

INFORME DEL AUDITOR INTERNO, sobre los sistemas, procesos, seguridad de la información, infraestructura y controles de tecnología de la información al 30 de noviembre de 2024.

Unidad de negocio: **Monedero Electrónico XIGA, S.A. de C.V.**

Miembros del Consejo de Administración y Miembros del Comité de Auditoría

Presentes.-

Me dirijo a ustedes para compartir los resultados de la auditoría interna realizada sobre el entorno de tecnologías de la información de **Monedero Electrónico XIGA, S.A. de C.V.** (en adelante, **XIGA**), en cumplimiento con el Plan Anual de Auditoría Interna con enfoque en Tecnología de la Información.

Esta auditoría sobre los sistemas, procesos, seguridad de la información, infraestructura y controles de tecnología de la información abarcó hasta el 30 de noviembre de 2024 y tuvo como objetivo evaluar los procesos y el diseño de los controles de Administración de Cambios, Administración de Usuarios (tanto internos como externos) y las operaciones de los principales sistemas utilizados en la empresa, incluyendo ERP, TRESS y CONTPAQi.

Asimismo, se llevó a cabo un análisis de la infraestructura que soporta estos sistemas, garantizando el adecuado procesamiento de información y transacciones. La revisión se centró en evaluar el diseño de los controles en relación con los objetivos de control establecidos, con el propósito de identificar áreas de mejora y optimizar la eficiencia en los procesos de tecnología de la información.

En mi calidad de Gerente Auditor Interno de Tecnologías de la Información, mi responsabilidad es emitir una opinión sobre la descripción de la unidad negocios XIGA, con respecto al diseño y efectividad de los controles implementados en cumplimiento con los objetivos de control establecidos en los procesos previamente mencionados.

Las actividades de auditoría se llevaron a cabo en estricta conformidad con la Norma para Atestiguar 7090 y las normas internacionales aplicables al ejercicio profesional de la auditoría interna, en dichos estándares se encuentran especificados en el Informe de Atestiguamiento sobre los Controles de una Organización de Servicios, emitido por el Instituto Mexicano de Contadores Públicos (IMCP).

El cumplimiento de estas normas garantiza la planificación y ejecución de procedimientos, asegurando un nivel razonable de confianza en que los procesos de tecnología de la información y sus controles operan correctamente y han sido diseñados conforme a los principios de seguridad, transparencia y eficiencia operativa.

Este informe tiene como objetivo evaluar el diseño y la operatividad de los controles de tecnologías de la información en el entorno de una funcionalidad de monederos electrónicos, para ello, se han ejecutado procedimientos destinados a recopilar evidencia sustancial sobre la infraestructura tecnológica, los sistemas informáticos y la efectividad de los controles implementados en la organización.

La selección de los procedimientos de auditoría se ha realizado conforme al criterio profesional del auditor interno, considerando las mejores prácticas y estándares aplicables, asimismo, se ha llevado a cabo una evaluación rigurosa de las pruebas aplicadas a los controles con el propósito de determinar su adecuación, fiabilidad y cumplimiento normativo.


Es importante señalar las limitaciones inherentes a los controles en una organización como Monedero Electrónico XIGA, S.A. de C.V.. Si bien la descripción de XIGA y su proveedor de servicios han sido diseñados para cumplir con los marcos normativos de COSO, ITIL, ISO 27001 y COBIT, es fundamental considerar que, por su propia naturaleza, los controles operan con un grado de razonabilidad, lo que implica que no pueden prevenir ni detectar en su totalidad errores u omisiones en los procedimientos o en el registro de transacciones.

En este contexto, con base en los aspectos detallados en el presente informe y en los criterios de evaluación previamente descritos, emito mi opinión sobre los sistemas **ERP, TRESS y CONTPAQi** conforme a lo siguiente:

- Administración de cambios: El diseño de los controles y su implementación al 30 de noviembre de 2024 es razonablemente adecuado.
- Administración de usuarios (internos y externos): El diseño de los controles y su implementación al 30 de noviembre de 2024 es razonablemente adecuado.
- Operaciones: El diseño de los controles y su implementación al 30 de noviembre de 2024 es razonablemente adecuado.
- Seguridad física y lógica: Las políticas correspondientes han sido aplicadas de manera razonable al 30 de noviembre de 2024.

Quedo atento ante cualquier consulta adicional.

ATENTAMENTE



Francisco José Morales Gortáez
MAP, CPC
Gerente de Auditoría Interna.

Tijuana, Baja California a 17 de diciembre de 2024.

Aspectos Generales

Este informe, elaborado por el equipo de Auditoría Interna en cumplimiento de las disposiciones del Comité de Auditoría, presenta un análisis integral de los sistemas, procesos, infraestructura y controles de tecnologías de la información implementados en nuestra organización.

Como parte del compromiso con el gobierno corporativo de Monedero Electrónico Xiga, S.A. de C.V., se reconoce la importancia estratégica de contar con un marco robusto de controles internos, especialmente en el ámbito de la tecnología de la información, garantizando la seguridad, confidencialidad e integridad de los datos tanto de la empresa como de sus clientes.

En este contexto, Monedero Electrónico Xiga, S.A. de C.V. opera como una unidad de negocio del Grupo Enerser, bajo un marco institucional que establece una estructura de gobernanza y supervisión, con un Consejo de Administración que mantiene comunicación directa con el Comité de Auditoría. Dentro de sus atribuciones, el Comité de Auditoría es responsable de definir e implementar estrategias y programas de Auditoría Interna, incluyendo la supervisión de las Unidades de Negocio del grupo.

En cumplimiento de estos lineamientos, el Comité de Auditoría ha instruido la ejecución anual del "Informe de Sistemas, Procesos, Infraestructura y Controles de Tecnologías de la Información", con el propósito de evaluar la efectividad y cumplimiento de los controles generales de Tecnología de la Información en Monedero Electrónico Xiga, S.A. de C.V.

A través de este informe, nuestro objetivo es proporcionar una visión integral y estratégica sobre la postura de seguridad y cumplimiento de Tecnología de la Información, identificando áreas de oportunidad y mejoras que fortalezcan nuestros controles internos y permitan mitigar los riesgos asociados a la tecnología de la información.

Alcance del Informe sobre Controles Generales de Tecnología de la Información

Este informe tiene como finalidad evaluar la efectividad y cumplimiento de los controles generales de tecnología de la información (TI) en Monedero Electrónico Xiga, S.A. de C.V., conforme a los marcos normativos de COBIT, ITIL, ISO 27001 y el Principio 11 de COSO.

El objetivo es garantizar que los controles implementados:

- Se alineen con un enfoque de gestión de riesgos.
- Sean efectivos para mitigar, eliminar, transferir o absorber los riesgos residuales.
- Operen de acuerdo con los parámetros definidos.

El presente análisis incluye, pero no se limita, a los siguientes aspectos:

1. Evaluación del gobierno de TI

- Análisis de la estructura organizativa, roles y responsabilidades en la gestión de TI.
- Evaluación de alineación con los principios de COBIT en términos de control y supervisión.

2. Gestión de servicios de TI (ITIL)

- Evaluación de la entrega, soporte y mejora continua de los servicios de TI.
- Aplicación de las mejores prácticas definidas en el marco de ITIL.

3. Seguridad de la información (ISO 27001)

- Análisis de los controles de seguridad de la información aplicados.
- Protección de los activos de información conforme a los estándares de ISO 27001.

4. Evaluación de controles generales de TI (COSO - Principio 11)

- Verificación del cumplimiento del Principio 11 de COSO, relativo a la necesidad de establecer controles efectivos de TI y comunicaciones.

5. Gestión de riesgos de TI

- Análisis de los procesos de gestión de riesgos en el área de TI.
- Validación de la alineación con las estrategias corporativas de mitigación de riesgos.

6. Validación de implementación de controles

- Revisión de la implementación y funcionamiento de los controles establecidos.
- Pruebas de efectividad y operatividad en entornos reales.

El análisis comprende el período hasta el 30 de noviembre de 2024 y tiene como propósito garantizar que los controles generales de TI en Monedero Electrónico Xiga, S.A. de C.V. se encuentren alineados con las mejores prácticas y marcos normativos aplicables, priorizando la gestión de riesgos y la efectividad operativa.

Alcance de la Revisión del Contexto Tecnológico de Aplicaciones Administrativas

El presente informe aborda la revisión del entorno tecnológico de Monedero Electrónico Xiga, S.A. de C.V., con un enfoque en las principales aplicaciones utilizadas en la gestión operativa, contable y financiera de la organización.

1. Aplicaciones evaluadas

1.1. ERP (Enterprise Resource Planning)

- Propiedad de Grupo Enerser y desarrollado por Grupo Nexus (GLOBAL NEXUS S. DE R.L. DE C.V.).
- Funcionalidad: Gestión de clientes, tesorería (ingresos y pagos) y facturación.
- Infraestructura: Base de datos MS SQL, con más de 15 años de experiencia en su operación.
- Alcance de la revisión:
 - Enfoque en gestión de usuarios y cambios solicitados por Monedero Electrónico Xiga, S.A. de C.V..
 - Mantenimiento y desarrollo a cargo de Enerfuel Tech, S. de R.L. de C.V. (EFT), bajo acuerdo contractual.

1.3. TRESS

- Propósito: Sistema de gestión de nómina.
- Administración: Gerencia de Talento Humano del Grupo ENERSER.
- Uso en Monedero Xiga: Para pre-nómina y autorización de la nómina final.

2. SAP Business One

Durante mediados de 2024, Monedero Electrónico Xiga, S.A. de C.V. se realizó el proceso de migración de sus operaciones contables, financieras y fiscales al sistema SAP Business One, reemplazando progresivamente CONTPAQi.

2.1. Objetivo de la migración

- Garantizar una transición eficiente y sin interrupciones.
- Asegurar la integridad y exactitud de los datos financieros y contables.
- Cumplir con normativas y mejores prácticas en gestión financiera.

2.2. Fases del proceso

- Extracción y validación de datos desde CONTPAQi.
- Pruebas de integración con SAP Business One.
- Capacitación del personal en el nuevo sistema.
- Puesta en producción y monitoreo post-implementación.

3. Alcance y limitaciones de la revisión

- Enfoque en las aplicaciones utilizadas por Monedero Electrónico Xiga, S.A. de C.V..
- Revisión de gestión de cambios y evaluación de procesos dentro del ERP y CONTPAQi.
- Análisis de accesos y restricciones en CONTPAQi para usuarios de Monedero Xiga.

Este informe no contempla un análisis integral del ecosistema de TI de Grupo Enerser, sino exclusivamente los aspectos operativos y funcionales de Monedero Electrónico Xiga, S.A. de C.V., asegurando que los controles, accesos y procedimientos cumplan con las normativas y políticas establecidas.