORIO DE LA
EMPRESA DE SERVICIOS SANITARIOS DEL PARAGUAY SA
(ESSAP SA)

Tenemos a bien presentarles el resultado de nuestra evaluación actualizada del ambiente tecnológico y de los sistemas informáticos aplicados en la entidad, el alcance de los controles se detalla a continuación:

- Relevamiento de la estructura organizativa y de las normas vigentes en el departamento de tecnología informática de la entidad, poniendo especial énfasis en la adecuada separación de funciones y responsabilidades.

- Relevamiento de las normas y procedimientos vigentes para minimizar el riesgo de cambios a los programas y evitar modificaciones no autorizadas a los sistemas de aplicación utilizados por la entidad.

- Relevamiento de las políticas de seguridad de datos vigentes en la entidad que minimicen la posibilidad de accesos no autorizados a los datos y programas.

- Relevamiento de los planes de contingencia desarrollados por la entidad a efectos de asegurar la continuidad del procesamiento de la información en caso de interrupciones en los servicios, originados por desastres u otras contingencias.

- Aplicación de herramientas de auditoría a efectos de analizar los parámetros de seguridad de los sistemas y la adecuación de los mismos a las políticas de seguridad vigentes en la entidad.

Controles sobre las aplicaciones de los sistemas

- Relevamiento y verificación sobre bases selectivas de los controles de acceso existentes en los mencionados sistemas de aplicación.

- Relevamiento y verificación sobre bases selectivas de los controles de ingreso en los mencionados sistemas de aplicación.

- Relevamiento de los controles de procesamiento en los mencionados sistemas de aplicación.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

En base a la labor realizada, en el marco de la auditoría del área de tecnología de la información de la **EMPRESA DE SERVICIOS SANITARIOS DEL PARAGUAY S.A (ESSAP SA)** por el ejercicio cerrado al 31 de diciembre de 2014, han llegado a nuestro conocimiento ciertos asuntos relacionados con la organización del área mencionada, que si bien no afectan la capacidad de la misma para procesar, registrar, resumir o reportar información financiera, su corrección puede mejorar la seguridad referente a la producción de la misma.

ESSAP aplica el sistema de gestión financiero, administrativo y contable, cuyo lenguaje de programación es el Cobol; esta herramienta informática se encuentra con alto grado de obsolescencia, ha sido desarrollado en el año 1985 aproximadamente, uno de los mayores inconvenientes que experimenta este software es la discontinuidad del soporte y la poca disponibilidad de profesionales conocedores de la herramienta de programación, en la Entidad existe un solo profesional conocedor de los códigos fuentes y de la estructura de las tablas del sistema, lo que le genera una alta dependencia y alto riesgo de continuidad del servicio en caso de algún siniestro.

*Debido a la gran infraestructura que representa la **ESSAP SA**, se observa la necesidad de la aplicación e implementación de normas de buenas prácticas de gestión de tecnología de la información, por citar algunos el Cobit (Control Objectives for Information and Related Technology), Itil (Information Technology Infrastructure Library), o normas nacionales aplicados a entidades financieras como el MCIIEF (Manual de Control Interno Informático para Entidades Financieras).*

La ESSAP SA *se soporta en su sistema de información, y de manera que las gestiones puedan ser eficientes, las mismas deberán estar establecidas en un marco de gobernabilidad de TI, aplicando un conjunto de herramientas de ayuda, que permita a los administradores unir los conceptos de requerimientos de control, consideraciones técnicas y riesgos del negocio. Estas normativas permiten el desarrollo de una política clara y de buenas prácticas para control de TI. De manera que la misma pueda ser exitosa, se deben reconocer los beneficios de esta tecnología, y su utilización adecuada puede permitir impulsar el valor de sus gestiones.*

Nuestra revisión del área tecnológica se limita a emitir las recomendaciones tendientes a mejorar el control interno, no así en descubrir y señalar desfalcos y otras regularidades, por lo que no asumimos responsabilidad sobre su detección.

Quedamos a su total disposición para cualquier aclaración y/o ampliación que estimen conveniente con respecto al contenido del presente informe especial.

Atentamente,

Asunción, 07 de abril de 2015.

DR. NELSON DÍAZ ROJAS
CYCA – CONTADORES Y CONSULTORES ASOC.
MATRÍCULA PROFESIONAL CCPN° F-3

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

DESARROLLO DE LA EVALUACIÓN DEL ÁREA TI DE LA EMPRESA DE SERVICIOS SANITARIOS DEL PARAGUAY S.A. (ESSAP SA)

Hemos evaluado el sistema de información de la entidad a fin de inferir el grado de confianza que pueda otorgarse al mismo en cuanto a su capacidad de procesos, integridad de procesamiento de datos y seguridad física y lógica. Con esta finalidad, hemos aplicado cuestionarios y entrevistas con los diferentes responsables del área de T.I. para las áreas de organización general, infraestructura y seguridad.

A fin de esta evaluación hemos adoptado como marco de referencia los objetivos por área especificado por el COBIT (Control Objectives for Information and Related Technology) determinadas por la ISACA (Information System Audit and Control Administration).

Hemos mantenido entrevistas y acompañamiento para el trabajo de campo con los siguientes profesionales:

- Lic. Vicente Jesús María Insfran Elizeche – Gerente de Tecnología y Desarrollo Informático
- Lic. Víctor Benítez – Asesor de Sistemas

Incorporamos al presente informe nuestros comentarios y recomendaciones sobre el particular. Los temas observados junto con nuestras recomendaciones para su corrección y la opinión, son detallados a continuación:

I. RECOMENDACIONES TENDIENTES A MEJORAR EL CONTROL INTERNO DE LA GERENCIA DE TECNOLOGÍA Y DESARROLLO INFORMÁTICO

Hemos hecho una evaluación de los procesos de control interno del área de tecnología informática de la entidad, de lo que describimos las siguientes observaciones:

1. Situación actual de los sistemas informáticos en desarrollo y en producción

Detallamos los módulos desarrollados por el área de desarrollo de la entidad, para la gerencia financiera (sistema financiero), que para la puesta en producción se requiere la aprobación de las autoridades de la Entidad:

- Módulo de Fondo Fijo
- Módulo de Viáticos
- Módulo de Reembolsos de Gastos
- Módulo de Rendiciones de Gastos
- Módulo de Contratados
- Módulo de Facturas Varias (Proveedores)
- Módulo de Control de Documentos (Facturas)

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

- Módulo de Control de Expediente
- Módulo de Tesorería
- Módulo de Presupuestos
- Módulo de Contabilidad
- Módulo de Consultas web y móvil (Teléfono)

Módulos en producción:

- Lectura (Capital e Interior)
- Call Center
- Recursos Humanos (Sueldos)
- Funcionarios Contratados
- Control de Stock
- Control de Útiles
- Medidores
- Prestamos

Recomendamos la definición de la implementación de los sistemas del área financiera ya desarrollados, de manera a poder aprovechar los programas informáticos disponibles, de manera a reemplazar en la brevedad el sistema informático bajo plataforma Cobol.

2. Segregación de funciones de TI del sistema Cobol

Durante la realización de nuestra auditoría, hemos constatado que la administración, desarrollo y mantenimiento del sistema bajo plataforma Cobol, se encuentra a cargo de un solo profesional, que a la vez cumple la función de Gerente de TI.

La centralización de las tareas de administración, desarrollo y mantenimiento del sistema, implica que no habrá un control sobre las tareas del mismo, generando una alta dependencia sobre un mismo profesional, lo cual pone en riesgo de continuidad los servicios del área de TI.

Recomendamos que por un principio de seguridad de continuidad de los servicios de TI, la entidad evalúe la posibilidad de la descentralización de las actividades mencionadas.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

II. SEGUIMIENTO A LAS RECOMENDACIONES DE AUDITORIA EXTERNA EMITIDAS AL 31 DE DICIEMBRE DE 2013

1. Alta obsolescencia del sistema informático de gestión ESSAP

Hemos constatado que el sistema de gestión financiero, administrativo y contable, de la Entidad aplica un lenguaje de programación Cobol.
Este producto ha sido desarrollado en el año 1985 aproximadamente lo que demuestra un alto grado de obsolescencia, así como la discontinuidad del soporte y la poca disponibilidad de profesionales conocedores de la herramienta de programación.

Esta situación hace que no se disponga seguridad de la no inconsistencia y manipulaciones probables de datos, debido a la fragilidad de dicha herramienta y la alta obsolescencia del lenguaje de programación.

Recomendamos urgir la implementación del nuevo sistema integrado de gestión de servicio, actualmente en etapa de desarrollo.

Situación actual

En proceso. A la fecha de nuestra visita, no hemos evidenciado la un avance en el cambio de la actual herramienta informática, no obstante se dispone de una suite de sistemas ya desarrollados para el área financiera, y la decisión del llamado a licitación para la adquisición de un nuevo sistema informático de gestión comercial.

2. Diagnóstico de la organización de la Unidad Funcional de la Gerencia de Tecnología y Desarrollo Informático

Hemos hecho un relevamiento de la organización funcional del área tecnológica de la Entidad, del cual han surgido algunas observaciones que consideramos pertinente informar a las autoridades para su consideración, los cuales detallamos a continuación:

- Debilidades en el área de **DESARROLLO DE SISTEMAS**. Actualmente no se cuenta con suficientes programadores, lo que hace imposible cumplir a cabalidad con los proyectos disponibles, así como de la documentación apropiada de los sistemas informáticos.

- Debilidades en el área de **REDES Y SERVIDORES**, considerando la cantidad de infraestructura disponible y el crecimiento de la entidad en materia de tecnología, lo que hace imposible cumplir a cabalidad con los proyectos disponibles.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

- Debilidades en el área de **SOPORTE TÉCNICO**, debido que con la estructura actual no se puede cumplir con los reclamos de los usuarios en tiempo oportuno, principalmente para los mantenimientos cronogramados y preventivos de los equipos y periféricos.

- Ausencia de un **COMITÉ DE TI**, en el que se pueda monitorear el cumplimiento de los planes y políticas que afectan al área de tecnología de la información.

- Ausencia del cargo de **ADMINISTRADOR DE SEGURIDAD DE TI**, nombrado por la Alta Gerencia, que cumpla con la función de establecer los procedimientos de seguridad a aplicar a los bienes tangibles e intangibles, así como la aplicación de normativas que afectan al área tecnológica.

En base a las observaciones mencionadas, **recomendamos** considerar lo siguiente:

- Crear un **COMITÉ DE TI (Tecnología de la Informática) o TIC (Tecnología de la Información y la Comunicación)**, para analizar y evaluar el sector tecnológico, creando planes institucionales con la participación de los principales sectores de la entidad.

- Considerar la **incorporación de PERSONALES TÉCNICOS**, principalmente para el **área de desarrollo, redes y soporte técnico**, teniendo en cuenta que **existen varios sistemas en proceso de desarrollo, en implementación y puesta en marcha,** así como de infraestructura de redes y servidores, y **necesidad de crear un esquema preventivo de mantenimiento de equipos computacionales.**

  Establecer como política la implementación de la figura del **ADMINISTRADOR DE SEGURIDAD DE TI,** de manera a cumplir con los requisitos de seguridad establecidos en las normas internacionales de buenas prácticas de TI.

- Crear **POLÍTICAS DE CAPACITACIONES A LOS FUNCIONARIOS DE TI** de la entidad, así como para los usuarios de informática en general, considerando principalmente la implementación de nuevas soluciones tecnológicas.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado un proyecto para la incorporación de personales técnicos para la Gerencia de Tecnología y Desarrollo Informático.

CYCA
CONTADORES Y CONSULTORES ASCC.
Dr. NELSON DIAZ ROJAS (Socio)

3. Desarrollo del Manual de Gestión de Tecnología de la Información, adecuado a las normas internacionales de buenas práctica COBIT 4.1

Hemos observado que la entidad aplica diversos procedimientos y manuales para las gestiones del área tecnológica, no obstante no se tiene un patrón uniforme a seguir respetando las normas internacionales de buenas prácticas.

Debido a ello, **recomendamos** la elaboración de un Manual de Gestión de Tecnología e la Información, adecuado a las normas internacionales de buenas prácticas Cobit 4.1, que tendrá como objetivo la estandarización de las documentaciones y gestiones del sector tecnológico.
Citamos los dominios e indicadores principales de dicho estándar:

Planificación y Organización

- PO2 Definición de la arquitectura de información
- PO3 Determinación de la dirección tecnológica
- PO4 Definición de la organización de la Unidad de TI
- PO6 Administración de Talentos Humanos
- PO7 Cumplimiento de requisitos externos
- PO8 Administración de proyectos
- PO9 Administración de la calidad

Adquisición e Implementación

- AI1 Identificación de soluciones
- AI2 Desarrollo y mantenimiento de software de aplicación
- AI3 Adquisición y mantenimiento de tecnología
- AI4 Instalación y autorización de sistemas
- AI5 Administración de cambios

Producción y Servicios

- PS1 Administración de servicios de terceros
- PS2 Garantizar la continuidad del servicio
- PS3 Garantizar la seguridad de los sistemas
- PS4 Asistencia y asesoría a usuarios
- PS5 Administración de datos
- PS6 Administración de soportes
- PS7 Administración de operaciones

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

Monitoreo

- M1 Implementación de una Auditoría Interna de TI

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado un plan de desarrollo de un Manual de Gestión de TI.

4. Comité de Tecnología de la Información

ESSAP SA no cuenta con un Comité de Tecnología de la Información, que tenga como función básica el de dar seguimiento y evaluar la instrumentación de Planes de Desarrollo Informático.
El no contar con el Comité de Tecnología de la Información puede producir que la entidad desconozca las prioridades del área tecnológica, lo cual podría afectar el desarrollo tecnológico y operativo eficiente de la misma.

Recomendamos crear el Comité de Tecnologías de la Información, cuyas funciones generales sean las siguientes:

- Elaborar el Plan de Desarrollo Informático de la entidad.
- Dar seguimiento y evaluar la instrumentación del Plan de Desarrollo Informático, así como el cumplimiento de las normas, políticas y lineamientos que se establezcan.
- Promover, aprobar y establecer normas, políticas y lineamientos para la administración, crecimiento, homogenización, uso y aprovechamiento de los recursos de tecnología de información y comunicaciones.
- Establecer los mecanismos de coordinación entre los diferentes sectores de la entidad, con el fin de mejorar el uso y aprovechamiento de bienes y servicios de tecnología de información y comunicaciones.
- Promover el uso de estándares tecnológicos que faciliten las funciones de las áreas de la entidad y la interoperabilidad de sus sistemas de información.
- Brindar una orientación estratégica a la **ESSAP SA** respecto a las Tecnologías de Información, garantizando así, que tanto la estrategia como los objetivos se distribuyan en cascada hacia los diferentes sectores y otorgando confianza entre la entidad y los recursos tecnológicos.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

- Promover la modernización del entorno de tecnología de la entidad conforme a los avances que surjan en el mercado nacional e internacional, en materia de tecnología de información y comunicaciones;

- Definir una metodología que permita apoyar el proceso de análisis de los requerimientos de bienes y servicios de tecnología de información y comunicaciones, para su alineación con los objetivos estratégicos;
- Otras que le confiera el Presidente de la entidad.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita no hemos evidenciado la conformación de un Comité de TI.

5. No disponibilidad de un Administrador de Seguridad TI

No hemos identificado la figura de un administrador de seguridad de TI, nombrado por la **ESSAP SA**, que cumpla con la función de establecer los procedimientos de seguridad a aplicar a los bienes tangibles e intangibles, así como la aplicación de normativas que afectan al área tecnológica.

La Alta Gerencia debe asignar formalmente la responsabilidad de asegurar tanto la seguridad lógica como la física de los activos de TI de la entidad a un Administrador de Seguridad de TI, el cual reporte a la Alta Gerencia, no dependiendo de la Gerencia de Tecnología y Desarrollo Informático.

Citamos algunas de las funciones principales que deberá realizar dicho Administrador:

- Asegurar que los diferentes usuarios estén cumpliendo con la Política Corporativa de Seguridad.
- Asegurar la actualización de la Política de Seguridad acorde con los cambios en la configuración de la tecnología y su enlace con otras políticas y procedimientos de la entidad.
- Asegurar que los controles sean los adecuados para prevenir el acceso no autorizado a los archivos de la **ESSAP SA**: datos, software, equipamientos, suministros.
- Mantener las reglas de acceso a los datos y a los demás recursos de TI.
- Evaluar el impacto de las solicitudes de cambio a la seguridad.
- Monitorear las violaciones de seguridad y tomar acciones correctivas para asegurar que provea la seguridad adecuada.
- Revisar y evaluar periódicamente la Política de Seguridad y sugerir a la Alta Gerencia que los cambios que considere necesarios.
- Preparar y monitorear el programa de concientización de la Seguridad para los funcionarios de la entidad.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

- Mantener adecuados contactos con autoridades policiales o de seguridad, organismos reguladores, proveedores de servicios de información y operadores de telecomunicaciones, miembros de grupos de seguridad y foros de la industria.
- Probar la arquitectura de seguridad para evaluar la fortaleza de seguridad y para detectar posibles amenazas.
- Traducir la información del proceso de evaluación de riesgos de la entidad en planes de Seguridad.
- Asegurar la actualización y prueba del plan de Contingencia.
- Participar de en las reuniones del Comité de Tecnología cuando se traten temas de Seguridad.
- Elaborar los informes con la frecuencia y contenido solicitados por la Alta Gerencia.

Las responsabilidades del Administrador de Seguridad de TI, al menos deben ser establecidas en el ámbito de la entidad como un todo, a fin de que se complementen y armonicen con las medidas de Seguridad General de la **ESSAP SA**. Si fuese necesario, se deben asignar responsabilidades de administración de seguridad adicional en los Sistemas Automatizados, para cumplir con los requisitos específicos de seguridad que ellos tengan.

Recomendamos establecer como política la implementación de la figura del Administrador de Seguridad de TI, de manera a cumplir con los requisitos de seguridad establecidos en las normas internacionales de auditoría informática y de buenas prácticas de TI.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos observado la creación de la dependencia de la Administración de Seguridad de TI.

6. Disponibilidad de las políticas de seguridad de sistemas de información

Hemos observado que la **ESSAP SA** no dispone de un plan de seguridad integral TI.

La falta del plan de seguridad TI podría afectar en la continuidad del funcionamiento de la institución en caso de alguna contingencia.

Recomendamos elaborar los planes de seguridad de la entidad. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información y de acuerdo al siguiente esquema:

Políticas y estándares de Seguridad del Personal
- Obligaciones de los usuarios
- Acuerdo de uso y confidencialidad
- Entrenamiento en Seguridad Informática

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

- Medidas disciplinarias

Políticas y estándares de seguridad física y ambiental

- Resguardo y protección de la información
- Controles de acceso físico
- Controles de salida y entrada de equipos y otros
- Pérdida de Equipos
- Protección y ubicación de los equipos
- Mantenimiento de los equipos
- Uso de dispositivos especiales
- Seguridad en áreas de trabajo

Políticas y estándares de seguridad y administración de operaciones de cómputo

- Uso de medios de almacenamiento
- Instalación de software
- Identificación del incidente
- Administración de la configuración
- Seguridad para la red
- Uso del correo electrónico
- Controles contra código malicioso e Internet

Políticas y estándares de controles de acceso lógico

- Controles de acceso lógico
- Administración de privilegios
- Administración y uso de passwords
- Control de accesos remotos

Políticas y estándares de cumplimiento de seguridad informática

- Derechos de propiedad intelectual
- Revisiones del cumplimiento
- Violaciones de seguridad informática

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos observado la disponibilidad de un documento de políticas de seguridad de sistemas de información.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

7. Documento de determinación de confidencialidad

Hemos observado que no se dispone un documento en el que el usuario se comprometa y acepte las condiciones de acceso a la red de área local y sistemas de información, para la totalidad de los usuarios.
La no disponibilidad de un documento firmado por los usuarios, señalando que comprenden y aceptan las condiciones para el acceso a la red, sistemas de información y determinación de confiabilidad, los mismos podrán acceder a cualquier unidad e infringir derechos no asignados sin ninguna restricción.

Recomendamos elaborar y aplicar un documento en el que el usuario se comprometa y acepte las condiciones del acceso a la red, sistemas de información y determinación de confiabilidad. Se debe requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso a la Red de Área Local y Sistemas de Gestión.

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos observado la disponibilidad de un documento confidencialidad de la información.

8. Disponibilidad de los planes de continuidad de las actividades de TI (Plan de contingencia)

No hemos podido observar que la **ESSAP SA** cuente con un plan formal respaldado por un documento escrito para casos de contingencias producidas por: Sabotajes, errores humanos, fallas de energía eléctrica, averías producidas en los equipos, incendios, relámpagos entre otros, que puedan dañar o destruir los datos de un computador, incluso el mismo hardware.

Todo sistema de seguridad integral debe incluir algún tipo de plan para recuperarse de imprevistos o un Plan de Contingencias.

El proceso de recuperación de imprevistos implica la posibilidad que una organización pueda continuar sus operaciones diarias, a pesar de que ocurra alguna contingencia, por medio de una serie de actividades coordinadas y previamente planeadas.

En caso de siniestro si los procedimientos de contingencia no están probados y con entrenamiento del personal responsable, pueden acontecer fallas y errores en las acciones de emergencia para proteger el patrimonio de la entidad.

Recomendamos elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la entidad. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información y de acuerdo al siguiente objetivo de control:

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

9. Documentaciones utilizadas por la Gerencia de Talento Humano para procedimientos de seguridad y comunicaciones de cambios y rotaciones de personales, entre otros

Hemos observado que no siempre la Gerencia de Talentos Humanos comunica oportunamente a la Gerencia de Tecnología y Desarrollo Informático los casos de rotación, despidos y/o renuncias de los funcionarios.

En algunos casos, ex-funcionarios poseen cuentas de usuario activas, y los transferidos de área continúan con acceso a módulos del área anterior. Esto puede ocurrir además con eventuales profesionales externos contratados en forma temporal, esto se da debido a la falta de comunicación entre las áreas involucradas.

Recomendamos que en todos los casos Gerencia de Talentos Humanos comunique inmediatamente por escrito a la Gerencia de Tecnología y Desarrollo Informático, los casos de rotación, despidos y/o renuncias de los funcionarios, de manera a inhabilitar al usuario.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado una gestión eficaz en la actualización de los datos de usuarios para las altas, bajas y modificaciones de perfiles, en los sistemas informáticos disponibles en la entidad.

10. Habilitación de los registros históricos y/o logs de auditorías que reporten sobre intentos de usuarios mal intencionados

Hemos observado que los registros históricos y/o logs de auditorías que reporten sobre intentos de usuarios mal intencionados no están activados para la totalidad de los servicios (servidores y conexiones remotas).

Al no estar activados los registros históricos y/o logs de auditorías, no se tendrá ningún registro o pruebas de usuarios mal intencionados.

La Gerencia de Tecnología y Desarrollo Informático debe establecer procedimientos para asegurar que periódicamente los Usuarios Propietarios de Sistemas y/o Datos, analizan los privilegios de acceso que han sido otorgados a los usuarios y se hallan vigentes, a fin de evaluarlos, efectuar las actualizaciones pertinentes y asumir formalmente el riesgo residual.

El Responsable de Seguridad de la información de la entidad deberá requerir al Administrador de Redes, la activación de los registros de auditoría a nivel de la LAN, de manera a registrar los intentos de acceso a usuarios no autorizados.

La Gerencia de Tecnología y Desarrollo Informático debe establecer procedimientos para asegurar que periódicamente los Usuarios Propietarios de Sistemas y/o Datos, analizan los privilegios de acceso que han sido otorgados a los

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

usuarios y se hallan vigentes, a fin de evaluarlos, efectuar las actualizaciones pertinentes y asumir formalmente el riesgo residual.

Situación actual
Pendiente de regularización. Debido a la no aplicación de plataformas de base de datos para la totalidad de los sistemas, no es posible la activación de la habilitación de pistas de auditorías LOG.

11. Resguardo de claves en sobre lacrado con conocimiento de la Alta Gerencia

Hemos observado que la Gerencia de Tecnología y Desarrollo Informático no realiza el procedimiento de resguardo de las claves Administradores de Base de Datos Servidores, Sistemas Aplicativos entre otros, en un sobre lacrado en caja fuerte.

En caso de ausencia o imposibilidad del personal con conocimiento de las claves el Directorio, Gerencia de Tecnología y Desarrollo Informático o funcionario de jerarquía a quien se autorice, no podrá acceder a la clave del o de los usuarios afectados.

Recomendamos que las claves sean resguardadas por escrito en un sobre lacrado en caja fuerte, de modo tal que las mismas puedan ser utilizadas en caso de suma necesidad por la Gerencia General, Gerencia de Tecnología y Desarrollo Informático o funcionario de jerarquía a quién se autorice.

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, el resguardo de contraseñas en sobre lacrado se encuentra pendiente.

12. Segregación de funciones de TI, servidores y base de datos

Durante la realización de nuestra auditoría, hemos constatado que la administración de la Base de Datos y Servidores, no se encuentran segregadas suficientemente. La administración de ambos servicios es realizada por el Departamento de Tecnología.

La centralización de las tareas de Administración de la Base de Datos y la Gestión de Servidores, implica que no habrá un control sobre las tareas del mismo, generando una alta dependencia sobre una misma estructura, lo que pone en riesgo de continuidad de los servicios de TI.
Recomendamos que por un principio de seguridad de datos, la entidad evalúe la posibilidad de la descentralización de las actividades de administración de la Base de Datos y Administración de Servidores, de manera a no desarrollar actividades incompatibles, que generen una falta de control y seguimiento.

CYCA

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, las funciones de administración de servidores y base de datos no se encuentran delegadas correctamente, existiendo alta dependencia en pocos funcionarios.

13. Prueba de recuperación de la información – Back up

Hemos observado que las pruebas sobre recuperación y de integridad de datos (backups), no se realizan a través de una planificación detallada que contenga la cantidad y frecuencia para la realización de estos procedimientos a lo menos durante el período de un año.

El no contar con un plan para pruebas sobre recuperación y de integridad de datos, podría ocasionar el incumplimiento del control de pruebas de resguardos y no aseguraría a la Entidad que sus datos están siendo completos y correctamente resguardados.

Recomendamos desarrollar un plan para pruebas sobre recuperación y de integridad de datos, al menos con acciones trimestrales, que garantice que los datos que están siendo resguardados son los necesarios para casos de contingencia.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la realización de pruebas de recuperación de las copias de respaldos.

14. Manuales de usuario del sistema

No hemos podido observar que la entidad disponga los manuales de usuarios de los sistemas informáticos, tanto impresos como interactivos, según relevamiento se disponen de instructivos o guías básicas de uso, lo que tampoco se encuentran actualizados.

La carencia de los manuales de usuarios no permitirá disponer de una ayuda en el momento necesario para la correcta aplicación de los sistemas informáticos.

Recomendamos que se desarrollen los manuales de usuarios de manera a que los operadores puedan disponer de un material de consulta o ayuda permanente, que permita a su vez una mejor utilización y aprovechamiento de las distintas opciones ofrecidas.

CYCA
CONTADORES Y CONSULTORES ASCC.
Dr. NELSON DIAZ ROJAS (Socio)

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de los manuales de usuarios de la totalidad de los sistemas informáticos.

15. Manual de documentación del sistema – Definición de la arquitectura de información (Diagrama de flujo de datos - AOO - UML)

No hemos evidenciado la disponibilidad de la totalidad de los diseños de procesos de los sistemas, como el diagrama de flujo de datos, en el que demuestren los procesos y/o actividades desarrollados a partir de una herramienta gráfica.

Consideramos que la entidad podrá aplicar cualquier herramienta que responda a los principios del diseño de procesos, (DFD – UML – AOO entre otros).

La no disponibilidad de los mencionados manuales no permitirá a la entidad disponer de herramientas para el análisis de los sistemas y facilidad del mantenimiento de los mismos.

Recomendamos el desarrollo del mismo para la totalidad de los sistemas, de manera a cumplir con los requisitos mínimos de documentaciones y disponer de materiales para el análisis de procesos de los sistemas.

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de los manuales de diseño de los sistemas informáticos.

16. Manual de documentación del sistema – Definición de la arquitectura de información (Diagrama entidad relación)

Hemos constatado que la entidad no dispone la documentación del diseño lógico, físico y conceptual de las tablas y relaciones de los mismos, para la totalidad de los sistemas de gestión.

La no disponibilidad de los mencionados manuales no permitirá a la entidad disponer de herramientas para el análisis de los sistemas y facilidad del mantenimiento de los mismos.

Recomendamos el desarrollo de la documentación para la totalidad de los sistemas, de manera a disponer de material para el análisis de normalización de datos y que esto permita realizar los mantenimientos permanentes del sistema.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de los manuales de diseño de los sistemas informáticos.

17. Propiedad y custodia de datos del sistema

Durante la realización de nuestro trabajo, no hemos observado una documentación formal en la que se especifique la independencia en el manejo de datos, así como en la responsabilidad en la generación de los mismos por cada área (usuarios).

La falta de una definición clara en el manejo de la información así como la falta de una reglamentación sobre ella, obliga al departamento de TI a la realización de tareas impropias de su área, y por lo tanto la responsabilidad no es asignada correctamente.

Recomendamos documentar claramente las responsabilidades en el manejo y custodio de los datos, definiendo la responsabilidad directa de los datos almacenados en cada uno de los módulos a los usuarios responsables de cada área, deslindando al área de informática de la administración de los mismos.

La Gerencia de Tecnología y Desarrollo Informático debe crear un procedimiento para nombrar formalmente a los Propietarios y Custodios de los Datos y Sistemas. Sus funciones y responsabilidades deben estar definidas claramente, en cuanto a decidir respecto a la clasificación de dichos datos en materia de seguridad, así como a los derechos de acceso.

Los datos de las operaciones ingresados a los Sistemas de TI deben estar sujetos a una variedad de controles para verificar la exactitud, integridad y validez, dichos controles deben ser aprobados por el Propietario de los Datos.

Además, deben establecerse procedimientos para asegurar que los datos de entrada se validan de acuerdo a los requerimientos y reglamentaciones vigentes.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la definición de los propietarios de datos de los sistemas informáticos.

18. Plan general de capacitación y entrenamiento del personal TI

La entidad no cuenta con un plan de capacitación y entrenamiento a los personales de TI, para las aplicaciones de herramientas de seguridad de servidores, lenguajes de programaciones, base de datos e internet. No obstante se realizan las capacitaciones de acuerdo a las necesidades operativas.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

El no contar con un plan general de entrenamiento y desarrollo para los funcionarios de TI, no permitirá tener conocimiento de las herramientas de punta para las aplicaciones en la institución.

Recomendamos el desarrollo de un plan anual de capacitación de acuerdo a las tecnologías utilizadas, así como para las aplicaciones a futuro.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de un plan general de capacitación y entrenamiento para funcionarios del área de TI.

19. Expiración de contraseñas de usuarios del sistema de gestión

Hemos constatado que para las claves de usuarios del sistema de Gestión Financiero, Administrativo y Contable, bajo plataforma Cobol, no se encuentra programado para un vencimiento periódico en forma automática.

La no programación de la expiración de las claves de accesos para los usuarios del sistema aplicativo, no garantiza la correcta seguridad lógica del posible acceso indebido a los sistemas aplicativos.

Recomendamos que todas las claves de usuarios disponibles en la entidad, sean programadas para un vencimiento obligatorio periódico de al menos cada dos meses, de manera a brindar seguridad de acceso lógico a los sistemas informáticos.

Recomendamos la aplicación única, exclusiva y confidencial de las claves de manera a deslindar responsabilidades sobre el uso indebido de los mismos.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la programación de las expiraciones de contraseñas para los sistemas informáticos.

20. Respaldo externo de datos (Back up)

Hemos constatado que las copias de respaldos no son resguardadas fuera del recinto de la entidad.

La no disponibilidad de una adecuada metodología de realización de copias de respaldos, así como la no disponibilidad de una copia externa resguardada en un sitio seguro fuera del recinto de TI y de la entidad, permitirá la perdida de informaciones ante siniestros, o en su efecto la dificultad o retraso en la recuperación de los datos.

CYCA
CONTADORES Y CONSULTORES ASOC.
Cr. NELSON DIAZ ROJAS (Socio)

Recomendamos que las copias de respaldos sean realizadas diariamente en el servidor y en dos copias externas, que una copia sea resguardada en la entidad fuerte de la oficina y la segunda copia en un lugar externo seguro o se contrate el servicio de una empresa especializada, previa autorización de los directivos. La recomendación obedece a que en caso de siniestro en la oficina actual, permitirá el recupero de las informaciones en el menor tiempo.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de las copias de respaldos resguardadas externamente.

21. Manual de funciones y procedimientos del departamento de TI

Hemos constatado que el manual de funciones y procedimientos del área de TI de la entidad no se encuentra actualizado y completo.

La institución debe asegurarse de que se establezcan las descripciones de cargos para el personal de servicios de TI y que las mismas sean actualizadas regularmente. Estas descripciones deben delinear claramente la autoridad y responsabilidades de cada cargo, deben incluir la definición de los niveles de formación, habilidades y experiencia que sean necesarios para los cargos de relevancia.

Recomendamos la actualización del mismo, de manera a disponer de informaciones íntegras y oportunas para la adecuada toma de decisiones.

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de los manuales y funciones de la Gerencia de TI.

22. Encuesta de satisfacción del cliente – Usuario final

No hemos observado que la Gerencia de Tecnología y Desarrollo Informático realice en forma periódica una encuesta de satisfacción del cliente (usuario de sistemas), con relación a la calidad funcional de los sistemas y servicios prestados por el departamento de TI.

La carencia de la misma no permitirá a la Alta Gerencia disponer de información que permita conocer el grado de aceptación por parte de los usuarios de la tecnología disponible en la entidad, así como el grado de satisfacción por los servicios prestados por el departamento de TI.

De manera a disponer de herramientas válidas para la toma de decisiones para la Alta Gerencia, **recomendamos** la realización de encuestas de satisfacción al menos una vez al año.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la realización de encuesta de satisfacción de usuarios.

23. Cronograma de mantenimiento de hardware

La Gerencia de Tecnología y Desarrollo Informático no cuenta con un cronograma de mantenimiento preventivo para el hardware disponible. En base a relevamiento hemos podido constatar que debido a la carencia de más personales técnicos, la Gerencia de Tecnología y Desarrollo Informático se limita en realizar los mantenimientos correctivos de los casos más urgentes.

La no disponibilidad de un cronograma de mantenimiento de los equipos computacionales y periféricos, no permitirá asegurar el buen funcionamiento del parque de hardware de la Entidad.

Recomendamos contar con un cronograma de mantenimiento para el hardware, de modo a asegurar que dichos mantenimientos, como la realización de trabajos especiales, sean realizados periódicamente y evitar situaciones lamentables por desperfectos o fallas que afecten el normal desenvolvimiento de las actividades diarias.

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de un cronograma de mantenimiento de equipos informáticos.

24. Plan de control de calidad de sistemas

Se ha observado que el área de desarrollo de sistemas no cuenta con un plan de control de calidad aplicada a la creación y corrección del software.

El no contar con un plan de calidad de software formalizado y aprobado por todas las partes involucradas, puede acarrear la falta de coherencia en la calidad del software.

La Gerencia de Tecnología y Desarrollo Informático debe asegurar que la implementación o modificación de sistemas contemplan la preparación de un Plan de Control de Calidad de Sistemas integrado con el Plan Maestro del Proyecto, formalmente revisado y aprobado por todas las partes involucradas

Recomendamos la creación, formalización y aprobación de un plan de calidad para cada proyecto de software a desarrollar y de acuerdo con el plan maestro.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ HOJAS (Socio)

Situación actual

Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de procedimiento para asegurar el control de calidad de los sistemas informáticos desarrollados.

25. Observaciones de la ubicación física de los servidores

Hemos realizado una evaluación de la ubicación física de la sala de servidores de la entidad. De la misma surgen algunas observaciones que consideramos convenientes informar a las autoridades para su consideración, según detallamos a continuación:

- El recinto hemos observado materiales inflamables.
- No se disponen rack cerrado para todos los servidores.
- El cableado de red se encuentra desordenado y no se encuentra certificado a través de una empresa especializada. Se han observado inclusive los dispositivos Switch directamente sobre la superficie, sin ninguna protección.
- No hemos observado registros a la sala, para trabajos especiales como mantenimiento de servidores.
- La puerta y paredes no representan seguridad para el recinto.
- El piso del recinto es de madera lo que representa un riesgo para el sector.
- No se dispone de aire acondicionado redundante.
- No se cuenta con generadores eléctricos, para caso de cortes de energía.

Las observaciones mencionadas no permitirán asegurar los equipos servidores y otros dispositivos disponibles.

De manera a brindar mayor protección a los equipos servidores y periféricos **recomendamos** lo siguiente:

- Establecer la seguridad requerida para el Datacenter, como ser paredes especiales contra incendios y puertas de seguridad de acceso que permita restringir los accesos a personas ajenas a la tarea de tecnología.
- Resguardar con Rack cerrado la totalidad de los equipos servidores.
- Considerar la revisión detallada del cableado de red, identificando los puntos críticos así como la certificación de la instalación.
- Registrar el acceso del personal, principalmente para realizar mantenimiento a los equipos.
- Realizar el mantenimiento permanente a los equipos servidores.
- Instalar los pisos falsos para el recinto.
- Instalar acondicionadores de aire redundante.
- Instalar un generador eléctrico que alimente al sector en caso de cortes de energía.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, las observaciones mencionadas referentes al Datacenter se encuentran pendientes de regularización.

26. Servidor espejado – Sitio alternativo (Alta disponibilidad)

Hemos observado que la Entidad no dispone de un servidor espejado – sitio alternativo – Alta disponibilidad y balaceo de carga como un CLUSTER de servidores, que permita registrar en línea todos los datos de los sistemas, fuera del DATACENTER CENTRAL.

La no disponibilidad del servidor espejado y sitio alternativo, pone en riesgo la continuidad de los servicios de TI, en caso de algún siniestro en el Datacenter.

Recomendamos como medida de seguridad que la entidad cuente con un servidor de respaldo espejado y un sitio de alta disponibilidad fuera del recinto de servidores, para casos de contingencias que pueda afectar al servidor de base de datos y aplicativos, que impidan proseguir con las operaciones cotidianas.

El objetivo de la recomendación es otorgar mayor seguridad, tanto a los datos administrados por la Entidad, como así también evitar contingencias que impidan el normal funcionamiento de los sistemas y de los nuevos proyectos encarados.

Situación actual
Pendiente de regularización. A la fecha de nuestra visita, no hemos evidenciado la disponibilidad de un servidor espejado.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

5. INFORME SOBRE LA EJECUCIÓN PRESUPUESTARIA DE LA EMPRESA DE SERVICIOS SANITARIOS DEL PARAGUAY SA - – ESSAP SA AL 31 DE DICIEMBRE DE 2014

INFORME DE LOS AUDITORES EXTERNOS INDEPENDIENTES SOBRE LA EJECUCIÓN PRESUPUESTARIA DE LA EMPRESA DE SERVICIOS SANITARIOS DEL PARAGUAY SA AL 31 DE DICIEMBRE DE 2014

SEÑORES
PRESIDENTE Y MIEMBROS DEL DIRECTORIO DE LA
EMPRESA DE SERVICIOS SANITARIOS DEL PARAGUAY SA
(ESSAP SA)

1. Hemos examinado la Ejecución de Ingresos y de Gastos de la **EMPRESA DE SERVICIOS SANITARIOS SA (ESSAP SA)**, por el periodo comprendido entre el 1º de enero y el 31 de diciembre de 2014, que comprende los ingresos percibidos y los gastos efectuados, según el Presupuesto de Ingresos y Gastos del Ejercicio 2014, aprobado por la Asamblea General Ordinaria de Accionistas (Acta Nº 40) de fecha 30 de diciembre de 2013, de conformidad con sus Estatutos Sociales.

2. La administración de la **ESSAP SA** es responsable de la preparación y presentación de la Ejecución Presupuestaria, de conformidad con la Ley N° 1535/99 y su reglamentación Decreto N° 8127/00 y de conformidad con las leyes, decretos vigentes y las normativas emanadas del Ministerio de Hacienda.

3. Nuestra responsabilidad es realizar el examen del informe de Ejecución Presupuestaria, de acuerdo a normas técnicas de aceptación internacional y principios presupuestarios generalmente aceptados, y así obtener evidencias respaldatorias válidas y suficientes que permitan fórmanos una opinión sobre la razonabilidad de la información auditada.

   Así también, su ajuste a la normativa vigente y el cumplimiento de lo establecido en el Presupuesto aprobado y asignado a la **ESSAP S.A.** Por lo tanto, nuestra labor se encuentra supeditada, en gran medida a que la administración nos suministre la información y documentación requerida en su oportunidad. Consideramos que la auditoria que hemos realizado constituye una base razonable para fundamentar nuestra opinión.

4. Como limitación al alcance de esta revisión de Auditoria de la Ejecución Presupuestaria informamos que debido a que los programas informáticos y códigos son diferentes, no pudo ser realizada una comparación contable entre las cuentas (rubros) de la Ejecución Presupuestaria y del Estado de Resultados.

5. Basados en nuestro examen de la evidencia que sustenta los supuestos, y a excepción con la situación observada en el punto 4., no ha surgido a nuestra atención que estos supuestos no proporcionan una base razonable para el presupuesto.

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)

Consideramos que la ejecución del presupuesto institucional, el cual no está en el formato del SIAF y está preparado en formato planillas Excel, en concordancia y de acuerdo al Presupuesto aprobado por la Asamblea General Ordinaria, en todo el aspecto significativo y de los resultados de la operaciones, por el periodo comprendido entre el 1º de enero y el 31 de diciembre de 2014, de la **EMPRESA DE SERVICIOS SANITARIOS SA (ESSAP SA).**

Asunción, 07 de abril de 2015.

DR. NELSON DÍAZ ROJAS
CYCA – CONTADORES Y CONSULTORES ASOC.
MATRÍCULA PROFESIONAL CCPN° F-3

CYCA
CONTADORES Y CONSULTORES ASOC.
Dr. NELSON DIAZ ROJAS (Socio)