Reporte de hallazgos

Hallazgo No.: 1

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos** — *Valor Económico*
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades (Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

La Subdirección de Desarrollo de Sistemas Informáticos no cuenta con políticas y procedimientos de administración de seguridad formalizadas, aprobadas y comunicadas al personal, las cuales corresponden a: análisis de vulnerabilidades, altas, bajas y cambios de usuarios en los sistemas, monitoreo de accesos, atención a incidencias de seguridad, creación y uso contraseñas, administración de dispositivos de red, administración de base de datos y redes.

Fundamento específico legal y/o técnico infringido

Anexo único del "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información" II.C. PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI).

Objetivo General: Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.

Objetivos específicos:
1. Establecer, operar y mantener un modelo de gobierno de seguridad de la información.
5. Establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.
7. Fomentar una cultura de seguridad de la información en la Institución.

Reglas del proceso:
5. El responsable de este proceso deberá establecer el equipo de respuesta a incidentes de seguridad de Tecnologías de la Información y Comunicaciones (TIC), equipo de respuesta a incidentes de seguridad (ERISC) y definir los roles y responsabilidades de sus integrantes, así como asegurarse de que éstos conozcan las reglas de operación del mismo y la guía técnica de atención a incidentes.
9. El grupo estratégico de seguridad de la información deberá asegurarse de que se integren al Sistema de Gestión de la Seguridad de Información (SGSI), controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La documentación de políticas y procedimientos de seguridad de TI no fueron documentadas a causa de la carga operativa que lleva a cabo la Subdirección de Desarrollo de Sistemas Informáticos. Asimismo, los cambios estructurales que se presentaron recientemente en la entidad.

Efectos

Omisiones en la seguridad de la red, sistemas, servidores, bases de datos y equipos de cómputo, conllevando a que los usuarios de la entidad comprometan la confidencialidad, integridad y disponibilidad de la información.

Recomendaciones

Correctivas

Diseñar, documentar y formalizar políticas y procedimientos específicos para establecer las directrices complementadas con base en mejores prácticas y estándares internacionales en la materia que contemplen los siguientes aspectos: análisis de vulnerabilidades, altas, bajas y cambios de usuarios en los sistemas, monitoreo de accesos, atención a incidencias de seguridad, creación y uso contraseñas, administración de dispositivos de red, administración de base de datos y redes.

Preventivas

La Subdirección de Desarrollo de Sistemas Informáticos deberá indicar dentro de sus políticas y procedimientos de Seguridad de Tecnologías de Información (TI) que estas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que dichas políticas y procedimientos fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 2

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos** — *Valor Económico*
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

La Subdirección de Desarrollo de Sistemas Informáticos no realiza un monitoreo periódico de los accesos a la red, servidores, bases de datos y sistemas, por lo que no es posible identificar si los usuarios conectados corresponden a usuarios efectivamente autorizados.

Fundamento específico legal y/o técnico infringido

Anexo único del "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información"
III.C. PROCESO DE ADMINISTRACIÓN DE LA OPERACIÓN (AOP)
Objetivos Específicos:
1. Operar la infraestructura y servicios de Tecnologías de la Información y Comunicaciones (TIC), de manera que puedan resistir fallas, ataques deliberados o desastres y, se recuperen los servicios de TIC de manera ágil y segura.
2. Asegurar la estabilidad y continuidad de la operación de la infraestructura de TIC en la aplicación de cambios y la solución de problemas e Incidentes, la implementación de aplicativos de cómputo, soluciones tecnológicas y nuevos servicios de TIC.

AOP 3 Monitorear la infraestructura de TIC en operación.
Descripción: Monitorear en los diferentes dispositivos de la infraestructura y de los servicios de TIC, la ejecución de las tareas de la operación, con el propósito de identificar eventos para prevenir o solucionar fallas e incidentes.

Factores Críticos:
El responsable de este proceso deberá:
1. Revisar que se registre cualquier tarea ejecutada como parte de la operación, a efecto de contar con registros que permitan identificar la causa raíz de incidentes, así como confirmar la ejecución satisfactoria de las tareas de la operación.
2. Identificar los eventos que se presenten en la operación de la infraestructura y de los servicios de TIC.
3. Dar seguimiento a los eventos e incidentes que se presenten en la operación y registrar aquellos que aporten experiencia y conocimiento, con el propósito de apoyar el análisis para la solución de problemas o la prevención de incidentes, así como la mejora de las tareas de operación en la Institución y estar en posibilidad de transmitirlas a otras Instituciones.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos no ha definido adecuadamente las funciones y responsabilidades del personal que deberá llevar a cabo los monitoreos de acceso a la red, servidores, base de datos y sistemas de la entidad.

Efectos

El no realizar un monitoreo de los usuarios que acceden a la red, servidores, bases de datos y sistemas; podría suscitarse que usuarios no autorizados puedan estar conectados y provocar daños irreversibles a la información registrada en las bases de datos o bien, interrumpir la continuidad de las operaciones de la Institución.

Recomendaciones

Correctivas

Establecer mecanismos que permitan realizar periódicamente monitoreos de accesos a la red, servidores, bases de datos y sistemas, con el objetivo de identificar usuarios no autorizados o actividades inusuales. Asimismo, generar el soporte documental de las acciones realizadas derivado del control.

Preventivas

Formalizar las actividades del monitoreo de acceso a la red, servidores, base de datos y sistemas de la entidad, a través de políticas y procedimientos, los cuales deben ser revisadas o actualizadas al menos una vez al año, con la finalidad de corroborar que dichas políticas y procedimientos fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 3

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	Subdirección de Desarrollo de Sistemas Informáticos
Valor Económico	
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades (Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

La Subdirección de Desarrollo de Sistemas Informáticos no realiza un análisis de vulnerabilidades de Tecnología de información (TI), debido a que no nos fue proporcionado los reportes de análisis de vulnerabilidades TI, mismos que de acuerdo al entendimiento son realizados por el proveedor Axtel. Asimismo, no identificamos evidencia de los planes de acción que se llevan a cabo para la corrección de las alertas identificadas en el Firewall, lo cual genera un riesgo en los niveles de seguridad de la red.

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).

Capítulo III
Artículo 18.- Las Instituciones, en lo referente al software de capa intermedia, deberán observar lo siguiente:
I. Estandarizar, al interior, el software de capa intermedia a utilizar;
II. Establecer servidores de presentación para los diversos aplicativos de cómputo existentes, y
III. Ejecutar rutinas de análisis de vulnerabilidades acordes con el software de capa intermedia que se establezca, a fin de disminuir el riesgo por falta de disponibilidad.

Capítulo IV
Sección I
Artículo 26.- Las Instituciones conforme a lo indicado en el MAAGTICSI, previo al inicio de la puesta en operación de un aplicativo de cómputo, realizarán el análisis de vulnerabilidades correspondiente, el cual preferentemente será realizado por un tercero, distinto a quién desarrolló el aplicativo. El resultado del análisis deberá preservarse para efectos de auditoría.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos no ha definido las funciones y responsabilidades del personal que llevara a cabo los análisis de vulnerabilidades de TI.

Efectos

La seguridad de la red de la entidad podría comprometerse a consecuencia de alguna vulnerabilidad no atendida, provocando que se afecte la disponibilidad e integridad de la información almacenada o procesada en los recursos tecnológicos de la entidad.

Recomendaciones

Correctivas

Establecer y realizar un análisis mensual de las vulnerabilidades de TI en los servidores. bases de datos, antivirus, firewall y bitácoras de auditoría del mismo. Asimismo, la Subdirección de Desarrollo de Sistemas Informáticos tendrá que documentar a través de un reporte las vulnerabilidades identificadas y planes de acción para la atención de las mismas, en apego a las políticas y procedimientos de seguridad de TI.

Preventivas

La Subdirección de Desarrollo de Sistemas Informáticos debe formalizar los análisis de vulnerabilidad de TI en una política y procedimiento, considerando un periodo mensual y los responsables para dichas actividades. Asimismo, la Subdirección de Desarrollo de Sistemas Informáticos deberá indicar dentro de sus políticas y procedimientos de Seguridad de Tecnologías de Información (TI) que estas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que dichas políticas y procedimientos fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 4

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos** — *Valor Económico*
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

El directorio activo del servidor LICONSA.CENTRAL, no tiene configurado los parámetros de seguridad de las contraseñas, los cuales se listan a continuación:

1. Cambio de contraseñas periódico.
2. Histórico de contraseñas establecido en 1.
3. Contraseñas complejas.
4. Bloqueo de cuentas por acceso de intentos fallidos.

Fundamento específico legal y/o técnico infringido

Anexo único del "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información"

ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.
Descripción: Definir los controles mínimos de seguridad de la información e integrarlos al SGSI, para su implementación a través de los diversos procesos de la UTIC y de aquellos procesos de la Institución que contengan activos de TIC y TO, activos de información e infraestructuras de información esenciales y, en su caso, críticas.

Factores Críticos:
El grupo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:

h) Asignación de usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.

AOP 1 Establecer el mecanismo de operación y mantenimiento de los sistemas, aplicaciones, infraestructura y servicios de TIC.
Descripción: Establecer las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC, así como el mantenimiento a los componentes de infraestructura.

5.- Implementar, en la realización de las tareas de instalación y mantenimiento de la infraestructura tecnológica, los controles de seguridad del SGSI, que consideren cuando menos:

e.- Modificar, en los componentes instalados, las contraseñas originales, configuraciones y parámetros que puedan afectar la seguridad y suprimir los accesos temporales utilizados en la instalación.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos no ha definido cuales son los parámetros de seguridad de contraseña (cambio de contraseñas periódico, histórico de contraseñas establecido, contraseñas complejas y bloqueo de cuentas por acceso de intentos fallidos) que serán aplicables a la operación de la entidad.

Efectos

El no tener configurado los parámetros de seguridad, tales como: cambios de contraseñas, contraseñas complejas, histórico de contraseñas y bloqueo por intentos fallidos; provocaría que los ataques de usuarios maliciosos se realicen con éxito y afectar la integridad y disponibilidad de la información.

Recomendaciones

Correctivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe evaluar la factibilidad en la configuración de los parámetros de seguridad de contraseña tomando en consideración lo siguiente:

1. Cambio de contraseñas periódico cada 60 o 90 días.
2. Histórico de contraseñas contemplando al menos 5 contraseñas utilizadas.
3. Contraseñas complejas considerando una longitud mínima de 8 (mayúsculas, minúsculas, números y caracteres especiales).
4. Bloqueo de cuentas por accesos fallidos de 3 a 5.

Preventivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe formalizar los parámetros de seguridad de contraseñas en una política de seguridad de TI y verificar el cumplimiento de la misma. Asimismo, la Subdirección de Desarrollo de Sistemas Informáticos deberá indicar dentro de sus políticas y procedimientos de Seguridad de Tecnologías de Información (TI) que estas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que dichas políticas y procedimientos fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 5

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos**
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Valor Económico

Clasificación del hallazgo

Bajo Riesgo (BR): X | Mediano Riesgo (MR): | Alto Riesgo (AR):

Hallazgo recurrente

Ejercicio de origen | SI | NO X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI | NO X

El hallazgo esta atendido

SI | Fecha de solventación: | NO X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

Se identificó un número elevado de cuentas con perfil de Administrador, por lo cual desconocemos si cada cuenta asignada requiere dichos privilegios de acceso al servidor LICONSA.CENTRAL, mismas que se detallan: LICONSA\Administradores de organización, Administrador, sccm_admin, admingms, jcuellar, soportegms, LICONSA\Administrador, LICONSA\Admins. del dominio, directorio, amc, ITAdmin, admin, admin2, Liconsa, producción, bss, lolazagasti, admin.bss, bss.administrator, LICONSA\sccm_admin, LICONSA\admingms, LICONSA\soportegms, LICONSA\admingmn, LICONSA\directorio, LICONSA\ITAdmin, LICONSA\aesanchez, LICONSA\yherrejonm, LICONSA\ASRASCON4$, LICONSA\ASRASCON2$, LICONSA\dvega, LICONSA\admin, LICONSA\RSANCHEZV$, LICONSA\lharguello, LICONSA\AESANCHEZP$, LICONSA\admin2, LICONSA\LZSANCHEZ$, LICONSA\lvillag, LICONSA\asrascon, LICONSA\dperez, LICONSA\ASRASCON$, LICONSA\mcastilloc, LICONSA\janunezv, LICONSA\LHARGUELLO$, LICONSA\rpat, LICONSA\ASRASCON5$, LICONSA\aesanchezp, LICONSA\ASRASCON3$.

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).
Artículo 13.- En el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente:

VII. Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información que se definan atendiendo a lo previsto en el MAAGTICSI,

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos no tiene delimitado la asignación de cuentas de acceso con perfil de "Administrador" en el servidor LICONSA.CENTRAL.

Efectos

El tener un número elevado de cuentas con perfil de administrador en el servidor central de la Entidad; podría generar que usuarios con conocimientos informáticos avanzados puedan realizar un ataque de enumeración de cuentas, pudiendo generar impactos en la confidencialidad, integridad y disponibilidad de la información.

Recomendaciones

Correctivas

La Subdirección de Desarrollo de Sistemas Informáticos, deberá realizar un análisis de los usuarios que tienen los perfiles de administrador, correspondientes a: LICONSA\Administradores de organización, Administrador, sccm_admin, admingms, jcuellar, soportegms, LICONSA\Administrador, LICONSA\Admins. del dominio, Administrador, soportegms, sccm_admin, admingms, jcuellar, directorio, amc, ITAdmin, admin, admin2, Liconsa, producción, bss, lolazagasti, admin.bss, bss.administrator, LICONSA\sccm_admin, LICONSA\admingms, LICONSA\soportegms, LICONSA\admingmn, LICONSA\directorio, LICONSA\ITAdmin, LICONSA\aesanchez, LICONSA\yherrejonm, LICONSA\ASRASCON4$, LICONSA\ASRASCON2$, LICONSA\dvega, LICONSA\admin, LICONSA\RSANCHEZV$, LICONSA\lharguello, LICONSA\AESANCHEZP$, LICONSA\admin2, LICONSA\LZSANCHEZ$, LICONSA\lvillag, LICONSA\asrascon, LICONSA\dperez, LICONSA\ASRASCON$, LICONSA\mcastilloc, LICONSA\janunezv, LICONSA\LHARGUELLO$, LICONSA\rpat, LICONSA\ASRASCON5$, LICONSA\aesanchezp, LICONSA\ASRASCON3$, evaluando si dichos permisos corresponden a la función y naturaleza de la responsabilidad de cada usuario, con la finalidad de restringir los roles de Administrador. Asimismo, omitir el uso de cuentas genéricas.

Preventivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe generar cartas responsivas para la asignación y autorización de los usuarios con perfil de Administrador, las cuales tendrán que contar con las firmas de los usuarios responsables que daran uso a dicha cuenta, así como el personal de la Subdirección de Desarrollo y Sistemas Informáticos que está otorgando el acceso.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna. de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 6

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos**
	Valor Económico
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

La Subdirección de Desarrollo de Sistemas Informáticos no tiene documentado los roles y perfiles de acceso de los siguientes sistemas:

1. SICOP-CONAC (Sistema de Control Presupuestal, Cuentas por Pagar y Bancos).
2. e-CONTABI (Sistema de Contabilidad General).
3. SICOPA (Sistema de Control de Padrón de Beneficiarios).
4. SIIBOP (Sistema Integral de Información Básica de la Operación de Planta).
5. SIVICOP (Sistema de Evaluación de Inventarios y Costo de Producción).

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).

Artículo 13.- En el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente:
VII. Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información que se definan atendiendo a lo previsto en el MAAGTICSI.

Anexo único del "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información"
II. PROCESOS DE ORGANIZACIÓN.
II.C Proceso de Administración de la Seguridad de la Información (ASI)
ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información
Factores Críticos:
El grupo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:
1. Definir los controles de seguridad necesarios para salvaguardar a los activos de TIC, los activos de información y las infraestructuras críticas de la Institución, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:
b) La designación de personal en las áreas relacionadas con el manejo, administración y gestión de los activos de información de la Institución, con apego a las disposiciones jurídicas aplicables y considerando los procedimientos que, en su caso, se tengan implementados en el área o unidad administrativa de que se trate.
g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien cuando por algún motivo el nivel de privilegios de acceso asignado cambie.
h) Los criterios de asignación de usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos no cuenta con la información de los usuarios que tienen acceso a los sistemas que se mencionan en la presente observación, debido a que las áreas administrativas y operativas de la Entidad no ha proporcionado dicha información para la documentación de los roles y perfiles de acceso por parte de la Subdirección de Desarrollo de Sistemas Informáticos.

Efectos

El no tener documentado y formalizado los perfiles de acceso de los sistemas de información críticos; podría generar conflictos de segregación de funciones, ya que el personal podría tener habilitados privilegios para modificar información o parámetros del sistema que no correspondan a sus funciones, afectando la confidencialidad, integridad y disponibilidad de la información.

Recomendaciones

Correctivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe solicitar la información a las áreas administrativas y operativas de los perfiles y roles de acceso de los usuarios que tienen acceso a los sistemas de información descritos en la observación, con la finalidad que la Subdirección de Desarrollo de Sistemas Informáticos documente y formalice las matrices de roles y perfiles de acceso de los sistemas de información (SICOP-CONAC, CONTABI, SICOPA, SIIBOP y SIVICOP).

Cabe mencionar que la autorización de las matrices de roles y perfiles de acceso de los sistemas SICOP-CONAC, CONTABI, SICOPA, SIIBOP y SIVICOP, deberán de contar con la autorización de los titulares y dueños de la información que se procesa en dichos sistemas, así como el visto bueno de la Subdirección de Desarrollo de Sistemas Informáticos.

Preventivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe realizar la revisión de los roles y perfiles de acceso de los usuarios que acceden a los sistemas SICOP-CONAC, CONTABI, SICOPA, SIIBOP y SIVICOP, con las áreas administrativas y operativas de la Entidad, lo anterior en apego a las políticas y procedimientos de seguridad de Tecnologías de Información, las cuales deberán indicar que estas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que dichas políticas y procedimientos fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 7

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos** — *Valor Económico*
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

Observamos que no se tiene documentado y formalizado una política y procedimiento para la generación de respaldos de información, por lo cual no se tiene definida una estructura que garantice que la información crítica sea respaldada correcta y oportunamente.

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).
Sección I
Artículo 27.- Las Instituciones mantendrán los componentes de software y de seguridad de los dominios tecnológicos actualizados para evitar vulnerabilidades, de acuerdo a lo que se establece en el MAAGTICSI, para lo cual implementarán, entre otros, elementos de seguridad de la información, los siguientes:
VII. Implementar medidas y procedimientos para el respaldo de información.

Anexo único del "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información"
II. PROCESOS DE ORGANIZACIÓN
II.A. PROCESO DE ADMINISTRACIÓN DE SERVICIOS (ADS).
Objetivo General:
Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de servicios de TIC que aporten beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución, con apego a la EDN y efectuar su instrumentación.
Objetivos Específicos:
1. Diseñar y mantener actualizada la arquitectura empresarial de los servicios de TIC y definir las especificaciones técnicas para satisfacer las necesidades actuales y proyectadas de la Institución, considerando que se deben incluir las definiciones de los niveles de seguridad, capacidad, disponibilidad y continuidad de la operación de TIC.
Reglas del proceso:
El Responsable del proceso Administración de Servicios (ADS) deberá asegurarse que el hardware y el software de recuperación utilizado en la aplicación del programa de continuidad sea funcional, para restablecer, probar y renovar los respaldos al menos semestralmente.
III.C. PROCESO DE ADMINISTRACIÓN DE LA OPERACIÓN (AOP).
Objetivo General: Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.
Objetivos Específicos:
Asegurar la estabilidad y continuidad de la operación de la infraestructura de TIC en la aplicación de cambios y la solución de problemas e Incidentes, la implementación de aplicativos de cómputo, soluciones tecnológicas y nuevos servicios de TIC.
Reglas del proceso:
Implementar, en la realización de las tareas de instalación y mantenimiento de la infraestructura tecnológica, los controles de seguridad del SGSI, que consideren cuando menos:
b. Efectuar el respaldo y protección de los datos almacenados en la infraestructura tecnológica, así como del software que se encuentre instalado.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo
N/A

Causas
La Subdirección de Desarrollo de Sistemas Informáticos, no tiene definido y formalizado una estructura de respaldos de información (diario, semanal, mensual y anual) de la Entidad.

Efectos
Omisiones de información crítica en los respaldos de información para la Entidad y establece una alta dependencia del personal que desempeña las actividades. Adicionalmente en caso de una contingencia o perdida de información ésta puede no estar disponible.

Recomendaciones
Correctivas
La Subdirección de Desarrollo de Sistemas Informáticos, debe diseñar, documentar y formalizar políticas y procedimientos específicos para realizar respaldos de información, con la finalidad de resguardar adecuadamente los activos lógicos de la entidad y asegurar la continuidad de las operaciones en caso de una contingencia.
Preventivas
La Subdirección de Desarrollo de Sistemas Informáticos, debe realizar una revisión de las políticas y procedimientos de respaldos de información para validar la vigencia y apego de las operaciones de la Entidad en temas de respaldos de información, las políticas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que dichas políticas y procedimientos fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes		
Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 8

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos**
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Valor Económico

Clasificación del hallazgo

Bajo Riesgo (BR):	X	Mediano Riesgo (MR):		Alto Riesgo (AR):	

Hallazgo recurrente

Ejercicio de origen		SI		NO	X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI		NO	X

El hallazgo esta atendido

SI		Fecha de solventación:		NO	X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

Derivado del análisis de cuentas de usuarios y perfiles de acceso que se tienen habilitados en los sistemas críticos, se identificó:

1.- **eCONTABI**:
- A.-128 Usuarios no identificados en los listados de RRHH.
- B.- 14 Usuarios activos en el sistema con estatus de baja en los listados de RRHH.
- C.- 8 usuarios con posibles conflictos de segregación de funciones.
- D.- 3 usuarios con dos cuentas de acceso.

2.- **SICOPA**
- A.-384 Usuarios no identificados en los listados de RRHH.
- B.- 22 Usuarios activos en el sistema con estatus de baja en los listados de RRHH.
- C.- 14 usuarios con posibles conflictos de segregación de funciones.
- D.- 248 Usuarios que no tienen asignado un responsable.
- E.-16 Usuarios con más de 2 cuentas de acceso.
- F.- Una cuenta de acceso asignada a dos usuarios.

3.- **SIVICOP**
- A.- 2 Usuarios activos en el sistema con estatus de baja en los listados de RRHH.
- B.- 1 Usuario con dos cuentas de acceso.

4.- **SIIBOP**
- A.- 79 Usuarios no identificados en los listados de RRHH..
- B.- 56 Usuarios activos en el sistema con estatus de baja en los listados de RRHH.
- C.- 2 Usuarios con 2 cuentas de acceso.

5.- **SICOP-CONAC**
- A.- 140 Usuarios no identificados en los listados de RRHH.
- B.- 84 Usuarios activos en el sistema con estatus de baja en los listados de RRHH.
- C.- 17 Usuarios con más de 2 cuentas de acceso.

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).
Artículo 13.- En el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente:
VII. Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información que se definan atendiendo a lo previsto en el MAAGTICSI.

Anexo único del "Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información".
II.B. PROCESO DE ADMINISTRACIÓN DE LA CONFIGURACIÓN (ACNF).
Objetivo General: Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la UTIC, cuando éstos así lo requieran para la operación del proceso respectivo.
Objetivos Específicos:
Identificar, registrar, controlar y verificar los datos de los elementos de configuración, así como la información relacionada con los mismos.
ACNF 1 Establecer la cobertura y el alcance de la administración de la configuración.
Factores Críticos:
3. Implementar acciones de control para la administración del repositorio de configuraciones, considerando al menos:
Las relativas a la administración de los usuarios del repositorio de configuraciones, incluyendo perfiles y permisos.

II. PROCESOS DE ORGANIZACIÓN.
II.C Proceso de Administración de la Seguridad de la Información (ASI).
ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.
Factores Críticos:
El grupo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:
1. Definir los controles de seguridad necesarios para salvaguardar a los activos de TIC, los activos de información y las infraestructuras críticas de la Institución, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:
b) La designación de personal en las áreas relacionadas con el manejo, administración y gestión de los activos de información de la Institución, con apego a las disposiciones jurídicas aplicables y considerando los procedimientos que, en su caso, se tengan implementados en el área o unidad administrativa de que se trate.
g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.
h) Los criterios de asignación de usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Entidad no cuenta con la plantilla de personal amplia que le permita realizar una adecuada asignación de los roles y perfiles de acceso en los sistemas que se listan en la presente observación.

Efectos

La inadecuada asignación de privilegios de accesos a los sistemas de información; provoca que los usuarios ingresen a menús que no competen a sus funciones y responsabilidades, además de poder modificar dicha información sin previa autorización.

Recomendaciones

Correctivas

La Subdirección de Desarrollo y Sistemas Informáticos, debe iniciar un proceso de revisión de los posibles conflictos de segregación de funciones que se identificaron en los sistemas eCONTABI, SICOPA, SIVICOP, SIIBOP y SICOP-CONAC, en coordinación con los titulares y dueños de la información de las áreas administrativas y operativas de la Entidad. con la finalidad de reestructurar los roles y perfiles de acceso.

Preventivas

La Subdirección de Desarrollo y Sistemas Informáticos, debe de llevar a cabo una revisión de los roles y perfiles de acceso de los sistemas eCONTABI, SICOPA, SIVICOP, SIIBOP y SICOP-CONAC en coordinación con los dueños y titulares de la información de las áreas administrativas y operativas de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 9

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos** — *Valor Económico*
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Clasificación del hallazgo

Bajo Riesgo (BR):	X	Mediano Riesgo (MR):		Alto Riesgo (AR):	

Hallazgo recurrente

Ejercicio de origen		SI		NO	X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI		NO	X

El hallazgo esta atendido

SI		Fecha de solventación:		NO	X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

Resultado del análisis de seguridad efectuado a las bases de datos Oracle, identificamos lo siguiente:

Sistema SIIBOP:

1. No está actualizada la base de datos.
2. La base de datos no tiene habilitado correctamente los perfiles de seguridad (DEFAULT y MONITORING_PROFILE).
3. 4 tablas que tienen utilizada su capacidad al 90%.
4. 7 usuarios con perfil de Default.
5. Está habilitado el privilegio PUBLIC en 7 tablas.
6. 4 Usuarios con sesiones simultaneas y sin un responsable asignado.
7. El parámetro ARCHIVELOG no está habilitado.

Sistema eCONTABI:

1. No está actualizada la base de datos.
2. La base de datos no tiene habilitado correctamente los perfiles de seguridad (DEFAULT y MONITORING_PROFILE).
3. 2 tablas que tienen utilizada su capacidad al 90%.
4. 11 usuarios con perfil de Default.
5. Está habilitado el privilegio PUBLIC en 7 tablas.
6. El parámetro ARCHIVELOG no está habilitado.

Sistema SICOPA:

1. No está actualizada la base de datos.
2. La base de datos no tiene habilitado correctamente los perfiles de seguridad (DEFAULT y MONITORING_PROFILE).
3. 3 tablas que tienen utilizada su capacidad al 90%.
4. 54 usuarios con perfil de Default.
5. Está habilitado el privilegio PUBLIC en 7 tablas.
6. 1 Usuario con sesiones simultaneas y sin un responsable asignado.
7. El parámetro ARCHIVELOG no está habilitado.

Sistema SICOP:

1. No está actualizada la base de datos.
2. La base de datos no tiene habilitado correctamente los perfiles de seguridad (DEFAULT y MONITORING_PROFILE).
3. 2 tablas que tienen utilizada su capacidad al 90%.
4. 802 Usuarios con perfil de Default.
5. Está habilitado el privilegio PUBLIC en 7 tablas.
6. 39 Usuarios con sesiones simultaneas y sin un responsable asignado.
7. El parámetro ARCHIVELOG no está habilitado.

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).
Artículo 17:
VI. Utilizar esquemas de consulta y acceso a directorio u otra base de datos normalizada para control de accesos y usuarios.

Anexo único del "Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información".
II.B. PROCESO DE ADMINISTRACIÓN DE LA CONFIGURACIÓN (ACNF).
Objetivo general: Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la UTIC, cuando éstos así lo requieran para la operación del proceso respectivo.
Regla 1: Identificar, registrar, controlar y verificar los datos de los elementos de configuración, así como la información relacionada con los mismos.
Regla 2: Mantener actualizada la información contenida en el repositorio de configuraciones y disponible para los servidores públicos de la UTIC involucrados en los diversos procesos.
II.C. PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI).
Objetivo General: Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.
Objetivo específico:
2. Efectuar la identificación de Infraestructuras de información esenciales y, en su caso, críticas, así como de activos clave de la Institución, y elaborar el catálogo respectivo.
3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.
4. Establecer un SGSI que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.
7. Fomentar una cultura de seguridad de la información en la Institución.
ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.
Factores Críticos:
1. Definir los controles de seguridad necesarios para salvaguardar los activos de TIC y TO, los activos de información y las infraestructuras de información esenciales de la Institución y, en su caso, las críticas, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:
a) Asegurar que los servidores y estaciones de trabajo, cuenten con software actualizado para detección y protección contra programas para vulnerar la seguridad de los dispositivos de TIC y TO, así como su información y los servicios que proveen. El software debe emitir reportes sobre el estado de actualización de los componentes sobre los que tienen cobertura.
f) Evitar el daño, pérdida, robo, copia y acceso no autorizados a los activos de información.
g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.
o) Contar con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos.
s) Establecer el mecanismo para garantizar la eliminación o modificación de los privilegios de acceso a la información del personal interno y proveedores de servicios, cuando terminen su relación contractual o cuando por algún motivo el nivel de privilegios de accesos asignados cambie.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos, no tiene establecido y formalizado los parámetros de seguridad de la base de datos referentes a: actualización de la base de datos, perfiles de seguridad (DEFAULT y MONITORING_PROFILE), notificación de la capacidad de las tablas de la base de datos, usuarios con perfil de Default, privilegios PUBLIC, sesiones simultaneas y el parámetro ARCHIVELOG, por lo cual, no se ha aplicado dicha configuración.

Efectos

La parametrización de contraseñas poco robustas, incrementa las posibilidades de suplantación de identidad por usuarios mal intencionados con conocimientos técnicos avanzados. causando la visualización no autorizada de información sensible para la Entidad.

Explotación de brechas de seguridad por usuarios mal intencionados con conocimientos técnicos avanzados en la instancia de base de datos a causa de la asignación de objetos sensibles al rol PUBLIC.

Recomendaciones

Correctivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe evaluar la factibilidad de cambiar la configuración de las bases de datos de la Entidad, mencionadas en la presente observación, tomando en consideración los siguientes puntos:

a) Inhabilitar y renombrar las cuentas de usuario creadas por default.
b) Inhabilitar servicios innecesarios y/o diferentes al propósito de la base de datos.
c) Revocar el acceso a los objetos críticos de la base de datos al rol PUBLIC.
d) Habilitar las políticas de complejidad y expiración de contraseñas para las cuentas de usuario privilegiadas, operativas y de aplicación.
e) Cifrar la comunicación entre el cliente y el servidor, así como cifrar la información sensible que reside en las bases de datos.
f) Monitorear el performance de la base de datos.

Lo anterior deberá ser probado en un ambiente de pruebas, con el objetivo de verificar su correcta funcionalidad.

Preventivas
La Subdirección de Desarrollo y Sistemas Informáticos, debe realizar una revisión de los parámetros de seguridad de las bases de datos mencionados en las acciones correctivas y en apego a las políticas y procedimientos de seguridad de Tecnologías de Información, dichas políticas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020

Reporte de hallazgos

Hallazgo No.: 10

Nombre del ente público:	Liconsa S.A de C.V
Periodo sujeto a revisión:	2019
Área Administrativa o Unidad:	**Subdirección de Desarrollo de Sistemas Informáticos**
Rubro afectado:	CONTROL INTERNO DE TECNOLOGIA DE LA INFORMACION
Cuenta afectada:	N/A

Valor Económico

Clasificación del hallazgo

Bajo Riesgo (BR):	Mediano Riesgo (MR):	Alto Riesgo (AR):
X		

Hallazgo recurrente

Ejercicio de origen	SI	NO
		X

El hallazgo procede del Reporte de Hallazgos Preliminares

SI	NO
	X

El hallazgo esta atendido

SI	Fecha de solventación:	NO
		X

Origen y Tipo de hallazgo

ORIGEN:	*TIPO:*	
INFORME DE AUDITORÍA INDEPENDIENTE	AUSENCIA DE CONTROL INTERNO	

Montos y cantidades
(Cifras en pesos)

Universo	Muestra	Observado	
		En relación al Universo	En relación a la Muestra
N/A	N/A	N/A	N/A

Descripción del hallazgo

Resultado del análisis de seguridad efectuado a los sistemas operativos GNU/LINUX, donde residen las aplicaciones críticas identificamos lo siguiente:

Sistema SIIBOP:

1.- No está actualizado LINUX.
2.- 3 Usuarios que tienen habilitado el cambio de contraseña y 3 parámetros que no cumplen con las recomendaciones de LINUX.
3.- 8 puertos abiertos con posibles vulnerabilidades.
4.- 2 cuentas de usuario con permisos CRON.
5.- Archivos binarios con permisos SETUID.

Sistema SICOP:

1.- No está actualizado LINUX.
2.- 5 Usuarios que tienen habilitado el cambio de contraseña y no está definido la longitud mínima de la contraseña.
3.- no se identificaron 4 archivos log.
4.- 1 puerto abierto con posibles vulnerabilidades.
5.- 4 cuentas de usuario con permisos CRON.
6.- Archivos binarios con permisos SETUID.
7.- Archivos sin grupo y con escritura.

Sistema eCONTABI:

1.- No está actualizado LINUX.
2.- 4 Usuarios sin un responsable.
3.- 3 Usuarios genéricos y 3 parámetros de seguridad no configurados acorde a las recomendaciones de LINUX.
4.- 2 puertos abierto con posibles vulnerabilidades.
5.- 3 cuentas de usuario con permisos CRON.
6.- 6 archivos binarios con permisos SETUID.
7.- 1 archivo sin propietario, 6 archivos sin un grupo asignado y archivos con permisos de escritura.

Sistema SICOPA:

1.- No está actualizado LINUX.
2.- 1 Usuario genérico, 2 sin un responsable, 3 parámetros de seguridad no configurados acorde a las recomendaciones de LINUX y no está habilitado el cifrado de contraseñas.
3.- 2 puertos abiertos con posibles vulnerabilidades.
4.- 7 archivos binarios con permisos SETUID.
5.- Archivos sin propietarios y con permisos de escritura.

Fundamento específico legal y/o técnico infringido

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" (ACUERDO).
Artículo 18.- Las Instituciones, en lo referente al software de capa intermedia, deberán observar lo siguiente:
II. Establecer servidores de presentación para los diversos aplicativos de cómputo existentes, y ejecutar rutinas de análisis de vulnerabilidades acordes con el software de capa intermedia que se establezca, a fin de disminuir el riesgo por falta de disponibilidad, de acuerdo a las guías de interoperabilidad que emita la Unidad a través de su portal.

Anexo único del "Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información".
II.C. PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI).
Objetivo General: Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.
Objetivo específico:
2. Efectuar la identificación de Infraestructuras de información esenciales y, en su caso, críticas, así como de activos clave de la Institución, y elaborar el catálogo respectivo.
3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.
4. Establecer un SGSI que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.
7. Fomentar una cultura de seguridad de la información en la Institución.
ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.
Factores Críticos:
1. Definir los controles de seguridad necesarios para salvaguardar los activos de TIC y TO, los activos de información y las infraestructuras de información esenciales de la Institución y, en su caso, las críticas, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:
a) Asegurar que los servidores y estaciones de trabajo, cuenten con software actualizado para detección y protección contra programas para vulnerar la seguridad de los dispositivos de TIC y TO, así como su información y los servicios que proveen. El software debe emitir reportes sobre el estado de actualización de los componentes sobre los que tienen cobertura.
f) Evitar el daño, pérdida, robo, copia y acceso no autorizados a los activos de información.
g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.
o) Contar con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos.
s) Establecer el mecanismo para garantizar la eliminación o modificación de los privilegios de acceso a la información del personal interno y proveedores de servicios, cuando terminen su relación contractual o cuando por algún motivo el nivel de privilegios de accesos asignados cambie.

Supuestos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Registro o actos Requisitar, solo en el caso de que sea hallazgo de alto riesgo

N/A

Causas

La Subdirección de Desarrollo de Sistemas Informáticos, no tiene establecido y formalizado los parámetros de seguridad de sistemas operativos referentes a: actualización de LINUX, cambio de contraseña, longitud mínima de la contraseña, habilitación de archivos Log, puertos abiertos, permisos CRON, permisos SETUID, archivos sin grupo y escritura, por lo cual, no se ha aplicado dicha configuración.

Efectos

Deriva en que los niveles de seguridad no sean robustos ante ataques de usuarios maliciosos, poniendo en riesgo la disponibilidad de los servicios.

Recomendaciones

Correctivas

La Subdirección de Desarrollo de Sistemas Informáticos, debe evaluar la factibilidad de cambiar la configuración de los sistemas operativos Linux de la Entidad, mencionadas en la presente observación, tomando en consideración los siguientes puntos:

1.- Mantener actualizado el sistema operativo LINUX.
2.- Habilitar cambio periódico de contraseña cada 60 o 90 días.
3.- Definir la longitud mínima de 8 caracteres en la contraseña.
4.- Habilitar los logs de auditoría.
5.- establecer seguridad a los puertos abiertos.
6.- Restringir la asignación de los permisos CRON (realización de tareas programadas).
7.- Restringir los permisos binarios SETUID sobre los archivos del sistema operativo.
8.- Asignar propietarios a los archivos del sistema operativo que no estén asignados a un grupo y restringir los permisos de escritura.

Lo anterior deberá ser probado en un ambiente de pruebas, con el objetivo de verificar su correcta funcionalidad.

Preventivas

La Subdirección de Desarrollo y Sistemas Informáticos, debe realizar una revisión de los parámetros de seguridad de los sistemas operativos Linux mencionados en las acciones correctivas y en apego a las políticas y procedimientos de seguridad de Tecnologías de Información, dichas políticas deben ser revisadas y actualizadas al menos una vez al año, con la finalidad de corroborar que fueron documentados y formalizados adecuadamente y están en apego a la operación de la Entidad.

Participantes

Lic. Cinthya Alejandra Zavala Martínez Subdirectora de Desarrollo de Sistemas Informáticos	C.P.C. Rualdo Otoniel García Ramos Auditor Externo Responsable de la Auditoría	C.P. María Esther Núñez Rojas Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública

Fecha de firma:	23/06/2020
Fecha compromiso de atención:	30/11/2020