SECRETARIA DE HACIENDA Y CREDITO PUBLICO

ANEXOS 23, 24, 25, 25-Bis, 28, 29, 30, 31 y 32 de la Resolución Miscelánea Fiscal para 2024, publicada el 29 de diciembre de 2023.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- HACIENDA.- Secretaría de Hacienda y Crédito Público.- Servicio de Administración Tributaria.

ANEXO 28 DE LA RESOLUCIÓN MISCELÁNEA FISCAL PARA 2024

Obligaciones y requisitos de los emisores de monederos electrónicos

Para los efectos del artículo 27, fracciones III, primer y segundo párrafos y XI de la Ley del ISR, en relación con las reglas 1.9., fracción XXVI, 3.3.1.8., 3.3.1.10., 3.3.1.17., y 3.3.1.19., se dan a conocer las obligaciones y requisitos de los emisores de monederos electrónicos utilizados en la adquisición de combustibles para vehículos marítimos, aéreos y terrestres y de vales de despensa, conforme a lo siguiente:

Contenido

A. Definiciones.

Para efectos del presente Anexo debe entenderse por:

I. Riesgo:

La probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de las Tecnologías de la Información y las Comunicaciones (TIC) y los activos de información.

II. Política:

Conjunto de reglas y prácticas definidas por las personas morales con el fin de regular la manera de dirigir, proteger y distribuir los recursos para llevar a cabo los objetivos estratégicos de las personas morales.

III. Grupos de interés especial:

Organizaciones, instituciones, empresas y cualquier otro grupo de entes que tengan como objetivo el monitoreo, mejora y prevención de incidentes de seguridad de la información y seguridad en aspectos de tecnología.

IV. Dispositivos móviles:

Los dispositivos de comunicación que pueden ser trasladados y operados en distintas ubicaciones geográficas, utilizados por las personas servidoras públicas del SAT y personas servidoras públicas del OIC, externos y terceros autorizados para el desempeño de sus funciones de manera remota o en sitio.

V. Monedero Electrónico utilizado en la adquisición de combustibles para vehículos marítimos, aéreos y terrestres:

Cualquier dispositivo tecnológico que se encuentre asociado a un sistema de pagos utilizado por los contribuyentes en la adquisición de combustibles para vehículos marítimos, aéreos y terrestres, dicho sistema deberá proporcionar los servicios de liquidación y compensación de los pagos que se realicen entre los contribuyentes obligados, los emisores de los monederos electrónicos y los enajenantes de combustibles.

VI. Monedero Electrónico de Vales de Despensa:

Cualquier dispositivo tecnológico que se encuentre asociado a un sistema de pagos, que proporcione los servicios de liquidación y compensación de los pagos que se realicen entre los patrones contratantes de los monederos electrónicos, los trabajadores beneficiarios de los mismos, los emisores autorizados de los monederos electrónicos y los enajenantes de despensas.

VII. Verificación:

Es el acto administrativo a través del cual se comprueba el cumplimiento de requisitos y obligaciones en materia de tecnologías de la información, confidencialidad, integridad, disponibilidad y seguridad de la información.

VIII. Dirección:

Nivel jerárquico con capacidad de toma de decisiones a nivel estratégico, con la finalidad de alcanzar los objetivos definidos por la empresa.

IX. Conflicto de intereses:

La posible afectación del desempeño imparcial y objetivo de las funciones de los servidores públicos en razón de intereses personales, familiares o de negocios.

X. Centro de Datos:

El espacio físico donde se concentran los recursos necesarios, consistentes en equipo informático y redes de comunicaciones para el procesamiento de la información de una Institución o proveedor de servicios

B. Monederos electrónicos utilizados en la adquisición de combustibles para vehículos marítimos, aéreos y terrestres.

I. Obligaciones y requisitos que los emisores de monederos electrónicos para la adquisición de combustibles para vehículos marítimos, aéreos y terrestres, deben cumplir en la verificación tecnológica.

Presentar la siguiente documentación o información:

1. Descripción del proceso de gestión de riesgos, el cual debe contener lo siguiente:

a) Lineamientos generados o adoptados por la persona moral para la identificación de escenarios de riesgo; identificación de riesgos a los que se encuentra expuesta la persona moral por la operación del monedero, tecnología utilizada, factores humanos, climatológicos y cambios en la legislación.

b) Lineamientos generados o adoptados por la persona moral para categorizar o tipificar los riesgos a los que se encuentra expuesta la persona moral y niveles de aceptación del riesgo definidos por la persona moral.

c) Lineamientos generados o adoptados por la persona moral para reducir los riesgos a niveles aceptables.

d) Lineamientos generados o adoptados por la persona moral para realizar la revisión permanente de los riesgos e identificar los cambios en el entorno que puedan incrementar el nivel de riesgo.

2. Análisis de riesgos realizado por la persona moral cuyo contenido debe incluir al menos las actividades relacionadas con el monedero electrónico, incluyendo la identificación de riesgos a los que se encuentra expuesta la persona moral, categorización y planes de remediación diseñados por la persona moral para reducir el impacto o probabilidad de materialización de los riesgos; el documento debe contemplar riesgos relacionados con todo aquel personal ajeno a la persona moral que tenga acceso a información de los contribuyentes.

3. Política de seguridad de la información, la cual debe contener lo siguiente:

a) Definición de seguridad de la información de la persona moral.

b) Normatividad, legislación y marcos de referencia aplicables a la persona moral.

c) Roles y responsabilidades de la persona moral respecto de la seguridad de la información.

d) La dirección debe manifestar su compromiso con la seguridad de la información.

e) Lineamientos de seguridad de la información de la persona moral.

f) Penalizaciones por incumplimiento de lo establecido en la política.

g) Lineamientos de atención a situaciones fortuitas relacionadas con la seguridad de la información.

h) Lineamientos de seguridad de la información para proveedores y todo aquel personal ajeno a la persona moral que tengan acceso a información de los contribuyentes.

i) El documento debe ser comunicado formalmente a todo el personal de la persona moral y generar evidencia de dicha comunicación.

j) Control de versiones de la política (fecha, participantes, control de cambios).

k) Periodicidad de revisión de la política.

4. Identificación de los diferentes puestos operativos definidos por la persona moral y sus respectivos roles, actividades y responsabilidades.

5. Documentación donde se especifique cómo la persona moral evita el conflicto de intereses de los diferentes puestos respecto a sus actividades, roles y responsabilidades.

6. Descripción del procedimiento mediante el cual la persona moral contactará al SAT para reportar fallas de infraestructura o incidentes que pongan en riesgo la confidencialidad, disponibilidad e integridad de la información de los contribuyentes.

7. Documentos o formularios de inscripción (RSS, listas de correo y boletines, entre otros) con grupos de interés especial.

8. Política de trabajo remoto para empleados, la cual debe contener lo siguiente:

a) Definición de trabajo remoto de la persona moral.

b) Condiciones mediante las cuales se autoriza el trabajo remoto.

c) Aprovisionamiento para el trabajo remoto.

d) Periodo de autorización de trabajo remoto.

e) Penalizaciones por incumplimiento de lo establecido en la política.

f) Lineamientos de atención a situaciones fortuitas.

g) Lineamientos para la cancelación de la autorización de trabajo remoto.

h) Control de versiones de la política (fecha, participantes y control de cambios).

i) Periodicidad de revisión de la política.

9. Procedimiento para la autorización de uso de dispositivos móviles (teléfono celular, tableta, entre otros) en el manejo de información de los contribuyentes por cualquier medio (correo electrónico, aplicativos, entre otros).

10. Procedimiento que realiza la persona moral para la selección del personal, verificación de desempeño e incidencias en empleos anteriores.

11. Términos y condiciones del empleo de acuerdo al puesto y la forma en que la persona moral comunica dicha información al personal que participa en el proceso de contratación.

12. Documentación acerca de la capacitación en materia de seguridad de la información que la persona moral provee a los empleados.

13. Procedimiento de terminación de la relación contractual con los empleados y cuando se modifiquen las actividades, roles y responsabilidades.

14. Inventario de activos de la persona moral vinculados a las actividades del monedero electrónico, el cual debe contener lo siguiente:

a) Identificador del activo.

b) Dirección IP del activo.

c) Características del activo (marca, modelo, serie, sistema operativo, entre otros).

d) Propietario del activo.

e) Responsable del activo.

f) Ubicación física del activo.

15. Política de uso aceptable de activos, la cual debe contener lo siguiente:

a) Definición de uso aceptable de activos de la persona moral.

b) Lineamientos bajo los cuales la persona moral considera el uso aceptable de activos.

c) Penalizaciones por incumplimiento de lo establecido en la política.

d) Lineamientos de atención a situaciones fortuitas.

e) Control de versiones de la política (fecha, participantes y control de cambios).

f) Periodicidad de revisión de la política.

16. Procedimiento de retorno de activos tangibles e intangibles de los empleados de la persona moral ante la terminación de la relación contractual, o ante cambios en las actividades, roles y responsabilidades.

17. Política de clasificación de la información, debe contener lo siguiente:

a) Definición de clasificación de información de la persona moral.

b) Rubros en los que será clasificada la información.

c) Lineamientos para la clasificación de información.

d) Penalizaciones por incumplimiento de lo establecido en la política.

e) Lineamientos de atención a situaciones fortuitas.

f) Control de versiones de la política (fecha, participantes y control de cambios).

g) Periodicidad de revisión de la política.

18. Procedimiento de etiquetado de información relacionada con las actividades del monedero electrónico, tanto en formato físico como en los sistemas de información.

19. Lineamientos para el manejo de información de acuerdo a su clasificación ya sea en formato físico o digital.

20. Procedimiento para autorizar y revocar el uso de medios removibles de almacenamiento utilizados por personal de la persona moral, traslado de los medios dentro y fuera de las oficinas de la persona moral o centro de datos.

21. Política de control de accesos a los sistemas, la cual debe contener lo siguiente:

a) Definición de acceso a los sistemas de la persona moral.

b) Directrices para el uso y operación de sistemas.

c) Penalizaciones por incumplimiento de lo establecido en la política.

d) Lineamientos de atención a situaciones fortuitas.

e) Control de versiones de la política (fecha, participantes y control de cambios).

f) Periodicidad de revisión de la política.

22. Documentación que describa las restricciones implementadas por la persona moral para el uso de redes y servicios de red ajenos a las actividades, roles y responsabilidades de los empleados y proveedores.

23. Procedimiento para realizar el registro e inhabilitar cuentas de usuario en los sistemas, redes y servicios de red relacionados con la actividad del monedero electrónico.

24. Documentación que describa las condiciones mediante las cuales la persona moral otorgará las facilidades y activos necesarios a los empleados para que éstos desempeñen sus actividades, lo anterior de acuerdo al puesto.

25. Procedimiento mediante el cual los administradores de los sistemas relacionados con las actividades del monedero electrónico gestionan los derechos de los usuarios, el cual debe contener lo siguiente:

a) Cuando un empleado es dado de alta.

b) Ante cambios en actividades, roles y responsabilidades del empleado.

c) Generación y gestión de cuentas privilegiadas en los sistemas.

d) Procedimiento mediante el cual los administradores de los sistemas verifican que los permisos y niveles de acceso de los empleados son correspondientes a sus actividades, roles y responsabilidades.

26. Procedimiento de gestión de información de autenticación a los sistemas relacionados con las actividades del monedero electrónico que la persona moral sigue para entregar dicha información a los empleados por primera vez, en caso que el usuario solicite cambio de información de autenticación y el cambio obligatorio de información de autenticación en el primer inicio de sesión de los usuarios.

27. Documentación que describa la comunicación de responsabilidades formalmente a los empleados una vez concluido el proceso de contratación.

28. Documentación que muestre los controles implementados en el inicio de sesión a los sistemas, redes y servicios de red relacionados con actividades del monedero electrónico, contra personal no autorizado o ajeno a la persona moral, y mecanismos en los sistemas que permitan el uso de contraseñas que cumplen con los requerimientos y mejores prácticas respecto a la longitud y composición.

29. Documentación que describa las condiciones bajo las cuales se autoriza el uso de herramientas de análisis de vulnerabilidades, monitoreo de actividades y de cualquier otra naturaleza que puedan ser configuradas para omitir los controles de seguridad de los sistemas para cumplir sus objetivos y que la persona moral necesite implementar; se debe mantener un registro permanente e independiente del listado de este tipo de herramientas.

30. Procedimiento mediante el cual la persona moral, autoriza el acceso al código fuente de los sistemas y aplicativos relacionados con las actividades del monedero electrónico.

31. Política de controles de cifrado, la cual debe contener lo siguiente:

a) Definición de los sistemas, redes y servicios de red que implementan controles de cifrado.

b) Condiciones para el uso de controles de cifrado.

c) Administración de llaves utilizadas en los controles de cifrado (uso, resguardo, disposición, entre otros).

d) Penalizaciones por incumplimiento de lo establecido en la política.

e) Lineamientos de atención a situaciones fortuitas.

f) Control de versiones de la política (fecha, participantes y control de cambios).

g) Periodicidad de revisión de la política.

32. Documentación que permita identificar los perímetros de seguridad para las áreas en las que se realiza el procesamiento de transacciones y de sistemas relacionados con el monedero electrónico.

33. Documentación que permita identificar los controles físicos de acceso al centro de datos de la persona moral, dichos controles deben impedir el acceso a personas que no cuenten con autorización, la persona moral debe mantener un registro permanente del personal autorizado para acceder al centro de datos.

34. Documentación que permita identificar los controles físicos de acceso a las oficinas de la persona moral (acceso principal, áreas de carga y descarga, entre otros), dichos controles deben impedir el acceso a personas que no cuenten con autorización; la persona moral debe mantener un registro permanente del personal autorizado para acceder a las oficinas de la empresa.

35. Documentación donde se identifiquen los controles implementados por la persona moral contra incendio, inundaciones, terremotos, manifestaciones y cualquier otro fenómeno meteorológico o social que ponga en riesgo la operación monedero electrónico en las oficinas y centros de datos.

36. Documentación donde se identifiquen las áreas seguras para el procesamiento de información de los contribuyentes en las oficinas de la persona moral y en el centro de datos.

37. Procedimiento para la gestión de activos, el cual debe contener lo siguiente:

a) Condiciones para la instalación de activos en el centro de datos y oficinas de la persona moral.

b) Requerimientos de seguridad en el cableado y redes inalámbricas.

c) Baja de equipos en las oficinas de la persona moral o el centro de datos.

d) Reúso de medios de almacenamiento.

e) Destrucción de medios de almacenamiento.

f) Borrado seguro de medios de almacenamiento.

38. Documentación que describa los equipos que dan soporte a la operación de activos relacionados con las actividades del monedero electrónico (plantas de luz, balanceadores de carga eléctrica, entre otros).

39. Documentación donde se identifiquen los planes de mantenimiento para los activos relacionados con las actividades del monedero electrónico.

40. Documentación que describa el procedimiento para proteger los equipos que sean utilizados para actividades relacionadas con el monedero electrónico y que se encuentren fuera de las oficinas de la persona moral.

41. Política de escritorio limpio y equipo desatendido, la cual debe contener lo siguiente:

a) Definición de escritorio limpio de la persona moral.

b) Definición de equipo desatendido de la persona moral.

c) Lineamientos para que los empleados mantengan escritorio limpio.

d) Lineamientos para equipos desatendidos.

e) Penalizaciones por incumplimiento de lo establecido en la política.

f) Lineamientos de atención a situaciones fortuitas.

g) Control de versiones de la política (fecha, participantes, control de cambios).

h) Periodicidad de revisión de la política.

42. Documentación que incluya el estudio de capacidad tecnológica, de personal e instalaciones para la operación del monedero electrónico, esta capacidad debe ser evaluada y los resultados documentados cada doce meses (de acuerdo al calendario fiscal).

43. Documentación que incluya el diagrama de interconexión de los activos relacionados con el monedero electrónico con los identificadores descritos en el inventario de activos, se deben separar físicamente o lógicamente los ambientes de desarrollo, pruebas y producción (operativo).

44. Documentación que describa las características de la solución que la persona moral implementa contra código malicioso (detección, prevención y recuperación de sistemas).

45. Política de respaldos de la persona moral, la cual debe contener lo siguiente:

a) Definición de respaldos de la persona moral.

b) Roles y responsabilidades para gestionar respaldos.

c) Listado de sistemas, activos y herramientas que deben ser sujetos a respaldo.

d) Definición de medios de almacenamiento autorizados para realizar respaldos.

e) Lineamientos para generación de respaldos.

f) Lineamientos para pruebas de respaldos.

g) Lineamientos para periodos de resguardo de respaldos.

h) Lineamientos para destrucción de respaldos.

i) Definición de ubicación física de respaldos fuera del centro de datos y controles de protección de acceso.

j) Penalizaciones por incumplimiento de lo establecido en la política.

k) Lineamientos de atención a situaciones fortuitas.

l) Control de versiones de la política (fecha, participantes, control de cambios).

m) Periodicidad de revisión de la política.

46. Documentación que permita identificar los registros de actividades de los sistemas de información, sistemas operativos y cualquier otro activo relacionado al monedero electrónico, los registros deben contener lo siguiente:

a) Identificador del usuario que realiza la actividad.

b) Descripción de la actividad realizada.

c) Origen de la conexión al sistema.

d) Resultado de la actividad efectuada.

e) Los registros deben ser generados como solo lectura para los usuarios.

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.

NOTA: La persona moral debe generar registros de actividades, administradores y cuentas privilegiadas, para lo cual debe contemplar lo descrito en el inciso e) dichos registros no deberán ser accedidos por administradores o cuentas privilegiadas.

47. Documentación técnica del protocolo NTP o equipo que implemente este protocolo utilizado para la sincronización de relojes de los sistemas, redes y servicios de red relacionados con las actividades del monedero.

48. Documentación que describa las configuraciones de los activos relacionados con las actividades del monedero electrónico, equipos de los empleados y equipos de red, debe contener lo siguiente:

a) Para equipos de empleados:

i. Protección del BIOS.

ii. Limitación de derechos de acceso para modificación del sistema operativo.

iii. Configuración de bloqueo automático por tiempo de inactividad.

iv. Restricción de instalación de programas.

v. Inhabilitación de puertos físicos utilizados en transferencia de información o almacenamiento (salvo autorización formal).

vi. Configuraciones de seguridad del fabricante (no deben derivar en incumplimiento de políticas de la persona moral).

vii. Inhabilitación de usuarios por defecto del sistema operativo.

b) Para activos relacionados con las actividades del monedero electrónico:

i. Protección del BIOS.

ii. Configuración de puertos, protocolos y servicios requeridos para su operación.

iii. Configuración de registros de actividades.

iv. Inhabilitación de puertos, protocolos y servicios no requeridos para su operación.

v. Inhabilitación de puertos físicos utilizados en transferencia de información o almacenamiento (salvo autorización formal).

vi. Instalación de sistema operativo en partición exclusiva.

vii. Configuración de reglas de filtrado de paquetes, detección y prevención de intrusos.

viii. Configuraciones de seguridad del fabricante (no deben derivar en incumplimiento de políticas de la persona moral).

c) Para equipos de red:

i. Configuración de registros de actividades.

ii. Configuración de gestión de tráfico de paquetes.

iii. Controles de seguridad en redes expuestas e internas en las oficinas de la persona moral y centro de datos.

iv. Segregación de redes.

49. Procedimiento mediante el cual la persona moral gestiona las vulnerabilidades técnicas de los activos relacionados con las actividades del monedero electrónico, equipos de los empleados y equipos de red, el cual debe contener lo siguiente:

a) Calendarización de análisis de vulnerabilidades.

b) Protocolo de análisis de vulnerabilidades.

c) Documentación de resultados de análisis de vulnerabilidades.

d) Clasificación de vulnerabilidades.

e) Lineamiento para el diseño de planes de remediación de vulnerabilidades.

f) Protocolo de pruebas de penetración para activos críticos.

g) Documentación de resultados de pruebas de penetración.

h) Lineamientos para el diseño de planes de remediación de resultados de pruebas de penetración.

50. Documentación que describa los controles implementados para la protección de transferencia de información contra intercepción, copia no autorizada, modificación, borrado, pérdida, transmisión de código malicioso; la persona moral debe contar con acuerdos firmados de transferencia de información con proveedores.

51. Acuerdos de confidencialidad celebrados con empleados y proveedores (se solicitará una muestra física y digital de originales durante la verificación).

52. Documentación que permita identificar controles implementados por la persona moral para servicios expuestos, la cual debe contener lo siguiente:

a) Controles de seguridad contra fraudes y filtración de información.

b) Controles para evitar transmisión incompleta de transacciones, mal enrutamiento, alteración de mensajes, revelación de información y copia no autorizada.

53. Política de desarrollo seguro de la persona moral, la cual debe contener lo siguiente:

a) Definición de desarrollo seguro de la persona moral.

b) Marco de referencia de desarrollo seguro, debe incluir la referencia en la documentación de cada desarrollo.

c) Lineamientos de seguridad para desarrollos internos y desarrollos requeridos a proveedores.

d) Lineamientos de aceptación de desarrollos.

e) Lineamientos para definir la propiedad intelectual de los desarrollos contratados con terceros.

f) Restricciones de cambios en *software* de propósito general (ofimática, diseño, base de datos, entre otros).

g) Lineamientos para establecer un entorno seguro para desarrollos realizados por empleados.

h) Penalizaciones por incumplimiento de lo establecido en la política.

i) Lineamientos de atención a situaciones fortuitas.

j) Control de versiones de la política (fecha, participantes y control de cambios).

k) Periodicidad de revisión de la política.

54. Documentación que describa la gestión de cambios en los sistemas relacionados con el monedero electrónico, la cual debe contener lo siguiente:

a) Protocolo de control de cambios.

b) Formatos utilizados para el control de cambios.

c) Esquema de autorización de control de cambios.

d) Pruebas de los cambios en ambientes de desarrollo, pruebas y producción (operación).

e) Documentación de resultados de pruebas mencionadas en el inciso anterior.

f) Pruebas después de la liberación del cambio.

g) Documentación de resultados de pruebas mencionadas en el inciso anterior.

h) Registro de control de versiones de los desarrollos.

i) Resguardo de repositorios de versiones de desarrollos.

55. Política de relaciones entre la persona moral y sus proveedores, la cual debe contener lo siguiente:

a) Definición de relaciones con proveedores de la persona moral.

b) Lineamientos para definir alcance y objetivo de los acuerdos con proveedores.

c) Lineamientos para definir las condiciones de entrega de servicio de los proveedores.

d) Lineamientos para autorizar el acceso a la información de contribuyentes a los proveedores.

e) Controles de seguridad para los servicios.

f) Inclusión de cláusula de auditoría para contratación de servicios con proveedores.

g) Lineamientos para realizar cambios en las condiciones de entrega de servicios.

h) Penalizaciones por incumplimiento de lo establecido en la política.

i) Lineamientos de atención a situaciones fortuitas.

j) Control de versiones de la política (fecha, participantes y control de cambios).

k) Periodicidad de revisión de la política.

56. Procedimiento de atención a incidentes que afecten la confidencialidad, integridad o disponibilidad de la información de los contribuyentes, el cual debe contener lo siguiente:

a) Roles y responsabilidades.

b) Clasificación de incidentes.

c) Documentación de incidentes.

d) Recolección de evidencia del incidente.

e) Alimentación de base de conocimientos.

f) Tabla de escalamiento.

g) Tiempos de respuesta.

h) Lineamientos para remediación de incidentes.

57. Documentación que describa los esquemas de alta disponibilidad que la persona moral implementa para las actividades relacionadas con el monedero electrónico.

58. Documentación que describa los planes de continuidad de la persona moral, la cual debe contener lo siguiente:

a) Determinación de escenarios que pongan en riesgo la continuidad del negocio.

b) Roles y responsabilidades para los planes.

c) Protocolos de respuesta ante ocurrencia de los escenarios descritos en el inciso a).

d) Documentación de resultados de la ejecución de los planes.

e) Diseño de pruebas de los planes.

f) Acondicionamiento para realizar pruebas de los planes.

g) Documentación de resultados de pruebas de los planes.

h) Adecuaciones a los planes.

i) Revisión periódica de los planes.

59. Documentación que describa los planes de recuperación de desastres de la persona moral, la cual debe contener lo siguiente:

a) Determinación de escenarios que la persona moral identifique como desastre.

b) Roles y responsabilidades para los planes.

c) Protocolos de respuesta ante ocurrencia de los escenarios descritos en el inciso a).

d) Documentación de resultados de la ejecución de los planes.

e) Diseño de pruebas de los planes.

f) Acondicionamiento para realizar pruebas de los planes.

g) Documentación de resultados de pruebas de los planes.

h) Adecuaciones a los planes.

i) Revisión periódica de los planes.

60. Documentación en la que se defina un calendario de verificaciones independientes de seguridad de la información. El término independiente se refiere a que debe llevarse a cabo por personal que no haya participado en el diseño o implementación de los controles o que pertenezca a las áreas evaluadas, el personal puede ser interno o externo.

61. Ejemplar del monedero electrónico, el cual debe incluir lo siguiente:

a) Nombre comercial del monedero electrónico.

b) Denominación social del emisor.

c) Identificador del monedero.

d) Número telefónico de atención al usuario o cliente.

62. Reglas de negocio respecto a la relación entre beneficiarios y vehículos autorizados.

63. Información del monedero electrónico, el cual debe incluir lo siguiente:

a) Tecnología implementada en el ejemplar.

b) Almacenamiento seguro de datos en el ejemplar.

c) Especificaciones de la tecnología del ejemplar.

64. Realización de pruebas al ejemplar, mismas que deben contemplar lo siguiente:

a) Verificación de protocolo de autenticación del beneficiario e identificación del vehículo.

b) Intento de adquisición de combustible con el monedero electrónico.

c) Verificación de condiciones de bloqueo del monedero.

d) Intento de adquisición de combustible con el monedero electrónico.

e) Verificación de condiciones de desbloqueo del monedero.

f) Intento de transacción con el monedero electrónico con combustible distinto al definido en el monedero.

NOTA: Las pruebas son enunciativas más no limitativas y se llevarán a cabo en sitio, el personal verificador puede realizar pruebas adicionales si lo considera necesario.

65. Documentación que describa la gestión de los procesos operativos relacionados con el monedero electrónico, la cual debe incluir lo siguiente:

a) Comunicación de protocolo de autenticación a beneficiarios y al uso del monedero electrónico.

b) Comunicación de protocolo de identificación de vehículos a beneficiarios.

c) Comunicación de protocolo de autenticación de beneficiarios a estaciones de servicio y al uso del monedero electrónico.

d) Comunicación de protocolo de identificación de vehículos a estaciones de servicio.

e) Protocolos de notificación a clientes, beneficiarios y estaciones de servicio en caso de existir cambios en el protocolo de autenticación de beneficiarios o identificación de vehículos.

f) Capacitación respecto a la administración de monederos por parte de los clientes.

g) Entrega la información de autenticación a clientes y beneficiarios, aceptación y resguardo de la información por parte de clientes y beneficiarios.

h) Protocolos para atención a clientes y beneficiarios, escalamiento de solicitudes y autorizaciones; debe incluir el protocolo para comunicar estos protocolos a clientes y beneficiarios.

i) Inhabilitación de monederos electrónicos o beneficiarios.

j) Inhabilitación de acceso a los sistemas a clientes y beneficiarios.

k) Cambios en los datos de clientes y beneficiarios.

Nota: La documentación señalada en los numerales 1, 2, 3, 8, 9, 10, 13, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 40, 41, 42, 43, 44, 45, 48, 49, 50, 53, 54, 55, 56, 57, 58, 59, 60 y 65 deberá de encontrarse firmada y rubricada por el representante legal o apoderado legal del tercero que solicita la autorización.

C. Monederos electrónicos de vales de despensa.

I. Obligaciones y requisitos que los emisores de monederos electrónicos de vales de despensa deben cumplir en la verificación tecnológica.

Presentar la siguiente documentación o información:

1. Descripción del proceso de gestión de riesgos firmado por la dirección, el cual debe contener lo siguiente:

a) Lineamientos para la identificación de escenarios de riesgo, identificación de riesgos a los que se encuentra expuesta la persona moral por la operación del monedero, tecnología utilizada, factores humanos, climatológicos y cambios en la legislación.

b) El documento debe contener los lineamientos para categorizar o tipificar los riesgos a los que se encuentra expuesta la persona moral y niveles de aceptación del riesgo definidos por el mismo.

c) El documento debe contener los lineamientos para reducir los riesgos a niveles aceptables por el tercero autorizado.

d) El documento debe contener los lineamientos para la revisión permanente de los riesgos para identificar los cambios en el entorno que puedan incrementar el nivel de riesgo para la empresa.

2. Análisis de riesgos realizado por la empresa cuyo alcance debe ser al menos las actividades relacionadas con el monedero electrónico de vales de despensa, el documento debe incluir la identificación de riesgos a los que se encuentra expuesta la persona moral, categorización y planes de remediación diseñados por la persona moral para reducir el impacto o probabilidad de materialización de los riesgos; contemplando los riesgos relacionados con proveedores y todo aquel personal ajeno a la persona moral que tenga acceso a información de los contribuyentes.

3. Política de seguridad de la información, la cual debe contener lo siguiente:

a) Definición de seguridad de la información de la persona moral.

b) Normatividad, legislación y marcos de referencia aplicables a la persona moral.

c) Roles y responsabilidades del personal de la persona moral respecto de la seguridad de la información.

d) La dirección debe manifestar su compromiso con la seguridad de la información.

e) Lineamientos de seguridad de la información de la persona moral.

f) Penalizaciones por incumplimiento de lo establecido en la política.

g) Lineamientos de atención a situaciones fortuitas relacionadas con la seguridad de la información.

h) Lineamientos de seguridad de la información para proveedores y todo aquel personal ajeno a la persona moral que tenga acceso a información de los contribuyentes.

i) El documento debe ser comunicado formalmente a todo el personal de la persona moral y generar evidencia de dicha comunicación.

j) Control de versiones de la política (fecha, participantes y control de cambios).

k) Periodicidad de revisión de la política.

4. Identificación de los diferentes puestos definidos por la persona moral y sus respectivos actividades, roles y responsabilidades.

5. Documentación donde se especifique cómo es que la persona moral evita el conflicto de intereses de los diferentes puestos respecto a sus actividades, roles y responsabilidades.

6. Descripción del procedimiento mediante el cual la persona moral contactará al SAT para reportar fallas de infraestructura o incidentes que pongan en riesgo la confidencialidad, disponibilidad e integridad de la información de los contribuyentes.

7. Documentos o formularios de inscripción (RSS, listas de correo, boletines, entre otros) con grupos de interés especial.

8. Política de trabajo remoto para empleados, la cual debe contener lo siguiente:

a) Definición de trabajo remoto de la persona moral.

b) Condiciones mediante las cuales se autoriza el trabajo remoto.

c) Aprovisionamiento para el trabajo remoto.

d) Periodo de autorización de trabajo remoto.

e) Penalizaciones por incumplimiento de lo establecido en la política.

f) Lineamientos de atención a situaciones fortuitas.

g) Directrices para la cancelación del aprovisionamiento de trabajo remoto.

h) Control de versiones de la política (fecha, participantes y control de cambios).

i) Periodicidad de revisión de la política.

9. Documentación para la autorización del uso de dispositivos móviles (teléfono celular, tableta, entre otros) en el manejo de información de los contribuyentes por cualquier medio (correo electrónico, aplicativos, entre otros).

10. Procedimientos que realiza la persona moral para la selección del personal, verificación de desempeño e incidencias en empleos anteriores.

11. Términos y condiciones del empleo de acuerdo al puesto y la forma como la persona moral comunica dicha información al personal que participa en el proceso de contratación.

12. Documentación acerca de la capacitación en materia de seguridad de la información que la persona moral provee a los empleados.

13. Procedimiento de terminación de la relación contractual con los empleados y cuando se modifiquen las actividades, roles y responsabilidades.

14. Inventario de activos de la persona moral vinculados a las actividades del monedero electrónico, debe contener lo siguiente:

a) Identificador del activo.

b) Dirección IP del activo.

c) Características del activo (marca, modelo, serie, sistema operativo, entre otros).

d) Propietario del activo.

e) Responsable del activo.

f) Ubicación física del activo.

15. Política de uso aceptable de activos, la cual debe contener lo siguiente:

a) Definición de uso aceptable de activos de la persona moral.

b) Lineamientos bajo las cuales la persona moral considera el uso aceptable de activos.

c) Penalizaciones por incumplimiento de lo establecido en la política.

d) Lineamientos de atención a situaciones fortuitas.

e) Control de versiones de la política (fecha, participantes, control de cambios).

f) Periodicidad de revisión de la política.

16. Procedimiento de retorno de activos tangibles e intangibles de los empleados de la persona moral ante la terminación de la relación contractual, o ante cambios en las actividades, roles y responsabilidades.

17. Política de clasificación de la información, debe contener lo siguiente:

a) Definición de clasificación de información de la persona moral.

b) Rubros en los que será clasificada la información.

c) Lineamientos para la clasificación de información.

d) Penalizaciones por incumplimiento de lo establecido en la política.

e) Lineamientos de atención a situaciones fortuitas.

f) Control de versiones de la política (fecha, participantes y control de cambios).

g) Periodicidad de revisión de la política.

18. Procedimiento de etiquetado de información relacionada con las actividades del monedero electrónico, tanto en formato físico como en los sistemas de información.

19. Lineamientos para manejo de información de acuerdo a su clasificación ya sea en formato físico o digital.

20. Procedimiento para autorizar y revocar el uso de medios removibles de almacenamiento utilizados por el personal de la persona moral, traslado de los medios dentro y fuera de las oficinas.

21. Política de control de accesos a los sistemas, la cual debe contener lo siguiente:

a) Definición de acceso a los sistemas del tercero autorizado.

b) Lineamientos para el uso y operación de sistemas.

c) Penalizaciones por incumplimiento de lo establecido en la política.

d) Lineamientos de atención a situaciones fortuitas.

e) Control de versiones de la política (fecha, participantes y control de cambios).

f) Periodicidad de revisión de la política.

22. Documentación que describa las restricciones implementadas por la persona moral para el uso de redes y servicios de red ajenos a las actividades, roles y responsabilidades de los empleados y proveedores.

23. Procedimiento para realizar el registro e inhabilitar cuentas de usuarios en los sistemas, redes y servicios de red relacionados con la actividad del monedero electrónico.

24. Documentación que describa las condiciones mediante las cuales la persona moral otorgará las facilidades y activos necesarios a los empleados para que estos desempeñen sus actividades, lo anterior de acuerdo al puesto.

25. Procedimiento mediante el cual los administradores de los sistemas relacionados con las actividades del monedero electrónico gestionan los derechos de los usuarios, el cual debe incluir lo siguiente:

a) Cuando un empleado es dado de alta.

b) Ante cambios en actividades, roles y responsabilidades del empleado.

c) Generación y gestión de cuentas privilegiadas en los sistemas.

d) Procedimiento mediante el cual los administradores de los sistemas verifican que los permisos y niveles de acceso de los empleados son correspondientes a sus actividades, roles y responsabilidades.

26. Procedimiento de gestión de información de autenticación a los sistemas relacionados con las actividades del monedero electrónico que la persona moral sigue para entregar dicha información a los empleados por primera vez, en caso de que el usuario solicite cambio de información de autenticación y el cambio obligatorio de información de autenticación en el primer inicio de sesión de los usuarios.

27. Documentación que describa la comunicación de responsabilidades formalmente a los empleados una vez concluido el proceso de contratación.

28. Documentación que muestre los controles implementados en el inicio de sesión a los sistemas, redes y servicios de red relacionados con actividades del monedero electrónico, contra personal no autorizado o ajeno a la persona moral, y mecanismos en los sistemas que permitan el uso de contraseñas que cumplen con los requerimientos y mejores prácticas respecto a la longitud y composición.

29. Documentación que describa las condiciones bajo las cuales se autoriza el uso de herramientas, análisis de vulnerabilidades, monitoreo de actividades y de cualquier otra naturaleza que puedan ser configuradas para omitir los controles de seguridad de los sistemas para cumplir sus objetivos y que la persona moral necesite implementar; se debe mantener un registro permanente e independiente del listado de este tipo de herramientas.

30. Procedimiento mediante el cual la persona moral, autoriza el acceso al código fuente de los sistemas y aplicativos relacionados con las actividades del monedero electrónico.

31. Política de controles de cifrado, la cual debe contener lo siguiente:

a) Definición de los sistemas, redes y servicios de red que implementan controles de cifrado.

b) Condiciones para el uso de controles de cifrado.

c) Administración de llaves utilizadas en los controles de cifrado (uso, resguardo, disposición, entre otros).

d) Penalizaciones por incumplimiento de lo establecido en la política.

e) Lineamientos de atención a situaciones fortuitas.

f) Control de versiones de la política (fecha, participantes y control de cambios).

g) Periodicidad de revisión de la política.

32. Documentación que permita los perímetros de seguridad para las áreas en las que se realiza el procesamiento de transacciones y de sistemas relacionados con el monedero electrónico.

33. Documentación que permita identificar los controles físicos de acceso al centro de datos de la persona moral, dichos controles deben impedir el acceso a personas que no cuenten con autorización, la persona moral debe mantener un registro permanente del personal autorizado para acceder al centro de datos.

34. Documentación que permita identificar los controles físicos de acceso a las oficinas de la persona moral (acceso principal, áreas de carga y descarga, entre otros), dichos controles deben impedir el acceso a personas que no cuenten con autorización, la persona moral debe mantener un registro permanente del personal autorizado para acceder a las oficinas de la empresa.

35. Documentación donde se identifiquen los controles implementados por la persona moral contra incendio, inundaciones, terremotos, manifestaciones y cualquier otro fenómeno meteorológico o social que ponga en riesgo la operación del monedero electrónico en las oficinas y centros de datos.

36. Documentación donde se identifiquen las áreas seguras para el procesamiento de información de los contribuyentes en las oficinas de la persona moral y en el centro de datos.

37. Procedimiento para la gestión de activos; el cual debe incluir lo siguiente:

a) Condiciones para la instalación de activos en el centro de datos y oficinas del tercero autorizado.

b) Requerimientos de seguridad en el cableado y redes inalámbricas.

c) Baja de equipos en las oficinas de la persona moral o el centro de datos.

d) Reúso de medios de almacenamiento.

e) Destrucción de medios de almacenamiento.

f) Borrado seguro de medios de almacenamiento.

38. Documentación que describa los equipos que dan soporte a la operación de activos relacionados con las actividades del monedero electrónico (plantas de luz, balanceadores de carga eléctrica, entre otros).

39. Documentación en la que se identifiquen planes de mantenimiento para los activos relacionados con las actividades del monedero electrónico.

40. Documentación que describa los procedimientos para proteger los equipos que sea utilizados para actividades relacionadas con el monedero electrónico y que se encuentren fuera de las oficinas de la persona moral.

41. Política de escritorio limpio y equipo desatendido, la cual debe contener lo siguiente:

a) Definición de escritorio limpio de la persona moral.

b) Definición de equipo desatendido de la persona moral.

c) Lineamientos para que los empleados mantengan escritorio limpio.

d) Lineamientos para equipos desatendidos.

e) Penalizaciones por incumplimiento de lo establecido en la política.

f) Lineamientos de atención a situaciones fortuitas.

g) Control de versiones de la política (fecha, participantes y control de cambios).

h) Periodicidad de revisión de la política.

42. Documentación que incluya el estudio de capacidad tecnológica, de personal e instalaciones para la operación del monedero electrónico, esta capacidad debe ser evaluada y los resultados documentados cada doce meses.

43. Documentación que incluya el diagrama de interconexión de los activos relacionados con el monedero electrónico con los identificadores descritos en el inventario de activos, se debe separar físicamente o lógicamente los ambientes de desarrollo, pruebas y producción (operativo).

44. Documentación que describa las características de la solución que la persona moral implementa contra código malicioso (detección, prevención y recuperación de sistemas).

45. Política de respaldos, la cual debe contener lo siguiente:

a) Definición de respaldos de la persona moral.

b) Roles y responsabilidades para realizar y gestionar respaldos.

c) Listado de sistemas, activos y herramientas que deben ser sujetos a respaldo.

d) Definición de medios de almacenamiento autorizados para realizar respaldos.

e) Lineamientos para generación de respaldos.

f) Lineamientos para pruebas de respaldos.

g) Lineamientos para periodos de resguardo de respaldos.

h) Lineamientos para destrucción de respaldos.

i) Definición de ubicación física de respaldos fuera del centro de datos y controles de protección de acceso.

j) Penalizaciones por incumplimiento de lo establecido en la política.

k) Lineamientos de atención a situaciones fortuitas.

l) Control de versiones de la política (fecha, participantes y control de cambios).

m) Periodicidad de revisión de la política.

46. Documentación que permita identificar los registros de actividades de los sistemas de información, sistemas operativos y cualquier otro activo relacionado al monedero electrónico, los registros deben contener:

a) Identificador del usuario que realiza la actividad.

b) Descripción de la actividad realizada.

c) Origen de la conexión al sistema.

d) Resultado de la actividad efectuada.

e) Todos los registros deben ser generados como solo lectura para todos los usuarios.

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada.

NOTA: La persona moral debe generar registros de actividades independientes para administradores y cuentas privilegiadas, debiendo contemplar lo descrito en el inciso e) dichos registros no deberán ser accedidos por administradores o cuentas privilegiadas.

47. Documentación técnica del protocolo NTP o equipo que implemente este protocolo y que sea utilizado para la sincronización de relojes de los sistemas, redes y servicios de red relacionados con las actividades del monedero.

48. Documentación que describa las configuraciones de los activos relacionados con las actividades del monedero electrónico, equipos de los empleados y equipos de red, la cual debe contener lo siguiente:

a) Para equipos de empleados:

i. Protección del BIOS.

ii. Limitación de derechos de acceso a configuraciones de sistema operativo.

iii. Configuración de bloqueo automático por tiempo de inactividad.

iv. Restricción de instalación de programas.

v. Inhabilitación de puertos físicos utilizados en transferencia de información o almacenamiento (salvo autorización formal).

vi. Configuraciones de seguridad del fabricante (no deben derivar en incumplimiento de políticas de la persona moral).

vii. Inhabilitación de usuarios por defecto del sistema operativo.

b) Para activos relacionados con las actividades del monedero electrónico:

i. Protección del BIOS.

ii. Configuración de puertos, protocolos y servicios requeridos para su operación.

iii. Configuración de registros de actividades.

iv. Inhabilitación de puertos, protocolos y servicios no requeridos para su operación.

v. Inhabilitación de puertos físicos utilizados en transferencia de información o almacenamiento (salvo autorización formal).

vi. Instalación de sistema operativo en partición exclusiva.

vii. Configuración de reglas de filtrado de paquetes, detección y prevención de intrusos.

viii. Configuraciones de seguridad del fabricante (no deben derivar en incumplimiento de políticas de la persona moral).

c) Para equipos de red:

i. Configuración de registros de actividades.

ii. Configuración de gestión de tráfico de paquetes.

iii. Controles de seguridad en redes expuestas e internas en las oficinas de la persona moral y centro de datos.

iv. Segregación de redes.

49. Procedimiento mediante el cual la persona moral gestiona las vulnerabilidades técnicas de los activos relacionados con las actividades del monedero electrónico de vales de despensa, equipos de los empleados y equipos de red, la cual debe contener lo siguiente:

a) Calendarización de análisis de vulnerabilidades.

b) Protocolo de análisis de vulnerabilidades.

c) Documentación de resultados de análisis de vulnerabilidades.

d) Clasificación de vulnerabilidades.

e) Lineamientos para el diseño de planes de remediación de vulnerabilidades.

f) Protocolo de pruebas de penetración para activos críticos.

g) Documentación de resultados de pruebas de penetración.

h) Lineamientos para el diseño de planes de remediación de resultados de pruebas de penetración.

50. Documentación que describa los controles implementados para la protección de transferencia de información contra intercepción, copia no autorizada, modificación, borrado, pérdida, transmisión de código malicioso; la persona moral debe contar con acuerdos firmados de transferencia de información con proveedores.

51. Acuerdos de confidencialidad celebrados con empleados y proveedores (se solicitará una muestra física y digital de originales durante la verificación).

52. Documentación que permita identificar controles implementados por la persona moral para servicios expuestos, la cual debe incluir lo siguiente:

a) Controles de seguridad contra fraudes y filtración de información.

b) Controles para evitar transmisión incompleta de transacciones, mal enrutamiento, alteración de mensajes, revelación de información y copia no autorizada.

53. Política de desarrollo seguro de la persona moral, la cual debe contener lo siguiente:

a) Definición de desarrollo seguro de la persona moral.

b) Marco de referencia de desarrollo seguro, se debe incluir la referencia en la documentación de cada desarrollo.

c) Lineamientos de seguridad para desarrollos internos y requeridos a proveedores.

d) Lineamientos de aceptación de desarrollos.

e) Lineamientos para definir la propiedad intelectual de los desarrollos contratados con terceros.

f) Restricciones de cambios en software de propósito general (ofimática, diseño, base de datos, entre otros).

g) Lineamientos para establecer un entorno seguro para desarrollos realizados por empleados.

h) Penalizaciones por incumplimiento de lo establecido en la política.

i) Lineamientos de atención a situaciones fortuitas.

j) Control de versiones de la política (fecha, participantes, control de cambios).

k) Periodicidad de revisión de la política.

54. Documentación que describa la gestión de cambios en los sistemas relacionados con el monedero electrónico de vales de despensa, la cual debe contener lo siguiente:

a) Protocolo de control de cambios.

b) Formatos utilizados para el control de cambios.

c) Esquema de autorización de control de cambios.

d) Pruebas de los cambios en ambientes de desarrollo, pruebas y producción (operación).

e) Documentación de resultados de pruebas mencionadas en el inciso anterior.

f) Pruebas después de la liberación del cambio.

g) Documentación de resultados de pruebas mencionadas en el inciso anterior.

h) Registro de control de versiones de los desarrollos.

i) Resguardo de repositorios de versiones de desarrollos.

55. Política de relaciones con proveedores, la cual debe contener lo siguiente:

a) Definición de relaciones con proveedores de la persona moral.

b) Lineamientos para definir alcance y objetivo de los acuerdos con proveedores.

c) Lineamientos para definir las condiciones de entrega de servicio de los proveedores.

d) Lineamientos para autorizar el acceso a la información de contribuyentes a los proveedores.

e) Controles de seguridad para los servicios.

f) Inclusión de cláusula de auditoría para contratación de servicios con proveedores.

g) Lineamientos para realizar cambios en las condiciones de entrega de servicios.

h) Penalizaciones por incumplimiento de lo establecido en la política.

i) Lineamientos de atención a situaciones fortuitas.

j) Control de versiones de la política (fecha, participantes y control de cambios).

k) Periodicidad de revisión de la política.

56. Procedimiento de atención a incidentes que afecten la confidencialidad, integridad o disponibilidad de la información de los contribuyentes, el cual debe contener lo siguiente:

a) Roles y responsabilidades.

b) Clasificación de incidentes.

c) Documentación de incidentes.

d) Recolección de evidencia del incidente.

e) Alimentación de base de conocimientos.

f) Tabla de escalamiento.

g) Tiempos de respuesta.

h) Lineamientos para remediación de incidentes.

57. Documentación que describa los esquemas de alta disponibilidad que la persona moral implementa para las actividades relacionadas con el monedero electrónico de vales de despensa.

58. Documentación que describa los planes de continuidad de la persona moral, la cual deben contener lo siguiente:

a) Determinación de escenarios que pongan en riesgo la continuidad del negocio.

b) Roles y responsabilidades para los planes.

c) Protocolos de respuesta ante ocurrencia de los escenarios descritos en el inciso a).

d) Documentación de resultados de la ejecución de los planes.

e) Diseño de pruebas de los planes.

f) Acondicionamiento para realizar pruebas de los planes.

g) Documentación de resultados de pruebas de los planes.

h) Adecuaciones a los planes.

i) Revisión periódica de los planes.

59. Documentación que describa los planes de recuperación de desastres de la persona moral, la cual debe contener lo siguiente:

a) Determinación de escenarios que la persona moral determine como desastre.

b) Roles y responsabilidades para los planes.

c) Protocolos de respuesta ante ocurrencia de los escenarios descritos en el inciso a).

d) Documentación de resultados de la ejecución de los planes.

e) Diseño de pruebas de los planes.

f) Acondicionamiento para realizar pruebas de los planes.

g) Documentación de resultados de pruebas de los planes.

h) Adecuaciones a los planes.

i) Revisión periódica de los planes.

60. Documentación donde se defina un calendario de verificaciones independientes de seguridad de la información. El término independiente se refiere a que debe llevarse a cabo por personal que no haya participado en el diseño o implementación de los controles o que pertenezca a las áreas evaluadas, el personal puede ser interno o externo.

61. Ejemplar del monedero electrónico de vales de despensa, el cual debe incluir lo siguiente:

a) Nombre comercial del monedero electrónico.

b) Denominación social del emisor.

c) Identificador del monedero.

d) Número telefónico de atención al usuario /cliente.

62. Información del monedero electrónico de vales de despensa, la cual debe incluir lo siguiente:

a) Tecnología implementada en el ejemplar.

b) Almacenamiento seguro de datos en el ejemplar.

c) Especificaciones de la tecnología del ejemplar.

63. Realización de pruebas al ejemplar, las cuales deben contemplar lo siguiente:

a) Verificación de protocolo de autenticación del beneficiario.

b) Intento de transacción con el monedero electrónico.

c) Verificación de condiciones de bloqueo del monedero.

d) Intento de transacción con el monedero electrónico.

e) Verificación de condiciones de desbloqueo del monedero.

f) Intento de transacción con el monedero electrónico con productos no autorizados.

NOTA: Las pruebas son enunciativas más no limitativas y se llevarán a cabo en sitio, el personal verificador puede realizar pruebas adicionales si lo considera necesario.

64. Documentación que describa la gestión de los procesos operativos relacionados con el monedero electrónico de vales de despensa, la cual debe incluir:

a) Comunicación del protocolo de autenticación a beneficiarios y uso del monedero electrónico.

b) Protocolos de notificación a clientes y beneficiarios en caso de existir cambios en el protocolo de autenticación.

c) Capacitación respecto a la administración de monederos de vales de despensa por parte de los clientes.

d) Entrega la información de autenticación a clientes y beneficiarios, aceptación y resguardo de la información por parte de clientes y beneficiarios.

e) Protocolos para atención a clientes y beneficiarios, escalamiento de solicitudes y autorizaciones; debe incluir el protocolo para comunicar estos protocolos a clientes y beneficiarios.

f) Inhabilitación de monederos electrónicos de vales de despensa o beneficiarios.

g) Inhabilitación de acceso a los sistemas a clientes y beneficiarios.

h) Cambios en los datos de clientes y beneficiarios.

Nota: La documentación señalada en los numerales 1, 2, 3, 8, 9, 10, 13, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 40, 41, 42, 44, 45, 48, 49, 50, 53, 54, 55, 56, 57, 58, 59, 60 y 64 deberá de encontrarse firmada y rubricada por el representante legal o apoderado legal de la persona moral.

Atentamente.

Ciudad de México, a 15 de diciembre de 2023.- En suplencia por ausencia del Jefe del Servicio de Administración Tributaria, con fundamento en el artículo 4, primer párrafo del Reglamento Interior del Servicio de Administración Tributaria, firma el Administrador General Jurídico, Lic. **Ricardo Carrasco Varona**.- Rúbrica.