

# UNIDAD DE AUDITORIA INTERNA

## INFORME UAI SRT N° 42/2017

**“Plan de Contingencia - Circular S.G.N. N° 02/2007”**



Superintendencia de  
Riesgos del Trabajo

Enero de 2018

**INFORME UAI SRT N° 42/17  
RESUMEN EJECUTIVO**

**“Plan de Contingencia - Circular S.G.N. N° 02/2007”**

**OBJETO**

Actualizar el relevamiento acerca de la existencia, actualización y suficiencia de un plan de contingencias destinado a asegurar la continuidad de las operaciones de los procesos críticos, siguiendo el marco general propuesto por la Circular 02/07 SIGEN.

**CONCLUSIÓN**

Como resultado de la tarea realizada, se estima concluir que, si bien el Organismo cuenta con razonables prevenciones para asegurar la continuidad de las operaciones de los procesos críticos, se advierte que la documentación referente al Plan de

Se mantienen vigentes observaciones formuladas en anteriores informes de esta Unidad y que a continuación se transcriben:

- Al no poseer un procedimiento desarrollado y aprobado que contemple la identificación, clasificación y categorización de los incidentes y los pasos a seguir por parte del Responsable de Seguridad de la información, ante eventuales incidentes en del Organismo; se incrementa el riesgo de incurrir en un incorrecto tratamiento de tales incidentes. (Informe UAI SRT N° 42/2010)
- La falta de actualización en la documentación del DRP ante cambios ocurridos tanto referida al hardware y software instalado, como también en el esquema del personal interno y proveedores externos; incrementa el riesgo de pérdida de eficacia o eficiencia ante una eventual necesidad de restaurar las funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción por la ocurrencia de un evento inesperado. (Informe UAI SRT N° 39/2014)
- Al extenderse la periodicidad de las pruebas del DRP mas allá de un año aniversario se incrementa el riesgo de no contar con una adecuada actualización del plan en cuanto su eficacia para restablecer los servicios ante la ocurrencia de un evento imprevisto o inesperado. (Informe UAI SRT N° 39/2014)
- Al no encontrarse formalmente establecidos los propietarios de la información y la criticidad de los datos no se da acabado cumplimiento a lo especificado en la Política de Seguridad de la Información, vigente en el Organismo. La situación descrita debilita la seguridad de la información y dificulta la identificación de

aquella cuya recuperación resulta prioritaria ante la eventual ocurrencia de un desastre. (Informe UAI SRT N° 39/2016 )

- Las Políticas de Seguridad de la Información vigentes en el Organismo no han sido actualizadas desde su aprobación, por Resolución SRT N° 231/2009. La situación descrita, al tiempo que contraviene las previsiones contenidas en las mismas políticas que prevén su periódica revisión y actualización, incrementa el riesgo de omitir el considerar mejores prácticas en la materia. (Informe UAI SRT N° 21/2017).
- Encontrándose inactivo el Comité de Seguridad de la Información no se da acabado cumplimiento, en esta materia, a lo dispuesto en la Política de Seguridad de la Información vigente incrementándose el riesgo de desatender las acciones a cargo de dicho Comité. (Informe UAI SRT N° 21/2017).

### **OPINION DEL AREA AUDITADA**

Los comentarios de la Subgerencia sobre la versión preliminar de este trabajo han sido considerados en la presente redacción definitiva

**Buenos Aires, 31 enero de 2018**

**INFORME UAI SRT N° 42/17**

**“Plan de Contingencia - Circular S.G.N. N° 02/2007”**

**INDICE**

<b>INFORME PRELIMINAR .....</b>	<b>I</b>
<b>1. OBJETO.....</b>	<b>I</b>
<b>2. ANTECEDENTES.....</b>	<b>2</b>
<b>2.1. NORMATIVOS.....</b>	<b>2</b>
<b>2.2. DOCUMENTALES.....</b>	<b>2</b>
<b>3. ALCANCE .....</b>	<b>2</b>
<b>4. DESARROLLO.....</b>	<b>2</b>
<b>4.1. MARCO DE REFERENCIA.....</b>	<b>2</b>
<b>4.2. PROGRAMA DE TRABAJO .....</b>	<b>3</b>
<b>4.2.1. CAPÍTULO 3 .....</b>	<b>3</b>
<b>4.2.1.1. RESPONSABLE DE LA SEGURIDAD INFORMÁTICA .....</b>	<b>3</b>
<b>4.2.1.2. RESPONSABLE DEL ÁREA INFORMÁTICA.....</b>	<b>3</b>
<b>4.2.2. CAPÍTULO 4 .....</b>	<b>4</b>
<b>4.2.2.1. ORGANIZACIÓN DE LA SEGURIDAD.....</b>	<b>4</b>
<b>4.2.3. CAPÍTULO 5 .....</b>	<b>4</b>
<b>4.2.3.1. CLASIFICACIÓN Y CONTROL DE ACTIVOS .....</b>	<b>4</b>
<b>4.2.4. CAPÍTULO 6 .....</b>	<b>5</b>
<b>4.2.4.1. SEGURIDAD DEL PERSONAL .....</b>	<b>5</b>
<b>4.2.5. CAPÍTULO 7 .....</b>	<b>5</b>
<b>4.2.5.1. SEGURIDAD FÍSICA Y AMBIENTAL .....</b>	<b>5</b>
<b>4.2.6. CAPÍTULO 8 .....</b>	<b>6</b>
<b>4.2.6.1. PROCEDIMIENTOS DE MANEJO DE INCIDENTES .....</b>	<b>6</b>
<b>4.2.6.2. MANTENIMIENTO.....</b>	<b>7</b>
<b>4.2.7. CAPÍTULO 9 .....</b>	<b>10</b>
<b>4.2.7.1. AISLAMIENTO DE LOS SISTEMAS SENSIBLES CAPÍTULO 9 .....</b>	<b>10</b>
<b>4.2.7.2. SINCRONIZACIÓN DE RELOJES.....</b>	<b>10</b>
<b>4.2.8. CAPÍTULO 11.....</b>	<b>10</b>
<b>4.2.8.1. ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL ORGANISMO .....</b>	<b>10</b>
<b>5. CONCLUSIÓN.....</b>	<b>I</b>
<b>6. OPINION DEL ARE AUDITADA.....</b>	<b>15</b>

## **1. OBJETO**

Actualizar el relevamiento acerca de la existencia, actualización y suficiencia de un plan de contingencias destinado a asegurar la continuidad de las operaciones de los procesos críticos, siguiendo el marco general propuesto por la Circular 02/07 SIGEN.

## **2. ANTECEDENTES**

### **2.1. Normativos**

- Circular S.G.N. N° 02/2007, “Evaluación del Políticas de Seguridad de la Información”.
- Disposición O.N.T.I. N° 06/2005
- Resolución S.R.T. N° 1343/2006 “Creación del Comité de Seguridad”.
- Resolución S.R.T. N° 01/2016 “Organigrama de la SRT” Anexo II
- Resolución S.R.T. N° 497/2017 “Manual de Procesos”
- Resolución S.R.T. N° 231/2009 “Política de Seguridad de la Información de la Superintendencia de Riesgos del Trabajo”.

### **2.2. Documentales**

- Instructivo de Trabajo N° 02/2007 – GNyPE
- DRP (Plan de Recuperación ante Desastres)
- Informe UAI SRT N° 42/2010 “Controles de Acceso”
- Informe UAI SRT N° 39/2016 “Base de Datos”
- Informe UAI SRT N° 21/2017 “Seguridad Informática”
- Informe UAI SRT N° 25/2016 “Infraestructura Tecnológica”

## **3. ALCANCE**

La tarea se desarrolló entre el 01/10/17 y el 31/12/17 de conformidad con Normas de Auditoría Gubernamental respecto del estado de situación existente en dicho lapso.

Los procedimientos cumplidos consistieron básicamente, en la realización de entrevistas, relevamiento documental y comprobaciones visuales, verificando en los Planes de Contingencia, los aspectos pertinentes a la seguridad de la información tal como lo propone el Instructivo de Trabajo N° 02/2007 GNyPE, dentro del marco general de la Circular 02/07 SIGEN (Evaluación del Políticas de Seguridad de la Información).

## **4. DESARROLLO**

### **4.1. Marco de Referencia**

La Decisión Administrativa 669/04 instruyó a los Organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156, a adecuar sus políticas de seguridad de la información, conforme a la Política Modelo

a dictar por la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros

Dicha Política Modelo fue establecida en la Disposición ONTI N° 05/2005.

La Sindicatura General de la Nación estableció pautas para verificar el cumplimiento de esas políticas elaborando para ello un Programa de Trabajo de doce capítulos comunicado mediante Instructivo de Trabajo N° 02/2007 – GNYPE.

## **4.2. Programa de Trabajo**

A continuación, para cada título, se transcribe el texto correspondiente que presenta el Anexo I del Instructivo de Trabajo N° 02/2007 – GNYPE; basándose en la numeración dada en la Disposición ONTI N° 06/2005. De dicho Anexo se han extraído las preguntas relativas al objeto del Informe.

### **4.2.1. Capítulo 3**

#### **4.2.1.1. Responsable de la seguridad informática**

3.5. Se encuentran las copias de seguridad y las claves de acceso debidamente protegidas ante casos de contingencia?

*Se encuentran protegidas, física y digitalmente. En medios físicos alojados en una caja ignífuga y digitalmente se encuentran en un datacenter externo.*

3.54 Existe algún procedimiento formalmente establecido para la realización y mantenimiento de las copias de seguridad de la información del Organismo?

*Sí existe. Este se encuentra en proceso de actualización debido a los cambios de locación (Sarmiento 1962) y a los nuevos sitios de contingencia (PVNet).*

3.55 Se designó formalmente al responsable de la realización de las copias de seguridad?

*Si, la Resolución SRT N° 01/2016 “Organigrama de la SRT” Anexo II, detalla en el Departamento de Comunicaciones y Seguridad dependiente de la Subgerencia de Sistemas, entre sus tareas, las de:*

- “Administrar y garantizar la realización de resguardos y pruebas de recuperación de la información”
- “Administrar, manejar y controlar las políticas de uso de los servicios de red y de la seguridad de la información”
- “Administrar, mantener y mejorar la solución de contingencias”.

#### **4.2.1.2. Responsable del área informática**

3.65. Existen políticas y procedimientos referentes a recuperación de información y continuidad de operaciones ante la ocurrencia de contingencias?

Existe un plan de contingencia (DRP<sup>1</sup>) documentado y desactualizado. Actualmente se está trabajando en modificaciones sustantivas de la plataforma tecnológica debido a la mudanza de la sede central donde se alojan los servidores principales y al establecimiento de un sitio de contingencia. La Subgerencia de Sistemas ha manifestado que finalizado estos objetivos procederá a actualizar los planes.

3.67 Cuenta el Organismo con antivirus y firewalls actualizados?

Si, posee el Trend Micro OfficeScan XG y Pfsense respectivamente.

3.69 Cuenta el centro de cómputos con sistemas de protección contra incendios?

Tanto el centro de cómputos de Bartolomé Mitre 751 como el de Moreno 401, poseen instalados elementos de detección y combate de incendios dentro y fuera de la sala de servidores (como ser detectores de humo y matafuegos).

3.70 Dispone el área de sistemas de protección contra fallas eléctricas?

Cuenta con llaves térmicas diferenciales y estabilizadas, independientes de las generales (exclusivas para los racks).

También dispone de un “Botón Anti Pánico” al lado de la entrada del Datacenter de Mitre 751 para liberar la apertura de la puerta.

3.74 Se cuenta con más de una persona capacitada para asegurar el funcionamiento de cada sistema?

La Subgerencia cuenta con más de una persona en casi todas las áreas. La excepción la constituye el Departamento de Seguridad y el de Redes y Servidores. El Organismo se encuentra en un proceso de búsqueda para ocupar esas posiciones.

## Capítulo 4

### 4.2.1.3. Organización de la seguridad

4.10 ¿Se designó a los propietarios de la información?

No se han designado formalmente los propietarios de la información, para los sistemas vigentes del Organismo, por lo que sigue vigente la Observación N° 1 del Informe N° 39/2016 “Base de Datos”.

## 4.2.2. Capítulo 5

### 4.2.2.1. Clasificación y control de activos

5.3 Los propietarios de la información ¿han clasificado la información de acuerdo con el grado de sensibilidad y criticidad?

Mediante Resolución SRT N° 497/17 “Manual de Procesos”, el Departamento de Estandarización y Documentación de Procesos diseñó la estructura documental del “Mapa de Procesos” del Organismo, donde están definidos claramente, los sistemas

<sup>1</sup> **DRP**, Plan de Recuperación ante Desastres. Denominación técnica tomada de las siglas del término inglés “Disaster Recovery Plan”

involucrados en cada uno de los procesos, tanto sustantivos, como los de apoyo, seguimiento y control.

#### **4.2.3. Capítulo 6**

##### **4.2.3.1. Seguridad del personal**

6.23 Existe un canal de comunicación formalmente establecido para informar y dar respuesta a incidentes indicando la acción que ha de emprenderse?

No se posee un canal formalmente establecido para informar y dar respuesta a incidentes. Por lo que continúa vigente la observación formulada en el Informe UAI SRT N° 42/2010 “Controles de Acceso” Observación N° 3, en la que se señala que el Organismo no posee un procedimiento desarrollado y aprobado que contemple la identificación, clasificación y categorización de los incidentes y los pasos a seguir por parte del Responsable de Seguridad de la Información, ante eventuales incidentes.

6.24 Se ha informado siempre en forma inmediata al responsable de seguridad informática ante la detección de un supuesto incidente?

Si. Los incidentes son reportados.

6.25 Qué medidas adopta el responsable de seguridad informática ante una emergencia?

Ver ítem 4.2.6.1, apartado 8.54

#### **4.2.4. Capítulo 7**

##### **4.2.4.1. Seguridad física y ambiental**

7.25 Los equipos redundantes y la información de resguardo (backup) ¿se almacenan en un sitio seguro y distante del lugar de procesamiento a fin de evitar daños ante eventuales contingencias en el sitio principal?

Los equipos redundantes, se encuentran en lugares seguros y lejos de la ubicación del datacenter principal. Con respecto a la información de resguardo, se almacena en lugares ignífugos, sin acceso público y distante.

7.30 Se realizó un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento a fin de definir qué componentes será necesario abastecer de energía alternativa? Identificar.

En el año 2011 se realizó un Informe de Evaluación de Riesgos - Summary”, donde se identifican y clasifican los posibles riesgos y las probabilidades de ocurrencia en las sedes de Mitre y Moreno. No fue actualizado posteriormente.

7.31 Se dispone de suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Organismo?

Tanto el datacenter de Mitre, como el de Moreno poseen UPS con autonomía de 30 minutos en las 2 fases eléctricas que alimentan los servidores. La Subgerencia de



Sistemas estima que éste es un tiempo acorde al requerido para la dotación de equipos de cada datacenter.

Con respecto al datacenter PVNet, que se posee como plan de contingencia, posee una certificación TIER II (TIER es una certificación o “clasificación” de un Data Center en cuanto a su diseño, estructura, desempeño, fiabilidad, inversión y retorno de inversión. TIER II, cuenta con UPS o fuente alternativa de electricidad en caso de emergencia, brindando una disponibilidad del 99,741%).

7.32 Los planes de contingencia ¿contemplan las acciones que han de emprenderse ante una falla de la UPS?

Existe un plan de contingencia documentado y desactualizado. Actualmente se está trabajando en modificaciones sustantivas de la plataforma tecnológica debido a la mudanza de la sede central donde se alojan los servidores principales y al establecimiento de un sitio de contingencia. Finalizado estos objetivos se procederá a actualizar los planes.

7.33 Los equipos de UPS ¿se inspeccionan y prueban periódicamente para asegurar si funcionan correctamente y si soportan la carga requerida durante un tiempo preestablecido?

Para realizar el mantenimiento y prueba de las UPS se ha contratado a un servicio terciarizado.

7.35 Los generadores son probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor?

La sede central de Mitre no posee generador y la Sede Moreno cuenta con grupo electrógeno en la terraza para uso exclusivo del centro de cómputos. La sede Sarmiento 1962 posee un generador y ya ha sido probado una vez.

7.37 Los interruptores de emergencia ¿se encuentran ubicados cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica?

Junto a la puerta entrada del Datacenter de Mitre 751, se dispone de un “Botón Anti Pánico” para liberar la apertura de la puerta ante una urgencia.

#### **4.2.5. Capítulo 8**

##### **4.2.5.1. Procedimientos de manejo de incidentes**

8.53 Existen procedimientos para los planes de contingencia normales?

Existen procedimientos para los planes de contingencia (DRP), no actualizados, ya que actualmente se está trabajando en modificaciones sustantivas de la plataforma tecnológica debido a la mudanza de la sede central (Mitre a Sarmiento), donde se alojan los servidores principales, como también tareas para finalizar la implementación de un sitio de contingencia (PVNet).

Continúa vigente la Observación N° 1 del Informe UAI SRT N° 39/2014 “Plan de Contingencia”.

8.54 Se definieron las primeras medidas a adoptar para responder ante las contingencias?

Acorde al Punto 2 - Marco de actividades (Actividades durante el desastre) del DRP del Organismo, las primeras medidas a adoptar para responder ante contingencias son:

“Una vez verificada la contingencia por el Coordinador, Disparar la alarma de emergencia. El coordinador Senior del DRP, será el encargado de agilizar las acciones, proporcionar las autorizaciones correspondientes para que el Plan se lleve adelante acorde a lo planificado.”

Primeras medidas:

- El Coordinador notifica al Coordinador Senior del DRP que la solución a la continuidad de las operaciones, superaran el tiempo de tolerancia.
- Se evalúa el alcance de la Emergencia que le ha sido reportada y decide el curso de acción.
- De no estar, acude al edificio afectado para recabar información.
- Toma la decisión de declarar o no el desastre, según informe brindado por los distintos grupos operativo y de Emergencia.
- Se asegura que todos los integrantes de los distintos grupos operativos de Emergencia estén notificados en caso de declararse el desastre.
- Toma medidas preventivas que permita mitigar los riesgos de la emergencia actual.

Ver ítem 4.2.1.2 – apartado 3.65.

8.57 Se comunicó la contingencia a las personas afectadas o involucradas con la recuperación?

Ver ítem 4.2.4.1 – (6.23).

8.58 Se notificó de la medida adoptada ante la contingencia a la autoridad y/o Organismos pertinentes?

No hay una comunicación formalizada. Ver ítem 4.2.4.1 – (6.23).

#### **4.2.5.2. Mantenimiento**

8.123 Se determinan los requerimientos para resguardar cada software o dato en función de su criticidad?

Los requerimientos para el resguardo de software se determinan para los desarrollos propios y para la información generada por el Organismo (bases de datos); no así para el software de terceros. Y no es referenciada en función de su criticidad, ya que el Organismo posee un esquema de resguardo Completo (o Total). Ver siguiente punto (esquema de Resguardo).

8.124 Se definió y documentó un esquema de resguardo de la información?

Está definido y no documentado. Pese a ello el esquema de resguardo de la información del Organismo, como procedimiento, se encuentra definido de la siguiente manera:

Los Back Up del Organismo se realizan “Completo” (Se resguarda toda la información existente), con una periodicidad diaria, variando únicamente la frecuencia de guardado. En ninguno de los casos se realiza back ups incrementales, ni diferenciales.

Frecuencia diaria (4 días hábiles martes a viernes), se guarda toda la semana. Ej: BKU del martes es pisado por el BKU del siguiente martes.

Back Up semanales (lunes), se guardan por un mes.

Back Up mensuales: primer lunes del mes. Se conservan por un año.

Back Up anuales: los dos primeros días hábiles del año, quedan permanentes.

8.125 Se prueban los sistemas de resguardo periódicamente para garantizar que cumplen con los requerimientos de los planes de continuidad de las actividades del Organismo?

Los sistemas de resguardo son utilizados diariamente.

Ver Frecuencia punto 4.2.6.2 – (8.124)

8.126 Se definen procedimientos para el resguardo de la información?

La Resolución SRT 1565/10 “Manual de Procedimientos Informáticos”, Capítulo 4: “Procedimiento para el resguardo de la Información” es el procedimiento normado y aprobado para el tratamiento del Back Up, con la salvedad que se han innovado ciertos procesos manuales con procesos automáticos programados, con un robot HP Storage Works 1/8 G2.

8.127 Se cuenta con un esquema de rótulo de las copias de resguardo que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente?

Se cuenta con un esquema de rótulos de cintas; controladas por medio de códigos de barra, el cual posee: ID del Dispositivo, fecha y hora de realización del Back Up y Tipo de Copia.

8.128 Existe un esquema de reemplazo de los medios de almacenamiento de las copia de resguardo?

Sí, se reemplazan los dispositivos anualmente de manera tal que un soporte se utiliza sólo durante el año calendario, luego se resguarda como backup anual.

8.129 Se almacena en ubicación remota un nivel mínimo de información de resguardo junto con registros exactos y completos de las copias de resguardo y los procedimientos documentados de restauración?

Todos los backs up realizados por el Organismo son resguardados en ubicación remota. En Moreno 401 se almacenan las cintas y en el datacenter PVNet se almacenan digitalmente en un servidor dispuesto para ello.

8.130 La información de resguardo ¿se almacena una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal?

Ver ítem 4.2.6.2, apartado 8.129.

8.131 Se tienen al menos tres generaciones de back-up o ciclos de información de resguardo para la información y el software esenciales para el Organismo?

Se guardan los backs up anuales, desde la implementación del procedimiento de back up, cumpliéndose el primer BK Anual en (2011).

8.132 Para la definición de información mínima a ser resguardada en el sitio remoto ¿se tiene en cuenta el nivel de clasificación otorgado a la misma en términos de disponibilidad?

Tal como se menciona en el esquema de resguardo de la información (ver ítem 4.2.6.2 – apartado 8.124), los Back Up del Organismo se realizan “Completo” (se resguarda toda la información existente). No se realiza en ninguno de los casos, back ups incrementales, ni diferenciales.

8.133 Se asigna a la información de resguardo un nivel de protección física y ambiental conforme a las normas aplicadas en el sitio principal?

La información del datacenter de Bartolomé Mitre 751 es copiada en cintas que posteriormente se resguardarán en el edificio de Moreno 401 en una caja ignífuga. La información virtual es guardada en el datacenter de PVNet. En ambos casos se cumple con los niveles de protección física y ambiental conforme a las normas de seguridad recomendadas, por las políticas de Seguridad de la Información del Organismo.

8.134 Se prueban los medios de resguardo?

Ver ítem 4.2.6.2 apartado 8.124

8.135 Se prueban periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento en el tiempo asignado a la recuperación en los procedimientos operativos

Todos los lunes se realizan pruebas de restauración de datos en cinta (archivos de usuarios, de correo, etc) seleccionadas de forma aleatoria.

Para las pruebas de recupero de Bases de Datos, se constató que se realizan, entre tres y cuatro recuperos al año, a pedido de usuarios de la SRT, por pérdida y/o extravío de información en diferentes bases de datos de producción.

#### 4.2.6. Capítulo 9

##### 4.2.6.1. Aislamiento de los sistemas sensibles capítulo 9

9.170 Qué recaudos de seguridad se adoptan para estos sistemas frente a ABM y modificaciones de perfiles de usuarios, políticas de resguardo, plan de contingencia y de recupero frente a desastres?

Los recaudos de seguridad son: controles de acceso físico a los servidores y lógico a los sistemas; logs de uso de los sistemas; back up y restore de todas las bases de datos del Organismo.

9.175 Se realizan pruebas sobre los planes de resguardo (backup), planes de contingencia planes de recupero ante desastres?

Ver ítem 4.2.6.2 apartado 8.135.

##### 4.2.6.2. Sincronización de relojes

9.240 Se dispone para dispositivos móviles planes de contingencia ante cualquier incidente o eventualidad en los cuales estuvieran expuestos los sistemas de información del Organismo?

En dispositivos móviles (notebook, ultrabook, netbook) pertenecientes a la SRT, se corren aplicaciones web de desarrollo propio, con accesos controlados a bases de datos del Organismo, residente en los servidores centrales. Por lo tanto, en dichos dispositivos no se guarda información del Organismo.

#### 4.2.7. Capítulo 11

##### 4.2.7.1. Administración de la continuidad de las actividades del Organismo

11.6 Se ha elaborado y documentado una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordadas?

Se dispone de un esquema de redundancia que permite restaurar la totalidad de bases de datos y servicios garantizando la continuidad de la totalidad de las actividades del Organismo.

11.7 Se han aprobado planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada?

El Organismo posee un Plan de Continuidad (DRP) que estuvo en el orden del día de la Reunión de Comité de Seguridad del 17/11/2011. Ver ítem 4.2.1.2 – apartado 3.65. Este Plan no ha sido actualizado

11.8 Se han coordinado pruebas y actualizaciones periódicas de los planes y procesos implementados?

Continúan vigentes las Observaciones N° 1 y N° 2 formulada en el Informe UAI SRT N° 39/2014 “Plan de Contingencia”, en la que recomienda la actualización del DRP y que se asegure la ejecución del plan de pruebas con una periodicidad suficiente para asegurar el mantenimiento de su eficacia en el tiempo, respectivamente.

11.9 Se ha considerado la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo?

El esquema de redundancia permite reestablecer la totalidad de las actividades del Organismo. Se cuenta con seguro anual para el equipamiento.

11.10 Se han identificado los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades como, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio?

Ver ítem 4.2.5.1 apartado 7.30.

11.11 Se han evaluados los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación?

Ver ítem 4.2.5.1 apartado 7.30.

11.13 Se han identificado los controles preventivos (sistemas de supresión de fuego detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales etc).

Se han identificado los controles preventivos y se los expone en el Informe UAI SRT N° 25/2016 “Infraestructura Tecnológica” y en el Informe de Evaluación de Riesgos - Summary”.

11.14 Han participado los propietarios de los procesos y recursos de información y el responsable de seguridad informática en los procesos de identificación y evaluación de riesgos?

Se interactuó con los participantes de Sistemas en la confección del “Informe de Evaluación de Riesgos - Summary”. Ver ítem 4.2.5.1., apartado 7.30.

11.15 Se consideraron todos los procesos de las actividades del Organismo sin limitarse a las instalaciones de procesamiento de la información?

El “Informe de Evaluación de Riesgos”, se realizó exclusivamente para incidentes informáticos.

11.16 Como resultado de la evaluación de riesgos ¿se ha desarrollado un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo?

Se ha realizado un DRP (Disaster Recovery Plan). Ver ítem 4.2.1.2 apartado 3.65)

11.17 El plan estratégico ha sido aprobado por el comité de seguridad de la información?

El plan estuvo en el orden del día de la Reunión de Comité de Seguridad del 17/11/2011. No se ha actualizado.

11.18 Dicho comité ¿ha elevado el plan estratégico a la máxima autoridad de la organización para su aprobación?



En la reunión del Comité de Seguridad del 17/11/2011, en donde estuvo el plan como orden del día, participó el Gerente General del Organismo. No se ha actualizado.

11.19 Los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo ¿han sido elaborados por los propietarios de procesos y recuperos de información con la asistencia del responsable de seguridad informática?

Los planes de contingencia fueron elaborados por una consultora y con la asistencia del responsable de seguridad informática. No obstante, actualmente se está trabajando en modificaciones sustantivas de la plataforma tecnológica debido a la mudanza de la sede central donde se alojan los servidores principales, como también al establecimiento de un sitio de contingencia. La Subgerencia de Sistemas ha manifestado que, finalizados estos objetivos, se procederá a actualizar los planes de contingencia dando intervención a los propietarios de los procesos.

11.21 Durante el proceso de planificación se han identificado acuerdos respecto de todas las responsabilidades y procedimientos de emergencia?

Los planes de contingencia fueron elaborados por una consultora y con la asistencia del responsable de seguridad informática.

11.22 Se ha realizado el análisis de los posibles escenarios de contingencia y definición de acciones correctivas a implementar en cada caso?

Sí, se ha realizado análisis de posibles escenarios de contingencia en el DRP. Pese a ello, no se encuentran vigentes, debido a que actualmente se está modificando sustantivamente la plataforma tecnológica debido a la mudanza de la sede central donde se alojan los servidores principales.

11.26 Se desarrolló el proceso de capacitación del personal involucrado en los procedimientos de reanudación y recuperación?

**Si. El personal está en conocimiento de sus roles.**

11.29 Se incluyeron procedimientos de divulgación en el plan de contingencia?

**No posee procedimientos de divulgación.**

11.31 Se adecuaron procesos específicos para el personal involucrado? ¿Cuenta el personal involucrado con documentación específica que indique cuál es su participación en el proceso de contingencia?

El DRP, posee en el punto 6 la conformación del “Equipo de Recuperación”, con Organigrama, Responsabilidades y Misiones de cada uno. Posee listados de personal bajo cada uno de los grupos con teléfonos y puesto que les compete.

Al día de la fecha estos listados se encuentran desactualizados. Igualmente, cada área reconoce y cuenta con un responsable de la tarea. La Subgerencia de Sistemas manifestó que a la brevedad actualizaría los listados.

11.34 Existen copias de los planes de contingencia almacenados en sitios alternativos?

Si, en cinta.

11.36 Están claramente especificados en cada plan de continuidad las condiciones para su puesta en marcha?

Se encuentran especificadas en el DRP. Ver ítem 4.2.1.2 apartado 6.65. Desactualizado.

11.37 Se designó a los responsables de ejecutar cada componente del mismo?

Si, en el DRP, Capítulo 6. Ver ítem 4.2.8.1 apartado 11.31. Desactualizado.

11.38 En caso de requerirse modificaciones ¿están las mismas aprobadas por el comité de seguridad de la información?

Actualmente el Comité de Control se encuentra inactivo, por lo que se encuentra vigente la Observación N° 2 del Informe UAI SRT N° 21/2017 “Seguridad Informática”.

11.39 Se designó para cada plan de continuidad un administrador y un encargado de coordinar las tareas definidas en el mismo?

Se posee un coordinador y un encargado para el DRP, no así para cada procedimiento.

Pese a ello, se posee un titular y suplente para cada Grupo del Recovery Team. Ver ítem 4.2.8.1 apartado 11.31. Desactualizado.

11.41 Se encuentran definidos los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana?

El Capítulo 8 “Procesamiento de Emergencia” del DRP, posee Alertas, Matriz de Escalamiento y Procedimientos de Recuperación de Incidentes. Desactualizado.

11.42 Existen procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas?

Ver ítem 4.2.8.1 – apartado 11.41.

11.43 Se redactaron los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo?

Ver ítem 4.2.8.1 – apartado 11.41.

11.46 Se encuentran documentadas las responsabilidades de las personas describiendo la responsabilidad de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles, mencionando alternativas cuando corresponda?

Sí, en el DRP, Capítulo 6. Ver ítem 4.2.8.1 – apartado 11.31. Desactualizado.



11.47 Se designó el responsable de declarar el estado de contingencia y se definieron detalladamente sus funciones?

Ver ítem 4.2.6.1 – apartado 8.54 “Primeras medidas”.

11.48 Se tiene conocimiento y disponibilidad en el Organismo de los planes de contingencia de los proveedores de los servicios utilizados, así como la obligación contractual de los mismos de disponer de dichos planes?

El Organismo no tiene disponible los planes de contingencia de los proveedores de los servicios utilizados. Se debería consultar a la Gerencia de Administración y Finanzas sobre la posibilidad de anexar a obligaciones contractuales el poner a disposición los planes de contingencia.

11.49 Existe un cronograma de pruebas periódicas de cada uno de los planes de contingencia?

No se posee un cronograma de pruebas, pese a ello se están haciendo pruebas en cada uno de los servidores por la migración del datacenter.

11.50 Se indica el cronograma de pruebas a los responsables de llevar a cabo cada una de las pruebas y de Elevar el resultado obtenido al comité de seguridad informática?

El DRP especifica las pruebas a llevar a cabo por sus responsables. Actualmente el Comité de Seguridad de la Información se encuentra inactivo, por lo que se encuentra vigente la Observación N° 2 del Informe UAI SRT N° 21/2017 “Seguridad Informática”.

11.51 Se utilizan técnicas para garantizar que los planes de contingencia funcionaran ante un hecho real?

Las técnicas utilizadas son las recomendadas por los especialistas del Soporte Premium de Microsoft.

11.52 Se efectuaron pruebas de discusión de diferentes escenarios evaluando diferentes alternativas de recuperación del negocio?

Ver ítem 4.2.8.1 – apartado 11.53.

11.53 Se realizaron simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión luego de incidentes o crisis)?

A mediados de 2016, se hicieron pruebas de laboratorio sobre el uso de los servicios de Always\_On<sup>2</sup> (servicio brindado por el nuevo datacenter de contingencia PVNet) sobre todos las bases de datos del Organismo.

11.54 Se efectuaron pruebas de recuperación técnica para garantizar que los sistemas de información puedan ser restablecido con eficacia?

<sup>2</sup> **Always On**, Es un datacenter paralelo al productivo, espejando la información como respaldo, donde también se encuentran los centros de proceso de datos y se encarga de estar 'siempre en funcionamiento'. En caso de un incidente o desastre, el Always On, levanta los procesos y el Negocio continúa.

Ver ítem 4.2.6.2 – apartado 8.135.

11.57 Se efectúan pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Organismo en paralelo con operaciones de recuperación fuera del sitio principal)?

A fin del 2017 se efectuaron pruebas de recuperación en un sitio alternativo (PVNet).

11.58 Se realizan pruebas de instalaciones y servicios de proveedores para garantizar, por medio de convenios por escrito, que los productos y servicios de proveedores externos cumplan con el compromiso contraído?

El Organismo posee un uso permanente de Servicios de enlaces, housing de servicios y ambiente virtualizado en locaciones remotas. (PVNet y Sarmiento).

11.61 Se revisan y actualizan periódicamente los planes de continuidad de las actividades del Organismo para garantizar su eficacia permanente?

Ver ítem 4.2.1.2 – apartado 3.65.

11.62 ¿Cuál fue el resultado de la última prueba? ¿Se registraron progresos respecto de la anterior?

Tanto las pruebas realizadas a mediados del 2016 y fines del 2017, tuvieron resultados satisfactorios. Se identificaron y corrigieron errores menores como así también fueron documentados.

11.66 Se definieron las modificaciones a los planes de contingencia que deben ser aprobadas por el comité de seguridad de la información? Se las implementó?

Ver ítem 4.2.8.1 – apartado 11.38

11.67 Se comunicó fehacientemente a todo el personal los planes de contingencia y las modificaciones realizadas a los mismos?

Todo el personal involucrado en los planes de contingencia, se encontraban fehacientemente comunicados.

## **5. CONCLUSIÓN**

Como resultado de la tarea realizada, se estima concluir que, si bien el Organismo cuenta con razonables prevenciones para asegurar la continuidad de las operaciones de los procesos críticos, se advierte que la documentación referente al Plan de Contingencias (DRP) y procedimientos de seguridad asociados no se encuentran actualizados en función de la situación relevada.

## **6. OPINION DEL AREA AUDITADA**

Los comentarios de la Subgerencia sobre la versión preliminar de este trabajo han sido considerados en la presente redacción definitiva.

**Buenos Aires, 31 Enero de 2018.**