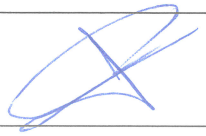
RESUMEN DE HISTORIA DE CAMBIOS

Revisión	Fecha	Razón del Cambio
00	11-12-2018	- Documento de nueva creación bajo el Sistema de Administración.
01	12-12-2018	- Se realizó modificación en el encabezado.
02	23-05-2019	- Se modificó punto 8.
03	22-05-2020	- Se realizó modificación en el nombre del Monedero.
04	21-05-2021	- Se realizó la revisión anual del documento.
05	20-05-2022	- Se realizó la revisión anual del documento. - Se cambió el título de TI-IT-INF-16 a XIGA-A28-IT-07.
06	19-05-2023	- Se realizó la revisión anual del documento.
07	17-05-2024	- Se realizó la revisión anual del documento.
08	07-04-2025	- Se actualizó la tabla de participantes y aprobaciones.

	Elaboró	Revisó	Aprobó
Nombre	Merced Ortiz	Miguel Ricario	Elodia Robles
Puesto	Coordinador de XIGA	Gerente de XIGA	Representante Legal
Firma			

1. Propósito

1.1. Establecer los mecanismos para gestionar los incidentes que ponen en riesgo la integridad de la información del Monedero Electrónico XIGA, haciendo que se conviertan en acciones de mejora continua reduciendo la brecha en la seguridad.

2. Alcance

2.1. Este plan queda acotado a los sistemas, elementos de infraestructura e información de terceros que existe en los sistemas del Monedero Electrónico XIGA.

3. Roles y Responsabilidades

3.1. Para atender los incidentes de inseguridad y derivar de las acciones de mejora, será necesario que los siguientes roles realicen las siguientes funciones.

3.2. **Usuario final.** Es el encargado de reportar inmediatamente a la mesa de ayuda el robo, extravío, el comportamiento anormal de sus dispositivos o aplicaciones, según se estipula en la política de servicios de TI.

3.3. **Operador de Mesa de ayuda**. Es el encargado de recibir el reporte y tomar las medidas necesarias para reducir el riesgo de exposición de los datos tomando las siguientes medidas:

3.3.1. En caso de robo o extravío, bloquear o restablecer las contraseñas de directorio activo, correo y otros sistemas.

3.3.2. En caso de pérdida de datos o comportamiento anormal de aplicaciones, deberá aislar el dispositivo de la red y hacer un diagnóstico.

3.3.3. Escalar vía correo electrónico con el encargado de infraestructura.

3.4. **Administrador de infraestructura**. El encargado de infraestructura deberá realizar las siguientes acciones:

3.4.1. Diagnosticar el problema.

3.4.2. Determinar el grado de exposición de los datos.

3.4.3. Implementar las medidas de remediación necesarias.

3.4.4. Informar a los implicados para tomar las medidas legales necesarias.

3.5. **Administrador de base de datos**. Será notificado en caso de considerar que el incidente de seguridad haya puesto en riesgo los datos para realizar una validación de la integridad.

3.6. **Dirección de TI.** Será el área encargada de gestionar el flujo de información a la Dirección General y al área Fiscal para hacer las notificaciones en caso de haber pérdida de información. En caso de un incidente menor que no implique perdida de datos, la Gerencia de TI deberá gestionar el cambio en las configuraciones, políticas, procedimientos y su inscripción en la base de conocimiento, esto para evitar en el futuro el mismo tipo de incidentes y permitir su rápida resolución en caso de reincidencias.

4. Clasificación de Incidentes

4.1. **Extravío o fallas de equipo.** Se consideran eventos de carácter menor, todos aquellos donde se extravíe una PC con información en discos encriptado o los datos en ellos sean ilegibles por falla de hardware.

4.2. **Ataque de software malicioso.** Son ocasionados por agentes de software como virus, troyanos, malware randsomware, etc. Serán considerados de grado menor siempre y cuando la información referente al monedero no quede expuesta o alterada y solo causen la interrupción o el mal funcionamiento de los equipos o sistemas.

4.3. **Fraude.** El resultante de que alguien trate de violar alguno de los mecanismos de seguridad del código QR, clonar y generar códigos inválidos y conseguir un cargo no autorizado, este tipo de incidentes deberán considerarse de grado mayor y deberá ser reportado inmediatamente para su investigación y solución.

4.4. **Ingeniería social.** Son aquellos donde cibercriminales utilizando engaños traten de impresionar a usuarios legítimos del sistema o clientes para robar identidades o información y utilizarla con fines no autorizados. La exposición de información por uno de estos ataques es considerada de carácter mayor y debe ser atendido con extremada urgencia.

4.5. **Ataque persistente dirigido.** Son aquellos ocasionados por hackers especializados durante largos periodos de tiempo, con el fin de obtener acceso a un sistema en específico mediante técnicas como fuerza bruta, phising, ataque a vulnerabilidades conocidas en versiones de software obsoletas y que conlleven el acceso no autorizado a los datos referentes al Monedero Electrónico XIGA. Este tipo de ataques serán considerados de carácter mayor y deberán ser tratados con extrema urgencia.

5. Documentación de incidentes

5.1. Ante una falla o posible sospecha de fraude, robo de identidad de un usuario o clonación de código QR, la mesa de ayuda deberá crear un ticket de servicio. Así como también a petición de un usuario, cliente o de alguna alarma en la consola del firewall.

5.2. Por parte del área de Infraestructura deberá llevarse una bitácora de los incidentes de seguridad, la cual deberá contener: fecha y hora del incidente, el tipo o clasificación del incidente, persona que lo reporto, diagnostico, solución y acción de mejora emprendida para efectos preventivos. Para tales efectos deberá llenarse el formato **XIGA-A28-F-25 Registro de incidentes de seguridad**.

6. Recolección de evidencia de incidentes

6.1. En el proceso de investigación que deberá realizar el área de Infraestructura, deberá recolectar evidencia para un diagnóstico exacto el cual pudiera en determinado momento para:

6.1.1. Generar una acción de mejora.

6.1.2. Tener evidencia para ejercer una acción legal.

6.1.3. Determinar el grado de afectación.

6.2. Entre las evidencias que deberán recolectarse están las siguientes: logs de sistemas operativos y aplicaciones, archivos dañados, configuraciones, captura de pantallas, logs de servidores DHCP y autenticación de Directorio Activo.

7. Alimentación de la base de conocimientos.

7.1. El formato **XIGA-A28-F-29 Base de conocimientos para atención de incidencias** deberá estar en constante actualización a medida que se completen los formularios en el **XIGA-A28-F-25 Registro de incidentes de seguridad**. Los cuales deberán convertirse en acciones de mejora que modifiquen el funcionamiento del código QR, configuraciones o procesos y en instrucciones para la mesa de soporte sobre cómo actuar ante dichos eventos en un futuro, permitiendo su rápida solución y reduciendo la superficie de exposición.

7.1.1. Detección: La organización identifica las fuentes de conocimiento las cuales pueden ser tanto internas a través de los reportes internos de incidentes en el formato **XIGA-A28-F-25 Registro de incidentes de seguridad** o externos a través de los clientes, proveedores, etc.

7.1.2. Captura: La empresa capta conocimiento crítico para poder cumplir con sus acciones y ponerlo a disposición del personal involucrado. Dependiendo del proceso, se pueden aplicar entrevistas, análisis de protocolos, simulaciones observación, análisis de documentos, entre otras.

7.1.3. Clasificación y almacenamiento: Estos procesos de clasificación para lograr el uso adecuado del conocimiento se guardan en un repositorio de base de conocimiento.

7.1.4. Distribución: Se realiza a través de los reportes consultables del formato **XIGA-A28-F-29 Base de conocimientos para atención de incidencias**, con el objetivo de poner a disposición del personal involucrado el conocimiento crítico, esto a través del sistema que utilice la organización.

8. Tabla de escalamiento

8.1. Las incidencias deberán ser gestionadas según la siguiente tabla de escalamiento:

Matriz de escalamiento Monedero Electrónico XIGA Atención a fallas e incidentes			
Tiempo de respuesta	Área	ROL Responsable	Extensión
0-2 horas	Mesa de Ayuda	Operador	664 633 3100 Ext. 5083 Corto 334
2-24 horas	Infraestructura	Encargado	664 633 3100 Ext. 5049 Corto 385
Más de 24 horas	Gerencia de TI	Gerente	664 633 3100 Ext. 5005 Corto 217

9. Tiempos de respuesta

9.1. Para los incidentes de seguridad de grado mayor se atienden de inmediato por mesa de ayuda en un máximo de 2 horas. Las excepciones que no quedaran resueltas de raíz, se escalan al Encargado de Infraestructura en un lapso de 2-4 horas. De no resolverse, el tiempo máximo de respuesta deberá ser menor a 24 horas con la Gerencia de TI para su investigación y solución definitiva.

10. Lineamientos para remediación de incidentes

10.1. Los criterios a seguir para solventar los incidentes de seguridad son los siguientes:

10.1.1. Actuar con sentido de urgencia.

10.1.2. Identificar el tipo de incidente e informar a la Gerencia.

10.1.3. En caso de tratarse de un ataque cortar el vector de ataque o aislar la afectación lo más rápido posible.

10.1.4. Que se convierta en una acción de mejora que impacte la base de conocimientos y prevenga en el futuro las mismas incidencias.

11. Documentos de referencia

Código	Documentos
N/A	-

12. Registros

Código	Registros	Tiempo de Conservación	Responsable de Conservarlo	Lugar de Almacenamiento
XIGA-A28-F-25	Registro de incidentes de seguridad	Indefinido	Infraestructura	Archivo digital
XIGA-A28-F-29	Base de conocimientos para atención de incidencias	Indefinido	Infraestructura	Archivo digital

13. Glosario

13.1. N/A.

14. Anexos

14.1. N/A.