Lotería Nacional

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2021-1-06HJY-20-0187-2022

Modalidad: Presencial

Núm. de Auditoría: 187

Criterios de Selección

Esta auditoría se seleccionó con base en los criterios establecidos por la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2021 considerando lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

Fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	437,938.6
Muestra Auditada	340,625.8
Representatividad de la Muestra	77.8%

El universo seleccionado por 437,938.6 miles de pesos corresponde al total de pagos de los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal de 2021; la muestra auditada está integrada por cuatro contratos y tres convenios modificatorios relacionados con el sistema integral del servicio de captación de apuestas en línea, el servicio de un centro de administración tecnológica (CAT Administrativo), así como el servicio de aprovisionamiento, migración, administración y operación de los servicios de cómputo (CAT Empresarial), con pagos por 340,625.8 miles de pesos que representan el 77.8% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Lotería Nacional (LOTENAL) en 2021, relacionada con el Ciberataque de mayo de 2021, la Ciberseguridad y la Continuidad de las Operaciones.

Antecedentes

En la fiscalización de la Cuenta Pública de 2015, se identificaron inconsistencias en la gestión de los contratos, así como en la seguridad de la información y continuidad de los servicios, respecto de las cuales se promovieron y emitieron las acciones correspondientes que obran en el informe individual de la auditoría número 92-GB "Auditoría de TIC".

Entre 2017 y 2021, la LOTENAL ha erogado 1,773,212.1 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

RECURSOS EROGADOS EN MATERIA DE TIC EN LOS ÚLTIMOS CINCO AÑOS EN LOTENAL

(Miles de pesos)

	2017	2018	2019	2020	2021	Totales
Monto por año	311,122.4	369,671.6	396,640.3	257,839.3	437,938.5	1,773,212.1

FUENTE: Información proporcionada por la Lotería Nacional.

Con base en el análisis de la gestión de las TIC efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados con el fin de establecer si son suficientes para el cumplimiento de los objetivos de las contrataciones y la función de las TIC sujetas a revisión y determinar el alcance, naturaleza y muestra de la revisión y se obtuvieron los resultados que se presentan en este informe.

Resultados

1. Análisis Presupuestal

De acuerdo con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal de 2021, publicado en el Diario Oficial de la Federación (DOF) el 30 de noviembre de 2020, se le aprobó a la LOTENAL un presupuesto de 2,826,472.6 miles de pesos en los capítulos 2000 y 3000; con las ampliaciones autorizadas, obtuvo un presupuesto modificado de 2,826,594.6 miles de pesos.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio de 2021, se concluyó que la LOTENAL tuvo un presupuesto ejercido de 2,534,377.1 miles de pesos en los capítulos 2000 y 3000, de los cuales, 437,938.6 miles de pesos corresponden a recursos relacionados con las TIC, que representan el 17.3% del presupuesto en los capítulos señalados, como se muestra a continuación:

RECURSOS EJERCIDOS EN LOTENAL EN LOS CAPÍTULOS 2000 Y 3000 DURANTE 2021

(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Recurso ejercido en TIC
2000	Materiales y suministros	5,379.7	3.6
3000	Servicios generales	2,528,997.4	437,935.0
	TOTAL	**2,534,377.1**	**437,938.6**

FUENTE: Elaborado con base en la información proporcionada por la LOTENAL.

Los recursos ejercidos en materia de las TIC por 437,938.6 miles de pesos se integran de la manera siguiente:

GASTOS EN TIC EN EL EJERCICIO DE 2021 EN LOTENAL

(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
2000		**MATERIALES Y SUMINISTROS**	**3.6**
3000		**SERVICIOS GENERALES**	**437,935.0**
	31401	Servicio telefónico convencional	303.1
	31904	Servicios integrales de infraestructura de cómputo	59,756.4
	32301	Arrendamiento de equipo y bienes informáticos	14,209.1
	32303	Arrendamiento de equipo de telecomunicaciones	22,169.1
	32701	Patentes, derechos de autor, regalías y otros	321,337.4
	33301	Servicios de desarrollo de aplicaciones informáticas	5,810.0
	33303	Servicios relacionados con certificación de procesos	6,176.2
	33604	Impresión y elaboración de material informático derivado de la operación y administración	2,876.4
	33901	Subcontratación de servicios con terceros (otros)	5,267.3
	35301	Mantenimiento y conservación de bienes informáticos	30.0
		TOTAL	**437,938.6**

FUENTE: Elaborado con información proporcionada por la LOTENAL.

Del universo seleccionado en 2021 por 437,938.6 miles de pesos que corresponde al total de pagos en contratos relacionados con las TIC, se erogaron 340,625.8 miles de pesos en cuatro contratos y tres convenios modificatorios que representan el 77.8% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS DE PRESTACIÓN DE SERVICIOS EJERCIDOS DURANTE 2021

(Miles de pesos)

Procedimiento de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		
				Del	Al	Mínimo	Máximo	Ejercido
Licitación Pública Internacional Plurianual Mixta	028-2014	IGT México Lottery, S. de R.L. de C.V., anteriormente denominada Gtech Servicios de México, S. de R.L. de C.V., en proposición conjunta con IGT Global Solutions Corporation, anteriormente denominada Gtech Corporation	Sistema Integral del Servicio de Captación de Apuestas en Línea (SISCAL)	19/12/2014	19/12/2020	981,680.0	2,454,200.0	0.0
	Quinto convenio modificatorio 028-2014			20/12/2020	02/03/2022	196,335.9	490,839.9	313,496.4
	Subtotales					1,178,015.9	2,945,039.9	313,496.4
Adjudicación Directa	014-2021	Internet Móvil S. de R.L. de C.V.	Servicio de un Centro de Administración Tecnológica (CAT) Administrativo	23/01/2021	30/08/2021	5,336.0	13,340.0	11,545.2
	Primer convenio modificatorio			31/08/2021	13/10/2021			
Adjudicación Directa	162-2021	Internet Móvil S. de R.L. de C.V.	Servicio de un Centro de Administración Tecnológica (CAT) Administrativo	14/10/2021	14/03/2022	3,428.5	8,006.6	1,982.6
	Primer convenio modificatorio			15/03/2022	31/03/2022			
Adjudicación Directa	124-2021	Triara.com, S.A. de C.V.	Servicio de aprovisionamiento y migración 2021, administración y operación de los servicios de cómputo 2021-2024 (CAT Empresarial)	02/10/2021	15/09/2024	365,249.1	401,774.0	13,601.6
	Totales					**1,552,029.5**	**3,368,160.5**	**340,625.8**

FUENTE: Elaborado con la información proporcionada por la LOTENAL.

Se verificó que los pagos se reconocieron en las partidas presupuestarias correspondientes; el análisis de los contratos de la muestra se presenta en los resultados subsecuentes.

2. Contrato número 028-2014 "Sistema Integral de Servicios de Captación de Apuestas en Línea (SISCAL)"

Se analizó la información del contrato número 028-2014 y sus convenios modificatorios suscritos con IGT México Lottery, S. de R.L. de C.V., en proposición conjunta con la empresa IGT Global Solutions Corporation, mediante el procedimiento de licitación pública internacional plurianual mixta, bajo la cobertura de los tratados de libre comercio, con fundamento en los artículos 24, 25, 26, fracción l, 26 bis, fracción III, 27, 28, fracción II, 29 y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, vigente del 19 de diciembre de 2014 al 19 de diciembre de 2020, por un monto mínimo de 981,680.0 miles de pesos y máximo de 2,454,200.0 miles de pesos, con objeto de prestar el "Sistema Integral del Servicio de Captación de Apuestas en Línea (SISCAL)"; mediante el quinto convenio modificatorio, se amplió el monto mínimo por 196,335.9 miles de pesos y el monto máximo por 490,839.9 miles de pesos, además se extendió el plazo al 2 de marzo de 2022; por los servicios devengados durante 2021 se efectuaron pagos por 313,496.4 miles de pesos y se determinó lo siguiente:

Alcance del servicio

Diseñar, construir e instalar un sistema integral para operar juegos en línea y en tiempo real que permita la venta y captura de apuestas a través de terminales punto de venta proporcionadas por el proveedor, el detalle de los servicios es el siguiente:

- Sitio central y alterno: infraestructura de cómputo nueva redundante de alta disponibilidad, el sitio alterno deberá contar con equipo de características idénticas al sitio central, equipos auxiliares y el sistema de comunicaciones necesario para permitir la continuidad de todas las operaciones.

- Línea de emergencia: centro de llamadas con el software y hardware necesario para proporcionar asistencia técnica especializada a los comercializadores autorizados del organismo.

- Centro de monitoreo: con herramientas que permitan alertar en línea y en tiempo real al personal del organismo ante cualquier incidente que se presente en el SISCAL.

- Terminales: un mínimo inicial de 10,000 terminales punto de venta para la toma de apuestas, el proveedor deberá cubrir los mantenimientos preventivos y correctivos para cada una de las terminales, así como los periféricos que pueda emplear.

- Aplicación informática (SISCAL): desarrollo de una aplicación informática que permita tener el control de las transacciones y operación que se realiza a través de las terminales de venta.

- Capacitación: programa completo e integral de capacitación en el uso de las terminales, periféricos y aditamentos, así como del sistema de captación de apuestas de los diversos juegos y sorteos, tanto actuales como futuros.

- Mantenimiento preventivo y correctivo: planes de mantenimiento del centro de llamadas, del sistema integral de comunicación para la red de toma de apuestas (sitio central) y de las terminales punto de venta.

Revisión técnica y funcional del contrato

El grupo auditor revisó el anexo y propuesta técnica, los entregables, las actas de entrega-recepción y realizó pruebas a las terminales punto de venta e identificó lo siguiente:

- Durante la revisión de la herramienta de monitoreo de los productos (PRONOSPORTS, GANA GATO, MELATE, TRIS, PROGOL, PROGOL ½ SEMANA, PROTOUCH, CHISPAZO, MELATE RETRO Y SUPER PAR), se validó el monto de las ventas diarias que se registran por medio de las terminales punto de venta, las cancelaciones (boletos no emitidos) y el pago de premios en tiempo real.

- De un universo de 90 interfaces se revisó una muestra de 20 (22.2%), con ésta se identificó que el proveedor transfiere archivos en formato TXT al organismo mediante el protocolo de transferencia de archivos (FTP), se verificó que la LOTENAL validó la cantidad de registros, de ventas reportadas, así como de la información contenida en los archivos (número de producto, número del sorteo, fecha del sorteo, número ganador, cantidad de ganadores y el monto del premio individual) datos que se reflejan en el portal web del organismo donde se dan a conocer los ganadores.

Pruebas de las terminales punto de venta

Del universo de las terminales punto de venta instaladas en el ejercicio de 2021 que corresponde a 1,178 unidades, se obtuvo una muestra de 89 (7.6%) para validar la prestación del mantenimiento preventivo; con las revisiones y documentación proporcionada por el organismo se validó que el mantenimiento cumplió con las condiciones del anexo técnico del contrato.

3. Contratos números 014-2021 y 162-2021 "Servicio de un Centro de Administración Tecnológica (CAT) Administrativo"

Se analizó la información del contrato número 014-2021 suscrito con Internet Móvil, S. de R.L de C.V., mediante adjudicación directa con fundamento en los artículos 25, 26, fracción III, 41, fracción V, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, vigente del 23 de enero al 30 de agosto de 2021, por un monto mínimo de 5,336.0 miles de pesos y máximo de 13,340.0 miles de pesos, para brindar el "Servicio de un Centro de Administración Tecnológica (CAT) Administrativo"; mediante el primer convenio modificatorio, se amplió la vigencia del contrato al 13 de octubre de 2021, durante el ejercicio 2021 se realizaron pagos por 11,545.2 miles de pesos. También se analizó el contrato número 162-2021 suscrito con el mismo proveedor, proceso de contratación y objeto del contrato mencionados anteriormente, vigente del 14 de octubre de 2021 al 14 de marzo de 2022, por un monto mínimo de 3,428.5 miles de pesos y máximo de 8,006.6 miles de pesos; mediante el primer convenio modificatorio, se amplió la vigencia al 31 de marzo de 2022, con presupuesto 2021 se realizaron pagos por 1,982.6 miles de pesos y se determinó lo siguiente:

Alcance del servicio

El aprovisionamiento de equipo informático, así como la migración gradual de los equipos de cómputo personal y bienes informáticos en un esquema de administración y gestión de los servicios.

Proceso de contratación

Como resultado de la revisión del expediente de contratación por parte del grupo auditor de conformidad con las disposiciones vigentes, se detectó que el análisis de la investigación de mercado del contrato número 014-2021 se encuentra incompleto.

Revisión técnica, funcional y administrativa

El grupo auditor revisó la documentación técnica (entregables, planes de trabajo, actas de entrega-recepción, entre otros) con la finalidad de corroborar el cumplimiento del prestador del servicio de los mecanismos de control, características técnicas, actividades y tiempos descritos en el anexo técnico del servicio; con base en los resultados se identificó lo siguiente:

Verificación de los servicios

De un universo de 371 equipos del sitio de Insurgentes se seleccionaron 75 (20.2%), para su revisión mediante la herramienta de monitoreo de acuerdo con las características del anexo técnico del contrato; en su análisis, se identificó lo siguiente:

- No se localizaron dos equipos (2.7%).

- No se encontraron ocho ratones y un teclado.

- Debido al incidente de seguridad de mayo de 2021 (el cual se reporta en el resultado número 5), el protocolo SMB (Servidor que gobierna el acceso a archivos y directorios) se encuentra bloqueado, lo que impidió la validación del componente de la imagen en los equipos.

- En relación con la fecha de adquisición de los equipos, se identificó que 38 fueron comprados en 2017 (50.7%); 28 en 2018 (37.3%); dos en 2019 (2.7%); uno en 2020 (1.3%) y seis en 2021 (8.0%).

- Con la herramienta de monitoreo se identificaron equipos instalados desde el ejercicio de 2017, contrario a lo establecido en el numeral “7. Descripción de los servicios administrados requeridos” del anexo técnico de ambos contratos donde se estipula que “… los equipos ofertados para la prestación de este servicio deberán ser vigentes, de línea, no remanufacturados …”.

El grupo auditor realizó un comparativo de las características técnicas del numeral “8. Equipo de cómputo” de la propuesta y anexo técnico de ambos contratos, donde se detallan los requisitos mínimos para las especificaciones de los equipos, los cuales no cumplen con lo requerido de conformidad con lo siguiente:

- Perfil PCA (personal operativo y usuarios en general): Fue requerido un procesador principal de 3.3 a 3.8 GHz (gigahertz) de frecuencia base, 4 Cores de cómputo y 6 Cores gráficos última generación, en contraste, el proveedor adjudicado tiene instalados equipos con menores capacidades en el rango de 1.8 a 4.0 GHz y de 3.00 a 3.5 GHz.

- Perfil PCB (personal operativo y hasta mandos medios): Fue solicitado un procesador principal de 3.6 a 4.0 GHz máximo, 4 Cores de cómputo y 6 Cores gráficos última

generación, sin embargo, se tienen instalados equipos en el rango de 3.00 a 3.5 GHz; en el caso de la memoria principal fue requerida de 8 GB SDRAM DDR3 a 2000 MHz (megahertz), no obstante, los equipos instalados tienen 4 GB DDR4 SDRAM.

- Perfil LP1 (personal de mandos medios o usuarios con movilidad): Fue requerida memoria principal de 8 GB DDR3L-1600 SDRAM, no obstante, se encuentra instalada memoria de 4 GB.

- Perfil LP2 (personal de altos mandos): Fue solicitado un procesador principal de 2.6 a 3.4 GHz 2 Cores, en contraste, se tienen instalados procesadores de 2.8 GHz; la memoria principal requerida fue DDR4 de 8 GB a 2133 MHz, no obstante, se tiene instalada memoria de 4 GB; en el caso del disco duro principal fue solicitado de 500 GB SATA de estado sólido, sin embargo, los equipos tienen instalado un disco de 256 GB.

Cabe señalar que como resultado de las consultas de las características técnicas de los equipos relacionados a los perfiles PCA, PBC, LP1 y LP2, se identificó que actualmente se encuentran fuera del mercado.

Por lo anterior, se realizaron pagos por 909.0 miles de pesos conformados por las erogaciones de 71 equipos que no cumplieron con los requerimientos de los numerales “7. Descripción de los servicios administrados requeridos” y “8. Equipo de cómputo” de los anexos técnicos de los contratos números 014-2021 y 162-2021. Asimismo, en relación con el complemento del universo de equipos del sitio de Insurgentes, se efectuaron pagos por 3,570.4 miles de pesos conformados por las erogaciones de 281 equipos que también incumplen los numerales señalados del anexo técnico de ambos contratos.

Lo anterior incumplió el Manual General de Organización de Pronósticos para la Asistencia Pública ahora Lotería Nacional, apartado VI, funciones 1, 9, 10 y 11 de la Dirección de Tecnología de la Información y Comunicaciones, funciones 2 y 11 de la Gerencia de Operación y Soporte; el Contrato número 014-2021, cláusulas primera, tercera y séptima; Anexo Técnico del contrato número 014-2021, numerales “3. Objetivo”, “4. Consideraciones”, “7. Descripción de los Servicios Administrados Requeridos" y “8. Equipo de cómputo”; el Contrato número 162-2021, cláusulas primera, tercera y séptima; Anexo Técnico del contrato número 162-2021, numerales “3. Objetivo”, “4. Consideraciones”, “7. Descripción de los Servicios Administrados Requeridos” y “8. Equipo de cómputo”.

En conclusión, respecto a los equipos del sitio de Insurgentes, el 50.7% se instalaron en 2017 y el 37.3% en 2018, en contravención de la descripción de los servicios administrados y los requisitos mínimos para las especificaciones de los equipos estipulados en los anexos técnicos, por los cuales se pagaron 4,479.4 miles de pesos que no cumplen con los requisitos del contrato; asimismo, no se cuenta con un programa de actualización de la infraestructura tecnológica de usuarios finales para renovar los equipos que se vienen instalando desde el ejercicio de 2017.

2021-1-06HJY-20-0187-01-001 **Recomendación**

Para que la Lotería Nacional implemente un programa de actualización de la infraestructura tecnológica de usuarios finales por equipos vigentes, de línea, no remanufacturados, de la más reciente generación liberada por los fabricantes, para renovar los equipos que se vienen instalando desde el ejercicio de 2017, con la finalidad de mitigar los riesgos debido a la obsolescencia y deficiencias en la operación de los equipos.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2021-1-06HJY-20-0187-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 4,479,381.71 pesos (cuatro millones cuatrocientos setenta y nueve mil trescientos ochenta y un pesos 71/100 M.N.), por los pagos de 352 equipos que se vienen instalando desde el ejercicio de 2017, en contravención de lo establecido en los numerales "7. Descripción de los servicios administrados requeridos" y "8. Equipo de cómputo" del anexo técnico de los contratos números 014-2021 y 162-2021, debido al incumplimiento de la descripción de los servicios administrados y los requisitos mínimos para las especificaciones de los equipos, más los rendimientos financieros generados desde la fecha de su pago hasta la de su recuperación en incumplimiento del Manual General de Organización de Pronósticos para la Asistencia Pública ahora Lotería Nacional, apartado VI, funciones 1, 9, 10 y 11 de la Dirección de Tecnología de la Información y Comunicaciones y funciones 2 y 11 de la Gerencia de Operación y Soporte; del Contrato número 014-2021, cláusulas primera, tercera y séptima; del Anexo Técnico del contrato número 014-2021, numerales "3. Objetivo", "4. Consideraciones", "7. Descripción de los Servicios Administrados Requeridos" y "8. Equipo de cómputo"; del Contrato número 162-2021, cláusulas primera, tercera y séptima y del Anexo Técnico del contrato número 162-2021, numerales "3. Objetivo", "4. Consideraciones", "7. Descripción de los Servicios Administrados Requeridos" y "8. Equipo de cómputo".

Causa Raíz Probable de la Irregularidad

Falta de monitoreo, supervisión y control en las investigaciones de mercado y contratación de los servicios.

4. Contrato número 124-2021 "Servicio de un Centro de Administración Tecnológica (CAT) Empresarial"

Se analizó la información del contrato número 124-2021 suscrito con TRIARA.COM, S.A de C.V., mediante adjudicación directa con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 41, fracción III, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 72, fracción III, de su Reglamento, vigente del

2 de octubre de 2021 al 15 de septiembre de 2024, por un monto mínimo de 365,249.1 miles de pesos y máximo de 401,774.0 miles de pesos, para brindar el "Servicio de un Centro de Administración Tecnológica (CAT) Empresarial"; durante el ejercicio de 2021, se realizaron pagos por 13,601.6 miles de pesos y se determinó lo siguiente:

Alcance del servicio

Aprovisionamiento de la infraestructura tecnológica, migración y administración de los servicios de cómputo del centro de datos con el objetivo de garantizar la continuidad de los servicios con infraestructura tecnológica de última generación, los servicios contratados son los siguientes:

- Administración del centro de datos.
- Administración de redes.
- Administración de seguridad (seguridad perimetral, protección de base de datos y protección de aplicaciones).
- Administración del procesamiento.
- Administración y crecimiento del almacenamiento.
- Crecimiento de memoria para servidores.
- Crecimiento de protección de base de datos.

Revisión técnica, funcional y administrativa

El grupo auditor revisó la documentación técnica (entregables, planes de trabajo, actas de entrega-recepción, entre otros), así como el funcionamiento del monitoreo de las capacidades de los servidores con la finalidad de corroborar el cumplimiento del contrato, e identificó lo siguiente:

Entregables

De la revisión de los entregables para la gestión de amenazas de ciberseguridad (SAS), respecto a las características requeridas del anexo técnico, se obtuvo lo siguiente:

VERIFICACIÓN DE ENTREGABLES DEL SERVICIO DE GESTIÓN DE AMENAZAS DE CIBERSEGURIDAD DEL CONTRATO NÚMERO 124-2021

Identificador	Descripción del Entregable	Cumplimiento
SAS5	Reporte técnico de las soluciones tecnológicas de seguridad • Actividad sospechosa relevante • Incidentes confirmados • Cambios relevantes y solicitudes de servicio • Baja de servicios • Rendimiento, disponibilidad y latencia • Gráficas • Anexos técnicos	Parcial
SAS6	Reporte ejecutivo del reporte técnico	Parcial
SAS7	Reporte detallado de incidentes de seguridad	Parcial
SAS20	Matriz de usuarios de las bases de datos	Parcial

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- No se cuenta con los reportes en archivos editables de las herramientas utilizadas por el proveedor para generar los análisis y resultados, con la finalidad de validar que la información de los reportes no se afectó o editó.

- No se tiene el detalle de los eventos reportados por las herramientas de ciberseguridad para prevenir y solucionar eventualidades.

En conclusión, se tienen deficiencias en el análisis de los reportes de ciberseguridad; además, no se cuenta con el detalle de los eventos para prevenir y solucionar las contingencias informáticas.

2021-1-06HJY-20-0187-01-002 **Recomendación**

Para que la Lotería Nacional fortalezca los procedimientos y controles para la validación de los entregables de seguridad de la información con los datos fuente generados por las herramientas de ciberseguridad de los prestadores de servicios, así como para que mejoren los mecanismos de alertamiento de los eventos anómalos para las acciones de prevención y mitigación de los incidentes informáticos, con el fin de mejorar la calidad de los entregables y asegurar el cumplimiento de los niveles de servicio y proteger los activos de información y datos sensibles del organismo público.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

5. Incidente de Seguridad Informática (Ciberataque)

Con el análisis de la información proporcionada por el organismo relacionada con la gestión de los controles y mecanismos de mitigación efectuados antes, durante y después del ataque

cibernético perpetrado en mayo de 2021, así como de la información vinculada con el incidente de seguridad informática, se verificó, de conformidad con los controles para la ciberseguridad y mejores prácticas, junto con las políticas, procedimientos y herramientas del organismo en la materia.

En el estudio de la documentación, se observó que el 14 de mayo de 2021 se presentó un incidente de seguridad informática que afectó servidores virtuales en ambiente productivo de Lotería Nacional que se encontraban administrados bajo el contrato número 012-2021 "Servicio de un Centro de Administración Tecnológica (CAT) Empresarial" por la empresa INNOB IT GROUP, S.A. de C.V.

El organismo informó que consistió en un secuestro de datos (ransomware) que tuvo como vector de entrada la cuenta institucional de dos usuarios vulnerados posiblemente por un ataque de suplantación de identidad (phishing), en donde fueron reveladas sus credenciales para el acceso a la red privada virtual (VPN) hacia el interior de la red de la Lotería Nacional, para atacar un servidor de aplicaciones de legado sin actualizaciones de seguridad.

Situación de la infraestructura antes del Ciberataque

En la revisión de la documentación con la que contaba el organismo antes del incidente de seguridad, se observó lo siguiente:

- El proveedor del contrato número 012-2021, de conformidad con el objeto y alcance de los servicios, tenía la responsabilidad de la administración, monitoreo y alertamiento de los servidores afectados para activar los servicios de seguridad informática; sin embargo, en los reportes mensuales de seguridad informática, no se identificó ningún aviso de comportamientos anómalos que pudiera advertir a los administradores del contrato para prevenir o mitigar el impacto del ataque cibernético; cabe señalar que el contrato no se diseñó para aplicar deductivas en caso de deficiencias en los servicios de ciberseguridad.

- En la revisión de los 23 servidores virtuales reportados por el organismo con afectaciones, el 30.4% tenía versiones de sistemas operativos fuera del soporte del fabricante, adicionalmente, se identificó que ninguno de los servidores contaba con soluciones para la prevención de pérdida de datos (DLP).

- Respecto a las actualizaciones de seguridad (parches) con las que contaban los servidores afectados, no se tiene constancia de que antes del incidente los servidores tuvieran los parches actualizados.

- Durante el ejercicio de 2020 y hasta antes del ciberataque, no se realizaron pruebas de penetración a la infraestructura y soluciones tecnológicas.

Controles y procedimientos implementados durante el Ciberataque

Como resultado del estudio de la documentación proporcionada por el organismo se identificó lo siguiente:

- El 20 de mayo de 2021 se presentó una denuncia formal ante la Fiscalía General de la República por los hechos que pudieran ser constitutivos de delito.

- Se afectaron 44 sistemas, aplicativos, software de gestión y base de datos, de los cuales cinco eran de criticidad alta (11.4%), 24 de criticidad media (54.5%) y 15 de criticidad baja (34.1%), el organismo informó que dichas afectaciones impidieron la operación entre 27 a 77 días de los sistemas críticos y secundarios.

Controles y procedimientos implementados después del Ciberataque

El grupo auditor analizó la documentación con la que contaba el organismo de manera posterior al incidente de seguridad y se observó:

Identificación de los vectores de ataque

- Se identificó un ransomware (secuestro de datos) que tuvo como vector de entrada a dos usuarios vulnerados por una suplantación de identidad con la finalidad de obtener sus credenciales de acceso a la red privada virtual (VPN) para llegar a la red institucional de la Lotería Nacional.

- Los entregables de los servicios de seguridad informática de enero a mayo de 2021 no reportaron comportamientos anómalos en las redes ni eventos relacionados con el ataque de suplantación de identidad que vulneró las cuentas de los usuarios afectados.

Identificación de los atributos del ataque

- El ataque inició en un servidor de aplicaciones de legado donde se identificó un software de escritorio remoto con un archivo que contenía información de la red institucional, así como software de escaneo de redes y una herramienta para la ejecución de un programa malicioso desde otra computadora.

- El servidor de aplicaciones de legado que fue atacado tenía una versión vulnerable de sistema operativo, asimismo, no contaba con soluciones ni actualizaciones de seguridad (parches) por parte del fabricante.

Identificación del malware (programa malicioso) y tipo de ataque

El ataque a la infraestructura del organismo tuvo un impacto en los servidores virtuales, lo que ocasionó el cifrado de bases de datos, archivos de texto y binarios, archivos de procesamiento interno, entre otros.

Gestión de usuarios de cuentas privilegiadas y genéricas

- Durante el ejercicio de 2021, el organismo no contaba con un procedimiento formalizado para la gestión de las cuentas privilegiadas ni genéricas.

- Se tienen deficiencias en la supervisión periódica de las actividades de las cuentas privilegiadas y genéricas para identificar infracciones a las políticas de seguridad, tampoco se cuenta con reportes de alertamiento sobre comportamientos anómalos.

- El catálogo de cuentas privilegiadas y genéricas con acceso a las aplicaciones críticas no cuenta con la trazabilidad para identificar las actividades realizadas por los usuarios en los servidores de misión crítica.

Gestión de actualizaciones de seguridad (parches)

- Se tienen deficiencias en la gestión de actualizaciones de seguridad (parches); asimismo, no se tiene constancia de las actividades de descubrimiento y evaluación de parches para la actualización de servidores e imágenes de los equipos de cómputo.

- No se tiene evidencia de las actualizaciones de seguridad antes del ciberataque en los servidores que fueron afectados por el incidente.

Revisión de las configuraciones de aislamiento y segmentación

El organismo informó que, en conjunto con el proveedor, implementó un firewall (cortafuegos) para proteger las aplicaciones web, configuró las redes privadas virtuales con autenticación de doble factor vía correo electrónico, ejecutó un análisis de vulnerabilidades para la detección de brechas de seguridad y también actualizó los sistemas operativos y los antivirus en los equipos de cómputo.

Evaluaciones del riesgo

- No se tiene constancia de la realización de un análisis de riesgos antes del incidente informático de mayo de 2021.

- El organismo informó que se encuentra en proceso de implementar un nuevo sistema de gestión de seguridad de la información, con la migración de la infraestructura tecnológica derivada del proceso de fusión de la Lotería Nacional.

Gestión de la vulnerabilidad

- El procedimiento de gestión de vulnerabilidades implementado después del ciberataque de mayo de 2021 no contiene los mecanismos para remediar las incidencias, la periodicidad para su ejecución, los responsables ni los productos generados.

- Durante el ejercicio de 2020 y hasta antes del ciberataque, no se realizó ninguna prueba de hackeo ético.

Respuesta a incidentes de seguridad

- Se activó el sitio secundario para operar como sitio primario, se tiene evidencia de la recuperación de los aplicativos, las bases de datos y los servidores afectados por el incidente informático.

- Se identificaron oportunidades de mejora para la protección de sistemas desarrollados en lenguajes de tercera generación con deficiencias en el control de versiones del código fuente, los cuales operan en servidores con sistemas operativos fuera de soporte del fabricante.

Recuperación de desastres y planes de continuidad del negocio

- Entre las actividades para la recuperación de los servicios afectados se cambiaron las contraseñas de los usuarios con privilegios de administración; se restauraron los respaldos de información en los servidores y bases de datos; se ejecutó un escaneo de vulnerabilidades a los servidores; se revisaron los equipos de cómputo con herramientas de detección de programas maliciosos; se realizó la segmentación de las redes institucionales; se configuró el acceso a las redes inalámbricas mediante la dirección de control de acceso a medios de cada dispositivo; así como el envío de boletines de concienciación de seguridad informática a todo el personal del organismo.

- A la fecha de la auditoría (mayo de 2022) se identificó que estaban pendientes de normalizar las solicitudes de servicio con un avance del 95.0% y las carpetas compartidas con un avance del 80.0%.

Revisión de servidores afectados por el Ciberataque

De un universo de 23 servidores afectados, el grupo auditor revisó 10 (43.5%) y obtuvo lo siguiente:

- En dos servidores (20.0%) no se configuraron las máquinas virtuales al no ser necesarias para la operación.

- En un servidor (10.0%) se observó el antivirus y los parches de seguridad actualizados.

- En otro servidor (10.0%) no fue mostrado el antivirus, parches de seguridad ni respaldos debido a que sigue en proceso de migración.

- En tres servidores (30.0%) se encontró el antivirus y los respaldos diarios actualizados, así como los parches de seguridad desactualizados.

- En dos servidores (20.0%) se identificó la falta de actualización de los respaldos diarios, antivirus y parches de seguridad.

- Un servidor (10.0%) se encuentra aislado de la red y no se conecta a internet, no fue posible comprobar la actualización de los parches de seguridad ni antivirus.

Como resultado de la revisión de los procedimientos y controles relacionados con el incidente informático, los principales riesgos por las deficiencias en los controles para contener el ciberataque y proteger a los activos de información de la Lotería Nacional son los siguientes:

PRINCIPALES RIESGOS POR LAS DEFICIENCIAS EN LOS CONTROLES PARA IDENTIFICAR, CONTENER Y RESPONDER EL CIBERATAQUE

Factor Crítico	Riesgo
Gestión de usuarios de cuentas privilegiadas y genéricas	Se tienen deficiencias en el procedimiento para la asignación y mantenimiento de cuentas, así como para el monitoreo de las actividades realizadas por los usuarios, lo cual propicia el riesgo de que los atacantes identifiquen las vulnerabilidades de las cuentas privilegiadas para obtener sus credenciales y aprovechar las brechas de seguridad causando afectaciones en la infraestructura y soluciones tecnológicas.
Gestión de actualizaciones de seguridad (parches)	Se tienen insuficiencias en la gestión de las actualizaciones de seguridad, en consecuencia, los servidores no cuentan con la última versión de los parches liberados por los fabricantes, lo que ocasiona que los sistemas estén desprotegidos ante los atacantes, lo cual podría provocar la pérdida de información, denegación del servicio y la interrupción de las operaciones del organismo.
Mecanismos de monitoreo, detección y registro de transacciones	Se tienen oportunidades de mejora para el monitoreo de las transacciones dentro y fuera de la organización, lo cual aumenta el riesgo de la exfiltración de datos sensibles; asimismo, las deficiencias en el análisis de los registros de auditoría permitan que los atacantes pueden controlan los equipos durante mucho tiempo sin que nadie en la organización tenga conocimiento, lo que les da oportunidad para causar el mayor daño posible a los activos de información.
Evaluaciones del riesgo	Se tienen deficiencias en la identificación, evaluación y gestión de riesgos para detectar las vulnerabilidades de los sistemas y redes, lo cual podría propiciar la pérdida de datos, accesos no autorizados y la ruptura de la integridad de la información, así como la falta de medidas para evitarlos o mitigarlos.
Gestión de la vulnerabilidad y pruebas de penetración	Se tienen insuficiencias en la remediación de las vulnerabilidades de los sistemas y redes del organismo, lo cual propicia el riesgo de fallas e intrusiones que comprometen la integridad, disponibilidad y confidencialidad de la información; asimismo, se deben mejorar las pruebas de penetración periódicas para conocer las brechas en la seguridad y operación de los sistemas, con la finalidad de corregir las fallas y aumentar la capacidad de respuesta a los incidentes de seguridad informática.

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional y los resultados de las pruebas del grupo auditor.

Conclusiones

- El ciberataque fue mediante un secuestro de datos que tuvo como vector de entrada a dos usuarios vulnerados por una suplantación de identidad, con la cual se obtuvieron sus credenciales de acceso a la red privada virtual para atacar un servidor de aplicaciones de legado que operaba con una versión vulnerable del sistema operativo sin actualizaciones de seguridad.

- El proveedor que tenía la responsabilidad de la administración, monitoreo y alertamiento de los servidores para activar los servicios de seguridad informática no dio ningún aviso de comportamientos anómalos para tomar medidas de prevención y mitigación ante el ataque cibernético.

- Los servidores afectados tenían versiones de sistemas operativos fuera del soporte del fabricante; asimismo, ninguno de los servidores contaba con soluciones para la prevención de pérdida de datos ni con actualizaciones de seguridad (parches).

- Fueron afectados 44 sistemas y base de datos, de los cuales cinco eran de criticidad alta (11.4%), 24 de criticidad media (54.5%) y 15 de criticidad baja (34.1%), dichas afectaciones impidieron la operación del organismo de 27 a 77 días.

- Se identificaron deficiencias en la supervisión periódica de las actividades de las cuentas privilegiadas y genéricas para detectar infracciones a las políticas de seguridad, así como para la trazabilidad de las actividades realizadas en los servidores de misión crítica, tampoco se contaba con reportes para detectar comportamientos anómalos en las transacciones.

2021-1-06HJY-20-0187-01-003 **Recomendación**

Para que la Lotería Nacional implemente procedimientos y mecanismos de control para validar la configuración y actualización de las herramientas de seguridad informática, así como para especificar el detalle del precio, el alcance y los resultados de los entregables relativos a los servicios del centro de operaciones de seguridad y redes de cómputo con la finalidad de asegurar que las herramientas ejecuten un alertamiento preventivo para el tratamiento de eventos informáticos, así como para tener procedimientos definidos para el monitoreo, contención y respuesta ante un ataque cibernético.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2021-1-06HJY-20-0187-01-004 **Recomendación**

Para que la Lotería Nacional fortalezca las políticas, procedimientos y controles para mejorar la gestión de usuarios de cuentas privilegiadas y genéricas; la administración de las actualizaciones de seguridad (parches) en los servidores de todas las plataformas; la protección y segmentación de los servidores con aplicaciones de legado y sistemas desarrollados en lenguajes de tercera generación; los mecanismos de monitoreo, detección y registro de las transacciones; las evaluaciones del riesgo, así como la gestión de la vulnerabilidad y las pruebas de penetración con la finalidad de prevenir, contener y mitigar el impacto que podría ocasionar un ataque cibernético en la infraestructura, los sistemas y las operaciones del organismo.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2021-9-06HJY-20-0187-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en Lotería Nacional o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que, en su gestión, omitieron establecer y supervisar el cumplimiento de las medidas de seguridad referentes al procesamiento y salvaguarda de los activos de TIC, así como la implementación de políticas y soluciones de seguridad informática que aseguren la confidencialidad, disponibilidad e integridad de la información, lo que ocasionó un ataque cibernético mediante un secuestro de datos que tuvo como vector de entrada a dos usuarios vulnerados por una suplantación de identidad, con la cual se obtuvieron sus credenciales de acceso a la red privada virtual para atacar un servidor de aplicaciones de legado que operaba con una versión vulnerable del sistema operativo sin actualizaciones de seguridad; además, los servidores vulnerados no tuvieron protección contra la pérdida de datos, no contaban con las actualizaciones de seguridad (parches) ni antivirus, se tenían deficiencias en la gestión de cuentas privilegiadas y en la evaluación de riesgos, no se contaba con el monitoreo del comportamiento de las transacciones ni con el análisis de vulnerabilidades y pruebas de penetración a las soluciones e infraestructura tecnológica, lo que propició la interrupción de los procesos críticos del organismo, así como la pérdida de activos de información que vulneró la integridad, confidencialidad y disponibilidad de los datos del organismo, en incumplimiento del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, última reforma publicada el 23 de julio de 2018: Objetivo general del Proceso II.C Administración de la Seguridad de la Información (ASI) y Objetivo general del Proceso III.D Operación de los Controles de Seguridad de la Información y del ERISC (OPEC); del ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 6 de septiembre de 2021, Quinto, Sexto y Séptimo Transitorios, y del Manual General de Organización de Lotería Nacional de octubre de 2003, puesto "Dirección de Tecnología de la Información y Comunicaciones" apartado funciones: 6, 14, 15 y 17, "Gerencia de Operación y Soporte" apartado funciones: 2, 8 y 11.

6. Ciberseguridad

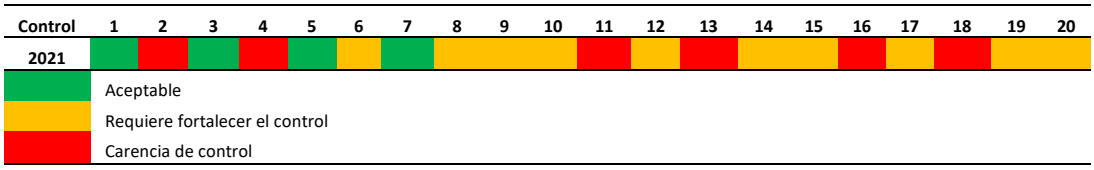
Se revisó la información proporcionada por la LOTENAL relacionada con la administración y operación de los controles de Ciberseguridad vinculados con la infraestructura y soluciones

tecnológicas de conformidad con los controles para la Ciberseguridad y sus mejores prácticas, así como en base a las políticas y lineamientos del organismo público en esta materia.

La revisión tiene por objeto proporcionar al organismo público una evaluación de la efectividad de la ciberdefensa con referencia a los controles críticos del Centro de Seguridad de Internet (CIS), con base en las mejores prácticas para la gestión de incidentes, administración de la configuración, seguridad de redes y servidores, gestión y conciencia de la seguridad, administración de la continuidad del negocio, gestión de la seguridad de la información, así como relaciones con terceros y prácticas de gobernanza.

El alcance de la auditoría consideró 20 controles de seguridad críticos (CSC) que incluyen 149 actividades de control individuales para evaluar el diseño y la efectividad operativa con sus respectivos objetivos de cumplimiento. Para la evaluación de los controles se consideraron tres niveles, los cuales se obtuvieron de conformidad con el porcentaje alcanzado en la evaluación de los subcontroles, en el caso del nivel "Aceptable" (más del 67.0%) se encontraron cuatro, se identificaron diez que "Requiere fortalecer el control" (entre el 33.0% y 67.0%), y los relacionados con "Carencia de control" (menos del 33.0%) fueron seis, de acuerdo con lo siguiente:

SEMÁFORO DE CUMPLIMIENTO DE LOS CONTROLES DE CIBERSEGURIDAD
EN LA LOTERÍA NACIONAL DURANTE 2021



FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Las observaciones más relevantes de cada uno de los controles de seguridad críticos son los siguientes:

CSC Control 1: Inventario y control de activos de hardware

EVALUACIÓN DEL CONTROL 1 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Inventario y control de activos de hardware	**13**	1	5	7	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Por lo anterior, se cumple con el objeto de gestionar activamente todo dispositivo de hardware en la red (inventario, seguimiento y corrección), de tal manera que sólo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados ni gestionados sean detectados para prevenir que obtengan acceso.

CSC Control 2: Inventario y control de activos de software

EVALUACIÓN DEL CONTROL 2 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Inventario y control de activos de software	**13**	10	1	2	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen deficiencias en el proceso automatizado para el inventario, control y soporte de los activos de software.
- Se tienen insuficiencias en las listas blancas de aplicaciones para asegurar que sólo se ejecuta software autorizado y que todo el software no autorizado está bloqueado.
- Se tienen defectos en las herramientas automatizadas para detectar y eliminar el software no autorizado.

Por lo antes señalado, no se cumple con el objeto de gestionar activamente todo el software en la red (inventario, seguimiento y corrección), con la finalidad de que sólo el software autorizado esté instalado y pueda ejecutarse, de tal manera que el software no autorizado ni gestionado sea encontrado, para prevenir su instalación y ejecución.

CSC control 3: Evaluación continua de la vulnerabilidad y solución

EVALUACIÓN DEL CONTROL 3 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Evaluación continua de la vulnerabilidad y solución	**21**	5	4	12	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Por lo anterior, se cumple con el objeto de adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

CSC Control 4: Uso controlado de privilegios administrativos

EVALUACIÓN DEL CONTROL 4 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Uso controlado de privilegios administrativos	**17**	11	1	5	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias en el procedimiento para la autenticación de múltiples factores.

- Se tienen deficiencias en la administración remota de las consolas dedicadas.

- Se identificaron defectos en la ejecución de herramientas de scripting (secuencias de comandos).

- Se tienen insuficiencias en el monitoreo de los sistemas para emitir alertas sobre intentos fallidos de acceso con las cuentas con privilegios administrativos.

- Las cuentas con privilegios administrativos tienen defectos en la autenticación de dos factores.

- Se tienen insuficiencias con la bitácora y la herramienta automatizada para el inventario de las cuentas privilegiadas.

Por lo antes señalado, no se cumple con el objeto de implementar procesos y herramientas para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

CSC Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

EVALUACIÓN DEL CONTROL 5 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	**17**	2	2	13	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Por lo anterior, se cumple con el objeto de establecer, implementar y gestionar activamente (rastrear, informar, corregir) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

CSC Control 6: Mantenimiento, monitoreo y análisis de bitácoras de auditoría

EVALUACIÓN DEL CONTROL 6 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Mantenimiento, monitoreo y análisis de bitácoras de auditoría	**10**[1]	2	2	6	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Nota[1]: La evaluación se realizó en el 40.0% de los sistemas productivos que tienen una bitácora de actividades.

- Se tienen insuficiencias en el registro de anomalías del "inicio de sesión" de los sistemas e infraestructura tecnológica.

- Se tienen oportunidades de mejora en la elaboración de los informes de irregularidades de las bitácoras de los sistemas críticos.

- El 60.0% de los sistemas productivos tienen insuficiencias en el manejo de la bitácora de actividades.

Por lo antes señalado, no se cumple en su totalidad con el objeto de reunir, administrar y analizar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

CSC Control 7: Protección de correo electrónico y navegador web

EVALUACIÓN DEL CONTROL 7 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Protección de correo electrónico y navegador web	**22**	7	1	14	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Por lo anterior, se cumple con el objeto de minimizar la superficie de ataque y la oportunidad para atacantes de manipular el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.

CSC Control 8: Defensa contra software malicioso (malware)

EVALUACIÓN DEL CONTROL 8 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Defensa contra software malicioso (malware)	**11**	6	1	4	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen deficiencias en el manejo de la línea de comandos.

- Se tienen insuficiencias con las herramientas para proteger a las computadoras de amenazas emergentes y evitar que los programas afecten al organismo.

- Se tienen oportunidades de mejora con las herramientas sandboxing (para detectar ataques de malware y bloquearlos antes de que entren en la red).

- Se tienen defectos en las herramientas para eliminar el código malicioso del sistema después de su identificación.

Por lo antes señalado, no se cumple en su totalidad con el objeto de controlar la instalación, la propagación y la ejecución del código malicioso en múltiples puntos de la organización, al mismo tiempo que se optimiza el uso de la automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

CSC Control 9: Limitación y control de puertos de red, protocolos y servicios

EVALUACIÓN DEL CONTROL 9 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Limitación y control de puertos de red, protocolos y servicios	**4**	1	1	2	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen defectos en la lista de los servicios no autorizados en los equipos de cómputo final.

- Se tienen insuficiencias en la herramienta automatizada para descubrir puertos con la finalidad de identificarlos, clasificarlos y actualizarlos en las políticas del firewall perimetral.

Por lo anterior, no se cumple en su totalidad con el objeto de administrar (rastrear, controlar, corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

CSC control 10: Capacidad de recuperación de datos

EVALUACIÓN DEL CONTROL 10 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Capacidad de recuperación de datos	**8**	3	2	3	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias en el procedimiento de cifrado para la protección de las copias de seguridad.

- Se tienen deficiencias en la protección de copias de seguridad, en la rotación de los medios de almacenamiento y en el transporte a los sitios alternos.

- Se tienen insuficiencias en las pruebas de recuperación de los respaldos, dichas pruebas se realizan bajo demanda.

- Se tienen defectos para notificar a los responsables del sistema que una copia de seguridad ha fallado.

Por lo antes señalado, no se cumple en su totalidad con el objeto de verificar los procesos y herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de ésta.

CSC control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores

EVALUACIÓN DEL CONTROL 11 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	**6**	3	2	1	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias en los dispositivos de red para cumplir con la configuración de seguridad institucional y las actualizaciones de seguridad de los fabricantes (parches).

- Se tienen deficiencias en los mecanismos de doble autenticación para los dispositivos de red.

- Las herramientas automatizadas tienen insuficiencias para verificar las configuraciones de los dispositivos, así como para la detección de cambios en los componentes de seguridad perimetral.

Por lo anterior, no se cumple con el objeto de establecer, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad de la infraestructura de red utilizando un proceso de gestión de configuración y control de cambios riguroso para prevenir que los atacantes explotan los servicios y las configuraciones vulnerables.

CSC control 12: Límites de Defensa

EVALUACIÓN DEL CONTROL 12 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Límites de Defensa	**15**	7	3	5	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen deficiencias en el procedimiento para detectar conexiones no autorizadas fuera de los límites de la red.

- Se tienen insuficiencias con la herramienta de detección y prevención de intrusiones (IDS) para bloquear las direcciones o sitios sospechosos a la red interna.

- Se tienen defectos en la atención de las alertas y el tratamiento de los paquetes maliciosos identificados por el firewall (cortafuegos).

- Se tienen insuficiencias para la autenticación de dos factores, así como en la gestión de los cambios de configuración para bloquear el tráfico no autorizado por los sistemas de protección perimetrales.

Por lo antes señalado, no se cumple en su totalidad con el objeto de detectar, prevenir y corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.

CSC control 13: Protección de datos

EVALUACIÓN DEL CONTROL 13 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Protección de datos	**15**	11	1	3	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias en la metodología para la clasificación de datos y activos de información, así como en el procedimiento para la obsolescencia de los datos.

- El procedimiento de cifrado de disco duro tiene deficiencias para clasificar los tipos de equipos.

- Se tienen insuficiencias en la solución de prevención de perdida de datos (DLP), así como en la clasificación de datos sensibles.

- Se tienen defectos en la configuración de seguridad para los dispositivos USB, así como en la bitácora para alertar de accesos no autorizados o actividad inusual.

- El análisis y tratamiento de los accesos no autorizados durante la transferencia de archivos y filtrado de correo electrónico tiene deficiencias en su operación.

Por lo anterior, no se cumple con el objeto de gestionar los procesos y herramientas utilizadas para prevenir la exfiltración de datos, mitigar el efecto de la exfiltración de datos y asegurar la privacidad e integridad de la información sensible.

CSC control 14: Control de acceso basado en la necesidad de conocer

EVALUACIÓN DEL CONTROL 14 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Control de acceso basado en la necesidad de conocer	**5**	2	1	2	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen deficiencias en el procedimiento para el cifrado de información en tránsito por las redes de datos.

- La herramienta de descubrimiento activo para la información sensible almacenada, procesada o transmitida por las soluciones tecnológicas tiene insuficiencias para su operación.

Por lo antes señalado, no se cumple en su totalidad con el objeto de gestionar los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el acceso seguro a activos críticos (información, recursos, sistemas, entre otros) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen una necesidad y derecho a acceder a estos activos críticos basado en una clasificación aprobada.

CSC control 15: Control de acceso inalámbrico

EVALUACIÓN DEL CONTROL 15 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Control de acceso inalámbrico	**8**	2	5	1	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias con el sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.

- Se tienen deficiencias en la política “Trae tu propio dispositivo” (BYOD).

- La herramienta automatizada para restringir y eliminar puntos de conexión inalámbrica de dispositivos Bluetooth y NFC (comunicación de campo cercano) tiene insuficiencias en su operación.

Por lo anterior, no se cumple en su totalidad con el objeto de gestionar los procesos y herramientas utilizadas para rastrear, controlar, prevenir y corregir el uso seguro de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

CSC control 16: Supervisión y monitoreo de cuentas

EVALUACIÓN DEL CONTROL 16 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Supervisión y monitoreo de cuentas	**8**	6	1	1	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias para obtener el inventario de todas las cuentas administrativas, incluyendo dominio y cuentas locales, para asegurarse que sólo las personas autorizadas tienen privilegios elevados.

- El procedimiento y la herramienta para la desactivación automática de cuentas tiene deficiencias en su operación.

- Las bitácoras de monitoreo tienen defectos para alertar de los inicios de sesión sospechosos o para registrar los intentos de acceso fallidos en la infraestructura y soluciones tecnológicas.

Por lo antes señalado, no se cumple con el objeto de gestionar activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para los atacantes.

CSC control 17: Implementar un programa de concientización y entrenamiento de seguridad

EVALUACIÓN DEL CONTROL 17 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Implementar un programa de concientización y entrenamiento de seguridad	**6**	2	2	2	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- En el ejercicio de 2020 y hasta antes del ciberataque de mayo de 2021, no se realizó la concientización ni capacitación en materia de seguridad de la información para el personal del organismo.

- Se tienen insuficiencias en el programa de concienciación en materia de seguridad informática.

- El análisis de brechas de las habilidades del personal adscrito a las áreas de seguridad de la información tiene defectos en su instrumentación.

- Las encuestas sobre la concientización del personal dieron como resultado un bajo nivel de conocimiento de las políticas de seguridad de la información.

Por lo anterior, no se cumple en su totalidad con el objeto de gestionar todos los roles funcionales en la organización (priorizando aquellos que son misionales para la organización y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para soportar la defensa de la dependencia, así como desarrollar y ejecutar un plan integral para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concienciación.

CSC control 18: Seguridad del Software de Aplicación

EVALUACIÓN DEL CONTROL 18 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Seguridad del software de aplicación	**16**	10	1	5	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional

- Los lineamientos y estándares para regular el proceso de desarrollo y mantenimiento de sistemas no se encuentran formalizados ni autorizados.

- Se tienen insuficiencias en los procedimientos y herramientas para el análisis de la calidad del código previo a su liberación en ambiente productivo.

- El reporte de vulnerabilidades de alto riesgo en los desarrollos de sistemas y los planes de remediación de las fallas detectadas tienen deficiencias en su implementación.

- Las pruebas de interfaces y aceptación de los usuarios finales en los desarrollos de sistemas son insuficientes.

- Se tienen deficiencias en los controles de cambio aplicados en la migración de los ambientes de desarrollo, calidad y producción durante los ejercicios de 2020 y 2021.

- No se cuenta con un estándar para la compilación del código fuente en las diversas plataformas con desarrollos de sistemas.

Por lo antes señalado, no se cumple con el objeto de gestionar el ciclo de vida de seguridad de todo el software interno desarrollado y adquirido para prevenir, detectar y corregir las debilidades de seguridad.

CSC control 19: Respuesta y manejo de Incidentes de ciberseguridad

EVALUACIÓN DEL CONTROL 19 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Respuesta y manejo de Incidentes de ciberseguridad	**7**	3	0	4	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

- Se tienen insuficiencias con el plan de sensibilización para los empleados a cargo de la mesa de servicios.

- El procedimiento para la actualización de los escenarios de pruebas con las novedades detectadas durante el tratamiento de los incidentes tiene deficiencias en su implementación.

- La base de datos de las lecciones aprendidas durante el tratamiento de los incidentes tiene insuficiencias en su instrumentación.

De acuerdo con lo anterior, no se cumple en su totalidad con el objeto de proteger la información de la organización, ni su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión, entre otros) para descubrir rápidamente un ataque y luego contener de manera efectiva el daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.

CSC control 20: Pruebas de penetración y ejercicios de equipo rojo

EVALUACIÓN DEL CONTROL 20 DE CIBERSEGURIDAD EN LA LOTENAL

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Pruebas de penetración y ejercicios de equipo rojo	**11**[1]	1	3	7	

FUENTE: Elaborado con la información proporcionada por la Lotería Nacional.

Nota[1]: La evaluación se realizó con las evidencias presentadas a partir de septiembre de 2021.

- Las pruebas de penetración a la infraestructura tecnológica no se realizaron hasta septiembre de 2021.

- Se tienen insuficiencias en las acciones y tratamiento dado a los hallazgos de la ejecución de las pruebas.

- El procedimiento para el análisis de vulnerabilidades y pruebas de penetración a la infraestructura tecnológica tiene deficiencias en su implementación.

Por lo antes señalado, no se cumple en su totalidad con el objeto de probar la fortaleza general de la defensa de la entidad (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

En la revisión de los controles y procedimientos para la Ciberseguridad, se identificó que los principales riesgos por las deficiencias en los controles y sus consecuencias potenciales para las operaciones y activos de información de la Lotería Nacional son los siguientes:

PRINCIPALES RIESGOS POR LAS DEFICIENCIAS EN LOS CONTROLES DE CIBERSEGURIDAD

Factor Crítico	Riesgo
Inventario y control de activos de software	Las insuficiencias del inventario y control de activos de software propicia el riesgo de ejecución de software no autorizado en los dispositivos, lo cual podría introducir fallas en la seguridad o programas maliciosos de los atacantes por un sistema que se encuentre comprometido.
Uso controlado de privilegios administrativos	Las deficiencias en el control de los privilegios administrativos de las cuentas favorecen el riesgo de no poder rastrear, controlar, prevenir y corregir el uso, asignación y configuración de privilegios a los usuarios que lo requieran de conformidad con sus atribuciones y facultades.
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	Las insuficiencias en los dispositivos de red para cumplir con la configuración de seguridad institucional y las actualizaciones de seguridad de los fabricantes podrían poner en riesgo el proceso de gestión de configuración y el control de cambios para prevenir que los atacantes exploten servicios y configuraciones vulnerables.
Protección de datos	Las deficiencias en las políticas y procedimientos para la protección de datos podrían dificultar la prevención y mitigación de la exfiltración de información, además de poner en riesgo la privacidad e integridad de la información sensible.
Supervisión y monitoreo de cuentas	Las insuficiencias en la gestión del ciclo de vida de las cuentas del sistema y aplicaciones podrían generar brechas en la seguridad de los sistemas y aumentar las oportunidades de los atacantes para que puedan explotarlas.
Seguridad del software de aplicación	Los defectos en los mecanismos para prevenir, detectar y corregir debilidades de seguridad en los desarrollos de sistemas podrían propiciar vulnerabilidades en el código que serían explotadas por usuarios maliciosos.

FUENTE**:** Elaborado con la información proporcionada por la Lotería Nacional y las pruebas del grupo auditor.

Por lo anterior, se concluye que el 30.0% de los controles de seguridad críticos muestran deficiencias que ponen en riesgo a los activos de información, por lo que resulta prioritario fortalecer los controles relacionados con el inventario y el control de activos de software, el uso controlado de privilegios administrativos, la configuración segura de los equipos de red, la protección de datos, la supervisión y monitoreo de cuentas, así como la seguridad del software de aplicación, con la finalidad de prevenir, contener y mitigar un ataque cibernético.

2021-1-06HJY-20-0187-01-005 **Recomendación**

Para que la Lotería Nacional fortalezca las políticas, procedimientos y controles para la ciberdefensa del organismo, mejorando los controles relacionados con el inventario y control de activos de software; el uso controlado de privilegios administrativos; una configuración segura de los equipos de red; la protección de datos; la supervisión y monitoreo de cuentas, así como la seguridad del software de aplicación con la finalidad de asegurar el cumplimiento de los objetivos de ciberseguridad para la identificación, protección, detección, respuesta y recuperación ante los ataques cibernéticos.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

7. Continuidad de las Operaciones

En el análisis de la información proporcionada por la Lotería Nacional relacionada con la administración de los controles para la continuidad de las operaciones de la infraestructura y soluciones tecnológicas, con base en las disposiciones y mejores prácticas en la materia, así como de conformidad con las políticas y lineamientos del organismo, se observó lo siguiente:

Análisis de Impacto al Negocio (BIA)

- La priorización de las actividades no se encuentra en función de los valores del tiempo objetivo de recuperación (RTO) y punto objetivo de recuperación de datos (RPO).

- El servicio terciarizado de “Gestión de la continuidad del Negocio” incluye al BIA y se encuentra en una etapa temprana de licitación, por lo tanto, no se encuentra implementado ni se tienen los controles compensatorios aplicados por el organismo.

Plan de Continuidad del Negocio (BCP)

- No se tiene evidencia que demuestre que el plan de continuidad responde a los procesos críticos declarados en el análisis de impacto al negocio.

- El plan no describe las acciones a realizar para la continuidad y resiliencia de la infraestructura y servicios de las TIC.

- Se tienen insuficiencias en la priorización para la recuperación de los procesos y actividades, con el fin de asegurarse que la reanudación de servicios se encuentre alineada con las necesidades preferentes del organismo.

- No se tienen pruebas del plan de continuidad del negocio para confirmar que los servicios se recuperan de forma efectiva, que se atienden las deficiencias y se aplican las actualizaciones.

- Se tienen deficiencias en las actualizaciones del plan de continuidad, así como en las actividades para la difusión y capacitación del personal involucrado con las acciones de recuperación, tampoco se tienen definidas ni notificadas las funciones del personal para dar cumplimiento al plan.

- El plan de continuidad del negocio no se encuentra implementado, por lo tanto, no se puede asegurar la continuación de los servicios de las TIC.

Plan de Recuperación de Desastres (DRP)

- Se tienen insuficiencias en la implementación del plan de recuperación de desastres, el organismo manifestó que las actividades se encuentran en proceso de definición hasta la culminación del proceso de fusión de la Lotería Nacional.

- Se tienen deficiencias en la estrategia tecnológica para la recuperación de la operación crítica durante una contingencia.

- No se proporcionó evidencia para identificar a las personas que forman parte del grupo responsable de atender las contingencias.

- Se tienen insuficiencias en el monitoreo del estado y operación de los equipos dentro de los límites aceptables, así como en la coordinación para la instrumentación del plan de continuidad del negocio y el plan de recuperación de desastres.

- A la fecha de la auditoría (mayo de 2022), no se tiene implementado un plan de recuperación de desastres para soportar las procesos y operaciones críticas del organismo en caso de una contingencia o desastre.

Programa de Capacidad de la Infraestructura Tecnológica

- Se tienen insuficiencias en el programa de capacidad de la infraestructura tecnológica.

- Se tienen deficiencias en el balance entre la demanda de los servicios de las TIC y la capacidad de la infraestructura de las TIC para conocer la suficiencia de cada uno de sus componentes.

- Se tienen defectos en la identificación de los componentes de la infraestructura de las TIC que son necesarios para cumplir con los requerimientos de desempeño y disponibilidad de los servicios.

- Se tienen deficiencias en la identificación de los activos de las TIC que requieren actualizaciones, renovaciones o sustituciones, así como los tiempos y costos estimados en cada caso.

- Se tienen insuficiencias en la verificación de la capacidad, rendimiento y tendencias de la carga de trabajo de la infraestructura tecnológica, para comprobar el cumplimiento de los niveles de servicio acordados.

- Se tienen deficiencias en las acciones a realizar cuando la capacidad y rendimiento de la infraestructura tecnológica no se encuentre en los niveles requeridos para la operación.

Programa de Respaldos de Información

- Los procedimientos y lineamientos del programa de respaldo, restauración y almacenamiento no se encuentran alineados al análisis de impacto al negocio.

- Se tienen deficiencias en la comprobación de la capacidad de procesamiento y almacenamiento para la infraestructura de respaldos, almacenamiento y restauración de datos, así como en la frecuencia de los reportes con los recursos disponibles.

- Se tienen insuficiencias en las pruebas de restauración de los respaldos y medios de almacenamiento.

Gestión de Riesgos

- Se tienen deficiencias en la implementación de los programas para la gestión de riesgos.

- Se tienen insuficiencias en el análisis y la evaluación de riesgos durante el ejercicio de 2020 y hasta antes del ciberataque de mayo de 2021.

Como resultado de la revisión del proceso de continuidad de las operaciones, se identificó que los principales riesgos por las deficiencias en los controles y sus consecuencias potenciales para las operaciones y activos del organismo son los siguientes:

PRINCIPALES RIESGOS POR LAS DEFICIENCIAS EN LOS CONTROLES PARA LA CONTINUIDAD DE LAS OPERACIONES

Factor Crítico	Riesgo
Análisis de Impacto al Negocio	Las insuficiencias en la implementación del análisis de impacto al negocio ponen en riesgo los servicios, funciones, actividades y unidades administrativas que dan continuidad a la operación del organismo, además de aumentar la probabilidad de un impacto técnico, económico y reputacional por la interrupción de uno o más servicios de las TIC.
Plan de Continuidad del Negocio	Las deficiencias del plan de continuidad en los objetivos, las metas, los controles, los procesos y los procedimientos necesarios para la continuidad de las operaciones podrían generar el riesgo de que no se tengan las condiciones para asegurar que la operación de los servicios y procesos críticos sean restablecidos conforme a las necesidades del organismo.
Plan de Recuperación de Desastres	Las insuficiencias del plan de recuperación de desastres ponen en riesgo el restablecimiento de los sistemas, aplicativos e infraestructura tecnológica que soporta los procesos sustantivos del organismo, además de no poder verificar que los tiempos y objetivos de recuperación resultan satisfactorios para la continuidad de las operaciones.
Programa de capacidad de la infraestructura tecnológica	Los defectos en los componentes del programa de capacidad para la operación de los servicios de las TIC ponen en riesgo el aprovechamiento de los recursos, el cumplimiento de los niveles de servicio y las acciones de mantenimiento y gestión de la infraestructura tecnológica.

FUENTE: Elaborado con base en la información proporcionada por la Lotería Nacional.

Por lo anterior, se tienen insuficiencias en los mecanismos de resiliencia para adaptarse a interrupciones e incidentes con el fin de mantener la continuidad de las operaciones sustantivas y secundarias; asimismo, se tienen defectos en los componentes del programa de

capacidad para la operación de la infraestructura tecnológica que ponen en riesgo el aprovechamiento de los recursos y el cumplimiento de los niveles de servicio.

2021-1-06HJY-20-0187-01-006 **Recomendación**

Para que la Lotería Nacional fortalezca los mecanismos de revisión, actualización e implementación del análisis de impacto al negocio, plan de continuidad del negocio, plan de recuperación de desastres y programa de capacidad de la infraestructura tecnológica, con la finalidad de contar con un nivel de resiliencia que permita reanudar las operaciones con el menor impacto y tiempo posible, además de asegurar un óptimo nivel de servicio de la infraestructura y las soluciones tecnológicas en beneficio de los usuarios finales del organismo.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

Montos por Aclarar

Se determinaron 4,479,381.71 pesos pendientes por aclarar.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Liderazgo y dirección, Planificación estratégica y operativa, Controles internos, Aseguramiento de calidad y Vigilancia y rendición de cuentas.

Resumen de Resultados, Observaciones y Acciones

Se determinaron 7 resultados, de los cuales, en 2 no se detectaron irregularidades y los 5 restantes generaron:

6 Recomendaciones, 1 Promoción de Responsabilidad Administrativa Sancionatoria y 1 Pliego de Observaciones.

Consideraciones para el seguimiento

Los resultados, observaciones y acciones contenidos en el presente informe de auditoría se comunicarán a la entidad fiscalizada, en términos de los artículos 79 de la Constitución Política de los Estados Unidos Mexicanos y 39 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, para que en un plazo de 30 días hábiles presente la información y realice las consideraciones que estime pertinentes.

En tal virtud, las recomendaciones y acciones que se presentan en este informe de auditoría se encuentran sujetas al proceso de seguimiento, por lo que, debido a la información y consideraciones que en su caso proporcione la entidad fiscalizada podrán atenderse o no, solventarse o generar la acción superveniente que corresponda de conformidad con el marco jurídico que regule la materia.

Dictamen

El presente se emite el día 15 de junio de 2022, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, la administración de riesgos, la seguridad de la información, la continuidad de las operaciones, la calidad de datos, el desarrollo de aplicaciones y el aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que esto se realizó conforme a las disposiciones jurídicas y normativas aplicables y, específicamente, respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, la Lotería Nacional cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

- Respecto a los contratos para el servicio de un centro de administración tecnológica, se identificó que el 88.0% de los equipos del sitio de Insurgentes se instalaron en 2017 y 2018, en contravención de la descripción de los servicios administrados y los requisitos mínimos para las especificaciones de los equipos del anexo técnico, por los cuales se realizaron pagos por 4,479.4 miles de pesos que no cumplen con los requisitos del contrato.

- El ciberataque de mayo de 2021 fue mediante un secuestro de datos que obtuvo las contraseñas de dos usuarios por una suplantación de identidad, para ganar el acceso a la red privada virtual y atacar un servidor de aplicaciones de legado que operaba con una versión vulnerable del sistema operativo sin actualizaciones de seguridad; el proveedor responsable del monitoreo y alertamiento de los servidores no dio ningún aviso de comportamientos anómalos para tomar medidas de prevención y mitigación antes del incidente informático.

- Los servidores afectados por el ataque cibernético tenían versiones de sistemas operativos fuera del soporte del fabricante; además, ninguno contaba con soluciones para la prevención de pérdida de datos ni con las actualizaciones de seguridad (parches); asimismo, se identificaron deficiencias en la supervisión periódica de las actividades de las cuentas privilegiadas para detectar infracciones a las políticas de seguridad, así como transacciones irregulares en los servidores de misión crítica.

- En relación con el estado de la ciberseguridad, el 30.0% de los controles de seguridad críticos tienen deficiencias que ponen en riesgo a los activos de información, por lo tanto, se requiere fortalecer los controles del inventario de activos de software, el uso de privilegios administrativos en las cuentas, la configuración de los equipos de red, la protección de datos, la supervisión y el monitoreo de cuentas, así como la seguridad en los desarrollos de sistemas y aplicativos.

- Sobre la continuidad de las operaciones se tienen insuficiencias en los mecanismos de resiliencia para adaptarse a interrupciones e incidentes con el fin de mantener la continuidad de las operaciones, así como los defectos en el programa de capacidad de la infraestructura tecnológica para el aprovechamiento de los recursos y el cumplimiento de los niveles de servicio.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtro. Genaro Héctor Serrano Martínez	Mtro. Roberto Hernández Rojas Valderrama

Comentarios de la Entidad Fiscalizada

Es importante señalar que la documentación proporcionada por la entidad fiscalizada para aclarar o justificar los resultados y las observaciones presentadas en las reuniones fue analizada con el fin de determinar la procedencia de eliminar, rectificar o ratificar los resultados y las observaciones preliminares determinados por la Auditoría Superior de la Federación y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables; analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad comprende el análisis de las contrataciones vigentes, la determinación de la procedencia de su renovación, la pertinencia de realizar contrataciones consolidadas, y los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; validar la información del registro de accionistas para identificar asociaciones indebidas, subcontrataciones en exceso y transferencia de obligaciones; verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permiten su fiscalización, corresponden a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como la pertinencia de su penalización o deductivas en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, servicios administrados para la operación de infraestructura y sistemas de información, telecomunicaciones y demás relacionados con las TIC para verificar antecedentes, investigación de mercado, adjudicación, beneficios esperados, entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento y sustantivas), implementación y soporte de los servicios; verificar que el plan de mitigación de riesgos fue atendido, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información, como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo y pruebas de penetración a las redes y sistemas, entre otros.

7. Evaluar la gestión de los programas de continuidad de las operaciones en sus elementos como el análisis de impacto al negocio (BIA); el plan de continuidad del negocio (BCP); el plan de recuperación ante desastres (DRP) y las políticas de respaldos, replicación de datos, planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros.

Áreas Revisadas

La Dirección de Tecnologías de la Información y Comunicaciones adscrita a la Subdirección General de Administración y Finanzas, así como la Dirección de Marcas Tris y Chispazo adscrita a la Subdirección General de Servicios Comerciales, ambas subdirecciones de la Lotería Nacional.

Disposiciones Jurídicas y Normativas Incumplidas

Durante el desarrollo de la auditoría practicada, se determinaron incumplimientos de las leyes, reglamentos y disposiciones normativas que a continuación se mencionan:

1. Otras disposiciones de carácter general, específico, estatal o municipal: 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, artículos 21, 24 y 25 del Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, última reforma publicada el 23 de julio de 2018, en su objetivo general, Reglas 9, 10, 14; Actividad ADS 2, factores críticos 1, 2, 3 y 4 de la actividad ADS 3 y actividad ADS 4 del Proceso II.A. Administración de Servicios (ADS), Proceso II.C. Administración de la Seguridad de la Información (ASI), ASI 5 Elaborar el análisis de riesgos, ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información, Apartado III. B Proceso de Administración de Proveedores (APRO); procesos APRO 2 "Monitorear el avance y desempeño del proveedor", APRO 3 "Apoyo para la verificación del cumplimiento de las obligaciones de los contratos", objetivo general del Proceso III.C Administración de la Operación (AOP), objetivo general del Proceso III.D Operación de los Controles de Seguridad de la Información y del ERISC (OPEC); ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 6 de septiembre de 2021, Quinto, Sexto y Séptimo Transitorios; Estatuto Orgánico de Lotería Nacional, artículo 24, fracción I; Manual General de Organización de Pronósticos para la Asistencia Pública ahora Lotería Nacional, funciones 2, 4 y 7 de la Subdirección General de Informática, apartado VI, funciones 1, 6, 9, 10, 11, 14, 15 y 17 de la Dirección de Tecnología de la Información y Comunicaciones, funciones 2, 8 y 11 de la Gerencia de Operación y Soporte; Contrato número 014-2021, cláusulas primera, tercera, séptima; Anexo Técnico del contrato número 014-2021 numerales "3. Objetivo", "4. Consideraciones", "7. Descripción de los Servicios Administrados Requeridos" y "8. Equipo de cómputo", Contrato número 162-2021, cláusulas primera, tercera, séptima; Anexo Técnico del contrato número 162-2021 numerales "3. Objetivo", "4. Consideraciones", "7. Descripción de los Servicios Administrados Requeridos" y "8. Equipo de cómputo", "10.14. Servicio administrado de Seguridad SAS A" y "10.23 Entregables B"; Centro para la Seguridad de Internet Controles de Seguridad Críticos para una Ciberdefensa eficaz, versión 7; Norma

ISO 22301/2019 "Seguridad y Resiliencia - Sistemas de Administración de la continuidad de Negocio", apartados 4.3.2, 8.2 y 8.3.

Fundamento Jurídico de la ASF para Promover Acciones y Recomendaciones

Las facultades de la Auditoría Superior de la Federación para promover o emitir las acciones derivadas de la auditoría practicada encuentran su sustento jurídico en las disposiciones siguientes:

Artículo 79, fracciones II, párrafo tercero, y IV, de la Constitución Política de los Estados Unidos Mexicanos.

Artículos 10, fracción I, 14, fracción III, 15, 17, fracción XV, 36, fracción V, 39, 40, de la Ley de Fiscalización y Rendición de Cuentas de la Federación.