***UNIDAD DE AUDITORÍA INTERNA***

***INFORME UAI N.º 595***

# *GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD*

## *INFORME EJECUTIVO*

El presente Informe tiene por objeto evaluar el cumplimiento de las políticas y procedimientos en materia de Seguridad Informática, llevados adelante por la Gerencia de Tecnologías de Información y Comunicación del ENARGAS, con el objeto de identificar vulnerabilidades y debilidades de los sistemas de la organización, reforzando así la postura de seguridad en general.

Para ello, se efectuó el seguimiento de lo informado oportunamente por esta Auditoría Interna, a través del cumplimiento del Instructivo de Trabajo N.º 7/2024 de la Sindicatura General de la Nación. Es así que se relevaron aspectos vinculados con los siguientes ítems:

- ✓ Gestión de Incidentes de Seguridad
- ✓ Gestión de Contingencias
- ✓ Resguardo y Recuperación
- ✓ Análisis de Vulnerabilidades
- ✓ Protección de Software y Hardware
- ✓ Control de Criptomoneda

En este sentido, se efectuó el seguimiento de lo oportunamente relevado e informado por esta Unidad en cumplimiento del citado Instructivo de Trabajo en el mes de octubre de 2024.

En mérito al resultado del relevamiento realizado se entiende que el ENARGAS cuenta con herramientas y procedimientos en materia de ciberseguridad, no obstante lo cual no se ha realizado una revisión integral de la Política de Seguridad de la Información, aprobada en el año 2017, y de los procedimientos redactados (sin aprobación), a fin de contar con documentos actualizados, acordes a los avances tecnológicos, y con el conocimiento y consentimiento del personal, a través de la conformación y funcionamiento del Comité de Seguridad de la Información. Asimismo, observada la metodología de trabajo del Área de Seguridad, no se verificó el desarrollo de un Plan de Acción, en el cual se expliciten los objetivos fijados, los medios disponibles y los plazos de concreción establecidos.

Por ello se entiende necesario que la Gerencia de Tecnologías de la Información y Comunicación, a través del Área de Seguridad de la Información,

impulse la revisión integral de la Política de Seguridad de la Información vigente, y ponga en funcionamiento al Comité de Seguridad de la Información.

Asimismo, se recomienda la elaboración de un Plan de Trabajo Anual, que permita fijar los objetivos en materia de ciberseguridad, medios necesarios y plazos comprometidos. Todo ello con el objeto de proteger los activos críticos, los datos sensibles y los sistemas del Organismo, garantizando así la confidencialidad, integridad y disponibilidad de la información. Un Plan de Trabajo, desarrollado y aprobado, permite gestionar metódicamente vulnerabilidades, y deberá incluir la mitigación de riesgos de seguridad mediante la implantación de medidas técnicas, organizativas y legales, así como la capacitación y concientización del personal para reducir el error humano.

*A partir de las tareas desarrolladas y considerando el Alcance definido, se concluye que la Gerencia de Tecnología de la Información y Comunicación, a través del Área de Seguridad de la Información, posee un razonable grado de cumplimiento de los procedimientos que garantizan la seguridad de la información, no obstante lo cual se considera necesario que se efectúe una revisión integral de la Política de Seguridad de la Información actualmente vigente, y se elabore un Plan de Acción que permita identificar los objetivos fijados, medios necesarios y plazos comprometidos.*

# ***INFORME ANALÍTICO***

## *A.- OBJETO*

Evaluar el cumplimiento de las políticas y procedimientos en materia de Seguridad Informática, llevados adelante por la Gerencia de Tecnologías de Información y Comunicación del ENARGAS, con el objeto de identificar vulnerabilidades y debilidades de los sistemas de la organización, reforzando así la postura de seguridad en general.

Para ello, se efectuó el seguimiento de lo informado oportunamente por esta Auditoría Interna, a través del cumplimiento del Instructivo de Trabajo N.º 7/2024 de la Sindicatura General de la Nación.

## *B.- ALCANCE*

Se relevaron aspectos vinculados con el cuestionario impuesto por el Instructivo de Trabajo (IT) n.º 7/2024, relacionados con:

- ✓ Gestión de Incidentes de Seguridad
- ✓ Gestión de Contingencias
- ✓ Resguardo y Recuperación
- ✓ Análisis de Vulnerabilidades
- ✓ Protección de Software y Hardware
- ✓ Control de Criptomoneda

En este sentido, se efectuó el seguimiento de lo oportunamente relevado e informado por esta Unidad en cumplimiento del citado Instructivo de Trabajo en el mes de octubre de 2024.

Para ello se mantuvo entrevista con el responsable del Área de Seguridad de la Información, y se solicitó la documentación relacionada con los procedimientos desarrollados hasta el presente.

Se visualizaron las aplicaciones utilizadas y su funcionamiento.

Se tuvo en consideración la Política de Seguridad de la Información, aprobada por Resolución ENARGAS N.º I/4559/2017.

## *C.- COMENTARIOS, OBSERVACIONES Y RECOMENDACIONES*

A continuación, se enuncian los comentarios, observaciones y recomendaciones que han surgido de los elementos de juicio obtenidos durante el desarrollo de las tareas, en contenido y orden a lo dispuesto en el IT N.º 7/2024-SIGEN.

***C.1.- <u>Gestión de Incidentes de Seguridad</u>***

***1.1.- La organización ¿dispone de un procedimiento aprobado por la autoridad para el tratamiento y respuesta a incidentes de seguridad?***

A través de la Resolución ENARGAS N.º 4559/2017 (10/jul/2017) se aprobó la "Política de Seguridad de la Información". Allí se establecieron los plazos para la elaboración de los procedimientos que surgieran de dicha Política, y que se encontraban en cabeza del entonces Departamento de Tecnología de la Información y del responsable de Seguridad de la Información del ENARGAS, dependiente de dicho Departamento.

Se determinaron también plazos para la implementación de las responsabilidades asignadas y las medidas que debían adoptar y/o implementar las distintas unidades organizativas, estipuladas en la Política.

Se creó también el Comité de Seguridad de la Información, con la designación, a posteriori, de los integrantes de cada una de las unidades organizativas vigentes en aquella estructura.

En el Capítulo 16 de la Política se da tratamiento a la "Gestión de Incidentes en la Seguridad de la Información". Se definen allí el objetivo, alcance y responsabilidades. Se determina también que se establecerán procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

A la fecha no se han efectuado revisiones del documento aprobado oportunamente, considerando el tiempo transcurrido y los cambios en materia tecnológica.

Tampoco se ha formalizado la aprobación de Procedimientos de manejo de incidentes en materia de seguridad.

***1.2.- En caso de tratarse de organismos del Inc. a) del Art. 8° de la Ley N.º 24.156, ¿el organismo posee un procedimiento aprobado por la autoridad para reportar a la DNCIB, mediante el CERT.ar, los eventuales incidentes de seguridad que se produzcan dentro de sus ámbitos, dentro de las 48 horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia?***

En cumplimiento de la solicitud cursada por la Dirección Nacional de Ciberseguridad se han designado los puntos focales (enlaces responsables). A raíz de ello se reciben periódicamente reportes, vía mail y del sitio Cert.ar, de alertas sobre vulnerabilidades detectadas en los sistemas (v.gr. Windows Cloud) y su grado de severidad, con el detalle del impacto, producto afectado, recomendaciones y referencias normativas. Estas son analizadas por el personal del Área de Seguridad de la Información y, en caso de corresponder a productos utilizados en el ENARGAS, se siguen las recomendaciones recibidas, que en general se refieren a la procedencia de bajar actualizaciones a los sistemas.

De acuerdo a lo informado por el personal del Área, no se han recibido solicitudes de procedimientos escritos para efectuar reportes a la DNCIB.

***1.3.- En caso de tratarse de organismos del Inc. a) del Art. 8° de la Ley N.º 24.156, ¿los datos del punto focal se encuentran actualizados y han sido comunicados oportunamente a la DNCIB?***
Tal como se detalló en el punto anterior, fueron solicitados y comunicados por mail los datos de los puntos focales, y los mismos se encuentran actualizados.

***1.4.- ¿Cuenta con suficiente personal entrenado y capaz de responder eficientemente ante un incidente de ciberseguridad?***
Si, actualmente el Área cuenta con cuatro profesionales, incluyendo al responsable de la misma.

***C.2.- <u>Gestión de Contingencias</u>***

***2.1.- Ante la ocurrencia de una contingencia que comprometa la disponibilidad del CPD, ¿el Organismo cuenta con un Plan de Contingencia o Plan de Recuperación ante Desastres?***
El proyecto de Plan de Gestión de Contingencias se encuentra desarrollado, pero aún no ha sido aprobado. El responsable del Área informó que se esperará a contar con la nueva estructura del ENRGyE (Ente Nacional Regulador del Gas y la Electricidad), y la definición de sistemas y procedimientos de trabajo, para efectuar la revisión y aprobación final, a través de una nueva conformación del Comité de Seguridad de la Información.
Cabe destacar aquí que en oportunidad de comenzar las funciones del nuevo organismo se deberá efectuar una revisión integral de la actual Política de Seguridad de la Información, a fin de integrar los documentos vigentes en los actuales ENARGAS y ENRE.
El documento desarrollado contiene los siguientes puntos:

- ✓ Activos críticos
- ✓ Infraestructura TIC
- ✓ Objetivos del Plan de Recuperación de Incidentes
- ✓ Tipos de Incidentes Cubiertos
- ✓ Fases del Plan de Recuperación
  - Detección y Notificación:
  - Contención del Incidente:
  - Recuperación de Sistemas
  - Análisis Post-Incidente y Prevención
  - Roles y Responsabilidades
  - Estrategia de Backups y Redundancia
  - Plan de Comunicación Durante un Incidente
  - Indicadores de Éxito del Plan de Recuperación

***2.1.1.- ¿El Plan de Contingencia o Plan de Recuperación ante Desastres se encuentra documentado formalmente, es decir aprobado por la autoridad?***
En el punto anterior se detalló la situación actual.

***2.1.2.- ¿El Plan de Contingencia o Plan de Recuperación ante Desastres se encuentra probado formalmente?***
En el punto 2.1 se detalló la situación actual.

***2.1.3.- ¿Se han definido los sistemas críticos y su prioridad de recuperación?***
Los Activos críticos fueron definidos y son los siguientes:

- Bases de datos
    - Facturación
    - Usuarios
    - Datos operativos
- Servidores y Redes

No obstante, no hay definidas prioridades de recuperación.

***2.1.4.- ¿Se encuentran formalmente acordados los tiempos de recuperación para los servicios críticos?***
Los tiempos de recuperación no se encuentran definidos en el documento actual.

***2.1.5.- ¿Se han definido claramente los roles y responsabilidades de los equipos de trabajos encargados de la recuperación de los sistemas críticos?***
En el punto 5 del procedimiento desarrollado se han definido los roles y responsabilidades de: CISO (Director de Seguridad de la Información), SOC (Centro de Operaciones de Ciberseguridad), equipo de respuesta TI, y Comité de Crisis.

***2.1.6.- ¿Se han documentado detalladamente los procedimientos técnicos para recuperación de cada uno de los sistemas críticos?***
No se han desarrollado procedimientos técnicos específicos para la recuperación de los Activos Críticos. Sólo se encuentra documentado, sin aprobación formal, el Procedimiento de Gestión de Copias de Seguridad, que tiene una revisión (actualización) que data de marzo/2025.

***2.2.- Ante una contingencia que pudiera afectar el normal procesamiento de las operaciones en el CPD Principal, ¿el Organismo cuenta con un Sitio de Procesamiento Alternativo?***
El Ente tenía como sitio de Procesamiento Alternativo Microsoft Azure, el que por cuestiones presupuestarias debió reducirse. En la actualidad el Área de Seguridad se encuentra migrando la información a servidores propios, con lo cual terminada dicha migración, y de persistir las restricciones presupuestarias, el Sitio de Procesamiento Alternativo residirá y será administrado por el propio Organismo.

***C.3.- <u>Resguardo y Recuperación</u>***

***3.1.- ¿Se realizan backups periódicos de los datos, programas y configuración de todos los sistemas críticos?***

Cada 24 hs. se realizan los backups de las Bases de Datos y de las Aplicaciones, los que están a cargo del Área de Infraestructura. Los backups se realizan en Microsoft Azure.

***3.2.- ¿Existe un procedimiento documentado y aprobado por la autoridad para la realización de resguardo y recuperación de la información?***
Tal como se comentó en el punto 2.1.6 el Organismo cuenta con un Procedimiento de Gestión de Copias de Seguridad, que tiene una revisión (actualización) que data de marzo/2025, pero el mismo no ha sido aprobado formalmente.

***3.3.- Los resguardos ¿se almacenan en un sitio con acceso restringido y suficientes medidas de seguridad?***
Si, dado que se encuentran en los servers del Organismo y el sitio cuenta con acceso restringido y medidas de seguridad propias.

***3.4.- ¿Se mantiene un resguardo periódico en un sitio externo?***
Ver respuesta al punto 2.2.

***3.5.- ¿Se prueban los resguardos y su recuperación en forma periódica, para garantizar que cumplen con los requerimientos de los planes de continuidad de las actividades?***
Al igual que lo expresado en oportunidad de cumplimentar el IT N.º 7/2024, se realiza sólo de algunos sistemas por falta de disponibilidad de recursos de hardware.

***C.4.- <u>Análisis de Vulnerabilidades</u>***

***4.1.- ¿Se encuentran identificados los activos de información críticos y sus principales amenazas y vulnerabilidades?***
Se encuentran definidos los Activos Críticos, pero no las principales amenazas y vulnerabilidades.

***4.2.- ¿Se utilizan herramientas y aplicaciones de escaneo de vulnerabilidades (para infraestructura de red, sistemas operativos, bases de datos, aplicaciones, otro software instalado y de código abierto, nube, entre otros), a modo de ayudar a los administradores/propietarios a proteger los activos?***
Se utiliza la aplicación Wazuh (soluciones SIEM, de código abierto y gratuita, configurada para las características del Organismo) que permite efectuar análisis de registros (logs), monitoreos de integridad y tiene respuesta ante incidentes.
Para el monitoreo de tráfico y estado de los servidores se utiliza ZABBIX, pero este sistema no tiene alertas, con lo que se efectúa una visualización permanente de su estado a fin de detectar posibles eventos.
Asimismo, se encuentra en etapa de instalación de la plataforma Graylog para el análisis de registros (logs).

***4.3.- ¿Se revisan periódicamente los informes que producen las herramientas y aplicaciones de escaneo de vulnerabilidades?***

Se está instalando localmente la herramienta Greenbone, por la imposibilidad de subirla a Microsoft Azure (razones presupuestarias).

***4.3.1.- ¿Al encontrarse una vulnerabilidad, se efectúa un plan de acción a modo de remediar y proteger el activo?***
En aquellos casos en que se trata de software de terceros, como sistemas operativos, motores de base de datos, etc., en líneas generales las vulnerabilidades detectadas se solucionan bajando las actualizaciones de los sistemas, o aislando lo afectado en caso de no estar disponible aún (en el momento de la detección) la correspondiente actualización. En caso de ser una aplicación propia, o mantenida por el organismo, se realizan las modificaciones, los testeos correspondientes, y la implementación de la versión actualizada.

***C.5.- <u>Protección de Software y Hardware</u>***

***5.1.- ¿Se posee un inventario formal de software y hardware?***
La Gerencia de Tecnología de la Información y Comunicación, a través del Área de Infraestructura de TI, posee un sistema propio de inventario, independiente del que lleva al Área de Patrimonio de la Gerencia de Administración. Esta función se encuentra debidamente detallada en la estructura de la Gerencia.

***5.2.- ¿Cuentan con un procedimiento formal (aprobado por la autoridad) de gestión de inventarios de software y hardware?***
Por Resolución RESFC-2019-489-APN-DIRECTORIO#ENARGAS se aprobó el procedimiento de los Bienes de Uso del Organismo, que incluye el software y el hardware.

***5.3.-. ¿Se aplican mecanismos de control para asegurar la actualización del software con los parches y configuraciones de seguridad recomendadas en firewalls, terminales, red, servidores, dispositivos móviles y acceso remoto?***
Tal como se explicitó anteriormente, a través del Wazuh se detectan las vulnerabilidades y se procede a efectuar las actualizaciones recomendadas.

***5.4.- ¿Se limita el acceso a los servicios críticos como configuración de reglas de firewall, aplicaciones y herramientas de escaneo vulnerabilidades, y a las soluciones de seguridad?***
Este tipo de operaciones solo las pueden realizar aquellos agentes que posean claves de acceso con configuración de Administrador.

***5.5.- ¿Se utilizan soluciones de seguridad confiables en toda la infraestructura tecnológica de modo de proteger a todos los recursos críticos?***
Se utilizan todas las soluciones antes descriptas.

***5.5.1.- ¿Se utilizan sistemas de ciberseguridad biométrica?***
Los sistemas de ciberseguridad biométrica se utilizan sólo en el Data Center. Se está analizando ampliar su utilización en otras herramientas.

***5.5.2.- ¿Se utilizan sistemas de análisis de tráfico de red en tiempo real?***
Para el monitoreo de tráfico y estado de los servidores se utiliza ZABBIX.

***5.5.3.- ¿Se utilizan firewalls?***
Si, se utilizan firewalls.

***5.5.4.- ¿Se utilizan sistemas de prevención de intrusiones IPS?***
Se utiliza el Microsoft Defender, que ofrece protección en tiempo real contra virus, spyware y otras amenazas.

***5.5.5.- ¿Se utilizan sistema de detección de intrusiones IDS?***
Se utiliza el Microsoft Defender, que ofrece protección en tiempo real contra virus, spyware y otras amenazas.

***5.5.6 ¿Se utilizan aplicaciones de escaneo de vulnerabilidades de aplicaciones Web?***
Se están implementando controles y el uso de herramientas como "Zed Attack Proxy" (para el análisis puntual de aplicaciones) y "BeEF", recomendadas por la OWASP, para la detección de vulnerabilidades.

***5.5.7 ¿Se implementan técnicas antispam en los servicios de correo electrónico?***
Si, los existentes en el Windows 365 (por ej. Cuarentena).

***5.5.8 ¿Se utilizan redes virtuales privadas (VPN) para las conexiones remotas?***
Si, todo el personal puede conectarse remoto por VPN.

***5.5.9 ¿En el último año se efectuaron pruebas de intrusión (pentesting o hacking ético)?***
No, no se efectuaron pruebas.

***5.5.10 ¿Se utilizan antivirus y antispyware actualizados en los dispositivos tecnológicos?***
Se utiliza el Microsoft Defender.

***5.5.11 ¿Existen controles que garanticen que se utiliza sólo software aprobado por el Organismo?***
La instalación del software sólo se realiza bajo la supervisión de la Gerencia de Tecnologías de la Información y Comunicación, a través de sus profesionales que tienen clave de administrador.

***5.5.12.- ¿La política de contraseñas obliga el uso de contraseñas fuertes?***
Si, la política de contraseñas ha cambiado recientemente, y en la actualidad sólo se permiten contraseñas fuertes y además obliga a su cambio periódicamente.

***5.5.13.- ¿Cuentan con un esquema de múltiple factor de autenticación?***

El esquema de múltiple factor de autenticación solo es requerido para aquellos profesionales con perfil de administrador, y habilitado (a solicitud del interesado) para el resto del personal. El ingreso al data center es por huella digital, y el doble factor de autenticación se utiliza para ingresar a los sistemas y configuraciones con perfil de administrador.

### *C.6.- Control de Criptominería*

***6.1.- ¿Se instrumentan controles para detectar procesos no autorizados de minería de criptomonedas?***

El acceso al Centro de Procesamiento de Datos es restringido. Asimismo, se ha implementado un analizador de tráfico de red (Zabbix).

***Observación***

En mérito al resultado del relevamiento realizado se entiende que el ENARGAS cuenta con herramientas y procedimientos en materia de ciberseguridad, no obstante lo cual no se ha realizado una revisión integral de la Política de Seguridad de la Información, aprobada en el año 2017, y de los procedimientos redactados (sin aprobación), a fin de contar con documentos actualizados, acordes a los avances tecnológicos, y con el conocimiento y consentimiento del personal, a través de la conformación y funcionamiento del Comité de Seguridad de la Información.

Asimismo, observada la metodología de trabajo del Área de Seguridad, no se verificó el desarrollo de un Plan de Acción, en el cual se expliciten los objetivos fijados, los medios disponibles y los plazos de concreción establecidos.

***Recomendación***

*Se entiende necesario que la Gerencia de Tecnologías de la Información y Comunicación, a través del Área de Seguridad de la Información, impulse la revisión integral de la Política de Seguridad de la Información vigente, y ponga en funcionamiento al Comité de Seguridad de la Información.*

*Asimismo, se recomienda la elaboración de un Plan de Trabajo Anual, que permita fijar los objetivos en materia de ciberseguridad, medios necesarios y plazos comprometidos. Todo ello con el objeto de proteger los activos críticos, los datos sensibles y los sistemas del Organismo, garantizando así la confidencialidad, integridad y disponibilidad de la información.*

*Un Plan de Trabajo, desarrollado y aprobado, permite gestionar metódicamente vulnerabilidades, y deberá incluir la mitigación de riesgos de seguridad mediante la implantación de medidas técnicas, organizativas y legales, así como la capacitación y concientización del personal para reducir el error humano.*

## *D.- OPINIÓN DEL AUDITADO*

El contenido del presente Informe fue puesto en conocimiento de la Gerencia de Tecnologías de la Información y Comunicación mediante ME-2026-

09094938-APN-UAI#ENARGAS, a fin de que efectúe las consideraciones y comentarios que estime corresponder.

Atento que a la fecha no se ha recibido respuesta del auditado, se considera que comparte el contenido del presente Informe.

## *E.- CONCLUSIÓN*

A partir de las tareas desarrolladas y considerando el Alcance definido, se concluye que la Gerencia de Tecnología de la Información y Comunicación, a través del Área de Seguridad de la Información, posee un razonable grado de cumplimiento de los procedimientos que garantizan la seguridad de la información, no obstante lo cual se considera necesario que se efectúe una revisión integral de la Política de Seguridad de la Información actualmente vigente, y se elabore un Plan de Acción que permita identificar los objetivos fijados, medios necesarios y plazos comprometidos.

SUÁREZ TRILLO Beatriz

Firmado digitalmente por SUÁREZ TRILLO Beatriz
Fecha: 2026.01.28 10:48:26 -03'00'