AUDITORÍA INTERNA

AREA **TECNOLOGÍAS DE INFORMACIÓN**

INFORME DE AUDITORÍA **DEFINITIVO**

AI-008-2021

EVALUACIÓN DE LOS CONTROLES IMPLEMENTADOS PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DE LOS SERVICIOS DURANTE EL TELETRABAJO

Mayo 2021

AI-008-2021, Evaluación de los controles implementados para garantizar la seguridad de la información y la calidad de los servicios durante el teletrabajo

INDICE

AI-008-2021, Evaluación de los controles implementados para garantizar la seguridad de la información y la calidad de los servicios durante el teletrabajo

RESUMEN EJECUTIVO

¿Qué examinamos?

Se revisó todo el proceso técnico que se llevó a cabo en la implementación del teletrabajo a raíz de la emergencia nacional por la pandemia por COVID-19, dentro de los aspectos evaluados se encuentran:

- *Cumplimiento con las Políticas de la Información.*
- *Pruebas realizadas durante el proceso de configuración*
- *Verificación de que aquellos usuarios que hacen teletrabajo, cuentan con adenda del mismo firmada.*
- *Validación de que los funcionarios que hacen teletrabajo tienen puestos que así lo permiten*
- *Monitoreo de la infraestructura y atención de incidentes*
- *Generación de políticas o procedimientos relacionados a esta modalidad de trabajo.*

Basado en estos puntos se realizó una reunión con el jefe del Área de Tecnologías de Información y Comunicación para conocer desde su punto de vista, toda la labor realizada. Una vez con este se procedieron a efectuar reuniones con el personal del Departamento de Arquitectura y Comunicaciones, que fueron los responsables de configurar todo lo necesario para la implementación del teletrabajo. Sumado a esto, se solicitó al Departamento de Talento Humano la evidencia necesaria para conocer la lista de funcionarios que firmaron la adenda del contrato para realizar teletrabajo. De esta manera se llegó a conocer el detalle del trabajo realizado y los resultados desde el punto de vista técnico de los mismos.

¿Por qué es importante?

Es importante por la cantidad de funcionarios institucionales que actualmente se encuentran en la modalidad de teletrabajo, por lo que los controles internos para su implementación y seguridad a nivel de tecnologías de información juegan un papel primordial para el uso razonable que se le dé a esa modalidad.

¿Qué encontramos?

Tras la aplicación de las pruebas y la revisión de la evidencia, se lograron identificar situaciones que vulneran el sistema de control interno como: Documentación de las pruebas realizadas a la configuración de los equipos de comunicación y firewall institucional, Generación de políticas, instructiva o manual de usuarios relacionados con la modalidad de teletrabajo, Procedimiento para la atención de incidentes que pongan en riesgo la seguridad de la información en los sistemas o equipos de JASEC.

¿Qué sigue?

Para cada uno de los hallazgos identificados, se giran recomendaciones al Jefe de Área Tecnologías de Información y Comunicación, al Encargado de la Seguridad de la Información, Al Encargado de los Equipos de Comunicación, para que se apliquen a más tardar en setiembre 2021.

AI-008-2021, Evaluación de los controles implementados para garantizar la seguridad de la información y la calidad de los servicios durante el teletrabajo

10 de mayo del 2021

1. INTRODUCCIÓN

De acuerdo con lo establecido en los capítulos III de la Norma sobre valoración del riesgo y el V de las Normas sobre sistemas de información de las Normas de Control Interno para el Sector Público; y como respuesta a la aplicación del teletrabajo que se dio el año pasado como respuesta a la pandemia por COVID-19 es que se incluyó en el Plan Anual de Auditoría Interna un estudio sobre el proceso que llevó a cabo el Área de Tecnologías de Información y Comunicación para implementar el teletrabajo, donde se vieron aspectos que van desde la configuración de los equipos, hasta conocer el comportamiento que han tenido al día de hoy tanto los usuarios como la infraestructura involucrada en la prestación del servicio.

Viabilidad

Nº	Aspecto	Calificación	Justificación de la calificación
1	Disponibilidad de los criterios de auditoría	Cumple	JASEC cuenta con normativa interna vinculante para el tema de seguridad de la información, sumado a esto se cuenta con los contratos que fueron firmados por los colaboradores que hacen uso de la modalidad del teletrabajo.
2	Conocimientos y habilidades del equipo de auditoría	Cumple	Todo el equipo de auditoría involucrado en el estudio cuenta con la experiencia y conocimiento suficiente para la ejecución de este estudio
3	Disponibilidad de herramientas técnicas	Cumple	Se cuenta con las herramientas, equipo y técnicas necesarias para llevar a cabo el proceso de auditoría.
4	Disponibilidad de la evidencia (información)	Cumple	Se tiene acceso al SE-Suite, que es el sitio donde se tiene publicada toda la documentación oficial, sumado a esto se cuenta con la anuencia de los auditados para facilitar la evidencia necesaria y solicitada como parte de la ejecución de las pruebas.
5	Nivel de estabilidad del área de examen	Cumple	Si bien la labor de teletrabajo es algo nuevo dentro de la organización, desde hace un tiempo atrás ya JASEC contaba con una comisión que estaba viendo todo lo relacionado con este tema, con el fin de generar la políticas, procedimiento y demás información necesaria para la implementación de esta modalidad de trabajo. Sumado a esto, los aspectos que se van a revisar estuvieron y están a cargo del personal del Área de Tecnologías de Información y Comunicación, la cual cuenta con cerca de 9 años de mantener la misma jefatura y labores en general
Conclusión sobre la viabilidad del Proyecto:		Es viable	

Hipótesis

- El Área de Tecnologías de Información y Comunicación realizó un análisis de vulnerabilidades antes o durante la implementación del teletrabajo.
- Se lleva un monitoreo de la calidad de la conexión que tienen los colaboradores con los servidores de JASEC, para realizar teletrabajo.
- Se llevaron a cabo pruebas de concurrencia para configurar los servidores y VPN, en base a las necesidades de la organización.
- Se generaron las políticas de seguridad necesarias para implementar el teletrabajo en JASEC.

2. OBJETIVOS

2.1. Objetivo General

Identificar que el servicio de teletrabajo se está dando bajo las condiciones y seguridad de la información idónea para la cantidad de funcionarios que se apegaron a esta posibilidad.

2.2. Objetivos Específicos

2.2..1. Validar que el Área de Tecnologías de Información y Comunicación implementó las medidas de seguridad necesarias para cumplir con lo indicado en los documentos PATI-PR1-NR2 Política de Seguridad Informática y PATI.PR1.NR5 Marco normativo de la política de seguridad informática.

2.2..2. Comprobar que se lleva un monitoreo de la calidad de los enlaces VPN e incidentes de seguridad de la información que se pueden presentar con los colaboradores en teletrabajo.

2.2..3. Validar la existencia de pruebas de concurrencia para configurar los servidores y VPN, en base a la necesidad de la organización.

2.2..4. Comprobar que se generaron las políticas de seguridad necesarias para implementar el teletrabajo en JASEC

3. ALCANCE

3.1. Proceso Administrativo analizado

Las siguientes son las actividades del proceso administrativo analizado durante el proyecto:

- Disposición de la infraestructura administrativa
  - Ejecución de la disposición de la infraestructura administrativa
  - Revisión del estado y obsolescencia de la infraestructura administrativa
- Planificación de las necesidades de infraestructura administrativa
  - Diagnosticó de la infraestructura administrativa
  - Programación del mantenimiento preventivo, sustitución, mejora y servicios asociados de la infraestructura administrativa

3.2. Periodo de Ejecución

El estudio de auditoría se inició en el mes de enero y finalizó en abril del año 2021. El periodo evaluado durante su ejecución comprendió los meses de van de Enero 2020 a Abril del 2021.

3.3. Fuentes de Criterios

Para la formulación de los criterios a evaluar se tomaron las siguientes fuentes:

- PATI.PR1.NR2 Política de Seguridad de la Información v1 del 31/05/2019
- PATI.PR1.NR5 Marco Normativo de la Política de Seguridad de la Información, v 01 del 20/09/2019
- PATI.PR2.NR2 Políticas y estándares para la función informática, v 01 del 13/03/2020

3.4.Metodología

El presente estudio se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público y las Normas para el Ejercicio de la Auditoría Interna para el Sector Público, ambas emitidas por la Contraloría General de la República, y según lo respaldan los resultados del Programa de aseguramiento y mejora de la calidad de la actividad de esta Auditoría.

Para lo anterior se aplicó la metodología para proyectos de aseguramiento de control interno de la Auditoría Interna de JASEC, la cual contempla 3 actividades, a saber:

Actividad I- Planificación
Actividad II-Examen
Actividad III-Comunicación de Resultados

4. COMUNICACIÓN PRELIMINAR

El informe de auditoría en borrador fue remitido a la Administración Activa mediante el oficio AUDI-170-2021 el 30 de abril del 2021, en el cual se expuso los resultados y recomendaciones producto de este estudio, mismos fueron discutidos verbalmente el 7 de mayo del 2021; con Lic. José Pablo Salas Ramírez, Ing. Guillermo Gómez Tenorio, Ing. Eddy Martínez Picado, Ing. Norman Molina Castillo y Lic. Esteban Carmona Loría. Durante la presentación se tomó la decisión de anotar todas las observaciones hechas por los participantes en la minuta para que se atendieran de una vez en el informe definitivo y así la administración no haría uso de los 10 días para para la presentación de observaciones.

5. CONCLUSIONES

Basados en el alcance indicado, así como en los resultados de las pruebas de auditoría se concluye lo siguiente para cada uno de los objetivos del estudio:

Qué si bien el Área de Tecnologías de Información y Comunicación tomó medidas para asegurar la seguridad de la información para la modalidad de teletrabajo, hay algunos temas donde se podría mejorar, como en la documentación de manuales de usuarios para facilitar el uso de los sistemas que se involucran en el proceso. Así como generar los controles necesarios para asegurar la información que los funcionarios necesitan llevar a sus casas como parte de esta modalidad de trabajo. Además, se considera importante que se complemente con documentación todo el proceso realizado para configurar y probar los equipos de comunicación que permiten la conexión remota de los funcionarios.

En lo que respecta al primer objetivo específico, se identificó que no se generó ningún tipo de control para la salida de información oficial de JASEC, ya sea en forma física o por medio de dispositivos tecnológicos como CD's, DVD's o discos

duros. En cuanto a la configuración realizada a nivel del firewall JASEC permite que se cumplan con el resto de lineamientos indicados en los documentos PATI.PR1.NR2 y PATI.PR1.NR5

Para el segundo objetivo específico, se constató que el Departamento de Arquitectura y Comunicaciones no cuenta con un procedimiento detallado de las labores que se deben seguir cuando se da una violación a la seguridad en los sistemas de información; esto porque actualmente lo que se tienen son lineamentos muy generales sobre este tema, dentro de la Política de Seguridad de la Información y el Marco Normativo de la Política de Seguridad de la Información. Adicionalmente se comprobó que se cuenta con herramientas que permiten monitorear el estado de la red y los servidores, para identificar fallos o problemas con prontitud.

En cuanto al tercer objetivo específico, se tiene que no se documentan las pruebas técnicas realizadas por el personal del Departamento de Arquitectura y Comunicaciones como parte del proceso de parametrización de los equipos para la implementación del teletrabajo.

Por otra parte, en el cuarto objetivo específico, se determinó que los únicos lineamientos relacionados con el teletrabajo son los indicados en la adenda del contrato que se hizo a los funcionarios que laboran mediante esta modalidad, fuera de ello, no se generó ningún otro tipo de control, política o manual de usuario para este fin.

Tabla I
Criterios evaluados para el estudio AI-008-2021

#	OBJETIVO	RESULTADO DE LA EVALUACIÓN	PORCENTAJE DE CRITERIOS EVALUADOS POR NIVEL DE CUMPLIMIENTO PARA CADA OBJETIVO		
			Implementada	No Implementada	No Evaluado
1	Validar que el Área Tecnologías de Información y Comunicación implementó las medidas de seguridad necesarias para cumplir con lo indicado en los documentos PATI.PR1.NR2 Política de Seguridad Informática y PATI.PR1.NR5 Marco Normativo de la Política de Seguridad Informática	No Satisfactorio	75%	25%	0%
2	Comprobar que se lleva un monitoreo de la calidad de los enlaces VPN e incidentes de la información que se pueden presentar con los colaboradores en teletrabajo.	No Satisfactorio	75%	25%	0%
3	Validar la existencia de pruebas de concurrencia para configurar los servidores y VPN, en base a las necesidades de la organización.	No Satisfactorio	50%	50%	0%
4	Comprobar que se generaron las políticas de seguridad necesarias para implementar el teletrabajo en JASEC.	No Satisfactorio	0%	100%	0%

Fuente: Formulario F-EJE-043 Programa específico

6. RESULTADOS

Durante el desarrollo de los objetivos específicos del presente estudio y de conformidad con el alcance del mismo, se obtuvo resultados que de acuerdo con sus características se clasificaron en "*Aspectos Susceptibles de Mejora*", los cuales se mencionan a continuación:

6.1. Aspectos susceptibles de mejora

6.1.1 OBJETIVO ESPECÍFICO Nº1

Hallazgo: *Criterio N°3 "Se definieron lineamientos para los casos en los cuales los colaboradores necesiten llevarse documentos, discos duros, DVD's, etc.; a sus casas para desarrollar sus labores"*

De las consultas efectuadas al Jefe del Área de Tecnologías de Información y Comunicación y al Encargado de Seguridad de la Información, se identificó que tras la implementación del teletrabajo hace aproximadamente un año, no se ha generado ningún lineamiento, política o procedimiento para llevar un control sobre los documentos o medios de almacenamiento como los discos duros, CD's o DVD's; cuando los colaboradores necesitan sacar de las instalaciones de JASEC información para el trabajo de manera remota.

Hasta el momento el único control aplicado fue al inicio del proceso de implementación, cuando el Encargado de Seguridad de la Información consultó si algún funcionario iba a retirar algún medio de almacenamiento de las instalaciones para su casa, control que no se realizó más.

Luego de este control, el personal encargado de la seguridad de la información de JASEC indicó que no vio la necesidad de aplicar o definir algún tipo de control relacionado con la información física o digital que estuviera en discos duros, CD's o DVD's. Esto en parte porque todo el proceso se tuvo que llevar a cabo muy rápido que no permitió que se tomara en cuenta este aspecto; y además porque al día de hoy no se ha presentado ningún incidente relacionado con este tipo de información.

El riesgo que se presenta con esta situación es la pérdida o robo de la información que tiene el funcionario en su poder fuera de las oficinas, la cual es confidencial y podría afectar el negocio o hasta ser utilizada en perjuicio de JASEC, la cual, según las políticas de seguridad de la información, debe estar debidamente resguardada.

Recomendación

Al Jefe del Área de Tecnologías de Información y Comunicación se le recomienda:

6.1.1.1. Definir los lineamientos necesarios para que las jefaturas lleven un control de los medios de almacenamiento como discos duros, llaves mayas, CD's o DVD's; que los funcionarios se lleven a sus hogares para realizar teletrabajo.

Plazo para la implementación: junio, 2021

6.1.1.2 Definir las medidas necesarias de control para evitar que un disco duro, CD o DVD u otro medio electrónico que se pierda pueda ser accesado por una tercera persona.

Plazo para la implementación: agosto, 2021

6.1.2 OBJETIVO ESPECIFICO Nº2

Hallazgo: *Criterio N°8 "Se cuenta con un procedimiento que indique las labores a realizar si se identifica una violación a las políticas de seguridad de la información"*

De la información obtenida con el Encargado de la Seguridad de la Información se identificó que actualmente en la Política de Seguridad de la Información y en el Marco Normativo de la Política de Seguridad de la Información, se establecen los lineamientos que se deben seguir para atender cualquier incidente de seguridad que se pueda presentar en la infraestructura de JASEC, específicamente lo indicado en los procedimientos:

- PATI.PR1.NR2 Política de Seguridad Información, en el artículo N°19 indica:

> *"Todo incidente relacionado con seguridad de la información, deberá ser reportado por medio del Help-Desk cuando sea posible, y por medio de este canalizar a los responsables de resolverlo o administrarlo. Se debe implementar un proceso de administración de conocimiento para aprovechar las experiencias y determinar patrones o tendencias".*

- Y en el PATI.PR1.NR5 Marco Normativo de la Política de Seguridad de la Información, señala en el punto 4.7 Repuesta ante incidentes de Seguridad que:

> *"Una vez que los incidentes fueron reportados a las partes correspondientes, se debe proceder al seguimiento detallado de dichos incidentes, los cuales serán investigados por el Encargado de Seguridad Informática de la organización para determinar la severidad del mismo. Las violaciones de seguridad serán corregidas mediante acciones específicas de la Gerencia General o Subgerencia.*
> *Para el personal contratado y los empleados de la JASEC, la acción disciplinaria que se llevará a cabo será acorde con la severidad del incidente, con base en las conclusiones determinadas por la investigación. Las acciones disciplinarias pueden incluir, pero no limitarse a, la pérdida de privilegios de los recursos del procesamiento de datos, despido de consultores o empleados, cancelación de contratos u otras acciones que se consideren apropiadas. Las acciones disciplinarias serán aplicadas de acuerdo al artículo 308 y siguientes de la Ley General de Administración Pública.*
> *Para los incidentes externos o amenazas, se deben tomar acciones que aseguren que la integridad de la evidencia es mantenida y que de ser necesario se pueda aplicar una adecuada acción legal".*

Identificando que, en ambos casos, lo señalado es muy general y no detalla los pasos necesarios para estandarizar la atención y documentación si se efectúa una violación a las políticas de seguridad.

De las consultas efectuadas al Encargado de Seguridad de la Información, se obtuvo que hasta el momento no se han visto en la necesidad de documentar más el proceso que se debe seguir para atender los incidentes de seguridad de la información, ya que, cuando se presentan él es quien los atiende; y hasta el momento, por la cantidad, tipo de incidentes que se han presentado y la experiencia que tiene para ver este tipo de casos, no se ha visto en la necesidad de detallar más este proceso.

Con esta situación no se garantiza que la atención de los incidentes de seguridad de la información se dé de manera estandarizada para todos los casos, con el riesgo que la información no sea íntegra, completa y razonable, lo que podría provocar daños en la información que se maneja dentro de la red de JASEC.

Además, al no contar con una documentación detallada para la atención de este tipo de incidentes, se está centrando todo el conocimiento del proceso en un solo funcionario, el cual en cualquier momento podría tomar la decisión de irse de JASEC, llevándose consigo todo el conocimiento adquirido que no se documentó.

Recomendación

Al Encargado de la Seguridad de la Información se le recomienda:

6.1.2.1 Elaborar y oficializar un procedimiento detallando los pasos que se deben seguir para notificar, atender y documentar los incidentes de seguridad que se presentan en los sistemas y equipos tecnológicos de JASEC.

Plazo para la implementación: julio, 2021

6.1.3 OBJETIVO ESPECIFICO Nº3

Hallazgo: *Criterio N°9 "Se llevaron a cabo pruebas a las políticas de seguridad definidas en los servidores utilizados para la conexión de teletrabajo, y que las mismas hayan quedado debidamente documentas"*

Producto de la investigación realizada se logró identificar que, en el proceso de implementación del teletrabajo, el personal del Área de Tecnologías de Información y Comunicación definió como medida de seguridad, habilitar en el firewall Fortinet únicamente los puertos: PING, HTTP, HTTPS y TCP81.

Sumado, se limitó el acceso únicamente a los sistemas que los usuarios iban a necesitar, buscando así asegurar que la computadora que el usuario esté usando corresponda a la que tiene asignada en JASEC, accediendo mediante escritorio remoto, la cual es la que tiene todas las medidas de seguridad definidas por el Área Tecnologías de Información.

Sin embargo, durante este proceso de parametrización del firewall, no se documentaron las pruebas realizadas por el personal encargado, para validar que la configuración funcionaba de manera correcta; ya que todo este proceso de implementación se tuvo que hacer a la brevedad posible para poder cumplir con lo estipulado por las entidades gubernamentales.

Al respecto, se le consultó al Encargado de Seguridad de la Información señalando que en este proceso uno de los factores que más impacto tuvo fue el tiempo, porque la implementación del teletrabajo se realizó de manera inmediata, lo que no permitió que todo este proceso de implementación se llevara a cabo con los tiempos necesarios para hacer la documentación de las pruebas y configuraciones necesarias.

De lo anteriormente expuesto, se tiene que la principal consecuencia es la afectación en las labores de los funcionarios que realizan teletrabajo, esto por un fallo en el trabajo realizado, lo que comprometería la continuidad del servicio de JASEC, donde no se podrán atender a los clientes ni realizar los procesos internos de la institución.

Sumado a esto, al no haber documentado el proceso de configuración que se siguió, no se cuentan con los insumos necesarios para replicar el trabajo realizado para la implementación del teletrabajo, donde incluso se podrían cometer los mismos errores que se han materializado.

Recomendación

Al Encargado de la Seguridad de la Información se le recomienda:

6.1.3.1 Documentar todo el proceso de configuración del firewall y demás equipos que fueron necesarios para poder implementar el teletrabajo en JASEC.

6.1.3.2 Hacer y documentar una sesión de pruebas para validar que la configuración realizada al firewall es suficiente para cumplir con las medidas de seguridad de la información definidas por la organización en los documentos PATI.PR1.NR2 y PATI.PR1.NR5.

Plazo para la implementación: setiembre, 2021

Hallazgo: *Criterio N°10 "Se llevaron a cabo pruebas de concurrencia para asegurar que la configuración de los servidores utilizados en la conexión de teletrabajo responde a las necesidades de la organización"*

Se identificó que como medida para soportar la cantidad de conexiones que se iban a dar por medio de VPN, se amplió el ancho de banda del internet de JASEC, dada la urgencia de implementar el teletrabajo se hicieron las pruebas en caliente conforme se iban firmando los contratos, ya que cada vez más funcionarios se iban conectando bajo esta modalidad de trabajo, sin embargo, estas pruebas, y la configuración de los equipos de comunicación no quedaron documentadas.

Sobre el particular, el criterio brindado por el Encargado de Administrar los Equipos de Comunicación, que uno de los factores que más impacto tuvo fue el tiempo, porque la implementación del teletrabajo se realizó de manera inmediata, dada la situación de pandemia, lo que no permitió que todo el proceso de implementación se llevara a cabo en los tiempos necesarios para hacer la documentación de las pruebas y configuraciones necesarias.

Al no contar con evidencia de que las medidas tomadas en el momento funcionaron de manera correcta, tiene el riesgo de afectar a JASEC cuando se necesite replicar y conocer el trabajo realizado, ya que toda la experiencia ganada está en el personal que se involucró en el proceso, y se perdería si decidieran salir de la institución.

Sumado a esto, se tiene la afectación a las labores prestadas por los funcionarios de la institución, ya que ante un fallo se vería comprometida la continuidad de los servicios, afectando directamente a los clientes tanto en la atención de los mismos, como en el disfrute de los servicios de Energía e Infocomunicaciones.

Recomendación

Al Encargado de los equipos de comunicación se le recomienda:

6.1.3.3 Documentar toda la configuración y medidas que se tomaron sobre los equipos de comunicación para poder implementar el teletrabajo en JASEC.

6.1.3.4 Hacer y documentar una sesión de pruebas de concurrencia y saturación de la red para validar las medidas tomadas sobre los equipos de comunicación de JASEC a la hora de implementar el teletrabajo.

Plazo para la implementación: setiembre, 2021

6.1.4 OBJETIVO ESPECIFICO Nº4

Hallazgo: *Criterio N°11 "Comprobar que se hayan generado las políticas y procedimientos necesarios para hacer frente al teletrabajo"*

En relación a las políticas y procedimiento se logró identificar que no se generó nueva documentación (políticas, procedimientos, manuales, etc.) vinculada a la modalidad de teletrabajo.

Sobre este tema el Jefe del Área de Tecnologías de Información y Comunicación acota que cuando se implementó la modalidad de teletrabajo lo que se hizo fue ampliarles a más funcionarios la oportunidad de conectarse a los sistemas y equipos de JASEC mediante una conexión VPN, que era un aspecto que ya utilizaban los compañeros que se encargan de las labores de soporte técnico.

Durante el proceso de implementación el personal del Área encargado de la configuración de los equipos se centró únicamente en las labores técnicas, dejando de lado el procedimiento escrito, además, según lo indicado por el Jefe del Área hasta el momento de este estudio no se habían visto con la necesidad de generar algún tipo de documentación adicional relacionada con teletrabajo.

El hecho de no contar con políticas, procedimientos o manuales relacionadas a teletrabajo presenta el riesgo de que los funcionarios que se encuentran laborando en la modalidad de teletrabajo se sientan que están fuera de la "jurisdicción" de la normativa de JASEC, por esta razón es importante aclarar las políticas, procedimientos y manuales que rigen la función realizada desde sus hogares.

Además, al estar utilizando sistemas nuevos para realizar los mismos trabajos, a los funcionarios que efectúan teletrabajo se les presenta una serie de inconvenientes nuevos que les consumen tiempo laboral en atenderlos, muchos de los cuales necesitan la intervención del personal del Área de Tecnologías de Información y Comunicación para remediarlos, de ahí la importancia de documentar buenas prácticas y situaciones que se presentan frecuentemente para tratar de disminuir este tipo de incidentes.

Recomendación

Al Jefe del Área de Tecnologías de Información y Comunicación se le recomienda:

6.1.4.1 Generar un instructivo, manual o procedimiento, con información de medidas, cuidados, mejores prácticas y demás información que pueda ser de utilidad y guía para los colaboradores que están trabajando bajo la modalidad de teletrabajo, el cual debe ser actualizado al menos una vez al año.

Plazo para la implementación: setiembre, 2021

AI-008-2021, Evaluación de los controles implementados para garantizar la seguridad de la información y la calidad de los servicios durante el teletrabajo.

APÉNDICE A

Tabla II

Programa específico de Actividad de Examen AI-008-2021

#	CRITERIO A EVALUAR	ACTIVIDAD DE AUDITORÍA
A.	**OBJETIVO ESPECIFICO: Validar que el Área de Tecnologías de Información y Comunicación implementó las medidas de seguridad necesarias para cumplir con lo indicado en los documentos PATI.PR1.NR2 Política se Seguridad Informática y PATI.PR1.NR5 Marco normativo de la política de seguridad informática**	
1	El Área de Tecnologías de Información revisó que los equipos utilizados para hacer teletrabajo cumplen con lo indicado en los documentos PATI.PR1.NR2 y PATI.PR1.NR5	Hacer una reunión con el Encargado de Seguridad de la Información, para ver las medidas de control tomadas hacia los equipos personales de los colaboradores. Sumado a esto, tomar los documentos PATI.PR1.NR2 y PATI.PR1.NR5 y ver las medidas de seguridad que tienen que cumplir los equipos que se conectan a la red de JASEC para consultar la manera en la cual el personal del Área de Tecnologías de Información y Comunicación se garantiza que dichos equipos cumplen con estos aspectos. Documente esta actividad en la actividad de examen del SAI.
2	Las conexiones de VPN cumplen con las medidas de seguridad indicadas en los documentos PATI.PR1.NR2 y PATI.PR1.NR5	Tomar los documentos PATI.PR1.NR2 y PATI.PR1.NR5 y validar las políticas indicadas para conexiones remotas o de teletrabajo y validar que la configuración actual de los VPNs cumpla con dichos aspectos Documentar esta actividad en la actividad de examen del SAI
3	Se definieron lineamientos para los casos en los cuales los colaboradores necesiten llevarse documentos, discos duros, DVD's, etc.; a sus casas para desarrollar sus labores	Comprobar que se hayan definido y se cumplan políticas para los casos en los cuales los funcionarios que hacen teletrabajo, tienen que llevarse documentación oficial de JASEC a sus hogares Documentar esta actividad en la actividad de examen del SAI
4	Se cuenta con un listado de los funcionarios que tienen habilitada la opción de teletrabajo para revisar que realmente están haciendo uso de dicha modalidad	Solicitar al personal de Talento Humano un listado de todos los funcionarios que tienen permiso de realizar teletrabajo, para luego consultar al Departamento de Gestión de Arquitectura y Comunicaciones el listado de funcionarios que se han conectado a teletrabajo en fechas aleatorias. Documentar esta actividad en la actividad de examen del SAI
B.	**OBJETIVO ESPECIFICO: Comprobar que se lleva un monitoreo de la calidad de los enlaces VPN e incidentes de seguridad de la información que se pueden presentar con los colaboradores en teletrabajo**	
5	El Departamento de Gestión de la Arquitectura y Comunicaciones genera informes periódicos indicando el estado de la red, usuarios conectados y los incidentes de seguridad de la información que se pueden estar presentando en las conexiones.	Solicitar al Departamento de Gestión de Arquitectura y Comunicaciones los informes que se presentaron desde que se inició con el teletrabajo hasta enero del 2021, informando el estado de la red y los incidentes presentados Documente esta actividad en la actividad de examen del SAI.
6	Se cuenta con alguna herramienta o sistema que permita monitorear en tiempo real el estado de los servidores a los cuales se conectan los colaboradores	Revisar en vivo con el personal del Departamento de Gestión de Arquitectura y Comunicación las herramientas que tienen para monitorear el personal que hace teletrabajo, el estado de los servidores y de la red. Documente esta actividad en la actividad de examen del SAI.

AI-008-2021, Evaluación de los controles implementados para garantizar la seguridad de la información y la calidad de los servicios durante el teletrabajo.

#	CRITERIO A EVALUAR	ACTIVIDAD DE AUDITORÍA
7	Se definieron niveles de servicio para los incidentes que presenten los funcionarios que están haciendo teletrabajo.	Validar con el personal del Departamento de Gestión de la Arquitectura y Comunicaciones si se definieron acuerdos de nivel de servicio para luego validar que estos se estén cumpliendo al compararlos contra los informes presentados a la jefatura del Área de Tecnologías de Información y Comunicación. Documente esta actividad en la actividad de examen del SAI.
8	Se cuenta con un procedimiento que indique las labores a realizar si se identifica una violación a las políticas de seguridad de la información	Consultar al personal del Departamento de Gestión de la Arquitectura y Comunicaciones si se cuenta con un procedimiento para la atención de incidentes de seguridad, para luego solicitar una muestra de los que se han presentado desde enero del 2020 hasta enero del 2021, y así ver si a estos se les está dando el seguimiento adecuado. Documentar esta actividad en la actividad de examen del SAI
C. OBJETIVO ESPECIFICO: Validar la existencia de pruebas de concurrencia para configurar los servidores y VPN, en base a las necesidades de la organización		
9	Se llevaron a cabo pruebas a las políticas de seguridad definidas en los servidores utilizados para la conexión de teletrabajo, y que las mismas hayan quedado debidamente documentas	Solicitar al Encargado de la Seguridad de la Información la documentación de las pruebas realizadas a los servidores que se utilizan para el teletrabajo, De igual manera solicitar que se muestren las medidas de seguridad tomadas hasta el día de hoy para salvaguardar la seguridad de la información de los equipos de JASEC. Documente esta actividad en la actividad de examen del SAI.
10	Se llevaron a cabo pruebas de concurrencia para asegurar que la configuración de los servidores utilizados en la conexión de teletrabajo responde a las necesidades de la organización	Solicitar al Encargado de Seguridad de la Información la documentación de las pruebas de concurrencia que se han hecho sobre la conexión y servidores que se utilizan para el teletrabajo. Y ver un ejemplo en vivo de las mismas Documentar esta actividad en la actividad de examen del SAI
D. OBJETIVO ESPECIFICO: Comprobar que se generaron las políticas de seguridad necesarias para implementar el teletrabajo en JASEC		
11	Comprobar que se hayan generado las políticas y procedimientos necesarios para hacer frente al teletrabajo	Solicitar al jefe del Departamento de Gestión de Arquitectura y Comunicación los procedimientos, políticas o reglamentos generados para indicar las reglas que se deben cumplir cuando un funcionario realiza teletrabajo. Una vez con estas, identificar si las mismas están debidamente oficializadas y comunicadas al personal de la organización. Solicitar al jefe del Departamento de Gestión de Arquitectura y Comunicación los procedimientos, políticas o reglamentos generados para indicar las reglas que se deben cumplir cuando un funcionario realiza teletrabajo. Una vez con estas, identificar si las mismas están debidamente oficializadas y comunicadas al personal de la organización. Documente esta actividad en la actividad de examen del SAI.

Fuente: Papel de trabajo F-EJE-043 Programa específico

ÁPENDICE B

Tabla III Análisis de las observaciones recibidas de la administración

N° DE PÁRRAFO	RESULTADO, CONCLUSIÓN O RECOMENDACIÓN DE AI	OBSERVACIÓN DE LA ADMINISTRACIÓN	¿SE ACOGE? (SI, NO, PARCIAL)	JUSTIFICACIÓN AI
6.1.1.1	Recomendación	Consulta el Ing. Guillermo, en la conferencia final, que según lo que se establece en el marco normativo, se indica que el responsable de la información son los propietarios, y son los que deberían velar para que su personal no haga uso indebido de la información que manejan. Por esta razón es muy difícil para el área de TI lo realice igual se pueden establecer políticas o normativa pero no somos los responsables. Agrega el Ing. Eddy Martínez, que TI es el que facilita herramientas para hacer el trabajo más ágil, pero no así el responsable de la información de cada departamento. Considero importante valorar este aspecto. Comenta el Lic. Carmona, que, si es cierto que TI es el facilitador, pero también es el que debe indicar como se deben hacer o que genere algún control, por lo que se considera importante generar algún tipo de lineamiento para este caso en específico. Indica el Ing. Martínez	Si	La recomendación como está redactada incurre a la confusión de parte de los auditados, además de que, con lo comentado por los Ing. Guillermo Gómez y Eddy Martínez se identifica que el control debe llevar un enfoque un poco diferente, ya que el Área de Tecnologías de Información y

AI-008-2021, Evaluación de los controles implementados para garantizar la seguridad de la información y la calidad de los servicios durante el teletrabajo.

		que entonces no se refiere a la información en sí, sino más bien a los controles. También indica el Ing. Gómez que entonces sería transcribir lo que ya está establecido en el marco normativo, y que la información sensitiva se utilice por medio de las carpetas compartidas. Comenta el Lic. Carmona, que le parece importante definir un control que para los funcionarios que van a sacar información de las oficinas y están realizando teletrabajo, se tenga un control. Agrega si les parece que se debe cambiar la redacción de la recomendación para que esté más claro.		Comunicación debe establecer el lineamiento, pero son las jefaturas quienes deben ejecutarlo de manera directa. Y por tal razón se aplica la modificación.

Fuente: F-EJE-081 Análisis de las observaciones recibidas de la Administración