XIGA-A28-F-12 Evaluación y Análisis de Riesgos

MONEDERO ELECTRONICO XIGA, S.

Fecha

	Activos / amenazas / vulnerabilidades										Valores De Inherencia					Tratamiento del riesgo				Valores después del tratamiento			
No	Actividad (nombre de Riesgo)	Objetivo	Área responsable	Tipo de Riesgo	Nombre del activo	Categoría (activo	Propietario del activo	Amenaza	Vulnerabilidad	Descripción de Riesgo	Propietario del riesgo	Consecuencia	Probabilidad	Pondera ción de Riesgo	Descripción de Ponderación Riesgo	Controles existentes	Elección de opciones	Medios de Implementación	Descripción	Consecuencia	Probabilidad	Pondera ción de Riesgo	Descripción de Ponderación Riesgo
1	Desarrollo de aplicaciones	Contar con desarrollos que ayuden en la automatización de procesos y sistemas de información	Tecnologías de la Información	Informático	Desarrolladores	<<Personas>>	Área Desarrollo	Código malicioso	Bases de datos con protección inadecuada (vulnerable contra código malicioso)	Existe el riesgo de Desarrollo con errores de aplicaciones por protección inadecuada (vulnerable contra código malicioso). Esta situación se originaría por una vulnerabilidad asociada a activo "Desarrolladores" (Personas). De materializarse, podría derivar en daño en sistema, robo de datos y afectación de la operación.	Área de Desarrollo	2	2	4	Severidad Alta	Código seguro y pruebas de seguridad en desarrollo.	1. Elección de controles	8.24 Pruebas de seguridad en desarrollo y aceptación.	[illegible]	1	1	1	Severidad Baja
2	Aplicación de cobros y cierre(caja) (compra de combustible)	Realizar la aplicación oportuna de cobro	Crédito y Cobranza	Operativo	Analistas de crédito y cobranza	<<Personas>>	Usuario	Inadecuado control de servicio	Inadecuado control de servicio	Existe el riesgo en aplicación de pagos de los clientes (en tiempo, debido a que inadecuado control de servicio. Esta situación se origina por una vulnerabilidad asociada a activo "Analistas de crédito y cobranza" (Personas). De materializarse, podría derivar en inadecuado tiempo proceso de aplicación de cobro en aplicación, afectando la atención al cliente y de la operación.	Cliente	2	2	4	Severidad Alta	Clasificación semi-automática de riesgo.	1. Elección de controles	8.12 Gestión de cambios.	[illegible]	1	1	1	Severidad Alta
3	Servicio al cliente	Brindar asesoría a los clientes sobre el uso y bondades del sistema de monedero electrónico	Atención a clientes	Operativo	Analistas de atención a clientes	<<Aplicaciones y bases de datos>	Usuario	Mala asesoría al cliente	Inadecuado nivel de conocimiento y/o concientización de empleados	Existe el riesgo de servicio al cliente tenga mala asesoría al cliente debido a que inadecuado nivel de conocimiento y/o concientización de empleados. Esta situación se originaría por una vulnerabilidad asociada a activo "Analistas de atención a clientes" (Aplicaciones y bases de datos). De materializarse, podría derivar en mala asesoría al cliente, afectando aspectos del servicio.	Analista de atención a clientes	1	1	2	Severidad Media	Grabación de llamadas de los clientes	1. Elección de controles	6.3 Concientización, educación y capacitación sobre seguridad de la información. Realizar auditorías a llamadas de los analistas de clientes	1	1	2	Severidad Media
4	Uso de software con licencia en la operación de monedero	Contar con software disponibles para el desarrollo operativo del monedero	Tecnologías de la Información	Cumplimiento	Software de aplicaciones (con licencia)	<<Aplicaciones y bases de datos>	Gerencia Sistemas	Incumplimiento de relaciones contractuales	Software no documentado	Existe el riesgo de incumplimiento de Licencias de software. Esta situación se origina por una vulnerabilidad asociada a activo "Software de aplicaciones (con licencia)". De materializarse, podría derivar en pérdida de activos, ya que el incumplimiento puede incurrir en la terminación de permisos en uso de licencias de software, lo que podría interrumpir operaciones (TI).	Empresa	1	1	2	Severidad Media	Monitoreo de licencias activas	1. Elección de controles	5.9 Inventario de información y otros activos asociados. Realizar Auditorías Internas	1	1	2	Severidad Media
5	Desarrollo de aplicaciones	Contar con desarrollos que ayuden en la automatización de procesos y sistemas de información	Tecnologías de la Información	Informático	Software de sistemas	<<Aplicaciones y bases de datos>	Área Desarrollo	Errores de aplicaciones	Interfaz de usuario complicada	Existe el riesgo de errores de desarrollo de aplicaciones debido a que la interfaz de usuario se considera complicada. Esta situación se origina por una vulnerabilidad asociada a activo "Software de sistemas (Aplicaciones y bases de datos). De materializarse, podría derivar en afectación de la experiencia del cliente en la aplicaciones, afectando aspectos del servicio.	Área de Desarrollo	1	1	2	Severidad Media	Diseño de pantallas según multitudes sistema actualización e requerimiento de usuario	1. Elección de controles	8.25 Ciclo de vida de desarrollo seguro. Identificación de necesidades de los usuarios	1	1	2	Severidad Media
6	Desarrollo de aplicaciones	Contar con desarrollos que ayuden en la automatización de procesos y sistemas de información	Tecnologías de la Información	Informático	Bases de datos	<<Aplicaciones y bases de datos>	Área Desarrollo	Errores de Base de Datos	Requisitos para desarrollo de software no definidos con calidad	Existe el riesgo de errores de desarrollo de aplicaciones debido a que requisitos para desarrollo de software no definidos con calidad. Esta situación se origina por una vulnerabilidad asociada a activo "Aplicaciones y bases de datos. De materializarse podría requerir nuevo errores no detectados, modificación de usuarios y posibles vulnerabilidades de seguridad. Esta última, debido a que al tarde de comprensión y al pasar por otro requisitos de seguridad críticos pueden ser comprometidos ocasionando ataques, violaciones de datos, cómo incidentes de seguridad.	Área de Desarrollo	1	1	2	Severidad Media	Ambiente aseguramiento de Calidad (QA) para pruebas de la estructura correcta de las tablas de la BD (datos completos)	1. Elección de controles	8.31 Separación de los entornos de desarrollo, prueba y producción. Lograr adecuado control de ambiente	1	1	2	Severidad Media
7	Elaboración de contratos	Proteger los bienes de la empresa	Administración Jurídica	Fraude	Contratos	<<Documentación (en papel o formato electrónico)>	Jurídico	Incumplimiento de relaciones contractuales	Inadecuado nivel de conocimiento y/o concientización de empleados	Existe el riesgo de incumplimiento de relaciones contractuales debido a que inadecuado nivel de conocimiento y/o concientización de empleados. Esta situación se origina por una vulnerabilidad asociada a activo "Contratos" documentación (en papel o formato electrónico). De materializarse, podría derivar en incumplimiento de relaciones contractuales, afectando pérdidas financieras, daño a la reputación, responsabilidades legales e interrupciones operativas o de servicio.	Empresa	1	1	2	Severidad Media	Elaboración de contratos de acuerdo a políticas establecidas	1. Elección de controles	5.34 Cumplimiento de políticas, reglas y estándares de seguridad de la información. Auditorías internas y contratos.	1	1	2	Severidad Media
8	Custodia de expedientes de clientes	Asegurar que los expedientes mantengan su integridad	Crédito y Cobranza	Fraude	Archivos	<<Documentación (en papel o formato electrónico)>	Usuario	Destrucción de registros	Inadecuada supervisión del trabajo de los empleados	Existe el riesgo de fallas en la custodia de expedientes de clientes (conocidos) que destrucción de registros debido a que inadecuada supervisión del trabajo de los empleados. Esta situación se origina por una vulnerabilidad asociada a activo "Archivos" Documentación (en papel o formato electrónico). De materializarse, podría derivar en destrucción de registros, posibles filtraciones de datos, pérdida de confidencialidad y problemas de cumplimiento legal.	Empresa	1	1	2	Severidad Media	Todo el almacenamiento de documentos es digitalizado y almacenado a través de la plataforma OneDrive	1. Elección de controles	5.12 Clasificación de la información. Seguimiento a la política de clasificación y etiquetado de la información	1	1	2	Severidad Media
9	Gestión de presupuesto	Desarrollar un presupuesto que cubra todas las necesidades operativas, de tecnología, de personal para el adecuado funcionamiento del monedero	Gerencia de Monedero	Financiero	Presupuestos	Área (Departamentos de directorio), de la junta Facultades gerentes de unidades de negocio	Dirección Comercial	Presupuesto insuficiente para operar	Mala gestión presupuestaria	Existe el riesgo de que presupuesto insuficiente para operar debido a que mala gestión presupuestaria. Esta situación se originaría una vulnerabilidad asociada a activo "Presupuestos" (Área (Departamentos de directorio), de la junta Facultades gerentes de unidades de negocio). De materializarse, podría derivar en presupuesto insuficiente, inestabilidad financiera, pérdida oportunidades perdidas, dificultades para alcanzar objetivos para operar.	Usuario de monedero	1	1	2	Severidad Media	Comité de Presupuesto	4. Aceptación del riesgo	5.2 Funciones y responsabilidades de seguridad de la información. Cada departamento debería identificar las necesidades de la operación del monedero	1	1	2	Severidad Media
10	Disponibilidad de los equipos de computo	Garantizar que los equipos de computo de usuarios (laptoops) para el buen funcionamiento del monedero	Tecnologías de la Información	Informático	Computadoras de escritorio/portátiles	<<TI, comunicaciones y demás equipamiento>	Área de Compras	Fallas en equipos	Mantenimiento inadecuado	Existe el riesgo de que fallas en equipos de computo debido a que mantenimiento inadecuado. Esta situación se origina por una vulnerabilidad asociada a activo "Computadoras de escritorio/portátiles (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en fallas en equipos, afectando aspectos del servicio.	Usuario	1	1	2	Severidad Media	Mantenimiento preventivo cada 6 meses	1. Elección de controles	7.13 Mantenimiento de equipo. Seguimiento de los planes de contratos para mantenimiento de equipos	1	1	2	Severidad Media
11	Garantizar el suministro de energía eléctrica en los servidores	Asegurar que los servidores cuenten con energía eléctrica en todo momento	Responsable de mantenimiento (corporativo)	Operativo	Generadores de electricidad	<<TI, comunicaciones y demás equipamiento>	Mantenimiento	Fallas en equipos	Mantenimiento inadecuado	Existe el riesgo de que suministro de energía eléctrica en los servidores falle en equipos debido a que mantenimiento inadecuado. Esta situación se origina por una vulnerabilidad asociada a activo "Generadores de electricidad (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en fallas en equipos, afectando aspectos del servicio	Empresa	1	1	2	Severidad Media	Bitácora de mantenimiento	1. Elección de controles	7.13 Mantenimiento de equipo. Seguimiento de los planes existentes para mantenimiento de equipos de soporte para el servicio de energía eléctrica. **Para las instalaciones donde radica el Centro de Datos es contratado servicio con Proveedor.**	1	1	2	Severidad Media
12	Gestión de redes	Asegurar una adecuada gestión de los enlaces de comunicación	Coordinador de Infraestructura	Informático	Equipamiento de red	<<TI, comunicaciones y demás equipamiento>	Área de Infraestructura	Falla en los enlaces de comunicación	Inadecuada gestión de redes	Existe el riesgo de que falla en los enlaces de comunicación debido a que inadecuada gestión de redes. Esta situación se origina por una vulnerabilidad asociada a activo "Equipamiento de red" (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en interrupciones de seguridad, pérdida de datos, daño financiero y daño a la reputación de la empresa.	Empresa	1	1	2	Severidad Media	Aplicar la seguridad de la información en los acuerdos con proveedores.	1. Elección de controles	1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores. Contratación de enlaces redundantes	1	1	2	Severidad Media
13	Gestión de servidores	Asegurar la disponibilidad de los recursos de servidores	Coordinador de Infraestructura	Informático	Servidores	<<TI, comunicaciones y demás equipamiento>	Área de Infraestructura	Indisponibilidad del servicio por falla de Servidores	Degradación de servicio	Existe el riesgo de que indisponibilidad del servicio por falla de servidores debido a que degradación del servicio. Esta situación se origina por una vulnerabilidad asociada a activo "Servidores" (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en indisponibilidad del servicio por falla de servidores, interrupciones en las actividades en línea, pérdida de datos y pérdidas financieras.	Empresa	1	1	2	Severidad Media	Aplicar la seguridad de la información en los acuerdos con proveedores.	1. Elección de controles	1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores. Clúster de virtualización, con servidores redundantes.	1	1	2	Severidad Media
14	Gestión de los sistemas de telefonía	Garantizar el funcionamiento de los sistemas de telefonía	Coordinador de Infraestructura	Comunicaciones	Centrales telefónicas	<<TI, comunicaciones y demás equipamiento>	Área de Infraestructura	Falla en los enlaces de comunicación	Degradación del servicio	Existe el riesgo de que falla en los enlaces de comunicación de sistemas de telefonía debido a degradación del servicio. Esta situación se origina por una vulnerabilidad asociada a activo "Centrales telefónicas (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en falla en los enlaces de comunicación, fallas de líneas y servicio operativo que puedan afectar la comunicación, la productividad y la continuidad del negocio.	Clientes	1	1	2	Severidad Media	Aplicar la seguridad de la información en los acuerdos con proveedores.	1. Elección de controles	1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores. Conmutador virtual sobre clúster de servidores. Alertas, servicio empresariales de telefonía.	1	1	2	Severidad Media
15	Gestión de los sistemas de impresoras	Garantizar la disponibilidad de equipos de impresión	Gerencia de compras	Operativo	Impresoras	<<TI, comunicaciones y demás equipamiento>	Área de Compras	Fallas en equipos	Mantenimiento inadecuado	Existe el riesgo de que falla en equipos de impresoras debido a que mantenimiento inadecuado. Esta situación se origina por una vulnerabilidad asociada a activo "Impresoras" (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en fallas en equipos, afectando aspectos del servicio.	Usuario	1	1	2	Severidad Media	Mantenimiento a través de proveedor.	1. Elección de controles	7.13 Mantenimiento de equipo. En caso de falla de equipo el proveedor acude a la organización para dar soporte requerido.	1	1	2	Severidad Media
16	Garantizar el suministro de energía eléctrica en las oficinas	Asegurar que las oficinas cuenten con energía eléctrica en todo momento	Responsable de mantenimiento (corporativo)	Operativo	Suministro de energía eléctrica	<<Servicios tercerizados (Proveedores)>	Mantenimiento	Interrupción de suministro eléctrico	Mantenimiento inadecuado	Existe el riesgo de que interrupción de suministro eléctrico debido a que mantenimiento inadecuado. Esta situación se origina por una vulnerabilidad asociada a activo "Suministro de energía eléctrica" (Servicios tercerizados - Proveedores). De materializarse, podría derivar en problemas de productividad, seguridad afectar las operaciones, conflictos.	Empresa	1	1	2	Severidad Media	Generador de energía eléctrica.	1. Elección de controles	7.13 Mantenimiento de equipo. Seguimiento de los planes existentes para mantenimiento de equipos	1	1	2	Severidad Media
17	Mantenimiento a los sistemas de información	Garantizar que los sistemas de información se aplique a política de servicio	Servicios tercerizados	Informático	Mantenimiento de sistemas de información	<<Servicios tercerizados (Proveedores)>	Área de Infraestructura	Errores de mantenimiento	Mantenimiento inadecuado	Existe el riesgo de que los sistemas de información no se aplique a política de servicio. Esta situación se originaría por una vulnerabilidad asociada a activo "Mantenimiento de sistemas de información" (Servicios tercerizados - Proveedores). De materializarse, podría derivar en errores de mantenimiento, cambios significativos de reparación y reemplazo, posibles interrupciones de negocio, debido a fallas de sistema y la pérdida de confianza de los clientes que confían en la fiabilidad del sistema. También puede dificultar la resolución de errores de software.	Usuario	1	1	2	Severidad Media	Mantenimiento preventivo, así como cumplimiento de licencia.	1. Elección de controles	1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores. Monitoreo constante de aplicación de actualizaciones. Notificación al proveedor en caso de fallas y posibilidad de reinstalaciones.	1	1	2	Severidad Media
18	Protección de los sistemas de mensajería y correo electrónico	Proveedor de un sistema que garantice la protección de los equipos y software ante cualquier ataque SPAM	Servicios tercerizados	Informático	Servicios de correo y mensajería	<<Servicios tercerizados (Proveedores)>	Área de Infraestructura	Ataques de SPAM	Bloqueo de correo sin protección	Existe el riesgo en los sistemas de mensajería y correo electrónico por ataques de spam debido a que bloqueo de correo sin protección. Esta situación se originaría por una vulnerabilidad asociada a activo "Servicios de correo y mensajería" (Servicios tercerizados - Proveedores). De materializarse, podría derivar en ataques de spam, afectando por violaciones de datos, robo de identidad y pérdidas financieras, especialmente cuando se intercambia información confidencial a través de correos no cifrados o dañinos.	Empresa	1	1	2	Severidad Media	Chiteo de correo (o) Firewall	1. Elección de controles	6.3 Concientización, educación y capacitación sobre seguridad de la información. Concientizar al usuario sobre los ataques de SPAM. Seguimiento a reporte de estadísticas de seguridad.	1	1	2	Severidad Media
19	Cumplimiento a la normativa de anexo 28	Garantizar que la operación del monedero aplique los requerimientos de anexo 28 de SAT	Gerente de Monedero	Cumplimiento Normativo	Desconocimiento Normativo	Cambios en la regulación/ interpretación	Dirección Comercial	Incumplimiento de leyes	Inadecuado nivel de conocimiento y/o concientización de empleados	Existe el riesgo de cumplimiento de la normativa de Anexo 28, debido a inadecuado nivel de conocimiento y/o concientización de empleados. Esta situación se originaría por incumplimiento de la ley. De materializarse podría derivar en sanciones financieras, daño a la reputación, procedimientos legales y pérdida de clientes para empresa.	Empresa	1	1	2	Severidad Media	Cumplimiento de Anexo 28	1. Elección de controles	5.35 Revisión independiente de la seguridad de la información. Auditorías o revisiones internas independientes para seguimiento y cumplimiento de políticas y procedimientos	1	1	2	Severidad Media
20	Sistema de protección contra incendios	Asegurar que los sistemas de contra incendios funcionen de manera permanente	Inmobiliaria	Operativo	Incendios	<<<Naturaleza>>>	Inmobiliaria	Destrucción de registros	Susceptibilidad de equipamiento a la temperatura	Existe el riesgo natural de incendio, que provocaría destrucción de registros por la susceptibilidad de equipamiento a la temperatura. Esta situación se originaría por una vulnerabilidad asociada a activo "Incendios" (Naturaleza). De materializarse, podría derivar en destrucción de registros, afectando la productividad, interrupción de negocio, responsabilidades legales e inclusiones de lesiones.	Empresa	1	1	2	Severidad Media	Mantenimiento preventivo por parte de bomberos y plan de continuidad en caso de contingencia	1. Elección de controles	7.5 Protección de oficinas, habitaciones e instalaciones. Seguimiento de los planes de contingencia, mantenimiento de equipos y seguimiento a programas de protección civil (Extintores, cotejar sitio alterno.	1	1	2	Severidad Media
21	Plan de contingencia	Contar con protocolos de actuación ante siniestros	Inmobiliaria	Operativo	Siniestros	<<<Naturaleza>>>	Inmobiliaria	Destrucción de registros	Susceptibilidad de equipamiento a la humedad y a la contaminación	Existe el riesgo natural de siniestro, que derivaría en la destrucción de registros debido a que susceptibilidad de equipamiento a la humedad y a la contaminación. Esta situación se originaría por una vulnerabilidad asociada a "Siniestros" (Naturaleza). De materializarse, podría derivar en destrucción de registros, pérdidas financieras, interrupciones operativas.	Empresa	1	1	2	Severidad Media	Seguir controles de evacuación de usuarios según el plan de continuidad en caso de contingencia	1. Elección de controles	7.5 Protección de oficinas, habitaciones e instalaciones. Seguimiento de los planes de contingencia, mantenimiento de equipos y seguimiento a programas de protección Civil (Extintores, cotejar sitio alterno.	1	1	2	Severidad Media
22	Protección de la información de datos	Proteger la información de los clientes	Crédito y Cobranza Atención a Clientes Ventas Mantenimiento de Cartera	Fraude	Información de los clientes	Bases de datos	Admón. Base de datos	Fuga o intervención de información	Nivel de confidencialidad no definido con calidad	Existe el riesgo en la información de datos de los clientes por fuga o intervención de información debido a que nivel de confidencialidad no definido con calidad. Esta situación se originaría por una vulnerabilidad asociada a activo "Información de los clientes" (Bases de datos). De materializarse, podría derivar en problemas legales, daño a la reputación y pérdidas financieras.	Gerente de Tecnología de la información	1	1	2	Severidad Media	Acuerdos de confidencialidad no divulgación	1. Elección de controles	5.35 Revisión independiente de la seguridad de la información. Realizar auditorías a los clientes de usuarios a las bases de datos, y a los registros de clasificación interesada y confidencial.	1	1	2	Severidad Media
23	Aplicación (código)	Contar con una línea de estado con el servidor (mobile) adicionalmente garantizar la correcta operación del Monedero	Tecnologías de la Información	Informático	Aplicación (servidor)	<<TI, comunicaciones y demás equipamiento>	Área de Infraestructura	Falla en los enlaces de comunicación	Inadecuada gestión de redes	Existe el riesgo Aplicación (en Código) Falla en los enlaces de comunicación debido a que inadecuada gestión de redes. Esta situación se originaría por una vulnerabilidad asociada a activo "Aplicación (servidor)" (TI), comunicaciones y demás equipamiento). De materializarse, podría derivar en falla en los enlaces de comunicación, afectando aspectos del servicio.	Empresa	1	1	2	Severidad Media	Cumplimiento del mantenimiento preventivo.	1. Elección de controles	8.21 Seguridad de los servicios de red. Seguimiento de los planes de mantenimiento de equipos. Así como continua supervisión del funcionamiento de los servidores	1	1	2	Severidad Media

Elaboró: _____ Aprobó: _____

XIGA-A28-F-12
Rev.01/18