Secretaría del Trabajo y Previsión Social

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-0-14100-20-0393-2021

393-DE

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 2020 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	107,642.3
Muestra Auditada	69,520.8
Representatividad de la Muestra	64.6%

El universo seleccionado por 107,642.3 miles de pesos corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC), en el ejercicio fiscal 2020; la muestra auditada está integrada por dos contratos para prestar los servicios integrales de tecnología para la plataforma digital del Servicio Nacional de Empleo (SNE), así como el centro de atención telefónica para el SNE, Programa Jóvenes construyendo el Futuro y Procuraduría de la Defensa del Trabajo, con pagos ejercidos por 69,520.8 miles de pesos, que representan el 64.6% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Secretaría del Trabajo y Previsión Social (STPS) en 2020, relacionada con el ciberataque sufrido en marzo de 2020, Ciberseguridad y Continuidad de las Operaciones.

Antecedentes

En la fiscalización de la Cuenta Pública 2017, se practicó la auditoría número 405-DE "Auditoría de TIC", donde se detectaron deficiencias en la vigilancia de los contratos para evitar desviaciones en el cumplimiento de las especificaciones técnicas; en la verificación de entregables de las órdenes de trabajo; en los procedimientos de conciliación de las horas trabajadas por parte del proveedor; en el análisis de vulnerabilidades, riesgos y pruebas; así como en la administración de cambios, plan de calidad, gestión del código fuente y cierre de proyectos.

Asimismo, se identificaron irregularidades en los mecanismos de seguridad de los aplicativos antes de ponerlos en operación; en el cifrado de datos para transferir la información con protocolos seguros; en el resguardo del código de las soluciones tecnológicas para evitar que se copien con fines distintos a su desarrollo; en las reglas para construir contraseñas robustas y su tiempo de vida; en el monitoreo de las bitácoras de los aplicativos para detectar accesos no autorizados; así como en la administración de usuarios para la segregación de funciones, comprobación de autorizaciones de accesos y el manejo de cuentas con privilegios especiales.

Entre 2016 y 2020, la STPS ha erogado 383,389.4 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

RECURSOS EROGADOS EN MATERIA DE TIC - STPS

(Miles de pesos)

Periodo del Gasto	2016	2017	2018	2019	2020	Total
Monto por año	55,296.1	93,220.4	50,106.6	39,674.6	145,091.7	383,389.4

FUENTE: Elaborada con información proporcionada por la Secretaría del Trabajo y Previsión Social.

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 función de las TIC sujetas de revisión de la cual, así como determinar el alcance, naturaleza y muestra de la revisión, 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 2020 publicado en el Diario Oficial de la Federación el 11 de diciembre de 2019, se aprobó a la Secretaría del Trabajo y Previsión Social (STPS) un presupuesto de 28,860,748.2 miles de pesos.

Con el análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2020, se concluyó que la STPS tuvo un presupuesto ejercido de 28,017,868.0 miles de pesos, de los cuales, 145,091.8 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 0.5% del presupuesto, como se muestra a continuación:

RECURSOS EJERCIDOS EN LA SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL DURANTE 2020
(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Recursos ejercidos en TIC
1000	Servicios personales	2,058,208.9	25,289.2
2000	Materiales y suministros	16,529.2	34.4
3000	Servicios generales	746,825.9	119,768.2
4000	Transferencias, asignaciones, subsidios y otras ayudas	25,189,697.0	0.0
5000	Bienes muebles, inmuebles e intangibles	6,607.0	0.0
	TOTAL	**28,017,868.0**	**145,091.8**

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

Los recursos ejercidos en materia de las TIC por 145,091.8 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2020 EN LA STPS
(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**25,289.2**
2000		**MATERIALES Y SUMINISTROS**	**34.4**
3000		**SERVICIOS GENERALES**	**119,768.2**
	31101	Servicio de energía eléctrica	821.5
	31301	Servicio de agua	66.0
	31401	Servicio telefónico convencional	2,180.0
	31602	Servicios de telecomunicaciones	78,750.9
	32301	Arrendamiento de equipo y bienes informáticos	29,404.3
	33301	Servicios de desarrollo de aplicaciones informáticas	6,935.5
	33801	Servicios de vigilancia	415.1
	33901	Subcontratación de servicios con terceros	112.5
	34501	Seguros de bienes patrimoniales	197.4
	35101	Mantenimiento y conservación de inmuebles para la prestación de servicios administrativos	3.6
	35501	Mantenimiento y conservación de vehículos terrestres, aéreos, marítimos, lacustres, fluviales	15.9
	35801	Servicios de lavandería, limpieza e higiene	176.1
	35901	Servicios de jardinería y fumigación	0.6
	39801	Impuesto sobre nóminas	688.9
		TOTAL	**145,091.8**

FUENTE: Elaborado con información proporcionada por la STPS.

Diferencias por redondeo.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual

de 25,289.2 miles de pesos durante el ejercicio fiscal 2020; considerando 69 plazas, el promedio anual percibido por persona fue de 366.5 miles de pesos.

Del universo seleccionado en 2020 por 107,642.3 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 69,520.8 miles de pesos en dos contratos que representan el 64.6% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS DE PRESTACIÓN DE SERVICIOS EJERCIDOS DURANTE 2020

(Miles de pesos)

Procedimiento de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		
				Del	Al	Mínimo	Máximo	Ejercido
Adjudicación directa	RF-043-2019	INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación	Servicios integrales de tecnología para la Plataforma Digital del SNE 2019-2021	01/11/2019	31/12/2021	43,857.3	61,400.2	20,118.5
Licitación Pública Nacional Electrónica	RF-057-2019	Wise Interactions, S.A. de C.V. y Grupo de Tecnología Cibernética, S.A. de C.V.	Servicio del centro de atención telefónica para el Servicio Nacional de Empleo, Programa Jóvenes construyendo el Futuro y Procuraduría de la Defensa del Trabajo (PROFEDET)	25/11/2019	30/10/2021	129,708.5	280,400.9	49,402.3
						29,037.7	72,594.1	55,106.6
Totales						**173,565.8**	**341,801.1**	**69,520.8**

FUENTE: Elaborado con información proporcionada por la STPS.

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

2. Contrato número RF-043-2019 "Servicios Integrales de Tecnología para la Plataforma Digital del SNE 2019-2021"

Se analizó la información del contrato número RF-043-2019 celebrado con INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, mediante el procedimiento de adjudicación directa, de conformidad con lo dispuesto en el artículo 1º, quinto párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, vigente del 1º de noviembre de 2019 al 31 de diciembre de 2021, por un monto mínimo de 43,857.3 miles de pesos y un máximo de 61,400.2 miles de pesos, para prestar los "Servicios Integrales de Tecnología para la Plataforma Digital del SNE (Servicio Nacional de Empleo) 2019-2021"; por los servicios devengados durante 2020 se efectuaron pagos por 20,118.5 miles de pesos, y se determinó lo siguiente:

Alcance del servicio

Crear la Plataforma Digital del Servicio Nacional de Empleo (PDSNE) a través de la integración de componentes tecnológicos con la finalidad de contar con capacidades adicionales especializadas en materia de arquitectura empresarial y tecnologías de la información, bajo un modelo operativo de atención a componentes de creación de la PDSNE mediante órdenes de servicio, los componentes son los siguientes:

- Arquitectura e integración de la plataforma.
- Diagnóstico para la inclusión de los sistemas, herramientas y datos actuales.
- Incorporación de herramientas necesarias para el SNE.
- Desarrollo de nuevos sistemas y/o módulos complementarios.

Es importante mencionar que cada orden de servicio puede tener dos clasificaciones, la primera relacionada al componente y subcomponente de creación de la PDSNE que está atendiendo, y la segunda respecto al servicio que se está prestando el cual puede ser desarrollo evolutivo, mejora de aplicaciones y servicios adicionales.

Revisión de los Entregables

Durante las pruebas del grupo auditor, de un universo de 12 órdenes de servicio relacionadas con el desarrollo del Portal del Empleo, fueron revisadas las actividades del ciclo de vida de todas las órdenes, se identificó lo siguiente:

- Se observó que las órdenes no cuentan con todos los elementos definidos en el Anexo Técnico, como son el "*cronograma de las actividades y fechas específicas*", así como los "*perfiles y nombres de los integrantes del equipo, estimaciones de costo y fecha de inicio de atención del servicio*".
- Respecto del cronograma de las actividades y fechas específicas de la revisión de productos, la secretaría manifestó que para las órdenes de servicio (*STPS_OS001_ServiciosUX y STPS_OS001_PSUX_SS001*), sólo elaboró un cronograma de trabajo, en contravención del Anexo Técnico que establece acordar un cronograma específico detallado para cada orden de servicio.
- En relación con el reporte de avance sobre el cumplimiento de obligaciones, se identificó que seis órdenes (50.0%) fueron elaboradas después de los primeros 10 días hábiles del mes posterior a los servicios devengados, adicionalmente, no se cuenta con evidencia de su revisión por parte de la secretaría.

- La solicitud de servicio número "*Diseño_PE_SS001*" asociada a la orden de servicio "*STPS_OS001_ServiciosUX*", se generó después de los primeros cinco días hábiles del mes.

Pruebas de funcionalidad en el Sistema del Portal del Empleo

El grupo auditor realizó pruebas a las características técnicas y funcionales descritas en el Anexo Técnico, Entregables e Historias de usuario con la finalidad de verificar que el Sistema del Portal del Empleo se encontrara operando conforme a dichas funcionalidades; de un total de 71 pruebas realizadas, 23 (32.4%) cumplieron con las funcionalidades, 28 no cumplieron o fueron parciales (39.4%) y en 20 (28.2%) no se acreditó su funcionalidad, el detalle es el siguiente:

- El sistema no permite iniciar sesión con una cuenta de Facebook, Google ni LinkedIn, debido a que no solicita usuario ni contraseña para estas redes sociales.

- Respecto de la búsqueda de vacantes, el sistema no permite utilizar el criterio de salario.

- El sistema del Portal del Empleo no cuenta con una sección denominada "Actualmente tenemos" conforme se indica en la historia de usuario "*HU-BT-HO-SS-005"*, sólo muestra el número de "Ofertas de empleos actuales" y el número de "Candidatos actuales".

- Cuando se realiza una búsqueda de empleo, el sistema despliega una lista de 20 empleos por página y no de 50 como lo indica la historia de usuario "*HU-BT-BU-SS-006*".

- El sistema no cuenta con la opción para ordenar las ofertas de empleo por "experiencia" conforme se indica en la historia de usuario "*HU-BT-BU-SS-006*".

- Se identificó que en la historia de usuario "HU-BT-MP-CS-027" se requería una sección denominada "Expectativa laboral", la cual es diferente a la mostrada en la sección "Acerca de mi CV".

- Durante la consulta o modificación de las secciones "Acerca de mi CV", "Experiencia laboral", "Escolaridad", "Idiomas", "Datos personales", "Domicilio" y "Editar cuenta", el sistema muestra mensajes diferentes de los definidos en la historia de usuario "*HU-BT-MP-CS-027*".

- En la sección de datos personales, no se validan los datos ingresados en los campos "Número" y "Número de teléfono", asimismo, en la sección de "Domicilio" al ingresar el código postal no se precarga la entidad federativa ni el municipio.

- En el menú de "Ofertas de empleo", cuando se realizó el ejercicio de postularse a una oferta de auxiliar de administración, el sistema mostró dos postulaciones en lugar de una.

- En el menú "Notificaciones", las ligas del sistema remiten a la pantalla de inicio del portal en lugar de enviar a la información relacionada con la oferta de trabajo.

- El sistema no tiene habilitada la opción de cookies, que permite dar sugerencias cuando un usuario realiza búsquedas de empleo en el portal, ni la vista de mapa (geolocalización) de las ofertas de empleo.

Las pruebas anteriores se encuentran relacionadas con las 12 órdenes de servicio revisadas del Sistema del Portal del Empleo, no obstante, el portal no se encuentra operando en ambiente productivo, en consecuencia, las actividades para diseñar la experiencia de los usuarios del Portal del Empleo en su versión web y móvil, no han justificado su utilidad ni comprobado el gasto realizado para su construcción, asimismo, se corre el riesgo de que dicho desarrollo se vuelva obsoleto ya que las reglas de operación de la dependencia sufren actualizaciones que pudieran impactar en su diseño, el cual fue terminado en julio del 2020, esto es, desde hace 15 meses a la fecha de publicación del presente informe (octubre 2021).

Respecto de lo anterior, la secretaría manifestó que se continúa trabajando en el Sistema del Portal del Empleo, y que tiene previsto que éste podrá ser puesto en producción al término del contrato el 31 de diciembre de 2021, sin embargo, la secretaría debe aclarar y proporcionar la documentación adicional justificativa y comprobatoria por un monto de 7,158.8 miles de pesos, por concepto del pago de 12 órdenes de servicio relacionadas con el Sistema del Portal del Empleo, debido a que no cumplen con todas las funcionalidades señaladas en la documentación contractual ni se encuentran operando en un ambiente productivo como fue requerido en el Contrato y sus Anexos, con la finalidad de cumplir con el objetivo para la vinculación laboral entre los buscadores de trabajo y empleadores, así como justificar el gasto público erogado.

Lo anterior incumplió los artículos 1o, segundo párrafo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 24, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 7, fracciones I y VI, de la Ley General de Responsabilidades Administrativas; 66, fracciones I y III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; las cláusulas Cuarta "Forma y lugar de pago", Quinta "Pagos en exceso" y Novena "Responsables, supervisión y verificación" del contrato número RF-043-2019 y los apartados "Descripción de la solicitud" y "Justificación" de las Solicitudes de Servicio números "Diseño_PE_SS001", "CORE_SS_001", "PORTAL_SS_001", "PORTAL_SS_002", "MicroS_SS_001", "ValidaciónEmp_001" y "FERIAS_SS_001" del contrato número RF-043-2019.

Metodología para el Desarrollo de Soluciones Tecnológicas

El grupo auditor revisó el nivel de aplicación de la metodología para el desarrollo de soluciones tecnológicas, se identificó lo siguiente:

- No se cuenta con una metodología para el desarrollo de sistemas, los administradores de contratos no tienen referencia de ningún procedimiento para el mantenimiento de software.

- Se carece del análisis del modelo de estimación del costo y recursos humanos requeridos para el desarrollo de software por parte del proveedor, tampoco se tiene evidencia de la revisión por parte de la secretaría, tal como fue establecido en el Anexo Técnico del Contrato.

- Se carece de evidencia para comprobar que las órdenes de trabajo cumplen con los niveles de servicio establecidos en el Contrato.

- No se cuenta con planes para la ejecución de pruebas a los sistemas previo a su liberación al ambiente productivo, tales como estrés, desempeño, integrales, funcionales, entre otras.

- Se carece de evidencia de la aplicación de análisis de vulnerabilidades y revisiones de calidad del código fuente de los desarrollos de software antes de ser liberados al ambiente productivo.

- No se tiene constancia del monitoreo de la infraestructura tecnológica y componentes de software para la operación del Sistema del Portal del Empleo, con la finalidad de estimar el crecimiento conforme a la demanda de la base de datos, procesamiento, transmisión de datos, entre otros.

- No se proporcionó documentación que acredite la implementación de los mecanismos para asegurar la integridad, seguridad y disponibilidad de los sistemas, asimismo, no se cuenta con evidencia de las políticas definidas e implementadas para los respaldos de la información procesada en los sistemas.

- No se tiene un procedimiento para el registro, atención y solución de incidentes, que permita dar seguimiento a los eventos que se presenten en la operación de los desarrollos de software.

- El Sistema del Portal del Empleo no cuenta con bitácoras para detectar accesos no autorizados.

Como resultado de la revisión del desarrollo del Sistema del Portal del Empleo, los principales riesgos por la carencia o la inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la dependencia son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O LA INCONSISTENCIA DE LOS CONTROLES PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS

Factor crítico	Riesgo
Políticas, procedimientos y normas para el desarrollo y operación de los sistemas	No se tiene implementada una metodología de desarrollo de sistemas, tampoco políticas ni procedimientos para el registro, atención y solución de incidentes y problemas, ni para la ejecución de los respaldos de la información procesada en los sistemas; asimismo, se carece de mantenimiento preventivo a los sistemas, así como de un plan de capacidad para el uso del sistema e infraestructura requerida para el correcto desempeño de las aplicaciones; lo anterior genera la falta de control de las actividades durante la operación de los sistemas, además no se cuenta con roles, responsabilidades y tiempos definidos para cada actividad, lo que propicia el riesgo de que se presenten fallas y/o incidentes en los sistemas afectando las operaciones de la dependencia.
Análisis de Vulnerabilidades	La falta de ejecución de un análisis de vulnerabilidades a las solicitudes de desarrollo de sistemas antes de su puesta a producción puede representar un riesgo en la disponibilidad de las funcionalidades de los aplicativos, debido a la falta de protección de los recursos que forman parte del sistema a nivel datos, software, hardware, software de capa intermedia y telecomunicaciones.
Seguridad de la información desde el Diseño de los sistemas	Debido a la falta de controles de seguridad desde el diseño de los sistemas para la protección del código de los aplicativos, se pone en riesgo la integridad, confidencialidad y disponibilidad de la información del sistema, ya que no existen controles que impidan que la información procesada se copie, envíe, transmita o difunda por cualquier medio, con fines distintos al soporte de sus procesos.
Monitoreo de las bitácoras de auditoría de los sistemas	No se cuenta con pistas de auditoría ni bitácoras de transacciones de las bases de datos, por lo que no es posible detectar oportunamente movimientos irregulares o cambios no autorizados, en consecuencia, existe la probabilidad de que usuarios maliciosos puedan ejecutar transacciones no autorizadas que comprometan la integridad de los activos de información sin dejar rastros.

FUENTE: Elaborado con información proporcionada por la STPS y el resultado de las pruebas.

Se concluye que la secretaría debe aclarar y proporcionar documentación adicional justificativa y comprobatoria por un monto de 7,158.8 miles de pesos, por concepto del pago de 12 órdenes de servicio relacionadas con el Sistema del Portal del Empleo, debido a que no cumplen con todas las funcionalidades señaladas en la documentación contractual ni se encuentran operando en un ambiente productivo; adicionalmente, los funcionarios de la secretaría no atendieron las recomendaciones emitidas en el Informe Individual del Resultado de la Fiscalización Superior de la Cuenta Pública 2017 de la auditoría número 405-DE, relativas a implementar mecanismos de control para verificar la calidad del código fuente de los desarrollos de software, así como para la elaboración de políticas, normas y procedimientos para el desarrollo de soluciones tecnológicas; por último, los riesgos más importantes en el desarrollo de sistemas se encuentran en el análisis de vulnerabilidades de los aplicativos antes de su puesta en operación en el ambiente productivo, en la seguridad de la información desde el diseño de los sistemas, así como en el monitoreo de las bitácoras y registros de auditoría.

2020-0-14100-20-0393-01-001 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente políticas, procedimientos y normativas para mejorar el control interno en el desarrollo de soluciones tecnológicas, el análisis de vulnerabilidades de los aplicativos antes de su puesta en operación en el ambiente productivo, el plan de pruebas, la seguridad de la información desde el diseño de los sistemas, el monitoreo de las bitácoras y registros de auditoría, la administración de incidentes y problemas, los niveles de servicio, los respaldos de información, así como en los mantenimientos preventivos a los sistemas, con la finalidad de asegurar que los sistemas sean construidos, probados, instalados y desplegados de manera eficaz y eficiente en el ambiente productivo en beneficio de la Secretaría.

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.

2020-0-14100-20-0393-03-001 **Solicitud de Aclaración**

Para que la Secretaría del Trabajo y Previsión Social aclare y proporcione la documentación adicional justificativa y comprobatoria de 7,158,816.09 pesos (siete millones ciento cincuenta y ocho mil ochocientos dieciséis pesos 09/100 M.N.), por concepto de pago de 12 órdenes de servicio relacionadas con el Sistema del Portal del Empleo, debido a que no cumplen con todas las funcionalidades señaladas en la documentación contractual ni se encuentran operando en ambiente productivo como fue requerido en el contrato número RF-043-2019 Servicios Integrales de Tecnología para la Plataforma Digital del SNE 2019-2021 y sus Anexos; asimismo, la Secretaría manifestó que se continúa trabajando en el Sistema del Portal del Empleo y tiene previsto que éste podrá ser puesto en producción al término del referido contrato el 31 de diciembre de 2021, con la finalidad de cumplir con el objetivo para la vinculación laboral entre los buscadores de trabajo y empleadores, así como para justificar el gasto público erogado, en cumplimiento de lo establecido en los artículos 1o, segundo párrafo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 24 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 7, fracciones I y VI, de la Ley General de Responsabilidades Administrativas; 66, fracciones I y III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, Cláusulas Cuarta "Forma y lugar de pago", Quinta "Pagos en exceso" y Novena "Responsables, supervisión y verificación" del contrato número RF-043-2019; Apartado "Descripción de la solicitud" y "Justificación" de las Solicitudes de Servicio números "Diseño_PE_SS001", "CORE_SS_001", "PORTAL_SS_001", "PORTAL_SS_002", "MicroS_SS_001", "ValidaciónEmp_001", "FERIAS_SS_001" del contrato número RF-043-2019.

2020-9-14115-20-0393-08-001 **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 la Secretaría del Trabajo y Previsión Social 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, respecto del desarrollo de soluciones tecnológicas, omitieron atender las recomendaciones números 2017-0-14100-15-0405-01-003 y 2017-0-14100-15-0405-01-004, emitidas en el Informe Individual de auditoría número 405-DE correspondiente a la Fiscalización Superior de la Cuenta Pública 2017, relativas a implementar mecanismos de control para verificar la calidad del código fuente de los desarrollos de software, así como para la elaboración de políticas, normas y procedimientos para el desarrollo de soluciones tecnológicas, debido a que las deficiencias persisten en la carencia de la metodología para el desarrollo de sistemas, el análisis de vulnerabilidades del código fuente antes de su liberación al ambiente productivo, el plan de pruebas, la administración de incidentes y problemas, el plan de calidad y la gestión del código fuente; lo anterior propicia que los sistemas no cumplan con los requisitos funcionales, que presenten errores de procesamiento, que se entreguen fuera de los tiempos programados, así como la falta de protección contra códigos maliciosos, entre otros, lo cual pone en riesgo la operación de la Plataforma Digital del Servicio Nacional de Empleo, en incumplimiento de la Constitución Política de los Estados Unidos Mexicanos, artículo 134; de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1; de la Ley General de Responsabilidades Administrativas, artículo 7, fracciones I y V, y del Reglamento Interior de la Secretaría del Trabajo y Previsión Social publicado en el Diario Oficial de la Federación el 23 de agosto de 2019, artículo 26, fracciones I, II, IV y V.

3. Contrato número RF-057-2019 "Servicio del centro de atención telefónica para el Servicio Nacional de Empleo, Programa Jóvenes Construyendo el Futuro y Procuraduría de la Defensa del Trabajo (PROFEDET)"

Se analizó la información del contrato número RF-057-2019 celebrado con Wise Interactions, S.A. de C.V., en participación conjunta con Grupo de Tecnología Cibernética, S.A. de C.V., de conformidad con lo dispuesto en los artículos 26, fracción I, 26 Bis, fracción II, 27, 28 fracción I, 29 y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, mediante el procedimiento de Licitación Pública Nacional Electrónica Número LA-014000999-E79-2019, vigente del 25 de noviembre de 2019 al 30 de octubre de 2021, por un monto mínimo de 129,708.5 miles de pesos y monto máximo de 280,400.9 miles de pesos, con objeto del "Servicio para el centro de atención telefónica a usuarios de los servicios de la Secretaría del Trabajo y Previsión Social, para el Servicio Nacional de Empleo, Programa Jóvenes Construyendo el Futuro y para la Procuraduría de la Defensa del Trabajo (PROFEDET)"; con presupuesto de 2020 se realizaron pagos por 49,402.3 miles de pesos, y se determinó lo siguiente:

Alcance del servicio

El servicio consiste en la infraestructura, personal, sistemas, procesos y todos los elementos necesarios para la captación, contención y canalización de llamadas de los usuarios y su enlace con la institución mediante la instalación de los equipos y software requerido para interactuar con el conmutador de llamadas existente en la PROFEDET, así como el registro en el Sistema Integral de Procuración de la Defensa del Trabajo (SIPRODET).

La plataforma tecnológica del centro de contacto deberá contar con la supervisión de los agentes a través de internet, que permita conocer vía remota y en tiempo real los indicadores operativos de las campañas, asimismo, deberá incluir funcionalidades como la respuesta de voz interactiva, distribuidor automático de llamadas, integración del cómputo y la telefonía, servicio de chat, marcación predictiva y progresiva, buzón de voz, servicios de grabación y monitoreo de las llamadas.

Revisión de los Servicios

Para el análisis de los servicios del contrato, el grupo auditor seleccionó la campaña de Jóvenes Construyendo al Futuro la cual fue revisada al 100.0%, se observó lo siguiente:

Entregables

No fueron proporcionados 37 reportes correspondientes al periodo de 2020, cabe señalar que las penalizaciones y deductivas del contrato no consideraron medir el cumplimiento y la calidad de los entregables.

Verificación de los Servicios del Centro de Llamadas

El comportamiento de las llamadas durante el ejercicio de 2020 fue afectado por las actividades de orientación a la población sobre la situación laboral imperante en el país ante la emergencia sanitaria derivada del virus SARS CoV2 (Covid-19), debido a la participación extraordinaria de la secretaría en el Consejo de Salubridad General; lo anterior justificó la disminución de las llamadas telefónicas para la campaña Jóvenes Construyendo el Futuro.

Tiempo de sesión de Agentes

Se realizó el análisis de los reportes mensuales que forman parte de los entregables denominados “Reporte de conectividad de los agentes, con hora de ingreso, tiempo de conexión y desglose por estatus de actividad”, de los cuales se identificó lo siguiente:

- En relación con el reporte denominado “Half Atención y Consultas COVID-19 Consolidado” de abril a septiembre de 2020, se detectó que la diferencia entre la hora de inicio y fin de todas las llamadas es la misma (29 minutos con 59 segundos), sin embargo, este dato no coincide con lo reportado en el campo “Duración Promedio De Conversación” de cada una de las llamadas.

- En marzo y junio de 2020, fueron detectados cuatro agentes que no reportan llamadas recibidas ni contestadas, sin embargo, registran conectividad con un total de 22 horas en sesión.

- El plan de continuidad del negocio donde se definen los procedimientos para gestionar los incidentes en caso de un desastre, con la finalidad de recuperar los servicios en los centros de contacto fue actualizado el 22 de mayo de 2019.

Se identificaron deficiencias en los contratos para establecer deductivas por la falta de calidad en los servicios, en los reportes para asegurar la precisión de las cifras, así como en los planes de continuidad del negocio para recuperar la operación de los procesos de la secretaría.

2020-0-14100-20-0393-01-002 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente procedimientos de control y supervisión para asegurar que los contratos tengan establecidas deductivas por la falta de calidad en los servicios, así como actualizar y probar los planes de continuidad del negocio, con la finalidad de mejorar la calidad de los entregables y tener un óptimo nivel de resiliencia para la continuidad de los procesos de la secretaría en caso de contingencias.

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.

4. Incidente de Seguridad Informática (Ciberataque)

Con el análisis de la información proporcionada por la secretaría relacionada con la gestión de los controles y mecanismos de mitigación efectuados por la dependencia antes, durante y después del ataque cibernético perpetrado en marzo de 2020, 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 de la secretaría en la materia, lo siguiente:

Como resultado del estudio de la documentación, el 7 de marzo de 2020, se presentó un incidente de seguridad informática que afectó inicialmente a la plataforma de servidores virtuales Windows hospedados en la infraestructura de la nube de Azure de Microsoft, y de forma posterior a los equipos de usuario final de la dependencia, mediante conexiones con el protocolo Remote Desktop Protocol (RDP) a los servidores de misión crítica desde fuera de la red con direcciones del protocolo de internet catalogadas como maliciosas, dichos accesos se realizaron mediante una cuenta privilegiada que tenía una contraseña débil, con dicha cuenta comprometida se realizó el borrado de discos duros de los servidores y equipos, cabe señalar que no se identificaron notas de rescate de información ni evidencia de archivos encriptados.

Situación de la infraestructura previo al Ciberataque

- La Dirección de Seguridad de la Información y Comunicaciones (DSIC) de la STPS, administraba los 56 servidores Windows que fueron afectados (40.0% de un total de 140), los cuales contaban con antivirus y no estaban soportados por ningún contrato en el momento en que sucedió el incidente de seguridad; también se identificó que no estaban protegidos por agentes contra las amenazas persistentes avanzadas (APT) ni soluciones para la prevención de pérdida de datos (DLP); no se tiene constancia de que antes del incidente los servidores tenían instaladas las últimas actualizaciones de seguridad (parches).

- La DSIC administraba vía directorio activo a los 131 equipos de usuario final que fueron afectados (2.0% de un total de 6,675), los cuales contaban con antivirus, sistema de prevención de intrusiones (IPS) y protección APT a nivel de red, asimismo, se observó que no tenían instaladas soluciones DLP; no se tienen evidencias de las últimas actualizaciones de seguridad en los equipos de usuario final antes del incidente.

- No se proporcionó evidencia para acreditar que la dependencia realizó pruebas de penetración a sus redes y sistemas de manera previa al incidente de seguridad.

- Respecto a los servidores afectados, se identificó que éstos se encontraban en un esquema de infraestructura como servicio en la nube Azure de Microsoft, el cual se prestaba mediante el contrato número RF-117-2015 y sus convenios modificatorios para el licenciamiento y soporte del software con una vigencia hasta el 31 de diciembre de 2019, de tal manera que la dependencia no contaba con un contrato vigente para los servicios de soporte y mantenimiento de cómputo en la nube durante el ciberataque.

Controles y procedimientos implementados durante el Ciberataque

- Como resultado del estudio de la documentación, el sábado 7 de marzo de 2020, la Junta Federal de Conciliación y Arbitraje (JFCA) reportó a la Dirección de Servicios de Información (DSI) que los sistemas que usaban cotidianamente no estaban disponibles, la DSI identificó que la información que se encontraba en los discos duros de los servidores había sido borrada.

- Se convocó al Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC), para realizar una revisión del funcionamiento de la infraestructura física, y de la que se encontraba en la nube Azure de Microsoft, se identificó en primera instancia que se había perdido información en 45 servidores virtuales (50.0%) de un total de 90, y en 11 servidores físicos “on premise” (22.0%) de un total de 50.

- Como resultado de la pérdida de información en los servidores, de un total de 145 aplicaciones, se identificaron 45 sin afectación (31.0%) y 100 aplicativos afectados

(69.0%), de los cuales 60 fueron afectados de manera directa, 14, indirectamente por el borrado de las bases de datos, y 26, indirectamente por el borrado de otro aplicativo; cabe señalar que las actividades de recuperación comprometieron las evidencias del ciberataque ya que no se tiene evidencia de la implementación de una cadena de custodia para preservarlas.

- Se identificó que en los servidores afectados se hospedaban bases de datos que soportaban el Sistema de Información del Programa de Apoyo al Empleo y Sistema de Información de Movilidad Laboral, entre otras, junto con aplicativos como SharePoint, Sistema para la administración de configuraciones de servidores, estaciones de trabajo y equipos móviles, así como Controladores de dominio, por mencionar algunos, cuya afectación se extendió a las unidades administrativas de la dependencia en los equipos de usuario final.

- Debido al impacto que ocasionó el incidente en los equipos de la Secretaría, mediante el documento "carta-contrato" de fecha 12 de marzo de 2020, Microsoft puso a disposición de la Secretaría el programa ECIF (End Customer Investment Funds), mediante el cual ofreció los servicios de soporte premier sin costo, a fin de realizar un análisis de causa raíz del incidente de seguridad informática.

- Cabe señalar que la falta de un contrato de soporte vigente obedeció a los procedimientos de consolidación de servicios de TIC realizados por la Secretaría de Hacienda y Crédito Público en conjunto con la Coordinación de la Estrategia Digital Nacional, debido a esta situación la dependencia se encontraba en espera de la liberación del contrato marco de licenciamiento de Microsoft.

Controles y procedimientos implementados posterior al Ciberataque

Identificación de los vectores de ataque

- Del análisis causa raíz realizado por Microsoft, se identificaron accesos externos a la red mediante conexiones con el protocolo RDP desde varias direcciones del protocolo de internet maliciosas, a un servidor utilizando una cuenta con privilegios administrativos desde la cual fueron ejecutados comandos de forma remota para el formateo de las unidades de disco duro, afectando de esta manera a la infraestructura tecnológica de la dependencia.

- La Secretaría informó que no fue identificado el tipo de agente de amenazas (corporaciones, estados nacionales, hacktivistas, ciberterroristas, cibercriminales, empleados, entre otros), ni el objetivo del ataque.

Revisión del proceso de ataque generalizado

- Aun cuando la secretaría no tiene las técnicas para identificar los objetivos del ataque, en el reporte de seguridad realizado por Microsoft, se identificó que en los servidores

afectados se instaló un servicio para ejecutar procesos de forma remota en los sistemas.

- La dependencia proporcionó los formatos de incidentes donde como parte del diagnóstico de los servidores, se realizó el monitoreo del estado de la red mediante la plataforma de Azure, donde se indicó que no existen indicios que confirmen que existió sustracción de información de los servidores afectados por el incidente de seguridad.

- Como resultado de las afectaciones por el incidente de seguridad, se tuvo la falta de disponibilidad de los servicios, el borrado de datos de diversos aplicativos, los tiempos adicionales por la recarga de información y digitalización de expedientes, así como los retrasos en los reportes y consultas de información.

Gestión de usuarios de cuentas privilegiadas y genéricas

- El documento denominado "Configuración de política de contraseña en directorio activo" del 4 de junio de 2019, no tiene definidos los roles, responsables ni mecanismos para solicitar las altas, bajas y cambios de las cuentas. Asimismo, se observó que el "Procedimiento para depuración de cuentas administrativas en Directorio Activo" fue implementado después del incidente de seguridad de marzo 2020.

- La dependencia cuenta con procedimientos y políticas para el control de accesos con el mínimo privilegio, no obstante, no se tiene constancia de la implementación de dichas actividades antes del incidente de seguridad.

- No se proporcionó evidencia de los usuarios que tienen asignadas cuentas privilegiadas y genéricas, en donde se validen sus accesos a los sistemas críticos, las actividades que realizan, así como el cumplimiento de las políticas de seguridad institucionales; tampoco de las revisiones programadas de los privilegios de las cuentas antes del incidente de seguridad.

- Se carece de evidencia que permita corroborar que las contraseñas de las cuentas privilegiadas aplican los procedimientos para tener contraseñas robustas, evitar la reutilización de contraseñas, así como establecer un periodo de caducidad de la contraseña con la finalidad de evitar la suplantación de identidad. Cabe señalar que respecto a la cuenta privilegiada que fue vulnerada en el incidente de seguridad, no se proporcionó la carta responsiva del funcionario que la tenía asignada.

Gestión de actualizaciones de seguridad (parches)

- No se tiene constancia del procedimiento para realizar las actualizaciones de seguridad en la infraestructura tecnológica antes del incidente de seguridad.

- Se identificó que antes del incidente los equipos afectados no contaban con actualizaciones de seguridad (parches).

Revisión de las configuraciones de aislamiento y segmentación

- Con relación a los segmentos de red y las redes virtuales (VLAN), la secretaría informó que presentaron afectaciones debido al ciberataque, lo cual impactó en los servidores Windows y equipos de usuario final.

- Posterior al incidente de seguridad, fue implementado un firewall para proteger las aplicaciones web (WAF), además fueron configurados grupos de seguridad de red (NSG) para el bloqueo de los puertos en las máquinas virtuales de Azure.

Análisis de los mecanismos de monitoreo, detección y registro del incidente presentado

- Después del incidente de seguridad, fueron implementadas soluciones para recolectar las bitácoras de actividades dentro de la infraestructura, para el monitoreo de servidores en la nube y físicos, así como para la georeplicación de la infraestructura, entre otras.

Evaluaciones del riesgo

- Durante el ejercicio 2020, no se cuenta con evidencia que acredite la realización de la evaluación del riesgo.

- La secretaría proporcionó la metodología de riesgos, no obstante, no tiene definidas las acciones para realizar la identificación, clasificación y evaluación de los riesgos y amenazas, ni para la determinación del impacto y la probabilidad de ocurrencia sobre los sistemas de la dependencia.

Gestión de la vulnerabilidad

- En relación con el análisis de vulnerabilidades, no se encuentran definidos los roles, responsabilidades, periodos de tiempo y mecanismos de ejecución, entre otros elementos.

- No se tiene evidencia de la remediación de las vulnerabilidades identificadas en la infraestructura tecnológica, de los tiempos ni de los responsables de su resolución.

- Durante el ejercicio 2020, no se realizó el análisis de vulnerabilidades ni pruebas de penetración, derivado de los decretos de austeridad, asimismo, no se presentó el análisis realizado para justificar la falta de detección y resolución de los problemas de seguridad en las redes, infraestructura, aplicaciones, así como para establecer medidas para mitigarlos o eliminarlos.

- En diciembre de 2019 (tres meses antes al incidente de seguridad), un prestador de servicios especializado en seguridad de la información, informó a la dependencia de la existencia de la vulnerabilidad "Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)" en los equipos de la secretaría, misma que se refiere a la posible ejecución remota de código cuando un atacante no autenticado se conecta al sistema de destino mediante el protocolo RDP, sin embargo, la secretaría no realizó ninguna actividad para eliminar, corregir o mitigar dicha vulnerabilidad catalogada como crítica, la cual fue explotada por el hacker para el borrado de los discos duros de los servidores afectados durante el incidente de seguridad.

Investigaciones, retenciones legales y preservación

- El Director General de Asuntos Jurídicos de la secretaría presentó la denuncia correspondiente ante la Fiscalía General de la República, del análisis a la documentación proporcionada con la denuncia de hechos, no se acreditó que los sistemas contaban con mecanismos de seguridad, por lo tanto, aun cuando se presume la participación de al menos un individuo en el incidente de seguridad informática, no se tienen los elementos suficientes para imputar a persona alguna ni para fundar una acusación, por lo tanto, la Fiscalía determinó el no ejercicio de la acción penal.

Análisis forense

- En marzo de 2020, el prestador de los servicios administrados de seguridad de la información realizó el reporte de análisis forense y no identificó que se haya instalado software malicioso en los dispositivos. Cabe señalar que no se tiene constancia de la implementación de la cadena de custodia para preservar las evidencias, asimismo, el análisis causa raíz fue realizado por el proveedor que suministra la plataforma de sistemas que fue atacada, por lo que carece de la debida independencia en su realización.

Recuperación de desastres y planes de continuidad del negocio

- La dependencia no contaba con un plan de continuidad del negocio previamente al ciberataque.

- Respecto de los respaldos de información y copias de seguridad, se proporcionó evidencia de los respaldos históricos con los que contaba la dependencia, no obstante, dichos respaldos no cubrían todo el periodo de marzo de 2019 a marzo de 2020, lo que ocasionó que las actividades de recuperación de información no contaran con toda la información necesaria para volver al objetivo de punto de recuperación de los datos antes del ciberataque.

- En los documentos "Sesiones del ERISC", se asentaron las actividades realizadas por el personal de la DGTI para la recuperación de los servicios afectados, a fin de dar

prioridad a la continuidad operativa de los sistemas y aplicaciones, entre los trabajos realizados se encuentran la recuperación de la información de los equipos afectados, el rescate del código fuente, la restauración de los respaldos para reestablecer la operación de los sistemas de forma manual, la operación de nuevos servidores en la nube de Microsoft Azure, la revisión del servicio de Directorio Activo para identificar cualquier tarea programada no autorizada y usuarios sospechosos, la recuperación de las bases de datos mediante máquinas virtuales con el servicio de SQL server, el proceso de borrado y grabación de la imagen institucional en los equipos de usuario final, así como la evaluación y recuperación de los aplicativos.

Revisión de equipos de usuario final y servidores afectados por el Ciberataque

El grupo auditor revisó el estado de los equipos y servidores afectados por el incidente de seguridad, en lo que respecta al antivirus, actualizaciones de seguridad (parches), respaldos y situación de los equipos (operativo, en cuarentena, no operativo, apagado), de los que se identificó que habían sido recuperados del 10 al 17 de marzo de 2020.

Equipos de Usuario Final afectados

De un universo de 131 equipos de usuario final afectados, se obtuvo una muestra de 45 (equipos de escritorio y laptops) con un nivel del 90.0% de confianza y 10.0% de margen de error, de la cual se detectó lo siguiente:

- Se identificaron 22 equipos (48.8%) en los cuales no fue posible realizar las pruebas, debido a que la STPS informó que no cuenta con una herramienta para administrar dichos equipos y no fue posible ingresar a los mismos debido a que no fueron localizados los usuarios.

- En siete equipos (15.6%) se observó el antivirus y los parches de seguridad actualizados.

- En nueve equipos (20.0%) se detectó que no cuentan con la última versión de las actualizaciones de seguridad liberadas por el fabricante.

- En siete equipos (15.6%) se identificó que no cuentan con antivirus ni parches actualizados.

Servidores afectados

De un universo de 56 servidores afectados, se obtuvo una muestra de 32 con un nivel del 90.0% de confianza y 10.0% de margen de error, de la cual se identificó lo siguiente:

- Se detectó que 21 servidores virtuales (65.6%) se encuentran en la plataforma de Microsoft Azure y 11 (34.4%) corresponden a servidores físicos.

- De los 21 servidores Azure se observa que cuatro (19.0%) fueron apagados porque eran máquinas virtuales de prueba, los restantes 17 (81.0%) se encuentran en operación.

- En los 17 servidores virtuales en operación, se identificó que un servidor (5.9%) tiene instalada la distribución de Linux CentOS sin antivirus ni parches; otro servidor (5.9%) contiene la nómina y no se ingresó remotamente para evitar interrupciones por lo que no se validó el antivirus ni los parches y en otro servidor (5.9%) se verificó el antivirus, parches y copia de seguridad. Los 14 servidores restantes (82.3%) tienen el antivirus actualizado y cuentan con copia de seguridad, sin embargo, no cuentan con la última versión de las actualizaciones de seguridad liberadas por el fabricante.

- Los 11 servidores físicos fueron restaurados, cuentan con una solución antivirus y copia de seguridad, carecen de respaldos y no tienen la última versión de las actualizaciones de seguridad liberadas por el fabricante.

Como resultado de la revisión a los procedimientos relacionados con el ciberataque, los principales riesgos por la carencia o la inconsistencia de los controles y sus consecuencias potenciales para los activos de información de la secretaría son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O LA INCONSISTENCIA DE LOS CONTROLES RELACIONADOS CON EL CIBERATAQUE

Factor Crítico	Riesgo
Gestión de usuarios de cuentas privilegiadas y genéricas	La falta de gestión para la asignación y baja de cuentas, contraseñas débiles sin fecha de caducidad, carencia de monitoreo y trazabilidad en las actividades realizadas por los usuarios propician el riesgo de que los atacantes puedan obtener las credenciales y aprovechar las brechas de seguridad causando afectaciones en la infraestructura y soluciones tecnológicas.
Gestión de actualizaciones de seguridad (parches)	Se carece de la administración de las actualizaciones de seguridad, en consecuencia, los equipos 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 que podría provocar la pérdida de información, denegación del servicio y la interrupción de las operaciones de la secretaría.
Mecanismos de monitoreo, detección y registro de transacciones	La falta de monitoreo de las transacciones dentro y fuera de la organización, aumenta el riesgo de la exfiltración de datos sensibles, asimismo, las deficiencias en el análisis de los registros de auditoría, permite que los atacantes puedan controlar los equipos durante mucho tiempo sin que nadie en la organización tenga conocimiento, lo que les da oportunidad a causar el mayor daño posible a los activos de información.
Evaluaciones del riesgo	La carencia de identificación, evaluación y gestión de riesgos no permite detectar cualquier tipo de vulnerabilidad en los sistemas y redes que pueda potencialmente devenir en pérdida de datos, accesos no autorizados, ruptura de la integridad de la información, ni tomar las medidas para evitarlos o mitigarlos, lo que pone en riesgo la operación de los procesos sustantivos de la dependencia.
Gestión de la vulnerabilidad y pruebas de penetración	Se tienen deficiencias en la remediación de las vulnerabilidades de los sistemas y redes de la dependencia, lo que aumenta el riesgo de fallas e intrusiones que comprometen la integridad, disponibilidad y confidencialidad de la información, asimismo, la carencia de pruebas de penetración impide conocer las brechas en la seguridad y operación de los sistemas, con la finalidad de corregir las fallas y mejorar la capacidad de respuesta ante los incidentes de seguridad informática.

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

Conclusiones

- Antes del ciberataque, los servidores no estaban soportados por ningún contrato ni protegidos por agentes contra las amenazas persistentes avanzadas ni soluciones para la prevención de pérdida de datos, asimismo, los equipos de usuario final no tenían instaladas soluciones para prevenir la exfiltración de datos; los servidores y equipos de usuario final tampoco contaban con las ultimas actualizaciones de seguridad (parches) de los fabricantes.

- La falta de un contrato de soporte en el momento del ciberataque obedeció a los procedimientos de consolidación de servicios de TIC realizados por la Secretaría de Hacienda y Crédito Público en conjunto con la Coordinación de la Estrategia Digital Nacional, debido a esta situación la dependencia se encontraba en espera de la liberación del contrato marco de licenciamiento de Microsoft al momento del incidente de seguridad.

- Se carece de procedimientos para que las contraseñas de las cuentas privilegiadas sean robustas, para evitar la reutilización de contraseñas, así como para establecer un periodo de caducidad con la finalidad de evitar la suplantación de identidad.

- Respecto de los respaldos de información y copias de seguridad, se proporcionó evidencia de los respaldos históricos con los que contaba la dependencia, no obstante, dichos respaldos no cubrían todo el periodo de marzo de 2019 a marzo de 2020, lo que ocasionó que las actividades de recuperación de información no contaran con toda la información necesaria para volver al objetivo de punto de recuperación de los datos antes del ciberataque; asimismo, la dependencia no contaba con un plan de continuidad del negocio para responder ante el ataque cibernético.

- En el análisis causa raíz realizado por Microsoft, se identificaron accesos externos a la red mediante conexiones con el protocolo de escritorio remoto desde varias direcciones del protocolo de internet maliciosas a un servidor, que utilizó una cuenta con privilegios administrativos y contraseña débil desde la cual fueron ejecutados comandos de forma remota para el formateo de las unidades de disco duro de los servidores y equipos, lo que afecto la infraestructura tecnológica de la dependencia.

- El prestador de los servicios administrados de seguridad realizó el reporte de análisis forense, como resultado no identificó que se haya instalado un software malicioso en los dispositivos. Cabe señalar que no se tiene constancia de la implementación de la cadena de custodia para preservar las evidencias, asimismo, el análisis causa raíz fue realizado por el proveedor que suministra la plataforma de sistemas que fue atacada, por lo que carece de la debida independencia en su realización.

- En diciembre de 2019 (tres meses antes del incidente de seguridad), el prestador de servicios especializado en seguridad de la información informó a la dependencia de la existencia de una vulnerabilidad en el protocolo de escritorio remoto en los equipos de la secretaría, la cual se refiere a la posible ejecución remota de código cuando un atacante no autenticado se conecta al sistema de destino mediante el protocolo de escritorio remoto, sin embargo, la secretaría no realizó ninguna actividad para eliminar, corregir o mitigar dicha vulnerabilidad catalogada como crítica, la cual fue explotada por el hacker para el borrado de los discos duros de los servidores afectados durante el incidente de seguridad, lo que propició la falta de disponibilidad de los servicios, la pérdida de activos de información de diversos aplicativos, tiempos adicionales por la recarga de información y digitalización de expedientes, así como interrupciones y retrasos en la operación de la infraestructura y soluciones tecnológicas que soportan los procesos sustantivos de la secretaría.

2020-0-14100-20-0393-01-003 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente políticas, procedimientos y controles que permitan mejorar la administración de usuarios de cuentas privilegiadas y genéricas; la gestión de las actualizaciones de seguridad (parches) en los equipos y servidores de las plataformas Windows, Linux y demás utilizadas por la dependencia; los mecanismos de monitoreo, detección y registro de las transacciones; las evaluaciones del riesgo; la gestión de la vulnerabilidad y pruebas de penetración, así como para la activación del análisis causa raíz y forense con la debida cadena de custodia en los incidentes de seguridad informática, con la finalidad de mitigar el impacto que podría ocasionar un ataque cibernético en la infraestructura, sistemas y operaciones de la secretaría.

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.

2020-9-14115-20-0393-08-002 **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 la Secretaría del Trabajo y Previsión Social 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, respecto de la seguridad de la información y la operación de la infraestructura y soluciones tecnológicas, no cumplieron con sus funciones, lo que ocasionó que los servidores no tuvieran protección contra las amenazas persistentes avanzadas ni prevención de pérdida de datos, falta de actualizaciones de seguridad (parches) en los servidores y equipos de usuario final, carencia de pruebas de penetración a las redes y sistemas, falta de configuración de contraseñas robustas en las cuentas privilegiadas y genéricas, además de no contar con toda la información necesaria para volver al objetivo de

punto de recuperación de los datos previo al ciberataque; asimismo, aun sabiendo de la existencia de la vulnerabilidad que se refiere a la posible ejecución remota de código, cuando un atacante no autenticado se conecta al sistema de destino mediante el protocolo de escritorio remoto catalogada como crítica, no llevaron a cabo ninguna actividad para eliminar, corregir o mitigar dicha vulnerabilidad que fue explotada por el atacante cibernético para el borrado de los discos duros de los servidores afectados durante el incidente de seguridad, lo que causó la interrupción de los procesos críticos de la secretaría, así como la pérdida de activos de información que vulneró la integridad, confidencialidad y disponibilidad de la información de la dependencia, en incumplimiento de la Ley General de Responsabilidades Administrativas, artículo 7, fracciones I y V; del Reglamento Interior de la Secretaría del Trabajo y Previsión Social, publicado en el DOF el 23 de agosto de 2019, artículo 26, fracción X; 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 08 de mayo de 2014, última reforma publicada el 23 de julio de 2018, en sus procesos II.C Administración de la Seguridad de la Información (ASI) y III.D Operación de Controles de Seguridad de la Información y del ERISC (OPEC); del Manual de Organización de Procesos de la Dirección General de Tecnologías de la Información de julio de 2017, apartado Funciones del puesto Dirección de Seguridad de la Información y Comunicaciones.

5. Ciberseguridad y Continuidad de las Operaciones

Del análisis de la información proporcionada por la Secretaría del Trabajo y Previsión Social, relacionada con la administración y operación de los controles de ciberseguridad, vinculados con la infraestructura y soluciones tecnológicas, se revisó de conformidad con los controles para la ciberseguridad y sus mejores prácticas, y con base en las políticas y lineamientos de la dependencia en esta materia.

El objetivo de la auditoría de seguridad cibernética es proporcionar a la dependencia una evaluación de la efectividad de la ciberdefensa, con un enfoque en las acciones fundamentales para asegurar el cumplimiento de los controles de seguridad críticos para una ciberdefensa eficaz de conformidad con las mejores prácticas. El programa de auditoría incluye los procesos de gestión de incidentes, gestión de la configuración, seguridad de redes y servidores, gestión y conciencia de la seguridad, gestión de la continuidad del negocio, gestión de la seguridad de la información, relaciones con terceros y prácticas de gobernanza y gestión de las unidades administrativas y tecnologías de la información.

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 fueron considerados tres niveles, los cuales se obtuvieron de conformidad con el porcentaje alcanzado en la evaluación de los subcontroles con los rangos siguientes: Aceptable (más del 67.0%), Requiere Fortalecer el Control (entre el 33.0% y 67.0%) o Carencia de Control (menos del 33.0%), se observó lo siguiente:

Semáforo de Cumplimiento de los Controles de Ciberseguridad en la Secretaría del Trabajo y Previsión Social (STPS)

durante el ejercicio 2020

Control	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2020																				

Aceptable.

Requiere Fortalecer el Control.

Carencia de Control.

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

El detalle de las observaciones y hallazgos de cada uno de los controles de seguridad críticos es el siguiente:

CSC Control 1: Inventario de dispositivos autorizados y no autorizados

Evaluación del Control 1 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Inventario de dispositivos autorizados y no autorizados	**8**	1	2	5	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se cuenta con una herramienta institucional para el descubrimiento activo y pasivo de los equipos conectados en la red.

- Los equipos sin autorización no son eliminados ni puestos en cuarentena, aun cuando las interfaces de los conmutadores se encuentran deshabilitadas, no se tiene evidencia de la actualización automática del inventario.

Por lo anterior, no se cumple en su totalidad 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 de software autorizados y no autorizados

Evaluación del Control 2 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Inventario de software autorizados y no autorizados	**10**	5	-	5	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se cuenta con una herramienta automatizada para mantener el inventario de software actualizado, ni con un inventario del software en operación.
- Debido a que no se cuenta con una herramienta para el inventario de software, no se encuentra vinculada al inventario de activos de hardware.
- No se cuenta con sistemas que aíslen de manera lógica y física a las aplicaciones sensibles en la operación de la secretaría.

Por lo antes señalado, no se cumple en su totalidad 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 - Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

Evaluación del Control 3 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	**5**	1	1	3	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se proporcionó evidencia de las pruebas de la configuración segura en equipos portátiles y de escritorio por parte del proveedor en conjunto con la secretaría.

Por lo anterior, no se cumple en su totalidad 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 4 - Gestión continua de vulnerabilidades

Evaluación del Control 4 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Gestión continua de vulnerabilidades	**7**	5	1	1	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se cuenta con herramientas para el escaneo automatizado de vulnerabilidades.
- Sólo se realizan escaneos perimetrales en los cortafuegos, donde se exponen los hallazgos y las actividades de blindaje recomendadas.
- No se utilizan cuentas dedicadas al escaneo de vulnerabilidades.

Por lo antes señalado, no 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 5 - Uso controlado de privilegios administrativos

Evaluación del Control 5 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Uso controlado de privilegios administrativos	**9**	4	3	2	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se cuenta con herramientas automatizadas para el inventario de las cuentas administrativas, incluidas las cuentas de dominio y locales.
- La política de configuración de contraseñas y acceso de los perfiles en el directorio activo esta actualizada a junio de 2019.

- Los usuarios con acceso a las cuentas administrativas no utilizan equipos dedicados.

- Los sistemas no se encuentran configurados para registrar ni alertar los cambios de los miembros en los grupos administrativos, dichos grupos son administrados manualmente y se le da seguimiento hasta el momento en el que se retiran los privilegios.

- Se tiene una configuración parcial para la entrada de registros y alertas de inicio de sesión fallidos.

Por lo anterior, 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 6 - Mantenimiento, monitoreo y análisis de bitácoras de auditoría

Evaluación del Control 6 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Mantenimiento, monitoreo y análisis de bitácoras de auditoría	**8**	2	3	3	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se proporcionó evidencia de la configuración de las fuentes de tiempo para obtener y comprobar los horarios de sincronización entre los servidores y los dispositivos.

- No se tienen registros de auditoría, sin embargo, se cuenta con herramientas para el monitoreo y alertas de la infraestructura en operación.

- Se carece de registros detallados de las transacciones de las aplicaciones críticas.

- No se tiene implementada una herramienta para la Gestión de Eventos e Información de Seguridad (SIEM).

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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Protección de correo electrónico y navegador web	**10**	5	-	5	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se tienen deshabilitadas las interfaces (plug in) innecesarias de navegadores o clientes de correo electrónico.
- No se cuenta con límites para el uso de lenguajes de scripts en navegadores web ni en clientes de correo electrónico.
- Se carece de servicios de filtrado para el sistema de nombres de dominio (DNS) para bloquear el acceso a dominios maliciosos.
- La última versión del procedimiento para el bloqueo de correo basura (spam) es del ejercicio de 2018.
- No se aplican técnicas para crear un entorno dedicado para analizar, comprender y actuar sobre amenazas que no han sido detectadas por las medidas de seguridad convencionales (sandboxing).

Por lo anterior, no se cumple en su totalidad 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 código malicioso (malware)

Evaluación del Control 8 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Defensa contra malware	**8**	1	3	4	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- Las estaciones de trabajo no cuentan con soluciones para la prevención de pérdida de datos (DLP), los servidores no tienen agentes contra las amenazas persistentes avanzadas (APT) ni para soluciones DLP.

- Se carece de mecanismos para evitar la explotación de vulnerabilidades (prevención de ejecución de datos, diseño de espacio de direcciones, entre otras).

- No se cuenta con la configuración para evitar la ejecución automática del contenido de medios extraíbles.

- No se tienen procedimientos para la centralización y evaluación de los registros antimalware.

Por lo antes señalado, no se cumple en su totalidad con el objeto de controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar 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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Limitación y control de puertos de red, protocolos y servicios	**5**	1	3	1	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se realizan escaneos automáticos de puertos.

- La implementación de listas de reglas de seguridad para permitir o denegar el tráfico de red a los recursos conectados, no es proporcionada por todos los proveedores implicados en la operación de las redes.

Por lo anterior, no se cumple 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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Capacidad de recuperación de datos	**5**	1	-	4	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- Se tiene en operación el procedimiento de respaldos de infraestructura tecnológica.
- La dependencia manifestó que se aseguran de que los respaldos se encuentren completos con alertas por correo electrónico, no obstante, se detectó durante el periodo de marzo de 2019 a marzo de 2020, que no se tenían todos los respaldos para recuperar los servicios afectados por el ciberataque.

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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	**7**	-	2	5	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- Se cuenta con reglas de configuración de tráfico de los cortafuegos (firewalls).
- Se tiene aprobada la configuración de los equipos de red con alertas para las posibles desviaciones.
- Se encuentra en proceso de implementación la versión estable en los equipos de red.
- Se cuenta con sesiones cifradas para gestionar a los equipos de red.

- Se tienen perfiles y segmentos de red dedicados para las tareas administrativas.

Por lo anterior, 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 exploten servicios y configuraciones vulnerables.

CSC Control 12 - Defensa del perímetro (borde)

Evaluación del Control 12 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Defensa de borde	**12**	6	3	3	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se realizan escaneos de conexiones no autorizadas en los firewalls de la dependencia.

- No se configuran los sistemas de monitoreo para registrar los paquetes de red que pasan a través del límite en cada uno de los bordes de la red.

- No se encuentran implementados sistemas de detección de intrusos (IDS) basados en la red.

- Como consecuencia del recorte de presupuesto no se cuenta con sistemas de prevención de intrusos (IPS).

- No se cuenta con herramientas para realizar el análisis del flujo de datos en las redes.

- No se tienen mecanismos para descifrar el tráfico de red del servidor intermediario entre las conexiones de un cliente y un servidor de destino (Proxy) antes de analizar los contenidos.

- No se proporcionó evidencia de la autenticación multifactor para verificar el origen de las configuraciones.

Por lo anterior, no se cumple 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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Protección de datos	**9**	6	1	2	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- La clasificación de la información sensible no está definida con base en su impacto, sólo depende del grado de prioridad que puede ser alto, medio o bajo.
- No se proporcionó evidencia de la herramienta para monitorear y bloquear el tráfico de red no autorizado.
- No se realiza el monitoreo y detección de cualquier uso no autorizado de cifrado.
- No se tiene implementado el cifrado de discos duros de los dispositivos móviles.
- No se administran los dispositivos USB ni son bloqueados los puertos que ocupan en los equipos de cómputo.
- No se cuenta con ninguna configuración de lectura ni escritura de los sistemas para los medios removibles externos.
- Se carece de cifrado de la información compartida de USB a equipo y viceversa.

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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Bandera de cumplimiento de Control
Control de acceso basado en la necesidad de conocer	**9**	3	-	6	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se realizan pruebas al flujo de información mediante herramientas de análisis de vulnerabilidades.

- No se tiene segmentada la red con base en su nivel de sensibilidad.

- Se carece de herramientas automatizadas para el control de acceso a datos.

- Debido a la falta de la herramienta SIEM, no se imponen registros detallados para el cambio de datos sensibles.

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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Control de acceso inalámbrico	**10**	3	-	7	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- Se tiene el inventario de puntos de acceso inalámbrico autorizados.

- Se cuenta con herramientas de exploración de vulnerabilidades para detectar puntos de acceso inalámbricos no autorizados conectados a la red cableada.

- No se encuentran deshabilitados los accesos inalámbricos en los dispositivos.

- El manual de usuario de autenticación multifactor con última versión en 2018 no considera a la autenticación inalámbrica.

- La red inalámbrica se encuentra separada para dispositivos personales y equipos no confiables.

Por lo anterior, se cumple 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 - Monitoreo y control de cuentas

Evaluación del Control 16 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Monitoreo y control de cuentas	**13**	5	2	6	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- El manual de usuario de autenticación multifactor con última versión en 2018 no considera la autenticación para sistemas administrados localmente o por un tercero.
- No se cuenta con un inventario de cuentas organizadas por tipos de autenticación.
- Las cuentas no tienen fecha de vencimiento ni se deshabilitan automáticamente las cuentas inactivas, son desactivadas de manera manual.
- No existe un procedimiento para bloqueo de sesiones.
- No son monitoreados los intentos de acceso a las cuentas desactivadas.
- No se generan alertas por las desviaciones en el comportamiento de inicio de sesión de cuentas.

Por lo antes señalado, no se cumple en su totalidad 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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Implementar un programa de concientización y entrenamiento de seguridad	**9**	5	2	2	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se llevan a cabo análisis de brechas de las habilidades de los servidores públicos en materia de seguridad de la información.

- La capacitación sólo fue para la administración de las herramientas de seguridad de la información.

- Se tiene constancia de una sola campaña de concientización enviada mediante correo electrónico denominada "Recomendaciones de correo no deseado".

Por lo anterior, no se cumple 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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Seguridad del software de aplicación	**11**	4	1	6	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se proporcionaron evidencias para verificar los distintos tipos de pruebas aplicadas a los desarrollos de sistemas (estrés, desempeño, integrales, funcionales, usuario final, entre otras).

- No se utilizan algoritmos de cifrado ampliamente revisados y estandarizados.

- No se realiza el análisis de vulnerabilidades del software antes de su puesta en marcha en el ambiente productivo.

- No se utilizan plantillas de configuración estándar para endurecer la configuración de seguridad de las bases de datos.

Por lo antes señalado, no se cumple en su totalidad 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

Evaluación del Control 19 de Ciberseguridad en la STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Bandera de cumplimiento de Control
Respuesta y manejo de incidentes	**8**	2	1	5	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- La última actualización del documento de integración y operación del grupo estratégico de seguridad de la información fue en julio de 2019.

- No se cuenta con un sitio donde se publique la información relacionada con las notificaciones de anomalías e incidentes.

- No se planifican ejercicios ni escenarios rutinarios de respuesta a incidentes para mantener la conciencia en la respuesta a las amenazas.

- Se carece de evidencia documental de la implementación del esquema de priorización y puntuación de incidentes.

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 STPS

Control	Sub-Controles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Pruebas de penetración y ejercicios de equipo rojo	**8**	8	-	-	

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social.

- No se cuenta con un programa de pruebas de penetración a la infraestructura y soluciones tecnológicas.

- No se llevaron a cabo pruebas de penetración ni hackeo ético durante el ejercicio 2020.

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

Continuidad de las Operaciones

- En el procedimiento de operación para la continuidad del servicio ante contingencias en las aplicaciones y base de datos, no se tiene el inventario de los activos de información que se encuentran asociados al Plan de Recuperación en caso de Desastres (DRP).

- No se tiene evidencia de pruebas al DRP con la remediación de las incidencias detectadas, ni ajustes realizados a los aplicativos e infraestructura tecnológica.

- Se carece de un Plan de Continuidad de Negocio (BCP).

Como resultado de la revisión de los controles y procedimientos para la ciberseguridad, los principales riesgos por la carencia de los controles y sus consecuencias potenciales para las operaciones y activos de información de la secretaría son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE CIBERSEGURIDAD

Factor Crítico	Riesgo
Gestión continua de vulnerabilidades	Las deficiencias en la gestión de vulnerabilidades dificultan la evaluación continua de la información para identificar y remediar las vulnerabilidades, a fin de minimizar la ventana de oportunidad para los atacantes.
Uso controlado de privilegios administrativos	La falta de control de los privilegios administrativos propicia 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.
Limitación y control de puertos de red, protocolos y servicios	Las carencias en la gestión de los puertos no permiten conocer el uso operacional continuo de puertos, protocolos y servicios en los dispositivos en red, con la finalidad de minimizar las vulnerabilidades que se pueden aprovechar para acceder ilegalmente a las redes y sistemas.
Defensa del perímetro	Las deficiencias en la defensa del perímetro complican la detección y corrección del flujo de información que transfieren las redes de diferentes niveles de confianza para mitigar los eventos con un enfoque en datos que dañan la seguridad.
Protección de datos	La falta de cumplimiento de las políticas y procedimientos para la protección de datos dificulta la prevención y mitigación de la exfiltración de datos, con el fin de asegurar la privacidad e integridad de la información sensible.
Implementar un programa de concientización y entrenamiento de seguridad	La carencia de un programa y entrenamiento en seguridad de la información dificulta la identificación de los conocimientos, habilidades y capacidades para soportar la ciberdefensa de la dependencia, así como el desarrollo de un plan para fortalecer la seguridad mediante la capacitación y programas de concienciación.
Pruebas de penetración	La falta de pruebas de penetración impide probar la fortaleza general de la ciberdefensa de la secretaría (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

FUENTE: Elaborado con información proporcionada por la Secretaría del Trabajo y Previsión Social y las pruebas del grupo auditor.

Se concluye que los funcionarios públicos de la secretaría no atendieron las recomendaciones emitidas en el Informe Individual del Resultado de la Fiscalización Superior de la Cuenta Pública 2017, en la auditoría número 405-DE, para implementar las recertificaciones de accesos; el manejo de cuentas con privilegios especiales; las políticas para la composición y tiempo de vida de las contraseñas de los aplicativos, sistemas operativos y equipos de infraestructura tecnológica; el uso de protocolos de cifrado para las conexiones con terceros; la supervisión continua de las actividades de los proveedores; la configuración de las herramientas de filtrado para evitar accesos no autorizados, así como la ejecución de un análisis de vulnerabilidades al código fuente antes de su liberación al ambiente productivo; debido a las deficiencias que persisten en los controles: Gestión continua de vulnerabilidades; Uso controlado de privilegios administrativos; Limitación y control de puertos de red, protocolos y servicios; Defensa del perímetro; Protección de datos; Implementación de un programa de concientización y entrenamiento de seguridad, en la ejecución de Pruebas de Penetración a la infraestructura y soluciones tecnológicas.

2020-0-14100-20-0393-01-004 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social fortalezca los procedimientos y controles para la Gestión continua de vulnerabilidades; el Uso controlado de privilegios administrativos; la Limitación y control de puertos de red, protocolos y servicios; la Defensa del perímetro; la Protección de datos; la Implementación de un programa de concientización y entrenamiento de seguridad; así como la ejecución de Pruebas de Penetración a la infraestructura y soluciones tecnológicas; con la finalidad de asegurar el cumplimiento de los objetivos de ciberseguridad para la identificación, protección, detección, respuesta y recuperación de los incidentes 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.

2020-9-14115-20-0393-08-003 **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 la Secretaría del Trabajo y Previsión Social 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, respecto de la seguridad de la información y ciberseguridad, omitieron atender las recomendaciones números 2017-0-14100-15-0405-01-008 y 2017-0-14100-15-0405-01-009, emitidas en el Informe Individual de auditoría número 405-DE de la Fiscalización Superior de la Cuenta Pública 2017, para implementar las recertificaciones de accesos; el manejo de cuentas con privilegios especiales; las políticas para la composición y tiempo de vida de las contraseñas de los aplicativos, sistemas operativos y equipos de infraestructura tecnológica; el uso de protocolos de cifrado para las conexiones con terceros;

la supervisión continua de las actividades de los proveedores; la configuración de las herramientas de filtrado para evitar accesos no autorizados, y la ejecución de un análisis de vulnerabilidades al código fuente antes de su liberación al ambiente productivo; debido a las deficiencias que persisten en los controles: Gestión continua de vulnerabilidades; Uso controlado de privilegios administrativos; Limitación y control de puertos de red, protocolos y servicios; Defensa del perímetro; Protección de datos; Implementación de un programa de concientización y entrenamiento de seguridad, y en la ejecución de Pruebas de Penetración a la infraestructura y soluciones tecnológicas; lo anterior, podría causar un impacto negativo en la integridad, confidencialidad y disponibilidad de los activos de información, así como en la operación de los procesos sustantivos de la secretaría, en incumplimiento de la Ley General de Responsabilidades Administrativas, artículo 7, fracciones I y V; y del Reglamento Interior de la Secretaría del Trabajo y Previsión Social, publicado en el D.O.F. el 23 de agosto de 2019, artículo 26, fracciones II, IV, V, VII, VIII y X; del Manual de Organización y Procesos de la Dirección General de Tecnologías de la Información elaborado en julio 2017, numeral II.5.1; del Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, publicado en el D.O.F. el 08 de mayo de 2014, última reforma publicada el 23 de julio de 2018, Objetivo general del Proceso II.A Administración de Servicios (ADS), Objetivo general del Proceso II.C Administración de la Seguridad de la Información (ASI), y del Manual de Organización de Procesos de la Dirección General de Tecnologías de la Información de la Secretaría del Trabajo y Previsión Social publicado en julio de 2017, Objetivo general del Proceso III.D Operación de Controles de Seguridad de la Información y del ERISC, apartado Funciones del puesto Dirección de Seguridad de la Información y Comunicaciones.

Montos por Aclarar

Se determinaron 7,158,816.09 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 5 resultados, de los cuales, en uno no se detectó irregularidad y los 4 restantes generaron:

4 Recomendaciones, 1 Solicitud de Aclaración y 3 Promociones de Responsabilidad Administrativa Sancionatoria.

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 octubre de 2021, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y 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 se realizaron 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 Secretaría del Trabajo y Previsión Social cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con el contrato para la prestación de Servicios Integrales de Tecnología para la Plataforma Digital del Servicio Nacional de Empleo, la secretaría debe aclarar y proporcionar documentación adicional justificativa y comprobatoria por un monto de 7,158.8 miles de pesos, por concepto del pago de 12 órdenes de servicio relacionadas con el Sistema del Portal del Empleo, debido a que no cumplen con todas las funcionalidades señaladas en la documentación contractual ni se encuentran operando en ambiente productivo; asimismo, los riesgos más importantes en el desarrollo de sistemas se encuentran en el análisis de vulnerabilidades de los aplicativos antes de su puesta en operación en el ambiente productivo, en la seguridad de la información desde el diseño de los sistemas, así como en el monitoreo de las bitácoras y registros de auditoría.

- Respecto del servicio del centro de atención telefónica para el Servicio Nacional de Empleo, Programa Jóvenes Construyendo el Futuro y para la Procuraduría de la Defensa del Trabajo, se identificaron deficiencias en los contratos para establecer deductivas por la falta de calidad en los servicios, en los reportes para asegurar la

precisión de las cifras, y en los planes de continuidad del negocio para recuperar la operación de los procesos de la secretaría.

- Sobre el Incidente de Seguridad Informática (ciberataque) ocurrido el 7 de marzo de 2020, se identificó que antes del ciberataque, los servidores y equipos de usuario final no estaban soportados en ningún contrato ni protegidos con agentes contra las amenazas persistentes avanzadas ni soluciones para la prevención de pérdida de datos, tampoco contaban con las ultimas actualizaciones de seguridad (parches) ni con contraseñas robustas. Los respaldos de datos no cubrían todo el periodo de marzo de 2019 a marzo de 2020, lo que ocasionó que no se contara con toda la información necesaria para volver al objetivo de punto de recuperación de los datos antes del ciberataque, tampoco se contaba con un plan de continuidad del negocio para responder ante el ataque cibernético.

- En diciembre de 2019 (tres meses antes al ciberataque del 7 de marzo de 2020), la dependencia recibió un informe donde se señalaba la existencia de una vulnerabilidad en el protocolo de escritorio remoto en sus equipos, sin embargo, los funcionarios públicos responsables no realizaron ninguna actividad para eliminar, corregir o mitigar dicha vulnerabilidad catalogada como crítica, la cual fue aprovechada por el hacker para el formateo de las unidades de disco duro de los servidores y equipos de usuario final, lo que propició la falta de disponibilidad de los servicios, la pérdida de activos de información de diversos aplicativos, los tiempos adicionales por la recarga de información y digitalización de expedientes, así como las interrupciones y retrasos en la operación de la infraestructura y soluciones tecnológicas que soportan los procesos sustantivos de la secretaría.

- En relación con la Ciberseguridad y Continuidad de las Operaciones, se concluye que los funcionarios públicos de la secretaría no atendieron las recomendaciones emitidas en el Informe Individual del Resultado de la Fiscalización Superior de la Cuenta Pública 2017 en la auditoría número 405-DE, para implementar las recertificaciones de accesos; el manejo de cuentas con privilegios especiales; las políticas para la composición y tiempo de vida de las contraseñas de los aplicativos, sistemas operativos y equipos de infraestructura tecnológica; el uso de protocolos de cifrado para las conexiones con terceros; la supervisión continua de las actividades de los proveedores; la configuración de las herramientas de filtrado para evitar accesos no autorizados, y la ejecución de un análisis de vulnerabilidades al código fuente antes de su liberación al ambiente productivo; debido a las deficiencias que persisten en los controles asociados a la Gestión continua de vulnerabilidades; el Uso controlado de privilegios administrativos; la Limitación y control de puertos de red, protocolos y servicios; la Defensa del perímetro; la Protección de datos; la Implementación de un programa de concientización y entrenamiento de seguridad; así como en la ejecución de Pruebas de Penetración a la infraestructura y soluciones tecnológicas.

Los procedimientos de auditoría aplicados, la evidencia objetiva analizada, así como los resultados obtenidos fundamentan las conclusiones anteriores.

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, tales 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; 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); las políticas de respaldos, replicación de datos, planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros.

Áreas Revisadas

La Dirección General de Tecnologías de la Información adscrita a la Unidad de Administración y Finanzas de la Secretaría del Trabajo y Previsión Social.

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. Constitución Política de los Estados Unidos Mexicanos:

2. Ley Federal de Presupuesto y Responsabilidad Hacendaria:

3. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público:

4. Ley General de Responsabilidades Administrativas:

5. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria:

6. Otras disposiciones de carácter general, específico, estatal o municipal:

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.