

**INFORME UAI N° 10/20 de la UNIDAD DE AUDITORÍA INTERNA  
Infraestructura Crítica de Tecnología de la Información**

**CONTENIDO**

<b>INFORME EJECUTIVO .....</b>	<b>2</b>
<b>INFORME ANALÍTICO .....</b>	<b>5</b>
<b>I.- OBJETO .....</b>	<b>5</b>
<b>II.- ALCANCE .....</b>	<b>5</b>
<b>III.- COMENTARIOS Y CONSIDERACIONES .....</b>	<b>5</b>
<b>III.1.- Normativa de Aplicación .....</b>	<b>5</b>
<b>III.2.- Tareas realizadas .....</b>	<b>5</b>
<b>III.3.- Objetivos de Control.....</b>	<b>6</b>
<b>III.4.- Regularización de observaciones anteriores.....</b>	<b>11</b>
<b>IV.- OBSERVACIONES.....</b>	<b>11</b>
<b>V.- RECOMENDACIONES.....</b>	<b>11</b>
<b>VI.- OPINIÓN DEL AUDITADO.....</b>	<b>12</b>
<b>VII.- CONCLUSIÓN.....</b>	<b>13</b>

**INFORME UAI N° 10/20 de la UNIDAD DE AUDITORÍA INTERNA  
Infraestructura Crítica de Tecnología de la Información**

**INFORME EJECUTIVO**

**I.- OBJETO**

Verificar la aplicación de los controles presentados en el Instructivo de Trabajo N° 4/2020 SIN de la Sindicatura General de la Nación (SIGEN) "Infraestructura Crítica de Tecnología de la Información", en el ámbito del Ente Nacional Regulador de la Electricidad (ENRE).

**II.- ALCANCE**

El presente informe se basa en el relevamiento realizado sobre los Aspectos Descriptivos y Aspectos Generales de Control, conforme lo establecido en el Instructivo de Trabajo N° 04/20 SIN de SIGEN.

Se consideraron como objetivos de control, los temas propuestos en el Instructivo mencionado.

Dada la naturaleza de los temas abarcados en el presente informe, a continuación, se detallan las unidades de estructura relacionadas con los mismos:

- ✓ Área de Sistemas de Información (ASI)
  - División de Desarrollo de Sistemas
  - División de Seguridad Informática
  - División Administración de Servidores y Soporte Técnico
  - División de Redes y Comunicaciones

Las tareas realizadas se llevaron a cabo durante los meses de Noviembre y Diciembre 2020.

**III.- COMENTARIOS Y CONSIDERACIONES**

Se detallan en el Informe Analítico.

**IV.- OBSERVACIONES**

IV 1.- Política de Seguridad de la Información. A la fecha no se cuenta con un documento actualizado que identifique claramente los elementos de infraestructura crítica del Organismo. (Punto 1)



IV 2. Controles de acceso. En la actualidad el Responsable de Seguridad Informática (RSI), no lleva un registro de los sitios protegidos. (Punto 3)

IV 3.- Instalaciones de suministro de energía. No se dispone de múltiples líneas de suministro para evitar un único punto de falla en el suministro de energía. (Punto 5)

IV 4.- Suministro de energía ininterrumpible (UPS). Se observa que si bien se cuenta con un suministro de energía ininterrumpible (UPS), el mismo sólo asegura el apagado regulado y sistemático. (Punto 6)

IV 5. Generador de respaldo. Se observa que si bien el Edificio Madero, cuenta con un generador, el Organismo no se encuentra conectado al mismo, por deficiencias técnico-eléctricas. (Punto 7)

IV 6.- Respaldo o Backup. Se observa que no se encuentra formalmente documentado y aprobado el procedimiento de resguardo de la información del ENRE. (Punto 10)

IV 7.- Gestión de contingencias. Se observa que el ENRE no cuenta con un Plan de Contingencias o Plan de Recuperación de Desastres ante la ocurrencia de una contingencia prolongada que comprometa la disponibilidad del CPD, que permita mitigar los efectos de la misma. (Punto 15)

## **V.- RECOMENDACIONES**

V 1.- Política de Seguridad de la Información. Se recomienda actualizar el documento de análisis de riesgos de TI, como base para la identificación de la infraestructura crítica, (Punto 1)

V 2. Controles de acceso. Se recomienda la implementación de un registro de los accesos a los sitios protegidos. (Punto 3)

V 3.- Instalaciones de suministro de energía. Se recomienda analizar la situación de no contar con doble punto de suministro para evitar un único punto de falla en la energía eléctrica. (Punto 5)

V 4.- Suministro de energía ininterrumpible (UPS). Se recomienda evaluar por cuanto tiempo la UPS permite sostener las actividades críticas, y si tiene la autonomía requerida para tal efecto. (Punto 6)

V 5. Generador de respaldo. Se recomienda llevar adelante las gestiones para analizar y solucionar las deficiencias técnico-eléctricas que impiden la conexión del CPD del ENRE al generador del edificio. (Punto 7)

V 6.- Respaldo o Backup. Se recomienda continuar con las tareas necesarias que le permitan al ASI contar con un procedimiento de Backup documentado y formalmente aprobado. (Punto 10)

V 7.- Gestión de contingencias. Se recomienda que el ASI desarrolle un Plan de Contingencias o Plan de Recuperación de Desastres, que permita mitigar los efectos de una contingencia prolongada en el Centro de Procesamiento de Datos Principal. (Punto 15)

## **VI.- OPINIÓN DEL AUDITADO**

Se detalla en el Informe Analítico.



ENTE NACIONAL REGUL

"2020 - Año del General Manuel Belgrano"

## VII.- CONCLUSIÓN

Respecto del presente Instructivo de Trabajo N° 4/2020 SIN de SIGEN, denominado "Controles referidos a la Infraestructura Crítica de Tecnología de la Información", se señala que esta UAI, ha realizado el relevamiento requerido, al Área de Sistemas de Información (ASI) del ENRE, para desarrollar la actividad indicada. En tal sentido se concluye que, si bien en gran parte de los temas analizados, los controles sobre las infraestructuras críticas de TI, se gestionan de manera razonable, existen aún cuestiones pendientes que se deberán llevar adelante, generando cambios y de ese modo, permitir regularizar los cumplimientos parciales y los no cumplimientos pendientes a la fecha de cierre.

Lic. MONICA PASCUAL  
AUDITOR  
ENTE NACIONAL REGULADOR de la ELECTRICIDAD

**INFORME UAI N° 10/20 de la UNIDAD DE AUDITORÍA INTERNA**  
**Infraestructura Crítica de Tecnología de la Información**

**INFORME ANALITICO**

**I.- OBJETO**

Verificar la aplicación de los controles presentados en el Instructivo de Trabajo N° 4/2020 SIN de la Sindicatura General de la Nación (SIGEN) "Infraestructura Crítica de Tecnología de la Información", en el ámbito del Ente Nacional Regulador de la Electricidad (ENRE).

**II.- ALCANCE**

El presente informe se basa en el relevamiento realizado sobre los Aspectos Descriptivos y Aspectos Generales de Control, conforme lo establecido en el Instructivo de Trabajo N° 04/20 SIN de SIGEN.

Se consideraron como objetivos de control, los temas propuestos en el Instructivo mencionado.

Dada la naturaleza de los temas abarcados en el presente informe, a continuación, se detallan las unidades de estructura relacionadas con los mismos:

- ✓ Área de Sistemas de Información (ASI)
  - División de Desarrollo de Sistemas
  - División de Seguridad Informática
  - División Administración de Servidores y Soporte Técnico
  - División de Redes y Comunicaciones

Las tareas realizadas se llevaron a cabo durante los meses de Noviembre y Diciembre 2020.

**III.- COMENTARIOS Y CONSIDERACIONES**

**III.1.- Normativa de Aplicación**

- ✓ **Instructivo de Trabajo N° 04/20 SGN** "Infraestructura Crítica de Tecnología de la Información".
- ✓ **Resolución SGN N° 48/05:** Controles de Tecnología de la Información.

**III.2.- Tareas realizadas**



ENTE NACIONAL REGUL

"2020 - Año del General Manuel Belgrano"

El trabajo fue desarrollado considerando los temas propuestos en el IT N° 4/20, para lo cual se llevaron a cabo las siguientes tareas:

- ✓ Presentación formal al ASI del cuestionario recibido vía GDE por IF-2020-77797552-APN-SIN#SIGEN, de fecha 17/11/20, mediante Memorándum ME-2020-79660553-APN-UAI#ENRE, de la Unidad de Auditoria Interna, de fecha 18/11/20.
- ✓ Consultas vía correo electrónico con cada uno de los responsables de las unidades mencionadas y personal de las mismas, que participó en la elaboración de las respuestas, obteniendo de este modo la información y la correspondiente documentación de respaldo.
- ✓ Dichas unidades completaron, una copia del formulario del instructivo, la cual se incorporó al legajo de los papeles de trabajo del proyecto.
- ✓ Elaboración del presente informe.
- ✓ Posteriormente se procedió a realizar la carga en la página desarrollada por SIGEN a tal efecto.

### III.3.- Objetivos de Control

De acuerdo a lo indicado en el Instructivo de Trabajo N° 4/20 SIN de SIGEN, se realizó un relevamiento y análisis de los controles requeridos, en los que el foco de la labor fue puesto en los aspectos descriptivos y los aspectos generales de control de la Infraestructura Crítica de Tecnología de la Información.

La información relevada respecto de los aspectos descriptivos del Centro de Procesamiento de Datos (CPD) donde se alojan los servicios informáticos críticos del organismo, comprende:

- Administración propia o por terceros.
- Ubicación
- Provisión de energía eléctrica
- Provisión de enlace de telecomunicaciones
- Disponibilidad
- Sitio de procesamiento alternativo
- Impacto por contingencia

En cuando a los aspectos generales de control, se relevaron los siguientes temas:

1. Política de Seguridad de la Información.
2. Responsabilidad por la protección de la infraestructura crítica.
3. Controles de acceso.
4. Controles de acceso – Registro de Visita.



ENTE NACIONAL REGUL

"2020 - Año del General Manuel Belgrano"

5. Instalaciones de suministro de energía del CPD.
6. Suministro de Energía In-interrumpible (UPS).
7. Generador de Respaldo del CPD Principal.
8. Seguridad Física del CPD Principal.
9. Mantenimiento de los equipos críticos.
10. Respaldo backup.
11. Gestión de Incidentes.
12. Análisis de vulnerabilidad.
13. Protección.
14. Actualizaciones de software.
15. Gestión de contingencias.

### **Aspectos Descriptivos**

1. El CPD (Centro de Procesamiento de Datos) donde se alojan los servicios informáticos críticos del ENRE, es administrado por el Organismo.
2. Los servidores y equipos donde residen dichos servicios informáticos críticos, se encuentran ubicados físicamente en el CPD Principal (edificio Madero) y en el CPD Secundario (El CPD Secundario es otro centro de cómputos del Organismo, en el cual también residen servicios informáticos críticos), en este caso en el Edificio Suipacha.
3. El proveedor de energía eléctrica contratado para los servicios informáticos críticos del Organismo es EDESUR S.A. tanto para el CPD Principal del Edificio Madero, como para el CPD Secundario, del Edificio Suipacha.
4. En cuanto a los proveedores de enlaces de telecomunicaciones para los servicios informáticos críticos del Organismo, para el CPD principal, son las empresas IPLAN S.A. y Telefónica de Argentina S.A. y para el edificio Suipacha es Telefónica.
5. En principio el Organismo no tolera interrupciones, en su operación de servicios críticos. Tal es el caso de la Unidad Operativa de Atención al Público, de la cual depende el Call Center del ENRE que toma los reclamos de los usuarios, por lo que se requiere disponibilidad de los servicios 24 Hs. x 365 días. En cuanto al resto de los procesos tienen una tolerancia de 2 horas sin servicio.
6. Ante una contingencia que pudiera afectar el normal procesamiento de las operaciones en el CPD Principal, se cuenta como sitio de procesamiento alternativo, otras instalaciones en el Edificio Suipacha. Los sistemas se encuentran replicados en forma cruzada en los dos CPD del ENRE.



7. En cuanto a la infraestructura crítica en análisis, el impacto en relación a una posible contingencia sería público o social y en el ejercicio de las funciones propias.

## **Aspectos Generales de Control**

### **1. Política de Seguridad**

El ENRE posee una política de seguridad de la información, formalmente aprobada por Resolución ENRE N° 517/06 de fecha 22/06/2006, que fuera publicada en el Boletín Oficial N° 30.947 con fecha 14/07/2006.

Dicha política se actualizó posteriormente, para adecuarse a lo requerido en la Disposición ONTI N° 01/2015, siendo aprobada por Resolución ENRE N° 122/18.

Respecto de la identificación de los elementos de infraestructura crítica de tecnología de la información, el Área de Sistemas de Información (ASI) informa que existe un documento referido al análisis de riesgo que contiene dicha identificación, pero que no se encuentra actualizado. En tal sentido se propone realizar una actualización durante el 2021.

### **2. Responsabilidad por la Protección de la Infraestructura Crítica**

Se ha asignado formalmente la responsabilidad por la protección de las infraestructuras críticas de información a los jefes de las Divisiones del ASI: Administración de Servidores y Soporte Técnico, Comunicaciones y Redes, de Desarrollo de Sistemas y Seguridad Informática. Dicha asignación se concretó por Disposición ENRE N° 108/07 que define las responsabilidades de los mismos.

### **3. Controles de Acceso**

En la actualidad no se lleva un registro de los sitios protegidos. Se prevé la implementación de un sistema de control biométrico en el acceso al CPD, ya instalado en las sedes Suipacha y Florida. Asimismo, también se prevé implementar un registro de los accesos a los CPD. Asimismo, las visitas son acompañadas por personal del ASI.

El CPD Principal se encuentra ubicado en un lugar al cual no puede tener acceso el personal no autorizado, dado que existen los siguientes controles: Tarjetas magnéticas personalizadas para el acceso al edificio y al piso correspondiente y cerraduras en el sector de sistemas y en la sala del CPD.

Los controles asociados a la protección física de accesos al CPD, se realizan mediante cámaras Web, las que se activan fuera del horario habitual del personal del ASI.

### **4. Controles de Acceso – Registro de Visitas**

En la actualidad el ASI cuenta con un registro de visitas al CPD. Asimismo, las visitas son acompañadas por personal del sector.

Como se mencionara en párrafos anteriores, también cuenta con cámaras Web.

### **5. Instalaciones de Suministro de Energía del CPD**





El equipamiento está protegido con respecto a las posibles fallas en el suministro de energía eléctrica por medio de la UPS en función estabilizadora, que protege las instalaciones contra perturbaciones.

En la actualidad el edificio en el que se encuentra el CPD principal no dispone de múltiples líneas de suministro para evitar un único punto de falla en el suministro de energía.

## **6. Suministro de Energía In-interrumpible (UPS)**

El ENRE cuenta con un suministro de energía in-interrumpible (UPS) que sólo asegura el apagado regulado y sistemático del equipamiento que sustenta las operaciones críticas en el CPD Principal. No se ha informado, por cuanto tiempo permite operar la UPS.

Los equipos de UPS son inspeccionados y probados periódicamente para asegurar que funcionan correctamente. Estas tareas se realizan mediante la contratación de terceros para la revisión de los mismos.

## **7. Generador de Respaldo del CPD Principal**

De acuerdo a lo informado por el ASI, no se dispone de un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía eléctrica.

El edificio Madero cuenta con un generador del consorcio, pero el ENRE no se encuentra actualmente conectado por una falla en el tablero de conexión al Organismo.

## **8. Seguridad Física del CPD Principal**

En el CPD Principal se utiliza piso ducto y techo técnico. Asimismo, los cables de energía eléctrica se encuentran separados en bandejas o ductos diferentes de los de comunicaciones para evitar interferencias.

Por otra parte, cabe mencionar que el CPD cuenta con aire acondicionado principal y de respaldo. De todas formas, se recomienda realizar una revisión de la instalación eléctrica de los mismos, para corroborar que funcionan correctamente.

El CPD Principal cuenta con alarmas por alta temperatura. Se instalaron alarmas sonoras y visuales por alerta de temperatura.

En cuanto a los extinguidores, se cuenta con dos matafuegos manuales. Asimismo, dentro del CPD, existen detectores de humo.

## **9. Mantenimiento de los Equipos Críticos**

El ASI mantiene un listado actualizado del equipamiento crítico con el detalle de la frecuencia en que se realiza el mantenimiento preventivo. Se lo registra en la Base de Pedidos a Sistemas, como tareas realizadas por el ASI.

Se registran todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado, en la Base de Pedidos a Sistemas, como registro de todas las tareas efectuadas.

En general el mantenimiento de los equipos críticos se realiza on site. Asimismo, la información crítica se encuentra almacenada en storage de discos.

## **10. Respaldo o Back-Up**

Se realizan backups periódicos de los datos, programas y configuraciones de sistemas críticos.

Si bien el procedimiento de resguardo de la información crítica no se encuentra formalmente documentado y aprobado, surge de la base de documentación del ASI que existen varios instructivos de la División de Administración de Servidores y Soporte Técnico, a cargo de las tareas de backup y restauración.

Se cuenta con instalaciones de resguardo que garantizan la disponibilidad de toda la información y del software crítico del Organismo, mediante réplicas de dichos sistemas.

El Responsable del ASI dispone y controla la realización de las copias de resguardo críticas, así como la prueba periódica de su restauración e integridad.

Por otra parte, se almacenan copias de resguardo en otra ubicación diferente al CPD principal, en un sitio alejado al mismo. Las copias de backup se guardan en edificios cruzados.

## **11. Gestión de Incidentes**

En cuanto a los procedimientos formales de comunicación y de respuesta a incidentes críticos de seguridad de TI, se han aprobado los siguientes: - Procedimiento para la administración de incidentes (DI-2020-5-APN-ENRE3MDP), - Procedimiento para la detección de actividades no autorizadas en el acceso a sistemas y servicios de información (Disp. ENRE N° 54/15), - Procedimiento para la administración de problemas (DI-2020-6-APN-ENRE#MDP).

Los incidentes de seguridad son comunicados a través de las autoridades o canales apropiados tan pronto como es posible, tomando conocimiento el RSI de cualquier incidente o violación de seguridad.

## **12. Análisis de Vulnerabilidades**

De acuerdo a lo informado por el RSI, se realizan escaneos de vulnerabilidades con el sistema NEXUS, cada cuatro (4) meses, sobre sistemas operativos y servicios, además de servidores, equipos de red, como routers, firewalls y switches. En caso de detectar vulnerabilidades, se toman las medidas necesarias para tratar los riesgos asociados.

## **13. Protección**

El ASI utiliza herramientas de protección contra virus y otros softwares maliciosos, de modo de proteger a todos los recursos críticos.

## **14. Actualizaciones de software**

El ASI aplica mecanismos de control para asegurar la actualización del software con los parches y configuraciones de seguridad recomendadas.

## **15. Gestión de Contingencias**

Actualmente el ENRE no cuenta con Plan de Contingencia o Plan de Recuperación ante Desastres para mitigar los efectos que pudiera ocasionar la ocurrencia de una contingencia que comprometa la disponibilidad del CPD.



Si bien existen instructivos sobre los temas particulares de recuperación de backup, de instalación de servidores y las aplicaciones críticas están replicadas en otros servidores y en edificios cruzados, no se cuenta con un plan de contingencias propiamente dicho.

### **III.4.- Regularización de observaciones anteriores**

Del Informe UAI N° 12/14, se encuentran pendientes de regularización las siguientes observaciones asociadas al tema planteado en el presente informe:

N° 4.- Se observa que no se encuentra formalmente documentado y aprobado el procedimiento de resguardo de la información crítica del ENRE.

N° 6.- Se observa que el ENRE no cuenta con un Plan de Contingencias o Plan de Recuperación de Desastres que permita mitigar los efectos de una contingencia prolongada en el Centro de Procesamiento de Datos Principal.

## **IV.- OBSERVACIONES**

IV 1.- Política de Seguridad de la Información. A la fecha no se cuenta con un documento actualizado que identifique claramente los elementos de infraestructura crítica del Organismo. (Punto 1)

IV 2. Controles de acceso. En la actualidad el Responsable de Seguridad Informática (RSI), no lleva un registro de los sitios protegidos. (Punto 3)

IV 3.- Instalaciones de suministro de energía. No se dispone de múltiples líneas de suministro para evitar un único punto de falla en el suministro de energía. (Punto 5)

IV 4.- Suministro de energía ininterrumpible (UPS). Se observa que si bien se cuenta con un suministro de energía ininterrumpible (UPS), el mismo sólo asegura el apagado regulado y sistemático. (Punto 6)

IV 5. Generador de respaldo. Se observa que si bien el Edificio Madero, cuenta con un generador, el Organismo no se encuentra conectado al mismo, por deficiencias técnico-eléctricas. (Punto 7)

IV 6.- Respaldo o Backup. Se observa que no se encuentra formalmente documentado y aprobado el procedimiento de resguardo de la información del ENRE. (Punto 10)

IV 7.- Gestión de contingencias. Se observa que el ENRE no cuenta con un Plan de Contingencias o Plan de Recuperación de Desastres ante la ocurrencia de una contingencia prolongada que comprometa la disponibilidad del CPD, que permita mitigar los efectos de la misma. (Punto 15)

## **V.- RECOMENDACIONES**

V 1.- Política de Seguridad de la Información. Se recomienda actualizar el documento de análisis de riesgos de TI, como base para la identificación de la infraestructura crítica, (Punto 1)



V 2. Controles de acceso. Se recomienda la implementación de un registro de los accesos a los sitios protegidos. (Punto 3)

V 3.- Instalaciones de suministro de energía. Se recomienda analizar la situación de no contar con doble punto de suministro para evitar un único punto de falla en la energía eléctrica. (Punto 5)

V 4.- Suministro de energía ininterrumpible (UPS). Se recomienda evaluar por cuanto tiempo la UPS permite sostener las actividades críticas, y si tiene la autonomía requerida para tal efecto. (Punto 6)

V 5. Generador de respaldo. Se recomienda llevar adelante las gestiones para analizar y solucionar las deficiencias técnico-eléctricas que impiden la conexión del CPD del ENRE al generador del edificio. (Punto 7)

V 6.- Respaldo o Backup. Se recomienda continuar con las tareas necesarias que le permitan al ASI contar con un procedimiento de Backup documentado y formalmente aprobado. (Punto 10)

V 7.- Gestión de contingencias. Se recomienda que el ASI desarrolle un Plan de Contingencias o Plan de Recuperación de Desastres, que permita mitigar los efectos de una contingencia prolongada en el Centro de Procesamiento de Datos Principal. (Punto 15)

## **VI.- OPINIÓN DEL AUDITADO**

Como es habitual, se solicitó al Área la correspondiente opinión del auditado, respecto de los incumplimientos y los cumplimientos parciales, y su compromiso de acción reparadora. A continuación, se detallan para cada una de las observaciones planteadas, la respuesta del ASI.

VI 1.- Política de Seguridad de la Información. El ASI propone actualizar el documento de análisis de riesgos que identifica las infraestructuras críticas, en el último trimestre de 2021. (Punto 1)

VI 2. Controles de acceso. En la actualidad las visitas son acompañadas. Se prevé implementar un registro de los accesos a los CPD. (Punto 3)

VI 3.- Instalaciones de suministro de energía. El ASI considera que el tema no depende del Área de Sistemas y prevé revisarlo con el Departamento Administrativo. (Punto 5)

VI 4.- Suministro de energía ininterrumpible (UPS). El ASI considera que el tema no depende del Área de Sistemas y prevé revisarlo con el Departamento Administrativo. (Punto 6)

VI 5. Generador de respaldo. En opinión del ASI, sería importante que se le asigne a un especialista en instalaciones eléctricas el seguimiento y gestión del tema. El ASI considera que el tema no depende del Área de Sistemas y prevé revisarlo con el Departamento Administrativo. (Punto 7)

VI 6.- Respaldo o Backup. Si bien la División de Administración de Servidores y Soporte Técnico, a cargo de las tareas, cuenta con instructivos internos, en el transcurso de 2021 se desarrollarán los procedimientos de backup requeridos. (Punto 10)

VI 7.- Gestión de contingencias. Existen instructivos sobre temas particulares de recuperación de backup, de instalación de servidores y las aplicaciones críticas están replicadas en otros servidores y en edificios cruzados como así también los resguardos de información. Se solicitará



ENTE NACIONAL REGUL

"2020 - Año del General Manuel Belgrano"

una reactivación del Comité de Seguridad de la Información y del Comité de Sistemas, pues no estuvo operando por movimientos de personal. (Punto 15)

## VII.- CONCLUSIÓN

Respecto del presente Instructivo de Trabajo N° 4/2020 SIN de SIGEN, denominado "Controles referidos a la Infraestructura Crítica de Tecnología de la Información", se señala que esta UAI, ha realizado el relevamiento requerido, al Área de Sistemas de Información (ASI) del ENRE, para desarrollar la actividad indicada. En tal sentido se concluye que, si bien en gran parte de los temas analizados, los controles sobre las infraestructuras críticas de TI, se gestionan de manera razonable, existen aún cuestiones pendientes que se deberán llevar adelante, generando cambios y de ese modo, permitir regularizar los cumplimientos parciales y los no cumplimientos pendientes a la fecha de cierre.

Lic. MONICA PASCUAL  
AUDITOR  
ENTE NACIONAL REGULADOR de la ELECTRICIDAD