CAMINOS Y PUENTES FEDERALES DE INGRESOS Y SERVICIOS CONEXOS

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

NOVIEMBRE 2018

SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ÍNDICE

INTRODUCCIÓN

Las presentes directrices se establecen en apego al "ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias", mismo que tiene por objeto dictar lineamientos de observancia obligatoria en la Administración Pública Federal. Estas directrices forman parte de la base para establecer el Sistema de Gestión de Seguridad de la Información (SGSI) en CAPUFE, con el fin de proteger los datos y activos de información que soportan su operación, asegurar el cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), reducir los riesgos por el uso de las Tecnologías de la Información y Comunicaciones (TIC), así como para conformar el Modelo de Gobierno de Seguridad de la Información en Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE).

Dichas directrices están alineadas con los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI indicados en los estándares nacional NMX-I-27001-NYCE-2015 e internacional ISO/IEC 27001:2013.

OBJETIVO

Establecer la base normativa que soporte la implementación del Sistema de Gestión de Seguridad de la Información para contribuir al cumplimiento de leyes y regulaciones aplicables en materia de seguridad de la información, reducir los riesgos e impactos operativos, financieros, de imagen, de reputación, fortalecer la eficacia y eficiencia de los procesos de CAPUFE, así como reducir el número de observaciones resultado de auditorías tanto internas como externas.

ALCANCE

Las directrices aquí contenidas aplican a todos los servidores públicos de CAPUFE y externos, así como a la gestión, operación, información y activos de información que soportan los procesos sustantivos y adjetivos de CAPUFE.

FUNDAMENTO LEGAL

- Constitución Política de los Estados Unidos Mexicanos.
  D.O.F. 05-02-1917 y sus últimas reformas.

- Ley Federal de Transparencia y Acceso a la Información Pública.
  D.O.F. 09-05-2016 y sus últimas reformas.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
  D.O.F. 26-01-2017 y sus últimas reformas.

- Ley General de Responsabilidades Administrativas.
  D.O.F. 18-08-2016 y sus últimas reformas.

- Ley General de Transparencia y Acceso a la Información Pública.
  D.O.F. 04-05-2015 y sus últimas reformas.

- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
  D.O.F. 11-06-2003 y sus últimas reformas.

- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
  D.O.F. 21-12-2011 y sus últimas reformas.

- Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.
  D.O.F. 08-05-2014 y sus últimas reformas.

- Acuerdo mediante el cual se aprueban los lineamientos generales de protección de datos personales para el sector público.
  D.O.F. 19-12-2017 y sus últimas reformas.

- Lineamientos de Protección de Datos Personales.
  D.O.F. 30-09-2005 y sus últimas reformas.

- Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos.
  D.O.F. 22-07-2011 y sus últimas reformas.

DEFINICIONES

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para el Organismo, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Amenaza: Cualquier posible acto que pueda causar algún tipo de daño a los activos de información de CAPUFE.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Aplicativo: El software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de CAPUFE.

CAPUFE: Caminos y Puentes Federales de Ingresos y Servicios Conexos.

Centro: El Centro de Investigación y Seguridad Nacional, órgano desconcentrado de la Secretaría de Gobernación.

Compilador: Programa de cómputo que traduce un programa escrito en un lenguaje de programación a lenguaje máquina.

Confidencialidad: La característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.

Control: Mecanismo automatizado o manual utilizado para proteger los datos y activos de información, garantizando su confidencialidad, integridad y disponibilidad.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Dueño del activo de información: Servidor público de CAPUFE con nivel mínimo de Gerente, responsable de implementar y operar los controles que garantizan la confidencialidad, integridad y disponibilidad de los activos de información a su cargo.

Dueño de la información: Servidor público de CAPUFE con nivel mínimo de Gerente. Responsable de implementar y operar los controles que garantizan la confidencialidad, integridad y disponibilidad de la información a su cargo.

ERISC: Equipo de respuesta a incidentes de seguridad en TIC en la Institución.

Externo: Persona física o moral que presta algún servicio contractual a CAPUFE y que hace uso de información y/o cuenta con acceso a tecnologías de información y telecomunicaciones propiedad de CAPUFE.

GESI: Grupo estratégico de seguridad de la información. Integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo estratégico de seguridad de la información.

GTDTIC: Grupo de trabajo para la dirección de TIC, integrado por servidores públicos con nivel mínimo de Director de Área.

Impacto: El grado de los daños resultado de la materialización de un riesgo en un activo de información.

Información: Conjunto de datos que soportan el funcionamiento, procesos y toma de decisiones.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso y de la infraestructura tecnológica.

ISO/IEC 27001:2013: ISO 27001, Estándar internacional sobre los requerimientos de sistemas de gestión de seguridad de la información.

Lenguaje de programación: Es un conjunto de símbolos y reglas de sintaxis, el cual es interpretado por el lenguaje máquina para que los equipos de cómputo realicen tareas o procesos.

Lenguaje máquina: Sistema de códigos interpretados por microcircuitos o el procesador de una computadora para determinar las acciones que realizará.

MAAGTICSI: Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información.

NMX-I-27001-NYCE-2015: Norma mexicana sobre los requerimientos de sistemas de gestión de seguridad de la información.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de CAPUFE.

Roll back: Regreso a su estado original antes de realizar cambios en algún componente, servicio o control.

RSII: Responsable de la Seguridad de la Información en la Institución, es el Director de Administración y Finanzas, responsable del proceso de Administración de Seguridad de la Información (ASI) del MAAGTICSI.

Script: Bloque de instrucciones del sistema operativo de la computadora, que se ejecutan secuencialmente para completar una tarea.

Seguridad de la información: La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la responsabilidad, autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

SGSI: El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de procesos y controles, define las guías para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Sistema de información: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Software: Instrucciones, rutinas y programas elaborados en lenguajes de programación, para realizar una tarea específica.

Software de código abierto: También conocido como software libre. Es el software cuya licencia asegura que el código pueda ser modificado y mejorado por cualquier persona o grupo de personas con las habilidades correctas, debido a que el conocimiento es de dominio público.

STI: Subdirección de Tecnologías de Información.

TIC: Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Unidad: La Unidad de Gobierno Digital de la SFP.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC, aplicativos y sistemas de información de CAPUFE.

UTIC: La unidad administrativa en CAPUFE responsable de proveer de infraestructura y servicios de TIC a las demás áreas y unidades administrativas.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidad: La debilidad en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de información y a la infraestructura crítica.

LINEAMIENTOS GENERALES

Se debe definir un conjunto de directrices de seguridad de la información, publicadas y comunicadas a los servidores públicos y externos.

El Responsable de la Seguridad de la Información en la Institución (RSII) en CAPUFE, deberá definir una directriz general de seguridad de la información, la cual debe ser aprobada y comunicada por la Dirección General con el enfoque de CAPUFE para gestionar los objetivos de seguridad de la información.

La directriz general de seguridad de la información debe contener lo siguiente:

a) La definición de seguridad de la información, objetivos y principios para guiar todas las actividades relativas a seguridad de información.

b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información a los roles definidos.

c) Los procedimientos para el manejo de desviaciones y excepciones.

La directriz general de seguridad de la información debe ser apoyada por directrices sobre temas específicos, los cuales exigen la aplicación de los controles de seguridad de la información.

El conjunto de directrices de seguridad de la información debe atender los requerimientos de:

a) La estrategia de negocio.

b) Legislación, reglamentos, contratos y demás normatividad aplicable.

c) El entorno actual y futuro de amenazas a la seguridad de la información.

Los aspectos que cubren las directrices específicas son:

a) Protección de datos personales.

b) Cumplimiento de leyes y regulaciones.

c) Control de acceso a la información.

d) Desarrollo de sistemas.

DUEÑO DE LAS DIRECTRICES

El dueño de las directrices es el Responsable de la Seguridad de la Información.

REVISIÓN DE LAS DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

El RSII con apoyo del GESI deberá revisar una vez al año las directrices de seguridad de la información, actualizarlas y comunicarlas a los servidores públicos y externos.

REVISIÓN DEL CUMPLIMIENTO

La aplicación y observancia de éstas directrices es de carácter obligatorio, la revisión de su cumplimiento se hará bajo los términos y la frecuencia establecidos en el MAAGTICSI pudiendo ser, auditorías programadas, auditorías de seguimiento, revisiones particulares o cualquier otro medio autorizado. Las revisiones serán realizadas por el RSII y el GESI; así como por el Órgano Interno de Control, dependencias y entidades federales y/o consultores externos.

INCUMPLIMIENTO DE LAS DIRECTRICES

Las presentes directrices forman parte del SGSI de CAPUFE, con base en la actividad ASI 3, Diseño del SGSI Factor Crítico número 13 del proceso Administración de la Seguridad de la Información del MAAGTICSI, el RSII deberá hacer del conocimiento del OIC en CAPUFE y/o cuando corresponda, de las autoridades que resulten competentes, el incumplimiento del SGSI a efecto de que se determinen las responsabilidades que procedan en términos de los ordenamientos legales aplicables.

HOMOLOGACIÓN Y ESTANDARIZACIÓN

La supervisión de la implementación de los controles de seguridad para proteger la información y activos de información, estarán a cargo de Subdirección de Tecnologías de Información, y deben estar homologados evitando la existencia de varios controles para un mismo fin; deben estar enfocados a la efectividad y eficiencia en el uso de recursos (humanos, financieros y tecnológicos), y en la medida de lo posible deben estar automatizados evitando el uso de controles manuales.

Dichos controles deben documentarse, mantenerse, comunicarse e integrarse en el repositorio de documentos que la STI establezca para tal fin y debe ser accesible para quien lo necesite; deberán estar alineados con los estándares de seguridad de la información indicados en las leyes y regulaciones correspondientes, y en su caso, en los establecidos por el GESI.

DIRECTRICES

1. DIRECTRIZ GENERAL DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Proteger los datos y activos de información que soportan la operación de CAPUFE, cumplir con leyes y regulaciones, así como implementar un Sistema de Gestión de Seguridad de la Información.

1.1. Los datos y activos de información que soportan los distintos procesos de CAPUFE deben estar protegidos a fin de asegurar su confidencialidad, integridad y disponibilidad, para garantizar los derechos de los usuarios, las expectativas de asociados y entidades regulatorias; así como el logro de objetivos y estrategias de CAPUFE.

1.2. Se debe establecer el SGSI en cumplimiento con las leyes y regulaciones que así lo indican, reforzado con los requerimientos establecidos en el estándar nacional NMX-I-27001-NYCE-2015 y en el estándar internacional ISO/IEC 27001:2013, con el fin de reducir impactos adversos a CAPUFE por el uso de información y de las tecnologías de la información y comunicaciones.

1.3. Es responsabilidad de todos los servidores públicos y externos, en el ámbito de su competencia, cumplir con ésta directriz y las específicas para proteger la información que utilizan en el día a día.

1.4. Responsabilidades:

Director General

- Designar al responsable de la seguridad de la información en CAPUFE, quien deberá tener nivel jerárquico mínimo de Director de Área o equivalente.

- Autorizar y comunicar la directriz general de seguridad de la información para conformar el Modelo de Gobierno de Seguridad de la Información en CAPUFE.

Grupo de Trabajo para la Dirección de TIC

- Apoyar la implementación, operación y mejora del SGSI como se indica en los procesos de gobernanza establecidos en el MAAGTICSI.

Responsable de la Seguridad de la Información en la Institución

- Establecer el grupo estratégico de seguridad de la información.
- Elaborar, y con apoyo del GESI, revisar y mantener las directrices de seguridad de la información.
- Proporcionar la directriz general de seguridad de la información al Director General para su autorización y comunicación.
- Estar a cargo del proceso de administración de la seguridad de la información del MAAGTICSI.

Grupo Estratégico de Seguridad de la Información

- Apoyar al RSII en la revisión y mantenimiento de las directrices de seguridad de la información.
- Constatar la implementación del SGSI en CAPUFE y revisarlo anualmente a fin de verificar su cumplimiento.

Servidores públicos de CAPUFE y Externos

- Cumplir con la directriz general y las específicas de seguridad de la información.

2. DIRECTRIZ DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES

OBJETIVO

Proteger los datos personales utilizados por CAPUFE, conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

2.1. Las actividades propias para garantizar la protección, gestión y tratamiento de datos personales deberán realizarse con base en las responsabilidades y lo establecido en:

a) La LGPDPPSO;

b) El acuerdo mediante el cual se aprueban los lineamientos generales de protección de datos personales para el sector público.

2.2. Los responsables y/o encargados establecidos en la LGPDPPSO deberán implementar los controles que garanticen los derechos ARCO, la confidencialidad, integridad, disponibilidad y protección de los datos personales utilizados por las áreas, procesos, actividades, servidores públicos y externos.

2.3. Se deberá privilegiar el uso de controles automatizados, evitando al máximo posible el uso de controles manuales, los cuales son una vulnerabilidad y pueden comprometer la protección de los datos personales, los derechos ARCO y el cumplimiento de la LGPDPPSO.

2.4. Los externos que proporcionen bienes o servicios a CAPUFE deberán implementar controles que garanticen la protección de datos personales y el cumplimiento de la LGPDPPSO o de la LFPDPPP según aplique; lo anterior debe quedar establecido en el contrato o convenio correspondiente.

2.5. Los servidores públicos de CAPUFE que contraten o adquieran bienes o servicios con externos son responsables que éstos tengan implementados los controles que garanticen la protección de datos personales y el cumplimiento de la LGPDPPSO o de la LFPDPPP según corresponda.

2.6. EL RSII y el GESI deberán establecer un programa para verificar anualmente la eficacia de los controles implementados por los servidores públicos de CAPUFE y externos para proteger los datos personales y el cumplimiento de la LGPDPPSO o de la LFPDPPP según corresponda; identificando las brechas de seguridad, el impacto para CAPUFE y el tratamiento de los riesgos relacionados.

3. DIRECTRIZ DE CONTROL DE ACCESO

OBJETIVO

Asegurar que el acceso a la información está protegido, controlado y autorizado únicamente a personal que por razones de trabajo lo necesite, garantizando así su confidencialidad y calidad.

3.1. Se debe determinar un Dueño de la información (física o electrónica) quien será responsable de establecer controles, reglas, derechos, perfiles de usuario y autorizar o negar el acceso a la información a su cargo.

3.2. Se debe identificar a los Dueños de los activos de información (aplicativos, infraestructura, hardware y software) donde se recibe, procesa, comunica, transmite y almacena la información; el Dueño del (los) activo(s) será responsable de establecer los controles, reglas, derechos, perfiles de usuario y asignar o negar el acceso al(los) activo(s) a su cargo, previa autorización del Dueño de la información.

3.3. Los derechos de acceso deben asignarse bajo la premisa del “menor privilegio”.

3.4. Los mecanismos para controlar el acceso a la información deben ser físicos, técnicos y administrativos, con base en la criticidad de la información y del activo de información; la criticidad se puede determinar realizando la actividad ASI 6, integrar al SGSI controles mínimos de Seguridad de la Información del MAAGTICSI.

3.5. El acceso a la información deber ser ágil y rápido, mediante el uso de controles automatizados, evitando el uso de controles manuales. Se deben implementar controles complejos para acceder a información y activos con criticidad baja. Se deben implementar controles fortalecidos para acceder a información y activos con criticidad alta.

3.6. Para implementar controles de acceso se debe considerar, más no limitarse a lo siguiente:

a) Leyes, regulaciones y compromisos que apliquen.

b) Controles físicos y lógicos.

c) Solicitud de acceso al activo de información (sistema, aplicativo, servidor, red).

d) Perfiles de usuario.

e) Derechos de acceso de usuarios privilegiados (administrador de sistema operativo, administrador de base de datos).

f) Segregación de funciones.

g) Alta, baja y cambios de usuario.

h) Métodos de identificación, autenticación (simple o multifactor) y autorización.

i) Métodos de cifrado.

j) Revisión periódica de derechos de acceso.

k) Evaluación periódica de los controles.

l) Acceso remoto.

m) Bitácoras de acceso (logs).

4. DIRECTRIZ DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS

OBJETIVO

Garantizar la confidencialidad, integridad y disponibilidad de la información en los sistemas que soportan la operación de CAPUFE.

4.1. Los dueños de la información y de los activos de información que integran los sistemas, con el apoyo y supervisión de la Subdirección de Tecnologías de Información, deben implementar controles que garanticen la confidencialidad, integridad y disponibilidad de la información durante la adquisición y desarrollo de sistemas.

4.2. La identificación e implementación de los controles debe realizarse durante todas las etapas del ciclo de vida de los sistemas (análisis, diseño, desarrollo, pruebas e implementación).

4.3. Los controles deben ser probados, corregidos y verificados antes de implementar, o liberar a producción un sistema de información.

4.4. Los sistemas podrán ser implementados cuando los usuarios hayan aprobado su funcionalidad, usabilidad y calidad de la información, y el Dueño de la información autorice su liberación a producción.

4.5. Al implementar el sistema, los dueños de los activos de información que lo integran deberán establecer un periodo de monitoreo y realizar las acciones necesarias para asegurar la funcionalidad, usabilidad, calidad, confidencialidad, integridad y disponibilidad de la información, así como los requerimientos establecidos en los acuerdos de nivel de servicio.

4.6. Los sistemas deben estar documentados y actualizados, conteniendo al menos, lo siguiente:

a) Descripción y objetivo del sistema.

b) Nombre y puesto del Dueño de la información.

c) Nombre y puesto del Director o Gerente responsable del desarrollo y soporte del sistema.

d) Nombre de las Unidades Administrativas que utilizan el sistema.

e) Cantidad de usuarios que utilizan el sistema, tanto empleados de CAPUFE como externos.

f) Leyes y regulaciones que debe cumplir el sistema.

g) Activos de información, hardware y software que lo integran, su descripción y versión.

h) Diagrama de red claro y entendible, identificando redes LAN y WAN, activos de información e interconexión, protocolo de comunicación, cifrado, nombre, función y dirección IP de los activos.

i) Diagrama de flujo de datos claro y entendible, que describa la información y su flujo de punto a punto.

j) Diagrama de negocio, que describa el flujo de la información y las operaciones realizadas con ella en cada etapa del proceso sustantivo o adjetivo.

4.7. Cualquier modificación, actualización y mejora a los sistemas, deberá considerar los controles de seguridad que correspondan, registrarse en el control de cambios, planearse, probarse y autorizarse por el Dueño de la información antes de implementarse.

4.8. Los Dueños de los activos de información, deben programar y concretar calendarios de mantenimiento a los activos a su cargo, para garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas.

4.9. Periódicamente, se deberán analizar, evaluar y cerrar los riesgos de los sistemas.

4.10. Se deberán programar y concretar evaluaciones (auditorias, análisis de vulnerabilidades, pruebas de penetración) internas y externas a la seguridad de los sistemas, dichas evaluaciones deberán ser realizadas por entidades independientes del área a la que pertenece el Dueño de la

información y de la Subdirección de Tecnologías de Información; como resultado de las evaluaciones se deberán identificar y cerrar las brechas de seguridad.

4.11. Se deberá contar con planes de continuidad de negocio y de recuperación en caso de desastre, documentados, probados, eficaces y eficientes, para minimizar los impactos a CAPUFE provocados por fallas o indisponibilidad en el sistema, eventos naturales, humanos o técnicos.

4.12. Durante el proceso de adquisición, compra o arrendamiento de sistemas se debe considerar al menos lo siguiente:

a) El cumplimiento de las leyes y regulaciones que aplican.

b) Responsabilidades claras y puntuales del comprador, vendedor y terceras partes.

c) Garantía del producto.

d) Los requerimientos de seguridad de la información.

e) Documentación actualizada del sistema.

f) Pruebas, calidad, aseguramiento y puesta a punto del sistema.

g) Verificación de los controles de seguridad implementados para garantizar la confidencialidad, integridad y disponibilidad de la información y el sistema.

h) Plan de continuidad de negocio y plan de recuperación ante desastres del sistema.

i) Penalizaciones.

j) Acuerdos de Niveles de Servicio.

k) El derecho de CAPUFE a evaluar la seguridad del sistema mediante auditorias, análisis de vulnerabilidades y pruebas de penetración, o que contrate a un tercero para que lo realice.

l) El cierre de brechas de seguridad a la brevedad.