INFORME No. AI-009-2021

AUDITORIA INTERNA

Análisis de las gestiones de la Unidad de Tecnología de Información
para el resguardo y Seguridad de la Información

Setiembre 2021

Estudio No. ATI-007-2021

INDICE DE CONTENIDO

INFORME No. AI-009-2021

I. RESUMEN EJECUTIVO

El presente estudio de Auditoría, *tuvo como propósito analizar la labor de la Unidad Tecnología de Información, durante el período comprendido de junio 2020 a junio 2021, en cuanto a la prevención y detección de ciberataques,* con la finalidad de generar oportunidades de mejora que coadyuven a su fortalecimiento como componente del Sistema de Control Interno.

Entre los aspectos relevantes que afectan el cumplimiento de los objetivos de Control Interno (Artículo No.8 de la Ley General de Control Interno), se tiene:

a. Exigir confiabilidad y oportunidad de la información.

- La política de seguridad de la información establecida para el Instituto Nacional de Vivienda y Urbanismo, así como normativa complementaria de seguridad de información elaborados por la Unidad de Tecnología de Información, requiere la autorización y aprobación ("Revisado por" y el "Aprobado por") por parte de los funcionarios con potestades para concederlas, así como de un medio formal de cambios (control de versiones).

b. Garantizar eficiencia y eficacia de las operaciones.

- En el presupuesto 2021 no se cuenta con suficientes recursos presupuestarios, debido a recortes presupuestarios efectuados, para la contratación de servicios profesionales en efectuar ejercicios de intrusión/hacking ético sobre los sistemas más críticos y con especial atención en aquellos que sean directamente accesibles desde Internet, así como de la plataforma tecnológica.

  Las últimas pruebas de penetración Interna y externa de la infraestructura tecnológica del INVU – situación actual de los riesgos internos y externos de seguridad de la información se realizaron en el 2013 según la *Contratación Directa 2012CD*-000059-01. Sin embargo, la Unidad de Tecnología de Información realiza un testeo de forma diaria.

- Desde octubre 2017, la Auditoría Interna en informe Nº: IA-007-2017 denominado Estudio de cumplimiento de los criterios básicos de control indicados en las normas técnicas para la gestión y el control de las tecnologías de información en el INVU, recomendó la necesidad de elaborarse un plan de continuidad, así como de un plan de contingencias, los cuales se están presupuestando para el 2022.

Con fundamento en lo antes descrito y con el propósito de fortalecer a la Unidad de Tecnología de Información, se formulan las oportunidades de mejora, a las personas funcionarias correspondientes; para que se establezcan las acciones necesarias para solventar oportuna y eficazmente las situaciones descritas anteriormente, de acuerdo a lo establecido en la Ley General de Control Interno Nº 8292.

II. INTRODUCCION

Origen del Estudio

2.1. La Auditoría Interna realiza el presente estudio a fin de analizar las gestiones realizadas por la Unidad de Tecnología de Información en el resguardo y seguridad de la información, con fundamento en el Plan Anual de Trabajo de la Auditoria Interna del año 2021, conocido por los miembros de la Junta Directiva en la Sesión Extraordinaria Nº 6483 del 16 de febrero de 2021.

Objetivo General

2.2. Analizar las gestiones realizadas por la Unidad de TI para el resguardo y Seguridad de la Información.

Objetivos Específicos

2.3. 1. Evaluar las gestiones realizadas por la Unidad de TI para administrar los ataques a la red institucional y a la página web institucional.

2.4. 2. Validar si las acciones que se ejercen en la Unidad de Tecnología de Información, son eficaces y permiten salvaguardar la información ante ataques a la red institucional y a la página web.

Alcance

2.5. El alcance del estudio comprende la revisión de aspectos de control interno y normativos de la Unidad de Tecnología de Información para el periodo comprendido entre junio 2020 y junio 2021, el cual se amplió en aquellos casos en los que se consideró pertinente.

Normativa

2.6. La principal normativa observada en este estudio, fue la siguiente:

- Ley Orgánica del Instituto Nacional de Vivienda y Urbanismo, N° 1788.
- Ley General de la Administración Pública, Nº 6227.
- Ley General de Control Interno, N°8292.
- Normas Técnicas para la Gestión y Control de las Tecnologías de Información (N-2-2007-CO-DFOE)
- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- Normas para el Ejercicio de la Auditoría Interna en el Sector Público, (R-DC-119-2009).
- Normas Generales de Auditoría para el Sector Público (R-DC-064-2014).
- Manual Organizacional del Instituto Nacional de Vivienda y Urbanismo.
- Procedimientos internos.
- Mejores practicas

Metodología

2.7. El presente estudio es realizado de acuerdo con las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, emitidas por la Contraloría General de la República y demás normativa atinente.

Además, la metodología utilizada para el desarrollo de la revisión se enfocó en la aplicación de técnicas y prácticas de auditoría normalmente aceptadas, tales como entrevistas, verificaciones de documentos y al análisis de la normativa legal y técnica aplicable.

Implementación de recomendaciones (Ley General de Control Interno, articulo No. 36).

2.8. Este artículo establece un plazo de 10 días hábiles para que se ordene la implantación de las recomendaciones otorgadas. Si discrepa de éstas, en el transcurso de dicho plazo se debe elevar el informe a la Junta Directiva General, con copia a esta Auditoría, exponiendo por escrito las razones por las cuales objetan las recomendaciones del informe y proponiendo soluciones alternas para los hallazgos detectados.

Limitaciones

2.9. En la ejecución del presente estudio no se presentaron limitaciones.

Comunicación preliminar de los resultados de la Auditoría

2.10. Para la comunicación de las oportunidades de mejora y las recomendaciones que contiene el presente informe, se llevó a cabo una Conferencia de Resultados, el viernes 03 de setiembre del 2021, de forma virtual a través de la plataforma Teams, con las siguientes personas funcionarias: con la señora María Amalia Pessoa Araya, Encargada de la Unidad de Tecnología de Información y los señores Carlos Miranda Mora y Juan Carlos Astúa González, funcionarios de la Unidad de Tecnología de Información. Al respecto se obtuvieron los siguientes resultados:

Una vez realizados los comentarios por parte de las personas funcionarias de la Unidad de Tecnología de Información y aclarados algunos puntos por parte de esta Auditoría Interna, la señora María Amalia Pessoa Araya, manifestó estar de acuerdo con lo indicado en las Oportunidades de Mejora nos. 1 y 2 y las recomendaciones, nos 1, 2 y 3.

En relación con la Oportunidad de Mejora no. 3, las personas funcionarias de la Unidad de Tecnología de Información, externaron varios comentarios, los cuales serán incorporados en el presente informe en lo que corresponda.

III. RESULTADO

3.1 El presente estudio, permitió determinar una serie de elementos que cuentan con sus oportunidades de mejora, en cuanto al control interno de la Unidad de Tecnología de Información. En los apartados siguientes se detallan dichos elementos.

Oportunidad de Mejora No. 1: Política de Seguridad de Información

3.2 Se realizó una verificación a la Gestión de Tecnología de Información[1] específicamente a la seguridad de Información, identificándose que en el documento denominado **Gestión de Elementos de Seguridad Informática** (UTI-SRT-GESI-001 v2.0), se constituyen las políticas de seguridad de la información establecidas para el Instituto Nacional de Vivienda y Urbanismo, asimismo se cuentan con los siguientes documentos como complemento de seguridad de información, según detalle:

a. DI-SRT-PRCU-001 v1.0 (Políticas de restricción y control de usuarios para el uso de microcomputadoras)
b. UTI-SRT-PACCS-002 V2.0 (Política para el acceso a los cuartos de comunicaciones y servidores)
c. UTI-SRT-PAUC-002 V2.0 (Política para la administración de usuarios y contraseñas)
d. UTI-SRT-PRAU-008 V3.1 (políticas para el respaldo de archivos para los usuarios)
e. UTI-SRT-PRRD-009 V3.1 (Políticas para el respaldo y recuperación de datos)
f. UTI-SRT-PRAE-007 V2.0 (Política de restricción aplicadas a los equipos)
g. UTI-SRT-PEC-001 V1.0 (Política para el uso de los equipos de cómputo)
h. UTI-SRT-PDM-004 V2.0 (Política para el uso de dispositivos móviles)
i. UTI-SRT-PCE-003 V3.0 (Política para el uso de correo electrónicos)
j. UTI-EO-PSGC-004 V2.0 (Política del sistema de gestión de calidad)
k. UTI-EO-PAP-001 V2.0 (Política de administración de proyectos)
l. UTI-SRT-PRS-010 V1.0 (Política para el uso de redes sociales)
m. UTI-SRT-PLD-006 V1.0 (Política para el uso de laptop-desktop)

[1] ***Gestión de TI***: *Conjunto de acciones fundamentadas en políticas institucionales que, de una manera global, intentan dirigir la gestión de las TI hacia el logro de los objetivos de la organización. Para ello se procura, en principio, la alineación entre los objetivos de TI y los de la organización, el balance óptimo entre las necesidades de TI de la organización y las oportunidades que sobre ello existen, la maximización de los beneficios y el uso responsable de los recursos, la administración adecuada de los riesgos y el valor agregado en la implementación de dichas TI. Tales acciones se relacionan con los procesos (planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento), recursos tecnológicos (personas, sistemas, tecnologías, instalaciones y datos), y con el logro de los criterios de fidelidad, calidad y seguridad de la información. También se entiende como "Gobernabilidad de TI"*

n. UTI-SRT-PUI-013 V1.0 (Política para el uso de la información)
o. UTI-EO-PPC-003 V2.0 (Política del plan de comunicación)
p. UTI-SRT-PS-0011 V2.0 (Política para el uso del software)
q. UTI-SRT-PUG-012 V1.0 (Política para el uso del gafete)
r. UTI-EO-PGCTI-002 V2.0 (Política de continuidad de TI)
s. UTI-SRT-PI-005 V2.1 (Política para el uso de internet)
t. UTI-SST-PMS-001 V2.0 (Política mesa de servicios)

En verificación efectuada a las políticas indicadas anteriormente, se identificó que algunos de esos documentos han sido trasladados al Comité de Tecnología de Información para la respectiva revisión, no obstante, no han sido devueltos con las oportunidades de mejora que ha analizado dicho comité. Adicionalmente, se identificaron las siguientes oportunidades de mejora:

1. Se requiere de la autorización y aprobación ("**Revisado por**" y el "**Aprobado por**"), de parte de los funcionarios con potestades para concederlas, en el caso de políticas se requiere de la aprobación formal por parte del jerarca[2] (Junta Directiva).
2. La normativa anterior data de los años 2019 al 2021.
3. Se debe incorporar un medio formal de cambios (control de versiones).
4. Deben ser comunicados a todos los funcionarios del Instituto, dejándose evidencia de dicho acto.

3.3 La normativa interna debe ser revisada de forma periódica, para que se incorporen los criterios o directrices de acción elegidas como guías en el proceso Tecnología de Información establecidos en las políticas, las regulaciones, así como, documentar las mejoras continuas que deben ser observadas en los procesos mediante un medio formal de cambios (control de versiones), deben contar con la autorización y aprobación respectivas de parte de los funcionarios con potestades para concederlas. La información debe estar disponible, en forma ordenada conforme a criterios previamente establecidos para su uso y consulta, para asegurar la razonabilidad de las operaciones y el fortalecimiento de sistema de control interno, tal y como lo establecen las Normas de Control Interno y las sanas prácticas.

3.4 Sobre el particular, se le consultó a la Encargada de Tecnología de Información sobre los niveles de autorización y aprobación, a lo que indicó:

> *"Como ya le había indicado el día de la reunión, las políticas están en poder del Comité de TI para la revisión y aprobación de la cual estamos a la espera."*

3.5 Al respecto, la Ley General de Control Interno, Ley N° 8292, indica en el inciso b) del artículo 15, lo siguiente:

> *"**Artículo 15.—Actividades de control**. Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
> ***[...]***
> *b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
>
> *i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución…"*

3.6 Las Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), expresan lo siguiente sobre la gestión de la seguridad de la información:

> ***"5.2 Seguimiento y evaluación del control interno en TI***
> *El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas"*

3.7 Las Normas de Control Interno elaboradas por la Contraloría General de la República establecen lo siguiente:

> "***2.5.2 Autorización y Aprobación:*** *La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas,*

[2] ***Jerarca:*** *Superior jerárquico, unipersonal o colegiado del órgano o ente quien ejerce la máxima autoridad.*

que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales."

3.8 Asimismo, las buenas prácticas indican la importancia de contar con políticas, procedimientos y los mecanismos de control en los cuales se establezcan y se observen los niveles aprobación de los documentos que la institución elabore, sean estos, hecho por, revisado por y aprobado o autorizado por.

3.9 Cabe destacar que la ausencia de la aprobación de las políticas de seguridad de información podría originar el incumplimiento de los requerimientos normativos y de las disposiciones institucionales.

Oportunidad de Mejora No. 2: Pruebas de Penetración Interna y Externa de la Infraestructura Tecnológica

3.10 En seguimiento a la periodicidad con que la Unidad de Tecnología de Información aplica pruebas de penetración Interna y externa de la infraestructura tecnológica del INVU, así como la situación actual de los riesgos internos y externos de seguridad de la información, se identificó que la última contratación realizada fue en el 2012 mediante la *Contratación Directa 2012CD-000059-01.*

3.11 Cabe resaltar que para el 2019 mediante oficio GG-TI-041-2019 de fecha 01 de setiembre de 2019 la Unidad de Tecnología, gestionó el proceso de contratación de servicios profesionales para realizar un estudio de *ANALISIS DE VULNERAVILIDADES DEL INVU*; para su ejecución se contaba con 6 millones de colones de contenido presupuestario. Sin embargo, el 04/09/2019 el Encargado de la Unidad de Adquisición informó a la Unidad de Tecnología de Información que por indicaciones de la Jefatura Administrativo Financiero "…*este requerimiento no se va a ejecutar. Se procede a su archivo*…".

3.12 En la planificación del contenido presupuesto del 2020, no se incluyó la realización de un estudio de análisis de vulnerabilidades (ejercicios de intrusión/hacking ético sobre su plataforma tecnológica), dado que se estimaba realizarlo en el 2019.

3.13 Sobre el particular, se le consultó a la Encargada de Tecnología de Información las gestiones actuales sobre la existencia de ejercicios de intrusión (hacking ético), detección oportuna de actividades inusuales o anormales en los sistemas de la entidad, a lo que indicó lo siguiente:

"Para el presupuesto del 2021 se incluyó 9 millones para proceder a realizar los ejercicios de intrusión (hacking ético), pero nada más se aprobaron 2.7 millones, considerando que es un presupuesto insuficiente y el año pasado se realizaron varios recortes para el presupuesto 2021 sin consulta a la Unidad."

3.14 En la Conferencia de Resultados, llevada a cabo el 03 de setiembre de 2021, en la que se conversó sobre los resultados del informe borrador de Seguridad de la Información, la Encargada de la Unidad de Tecnología de Información indicó que:

"Si bien es cierto, no ha sido contratado dicho servicio por lo indicado, sin embargo, el compañero Miranda Mora realiza pruebas de penetración y de vulnerabilidades y tráfico de los paquetes de red en forma diaria."
(**Véase Anexo No.1**)

3.15 Por su parte las buenas prácticas de Gobierno de Tecnologías de Información incluidas en COBIT 5, indican lo siguiente sobre el tema de seguridad de la red:

*"**DSS05.02 Gestionar la seguridad de la red y las conexiones.** Utilizar medidas de seguridad y procedimientos de*
gestión relacionados para proteger la información en todos los modos de conexión. (…)

8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema."

3.16 Aunado a lo anterior, las buenas prácticas también encomiendan la importancia de realizar periódicamente ejercicios[3] de intrusión/hacking ético sobre su plataforma tecnológica; a los sistemas más críticos y con especial atención en aquellos que sean directamente accesibles desde Internet.

3.17 Cabe destacar que la ausencia de los ejercicios de intrusión/hacking ético eventualmente aumentan la posibilidad de amenazas, debido a que se desconoce cuáles pueden ser los puntos vulnerables y ante posibles ataques, se pueden presentar el robo de información, la indisponibilidad de servicios o el sabotaje de infraestructuras, entre otros, que pueden acarrear consecuencias económicas, legales y de imagen importantes.

Oportunidad de Mejora No. 3: Protocolos de gestión, respuesta y recuperación ante incidentes de seguridad

3.18 En febrero del 2021 ingreso un Malware (usaba los recursos del equipo para generar criptomoneda), el cual se presentó desde equipos de funcionarios del INVU (red interna), cuya particularidad fue que el problema se presentaba en un día y se resolvía, al día siguiente se suscitaba nuevamente al ingresar los funcionarios; lo cual evidenciaba que la activación del problema se daba con el ingreso de estos a sus equipos. Las implicaciones originadas fueron caídas súbitas de los sistemas, presentadas durante una semana antes de la detección y en los tres a cuatro días iniciales, lo cual requería de la intervención técnica.

3.19 En la identificación de los protocolos de gestión, respuesta, recuperación ante incidentes de seguridad, se identificó la existencia de procedimientos y manuales, así como de respaldos de la información, sin embargo, no existe un plan de contingencias para el caso de interrupción de las actividades, predeterminado los tiempos después de un evento no deseado para lograr regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información.

3.20 En entrevista efectuada a la Encargada de Tecnología de Información sobre la existencia de protocolos de gestión, respuesta, recuperación ante incidentes de seguridad y como han sido atendidos los ataques a la red institucional y a la página web, indicó lo siguiente:

> *El protocolo de gestión es solventado por parte del personal interno, posteriormente se procede a escalarlo a personal externo, dependiendo de la naturaleza del incidente a:*
> - *GDI: seguridad y antivirus*
> - *Soporte crítico: en caso aire acondicionado del centro de datos*
> - *Trango: base de datos y aplicativos de Oracle*
> - *InfosGroup: página WEB y portal de citas*
> - *Argos: sitio de Auditoría*
>
> *Atención de los ataques:*
> - *Se generaron separaciones de ambientes.*
> - *Se actualizaron antivirus.*
> - *Se modificaron las tareas de escaneo de los antivirus*
> - *Se generaron escaneo completo de los equipos afectados y se restablecieron las configuraciones.*
> - *Se realizó un escaneo profundo a toda la red.*

3.21 Sobre el particular, también se le consultó a la Encargada de Tecnología de Información, en cual procedimiento se encuentra contenido el protocolo de gestión indicado anteriormente. Al respecto manifestó:

> *…existen contratos de soporte con cada una de las empresas indicadas y es a ellas cuando se escala el problema si no se pudo resolver de manera interna. Es el protocolo que se realiza a juicio de experto.*
>
> *En paralelo, mucho de lo atinente a la detección de intrusiones corresponde a las labores de seguridad y monitoreo realizadas por el funcionario Lic. Carlos Miranda Mora, Profesional en Tecnologías de la Información y encargado de las redes y comunicaciones de la UTI.*
>
> *Como parte del PETI se encuentra el proyecto "(ITI-12) Definir y desarrollar un plan de continuidad apropiado para la Unidad de TI ante eventos que repercutan directamente el entorno operativo", para efectuar la totalidad del*

[3] *Estos ejercicios recrean un escenario similar a un ataque real, utilizando las técnicas, herramientas y conocimiento que un ciberdelincuente emplearía, por lo que resultan de gran utilidad para identificar vulnerabilidades de seguridad en la organización y facilitar su corrección y mitigación. Es recomendable que estos ejercicios se realicen desde el exterior y el interior de la organización (conexión a los sistemas como lo estaría un empleado).*

proyecto se solicitaron para el presupuesto 2021 la suma ¢20,746,800.00, monto que fue estimado por la empresa Deloitte en su oportunidad, pero no se nos asignó presupuesto para dicha actividad en el presente año.

La documentación a que Ud. hace referencia debe definirse dentro del plan de continuidad, sin embargo, dentro la documentación existente se encuentran los procedimientos para la implementación de parches relativos a la base de datos, operativos de los sistemas ABANKS, parches de seguridad de Windows y Office (que le fueran enviados), adicionalmente se cuenta con las actualizaciones automáticas realizadas por las casas matrices a nivel mundial de nuestros software de seguridad tales como McAfee, Forcepoint, IPS y el Next Generation Firewall, información que se encuentra en las bases de conocimiento de éstas, ubicadas en sus respectivas páginas web que son modificadas diariamente y dicha información está disponible para nosotros a modo de consulta.

Por lo anterior si contamos con procedimientos a seguir.

3.22 Se hace la aclaración que las interrupciones de las actividades por evento no deseado deben ser definidas en el plan de contingencias, dado que en el plan de continuidad se establecen las acciones y responsabilidades a efectuar en casos siniéstrales para la recuperación y la restauración parcial o total de los procesos según su criticidad. Además, se procedió a verificar si el protocolo de gestión, respuesta, recuperación ante incidentes de seguridad se encuentra incorporado en los procedimientos suministrados, obteniéndose el siguiente resultado:

a. *Procedimiento para la aplicación de parches de seguridad (UTI-SRT-PAPS-001)*
El objetivo de dicho procedimiento es delimitar, especificar y documentar el procedimiento por medio del cual se aplican los diversos y respectivos parches de seguridad y actualizaciones de los aplicativos de Microsoft. Además, dicho procedimiento cuenta con las siguientes recomendaciones:

i. Mantener las actualizaciones al día (con el objetivo de proveer una garantía y un grado de seguridad de que los equipos poseen por decirlo así un blindaje ante muchos de los ataques de entes externos).
ii. Efectuar campañas de concientización en los usuarios.
iii. Velar por el cumplimiento de la seguridad en todos los ámbitos (de los equipos y su información por parte de cada uno de los funcionarios).

b. *Procedimiento de aplicación de deltas (UTI-SAD-PAD-002)*
El procedimiento pretende servir como una guía práctica para realizar los procesos de aplicación de DELTAS (Modificaciones de Software enviado por la empresa ASI Group). El proceso de actualización de software debe considerar la importancia estratégica del proceso y el riesgo o la vulnerabilidad en el que se incurre al momento de realizar una aplicación o corrección en los códigos fuentes del Core Bancario.

c. *Aplicación de parches de bases de datos (UTI-SAD-PAD-001)*
El procedimiento pretende servir como una guía práctica para realizar los procesos de aplicación de PARCHES en la base de datos. Los parches que libera Oracle en su mayoría son soluciones (Fixes) a errores (Bugs) reportados, vulnerabilidades, rendimiento, entre otros, por esta razón es importante revisar que soluciona y si aplica a nuestra arquitectura.

Como se puede observar en el *Procedimiento para la aplicación de parches de seguridad* se identificó la *Actualización de antivirus*, siendo este un elemento dentro de las actividades definidas para la atención de ataques, en virtud de lo anterior se considera que las acciones definidas en el protocolo deben ser incorporados en la conformación del plan de contingencias, así como sus responsables.

3.23 Con la finalidad de aportar valor a la gestión institucional y cumplir con el control interno institucional, la Auditoria Interna en su estudio Nº: IA-007-2017 denominado *Informe de cumplimiento de los criterios básicos de control indicados en las normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), en el INVU*, recomendó la necesidad de elaborarse un plan de continuidad así como de un plan de contingencias; recomendación que fue reiterada en el informe AI-003-2020 denominado *Estudio de evaluación de Manejo de incidentes*, que dice:

> ***23.*** *Elaborar un plan de continuidad de negocio en coordinación de los diferentes departamentos del INVU, donde se establezcan las acciones y responsabilidades a efectuar en casos siniéstrales para la recuperación y la restauración parcial o total de los procesos según su criticidad, así como de un plan de contingencias para el caso de interrupción de las actividades, predeterminado los tiempos después de un evento no deseado para lograr regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información. Poner en práctica para ser probados mediante simulacros, evaluando su resultado y efectuando las acciones correctivas necesarias, según lo dispuesto en el numeral 1.4.7 de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).* ***Impacto: Alto***

*(**El subrayado no pertenece al original**)*

3.24 A la fecha la Unidad de Tecnología de Información ha reportado los siguientes avances en la atención de la recomendación; según detalle:

> *La UTI cuenta con planes para respaldos y recuperación de la información. Actualmente, se está trabajando en un plan formal de contingencias, en el cual se vean plasmados todos los procedimientos inherentes a recuperación y continuidad, de manera que pueda unificarse en un solo documento, permitiendo una mayor facilidad para su comprensión y gestión. Se está coordinando con un estudiante de Licenciatura en Administración de TI del TEC, estará realizando su proyecto de graduación en el INVU, el cual será la elaboración de un Plan de Continuidad.*

3.25 En la citada Conferencia de Resultados, llevada a cabo el 03 de setiembre de 2021, la Encargada de la Unidad de Tecnología de Información indicó que:

> *El plan de contingencia y de continuidad se encuentran en el PETI y se ha solicitado recursos presupuestarios para su ejecución en los años 2020 y en 2021que no fueron aprobados por la Administración superior, decisión que se sale de mi alcance. Sin embargo, se está presupuestando de nuevo para el 2022, dado que la coordinación con los estudiantes no fue posible.*
> *[…]*
> *Contamos con herramientas para dicho fin que le fueron indicadas y de las cuáles se desprenden contratos de soporte para la ocurrencia de eventualidades.*
> *[…]*
> *Por otra parte, se debe entender que la ocurrencia de un evento no deseado puede ser en cualquier horario, por lo que considero que esa Auditoría debe recomendar la generación de un rubro denominado disponibilidad o bien asignar horas extras para dicha actividad. No es posible obligar a un funcionario a trabajar sin pago.*

3.26 Por lo antes mencionado, es importante indicar que la Unidad de Tecnología de Información ha realizado esfuerzos con las herramientas que cuenta, para hacerle frente a los intentos de ataques que se pueden presentar. También, es valioso citar lo que nos indican las buenas prácticas sobre la importancia de estar protegidos ante ciberataques o ser capaz de detectarlos es igualmente fundamental la capacidad de reacción, tratamiento y respuesta ante los mismos. Por eso las organizaciones deben contar con adecuados procedimientos para gestionar incidentes, que incluyan al menos:

a. **Su correcta identificación y clasificación**, así como una estimación de su posible impacto (financiero, regulatorio, reputacional).
b. **Protocolos para su tratamiento** (comités de crisis, cascada de llamadas) y análisis (investigaciones forenses, activación de la póliza de un ciberseguro o de fraude).
c. **Notificación y escalado de los incidentes**: incluyendo posibles comunicaciones a clientes, medios de comunicación, organismos reguladores y alta dirección (Consejo de Administración y Comisión de Auditoría).
d. **Mecanismos, medidas y procedimientos para su mitigación**, como activación de Planes de Continuidad de Negocio (PCN) y de Contingencia Tecnológica (PCT), o aislamiento parcial y/o total de los sistemas expuestos a Internet.

3.27 El contar con procedimientos debidamente actualizados fortalece el Sistema de Control Interno ya que contribuye a normar y estandarizar los procesos necesarios para cumplir con determinado procedimiento; por lo que al encontrarse desactualizados se podría generar un debilitamiento del SCI.

3.28 En relación con la recomendación pendiente de atención la Encargada de Tecnología de Información aclaró que se han solicitado recursos en 2020 y 2021, los cuales no han sido aprobados y se espera contar con los recursos para el 2022, por consiguiente, es importante continuar las gestiones para la elaboración del plan de continuidad de negocio y el plan de contingencias considerando las sanas prácticas en la definición de dicho plan.

IV. CONCLUSIONES

4.1 De conformidad con los resultados obtenidos, se formulan los siguientes comentarios:

4.2 Para el fortalecimiento del sistema de control interno, la política de seguridad de la información institucional, así como los procedimientos internos elaborados por la Unidad de Tecnología de Información, deben contar con la autorización y aprobación (“Revisado por” y el “Aprobado por”), de los funcionarios con potestades para concederlas, así como de un medio formal de cambios (control de versiones).

4.3 Es importante que la administración activa valore la opción de realizar periódicamente ejercicios de intrusión/hacking ético sobre los sistemas más críticos y con especial atención en aquellos que sean directamente accesibles desde Internet, así como de la plataforma tecnológica.

4.4 Se requiere la atención oportuna a la elaboración de un plan de contingencias para el caso de interrupción de las actividades, predeterminado los tiempos después de un evento no deseado para lograr regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información. Así como de un plan de continuidad de negocio en coordinación de los diferentes departamentos del INVU, donde se establezcan las acciones y responsabilidades a efectuar en casos siniéstrales para la recuperación y la restauración parcial o total de los procesos según su criticidad.

V. RECOMENDACIONES

5.1 Para la implementación de las oportunidades de mejora, determinadas en el presente informe se proponen las siguientes recomendaciones, las cuales, de ser aplicadas en forma efectiva, agregarán un importante valor a la gestión y al robustecimiento de la Unidad de Tecnología de Información.

A la Encargada de la Unidad de Tecnología de Información o a quien, en su lugar ocupe el cargo:

No.	Detalle de la Recomendación	Riesgo
1	Establecer los mecanismos de control que correspondan, para que la política de seguridad de información institucional y los procedimientos internos cuenten con la autorización y aprobación de los funcionarios con potestades para concederlas y de un medio formal de cambios (control de versiones); con el objetivo de minimizar el riesgo de incumplimiento normativo. ***Ver Oportunidad de Mejora No. 1: Párrafos del 3.2 al 3.9***	Alto
3	Una vez aprobada la Política de Seguridad de Información institucional, efectuar su divulgación a todo el personal del Instituto, dejando evidencia de dicho acto. ***Ver Oportunidad de Mejora No. 1: Párrafos del 3.2 al 3.9***	Medio
2	Realizar las gestiones que correspondan para contar con el contenido presupuestario, para llevar a cabo las pruebas de penetración Interna y externa de la infraestructura tecnológica del INVU y situación actual de los riesgos, con el objetivo de minimizar los riesgos y la vulnerabilidad de la infraestructura tecnológica. ***Ver Oportunidad de Mejora No. 2: Párrafos del 3.10 al 3.17***	Alto

HENRY ARLEY PEREZ (FIRMA)
Firmado digitalmente por HENRY ARLEY PEREZ (FIRMA)
Fecha: 2021.09.10 14:09:45 -06'00'

Lic. Henry Arley P.
Auditor Interno.

RODRIGO QUIROS TORRES (FIRMA)
Firmado digitalmente por RODRIGO QUIROS TORRES (FIRMA)
Fecha: 2021.09.10 14:16:08 -06'00'

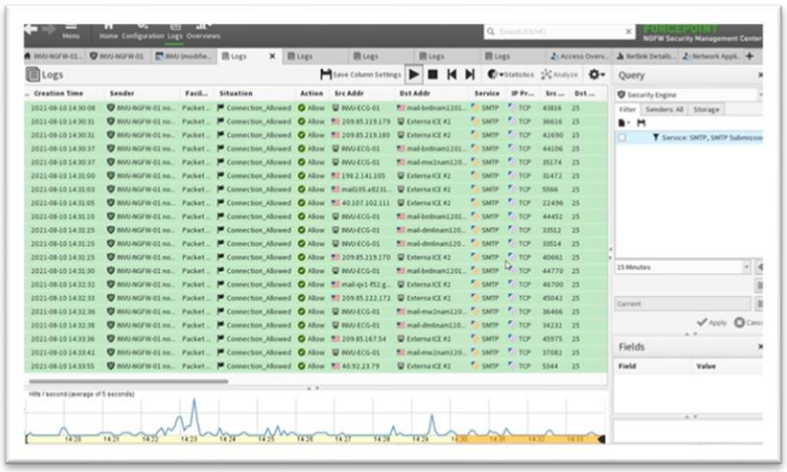
Lic. Rodrigo Quirós T.
Profesional Especialista
Auditoría Interna.

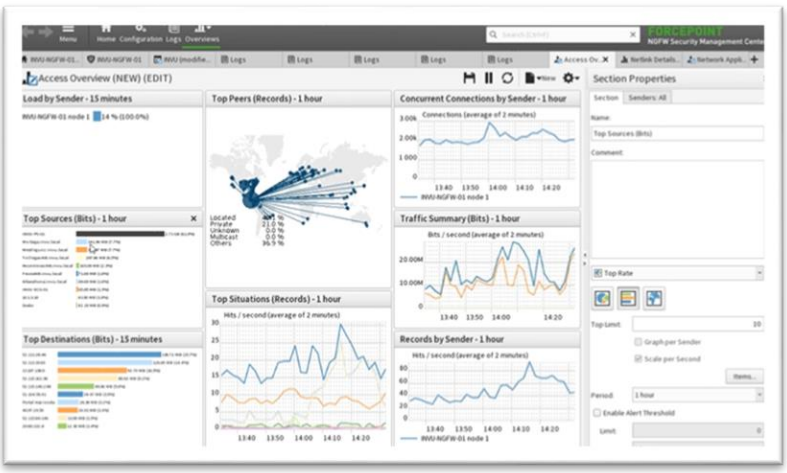
VI. REFERENCIAS BIBLIOGRÁFICAS

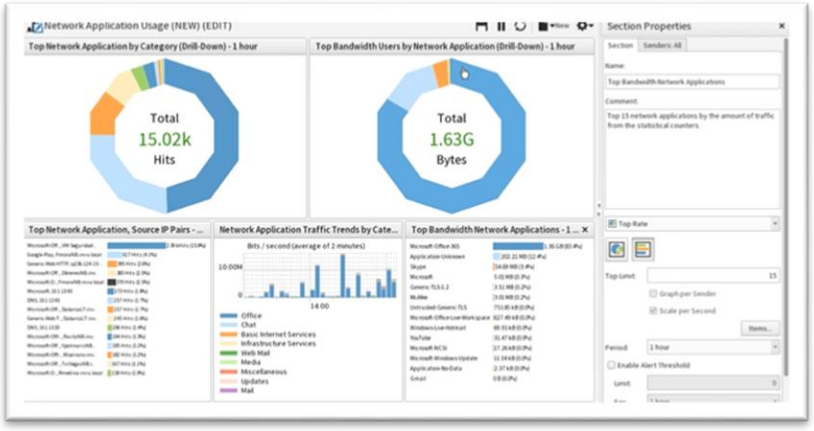
Instituto de Auditores Internos de España, Edición Consejeros. Junio 2017. Ciberseguridad - 10 Preguntas que un Consejero debe plantearse https://auditoresinternos.es/uploads/media_items/ciberseguridad-10preguntas-que-un-consejero-debe-plantear.original.pdf

VII. ANEXOS

Anexo 1. Pruebas de testeo efectuadas por la Unidad de Tecnología de Información de forma diaria:







Fuente: Unidad de Tecnología de Información.