

**INFORME UAI SRT N° 21/17**

**"Seguridad Informática"**

**INDICE**

<b>INFORME UAI SRT N° 21/17 .....</b>	<b>1</b>
<b>1. OBJETO .....</b>	<b>2</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>2.3. ESTÁNDARES .....</b>	<b>2</b>
<b>3. ALCANCE .....</b>	<b>3</b>
<b>4. DESARROLLO .....</b>	<b>3</b>
<b>4.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>3</b>
<b>4.1.1. OBSERVACIÓN.....</b>	<b>4</b>
<b>4.1.2. RECOMENDACIÓN .....</b>	<b>4</b>
<b>4.2. COMITÉ DE SEGURIDAD .....</b>	<b>4</b>
<b>4.2.1. OBSERVACIÓN.....</b>	<b>4</b>
<b>4.2.2. RECOMENDACIÓN .....</b>	<b>5</b>
<b>4.3. SEGREGACIÓN DE FUNCIONES Y RESPONSABILIDADES.....</b>	<b>5</b>
<b>4.4. ADMINISTRACIÓN DE CONTRASEÑAS .....</b>	<b>6</b>
<b>4.4.1. OBSERVACIÓN.....</b>	<b>7</b>
<b>4.4.2. RECOMENDACIÓN .....</b>	<b>7</b>
<b>4.5. ACCESO FÍSICO A LOS SERVIDORES.....</b>	<b>7</b>
<b>4.6. PUESTOS DE TRABAJO .....</b>	<b>8</b>
<b>4.7. TRABAJO REMOTO .....</b>	<b>8</b>
<b>4.8. SOFTWARE DE MONITOREO .....</b>	<b>9</b>
<b>4.8.1. OBSERVACIÓN.....</b>	<b>10</b>
<b>4.8.2. RECOMENDACIÓN .....</b>	<b>10</b>
<b>4.9. SEPARACIÓN DE AMBIENTES .....</b>	<b>10</b>
<b>4.10. INCIDENTES INFORMÁTICOS.....</b>	<b>11</b>
<b>4.11. INTERCONEXIÓN DE LA RED INFORMÁTICA.....</b>	<b>12</b>
<b>5. CONCLUSIÓN .....</b>	<b>15</b>
<b>6. OPINION DEL AREA AUDITADA.....</b>	<b>15</b>

## **1. OBJETO**

Obtener evidencias y extraer conclusiones acerca de la existencia, eficacia y suficiencia de políticas, procedimientos y actividades tendientes a asegurar la confidencialidad, integridad y disponibilidad de la información.

## **2. ANTECEDENTES**

### **2.1. Normativos**

- Resoluciones O.N.T.I. N° 06/2005 y 03/2013 "Política de Seguridad de la Información Modelo"
- Resolución S.G.N. N° 48/2005, "Normas de Control Interno para Tecnología de la Información".
- Resolución S.R.T. N° 1343/2006 "Comité de Seguridad"
- Circular S.G.N. 02/2007 "Evaluación de Políticas de Seguridad de la Información"
- Resolución S.R.T. N° 231/2009 "Política de Seguridad de la Información de la Superintendencia de Riesgos del Trabajo".
- Resolución S.R.T. N° 1565/10 "Manual de Procedimientos Informáticos – ANEXO"
- Disposición A.P.N. N° 03/2013 "Evaluación de las Política de Seguridad de la Información"
- Resoluciones S.R.T. N° 1/2016 y 712/17 "Estructura Orgánica funcional de la Superintendencia De Riesgos Del Trabajo (S.R.T.)" - Anexo II

### **2.2. Documentales**

- Instructivo de Trabajo N° 02/2007 GNyPE "Política de Seguridad de la Información"
- Acta Marco de Cooperación Institucional Ministerio de Trabajo – 56/2016
- Expediente S.R.T. N° 112858/16 "Convenio de Cooperación entre el Ministerio de Trabajo, Empleo y Seguridad Social y la Superintendencia de Riesgos del Trabajo"
- Convenio N° 01/16 - Convenio Marco con Provincia Net
- Convenio N° 10/16 - Convenio Específico Complementario N°1 con Provincia Net
- Expediente SRT N° 16564/16 "Convenio Marco de Acciones Estratégicas entre la SRT y PROVINCIA NET/GRUPO PROVINCIA."
- Convenio N° 34/16 - Convenio Interadministrativo Exp. SRT N° 121202/16
- Expediente S.R.T. N° 121202/16 "Convenio Interadministrativo con PROVINCIA NET"
- Informe de Evaluación de Riesgos – Summary v1.0.
- Acta de Incidentes.
- Topología del Organismo.

### **2.3. Estándares**

- CobIT 4.0

### 3. ALCANCE

La tarea se llevó a cabo entre Febrero y Julio de 2017, sobre el estado de situación existente en dicho período, desarrollándose de conformidad con las Normas de Auditoria Gubernamental.

Se realizaron entrevistas, relevamiento documental, comprobaciones visuales, pruebas sustantivas y de cumplimiento; y se desarrolló teniendo en cuenta determinados lineamientos del marco general que propone la Circular N° 02/07 SIGEN y en la Resolución SRT 231/09 (Políticas de Seguridad de la Información de la SRT).

Se verificó la administración de los usuarios de red, políticas, normas y procedimientos de seguridad de redes, como también de los protocolos y otros sistemas de seguridad (Aplicaciones de administración remota, VPN's, FTP's, etc.)

Se cotejó la adhesión al modelo de política de seguridad informática en cuanto refiere a este tema en particular.

Las cuestiones inherentes a Planes de Contingencia y DRP<sup>1</sup> (Plan de Recuperación ante Desastres) serán abordadas en un proyecto por separado.

### 4. DESARROLLO

#### 4.1. Políticas de Seguridad de la Información

En consonancia con lo dispuesto por la Decisión Administrativa N° 669/04, la Oficina Nacional de Tecnologías de Información (ONTI) mediante disposición N° 06/05 aprobó un Modelo de "Políticas de Seguridad de la Información"

En ese contexto, el Organismo por medio de la Resolución SRT N° 231/2009 aprobó la "Política de Seguridad de la Información de la Superintendencia de Riesgos del Trabajo", vigente.

En su oportunidad, como resultado de las actividades requeridas por la Circular SGN N° 02/2007, particularmente las inherentes a su capítulo 3, se evaluó que las políticas aprobadas por la Resolución antes mencionada cumple con las pautas lo dispuestas en dicho modelo.

A posteriori, por Disposición N° 03/2013, la ONTI aprobó una actualización del Modelo de Política, adecuándola a los cambios producidos en la norma *ISO/IEC27002*<sup>2</sup>, ampliando temas ya existentes e incorporando otros.

La norma vigente en el Organismo satisface, en líneas generales, los requerimientos del nuevo modelo.

En su apartado 3.1 la propia Política previene que sea revisada, al menos, con una periodicidad anual, a efectos de mantenerla actualizada, teniendo en cuenta posibles

<sup>1</sup> DRP, denominación técnica tomada de las siglas del término inglés "Disaster Recovery Plan"

<sup>2</sup> **ISO/IEC 27002** es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.

cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

#### **4.1.1. Observación**

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 descripta, 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.

#### **4.1.2. Recomendación**

Se recomienda a la Subgerencia de Sistemas impulsar la actualización de las Políticas de Seguridad de la Información, sobre base Modelo aprobado en el Anexo I de la Disposición ONTI. N° 03/2013

### **4.2. Comité de Seguridad**

Mediante Resolución SRT N° 1343/06, con las funciones definidas en su artículo 4º, se dispuso la creación del Comité de Seguridad integrado por un representante de todas las gerencias y subgerencias del Organismo.

En su Artículo 5º se asignó interinamente como Responsable de Seguridad de la Información de la S.R.T., al entonces Sr. Jefe del Departamento de Desarrollo y Soporte Informático. En virtud estructura orgánica funcional del Organismo vigente, se estima que tal responsabilidad recae actualmente en la Subgerencia de Sistemas.

La existencia de este tipo de Comité está contemplada en las Políticas del Organismo, como así también en el modelo aprobado en el Anexo I de la Disposición ONTI. N° 03/2013.

Entre las competencias del Comité se encuentra la de definir a los "propietarios de la información", cuestión no resuelta hasta la fecha, por lo que se estima mantener la vigencia la Observación que, con tal motivo, se formuló en ocasión del Informe UAI SRT N° 39/16. Que observa, que 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.

El Comité Seguridad de la Información no registra actividad.

#### **4.2.1. Observación**

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.

#### 4.2.2. Recomendación

Se recomienda a la Subgerencia de Sistemas impulsar el reinicio de las actividades del Comité de Seguridad de la Información.

#### 4.3. Segregación de funciones y responsabilidades

COBIT 4.1 declara en su Apéndice VII, que "*Segregación funciones / Separación de tareas*", es un control interno básico que previene y detecta errores o irregularidades por medio de la asignación a individuos diferentes, de la responsabilidad de iniciar y registrar las transacciones y la custodia de los activos.

El Marco de Trabajo COBIT, incluye en los Controles Generales de TI, Controles de Aplicación y Seguridad de la Información a la "Segregación de funciones", (entre otros controles) en el denominado, "Controles de Aplicaciones de los Procesos del Negocio".

En las estructuras organizativas vigentes en el periodo en examen (Resoluciones S.R.T. N° 01/16 y N° 712/17)" se asignan a la Subgerencia de Sistemas la responsabilidad primaria de entender en la evaluación, desarrollo, coordinación y ejecución de todas aquellas acciones que permitan implementar y mantener un servicio eficiente de procesamiento de información bajo la plataforma tecnológica correspondiente cumpliendo con las necesidades del Organismo.

De ella dependen los cuatro departamentos que seguidamente se mencionan detallando aquellas acciones que les han sido asignadas vinculadas con Seguridad Informática.

##### 1 Departamento de Comunicaciones y Seguridad:

- Instalar y mantener las redes de comunicación de voz y datos.
- Administrar, monitorear y controlar los servicios de comunicaciones de voz y datos de todo el Organismo.
- Participar en el diseño topológico e instalación primaria de dispositivos que hacen al servicio de comunicaciones de voz.
- Monitorear la operatividad de la totalidad del equipamiento informático y de telecomunicaciones de la organización, incluidos los servicios asociados (enlaces).
- Administrar y garantizar la realización de resguardo y pruebas de recuperación de la información.
- Administrar, mantener 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 contingencia.

##### 2 Departamento de Servidores Centrales y Equipamiento:

- Coordinar y planificar la instalación, mantenimiento y administración de los equipos centrales de procesamiento de datos, tanto en su operación local como remota, de acuerdo a los planes operativos establecidos.
- Instalar, administrar y mantener el software de base y de aplicación utilizados para la transmisión y recepción remota de datos.

- Instalar, administrar y mantener el software y hardware destinado a soportar la información del Organismo en los diferentes entornos de servicio.
- Entender en la definición de las políticas y estrategias de resguardo de la información, como así también velar por su correcto funcionamiento general, incluidos los procesos de recuperación.
- Formular las especificaciones técnicas de los pliegos de adquisición y contratación de equipos, servicios e insumos informáticos, así como en la recepción y control de su calidad y prestaciones proponiendo la renovación de equipos y actualización del software.
- Proponer la renovación de equipos y actualización del software en consonancia con las necesidades de las diferentes áreas del Organismo y/o la evolución de la tecnología en general.
- Intervenir, relevar y recomendar toda nueva plataforma de software o hardware destinada a satisfacer requerimientos en materia de tecnología.
- Administrar, monitorear y controlar los servidores del Organismo.

### **3 Departamento de Desarrollo**

### **4 Departamento de Soporte a Usuarios**

De acuerdo a la Resolución S.R.T. N° 231/09 Anexo I, el Gerente de Sistemas (con la estructura actual de Subgerente de Sistemas), cumple la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la S.R.T. Tiene la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

La Gerencia de Sistemas dispone de una adecuada delimitación de tareas y funciones entre sus sectores, acorde a las normativas vigentes.

#### **4.4. Administración de contraseñas**

Se ha verificado que, para todos los usuarios (internos y externos) que necesiten ingresar a las redes informáticas del Organismo, se han implementado una serie de premisas de logueo<sup>3</sup>, acordes a lo normado en la Resolución SRT N° 1565/10 "Manual de Procedimientos Informáticos", Capítulo 4 "Administración de Usuarios", y en base a la Resolución SRT N° 231/09 "Políticas de Seguridad de la Información", Punto 9.5.3 "Administración de contraseñas de Usuario", y el Punto 9.8.4 "Sistema de Administración de Contraseñas":

- ✓ En lo que a administración de contraseñas respecta:
  - Contraseñas individuales.
  - La contraseña caduca en 60 días.
  - Contraseña Robusta conteniendo letras, números y por lo menos un carácter especial, con mayúsculas y minúsculas.

<sup>3</sup> **Logueo:** Inicio de Sesión en una red Informática, PC o servicio.

- Una longitud de 8 caracteres mínima y un máximo de 16.
  - Bloqueo de la cuenta con 3 intentos de contraseña incorrecta y demorando 15 minutos para el desbloqueo de la misma.
  - Registro de las últimas (12) contraseñas utilizadas.
- ✓ Control de perfiles:
- Bloqueo y/o suspensión de servicios por inactividad mayor a 38 días.
  - Asignación de accesos y privilegios a usuarios por autorización jerárquica.
  - Limitación del Horario de Conexión de usuarios(es entre las 7:00 y las 21:00 hs.)

A la fecha no se encuentran habilitadas restricciones de Desconexión / Bloqueo de Terminales por Tiempo Muerto.

#### **4.4.1. Observación**

Al no poseer activa la restricción de "Tiempo Muerto", en las terminales del Organismo, donde se bloquee el equipo, al quedar inactivo por un tiempo previamente definido, no solo se estaría incumpliendo con lo normado en el punto 9.8.6 de las políticas de seguridad de la Información; como también se estaría arriesgando, a que personal no autorizado tenga acceso a equipos ya logeados en la red informática del Organismo.

#### **4.4.2. Recomendación**

Se recomienda implementar la restricción de "Tiempo Muerto", en las terminales de toda la Superintendencia de Riesgos del Trabajo, incluyendo las sedes periféricas (Moreno, Sarmiento y Reconquista), como también de las Comisiones Médicas del interior del país; desconectándose o bloqueándose después de un período determinado de inactividad.

#### **4.5. Acceso físico a los Servidores**

Los accesos físicos a las áreas críticas de la red - sala de servidores -, se encuentran protegidas por medio de un control biométrico, permitiendo el acceso solo a personal autorizado, con registro de entrada, salida (día y hora), id de usuario y sector al que pertenecen.

Sólo se encuentran autorizadas 17 personas de la Subgerencia de Sistemas; y por cuestiones de contingencia se ha configurado el acceso de otras 17 (16 de Seguridad / PFA y 1 del Dpto. de Patrimonio, Infraestructura y Logística).

Se cuenta con cámaras con detección de movimiento dentro y fuera del centro de cómputos, dando mayor seguridad y posibilidad de control a los ingresos y egresos.

Con este esquema se estima cumplido el requisito de "Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas" del punto 7.2. "Controles de Acceso Físico", de las Políticas de Seguridad de la Información de la SRT.



#### 4.6. Puestos de Trabajo

Se encuentran implementadas razonables medidas de seguridad física en los puestos de trabajo.

Por configuración de perfiles de acceso a la red, se ha limitado a los usuarios la posibilidad de instalación de software en las PC's.

También se encuentra impedido el acceso a los sistemas operativos en los puestos de trabajo para modificar la configuración del Perfil de Usuario en "Usuarios y Contraseñas".

Se ha configurado el Set Up de los equipos de escritorio, para que no se puedan iniciar desde diskette, CD o Pendrive, siendo el disco rígido, el primero y único para tal fin; luego se anuló el acceso a los "Set Up" de los equipos, poniendo clave administradora en el acceso

Se limitó el acceso a puertos USB, cuya habilitación debe ser justificada por el responsable del área requirente y se colocaron precintos numerados en los gabinetes de las Pc's.

#### 4.7. Trabajo Remoto

El apartado 9.11 de las políticas de seguridad de la información de la Superintendencia de Riesgos del Trabajo se refiere a "Computación Móvil, Trabajo Remoto"

Se considera trabajo remoto cuando se accede o trabaja alejado de las oficinas centrales o de las instalaciones de producción, mediante la utilización de las nuevas tecnologías de información y comunicación (TICs<sup>4</sup>).

En ciertas tareas, agentes del Organismo emplean esta modalidad, tal el caso de los fiscalizadores de la Gerencia de Prevención (GP) y las ATL, que mediante un equipo móvil acceden en consulta y carga consultando y cargando en un módulo de desarrollo propio "Acta Única", al sitio <http://sistemas.srt.gov.ar> (fiscalizadores de la GP) y los inspectores de las ATL, acceden únicamente al sitio [www.srtorg.gob.ar](http://www.srtorg.gob.ar). Las Extranet donde se encuentra montado el sistema de Acta Única poseen protocolo de comunicación HTTPS<sup>5</sup> mediante el certificado SSL<sup>6</sup>, brindando un adecuado nivel de seguridad para su acceso.

Por otro lado los administradores de red y servidores, pueden realizar administración remota de recursos tecnológicos, o sea que poseen acceso remoto a los servidores del Organismo, tanto de la sede Central (Bartolomé Mitre), las periféricas (Moreno,

<sup>4</sup> **TIC:** (Tecnologías de la Información y la Comunicación). Es el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información; como también administración de la red informática, que permite el proceso de dicha información para el trabajo. En estos recursos se pueden englobar la computadora, el fax, el teléfono móvil, Internet, correo electrónico, chat, llamadas sobre IP, videoconferencia, etc.

<sup>5</sup> **HTTPS:** Versión segura del protocolo HTTP. Utiliza una comunicación con un canal encriptado cifrado basado en SSL, creando un canal cifrado para enviar y recibir información sensible.

<sup>6</sup> **SSL:** (Secure Sockets Layer). El SSL es un protocolo de seguridad, diseñado por la empresa Netscape para proveer comunicaciones encriptadas en las redes.



Sarmiento y Reconquista), como también de las Comisiones Médicas del interior del país, para así poder controlar y brindar una solución más rápida ante posibles incidentes Informáticos.

Dicho acceso se realiza por medio de una VPN<sup>7</sup>. La VPN establece contacto entre máquinas que están alojadas remotas y de forma segura, ya que la conexión que se establece entre dichas máquinas, viaja totalmente cifrada, asegurando que los datos no sean vulnerables.

#### **4.8. Software de Monitoreo**

La Subgerencia de Sistemas dispone de diversos software para el monitoreo de redes y equipos a propósito de detectar posibles vulnerabilidades, malos usos y/o abuso de servicios informáticos, vínculos caídos (servidores o servicios), violaciones de las normas de acceso a servidores, Internet, Extranet, sniffers, accesos remotos, etc.

✓ Trend Micro

Para el servicio de antivirus, (sniffers, etc) y proxis (para control de navegación de los usuarios del Organismo y filtrado del SPAM del correo).

✓ GFI Languard

El Departamento de Servidores Centrales y Equipamiento, utiliza el "GFI Languard Network Security Scanner Solución" Versión 7 *TRIAL*<sup>8</sup> para el examen de dispositivos de red para detectar vulnerabilidades, puertos abiertos y servicios en ejecución, para así analizar el estado de seguridad de la red, mediante la generación de informes y poder realizar las correcciones pertinentes.

Al emplearse esta versión no se dispone de la totalidad de las funcionalidades del producto comercializado: programación de soluciones por medio de scripts, avisos a los administradores en forma online (vía correo o SMS), como también, soporte técnico, parches, etc.

✓ ITMetro

Software utilizado por los Departamentos de Comunicaciones y Seguridad y de Servidores Centrales y Equipamiento, para el monitoreo y chequeo de vínculos de servidores y servicios caídos, en cada una de las Comisiones Médicas de la SRT del territorio nacional.

✓ DameWare NT Utilities

Software utilizado por Soporte Técnico, para acceso remoto a los puestos de trabajo de todo el Organismo (Centrales, jurisdiccionales y Comisiones Médicas)

<sup>7</sup> **VPN:** La red VPN, (Virtual Private Network o Red Privada Virtual), conecta una PC a una red privada mediante acceso a Internet en forma segura.

<sup>8</sup> **TRIAL:** Trial es un tipo de software comercial que generalmente permite su uso con algún tipo de restricción (temporal o de otro tipo).

#### **4.8.1. Observación**

Actualmente, para el monitoreo de las redes se utiliza un software en versión de prueba (trial). Esta condición implica disponer menores funcionalidades y no contar con actualizaciones y soporte técnico.

#### **4.8.2. Recomendación**

Se recomienda que la Subgerencia de Sistemas analice la conveniencia de impulsar la adquisición de licencias que aseguren la mayor funcionalidad y soporte de un software para el monitoreo de redes.

### **4.9. Separación de Ambientes**

En las Políticas de Seguridad de la Información con Resolución SRT N° 231/2010, punto 8.1.5 del Anexo I, norma la "Separación de ambientes entre Instalaciones de Desarrollo e Instalaciones Operativas", detallando una serie de controles:

- a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
- b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
- c) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- d) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- e) El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

La separación de ambientes; junto con una adecuada segregación de funciones en los procesos del ciclo de vida de un desarrollo informático procura el control por oposición de intereses entre los esquemas de desarrolladores, administradores de redes y de bases de datos.

Se ha verificado en la Subgerencia de Sistemas del Organismo la existencia de un razonable esquema de separación de los ambientes de desarrollo, prueba y producción, separados, tanto en forma física, como en forma lógica.

El acceso en forma física, se detalla en el punto 4.2 "Acceso físico a los Servidores" del presente informe.

El acceso en forma lógica a los ambientes, se limita con los permisos otorgados a los usuarios; teniendo un esquema de control doble: por base de datos y por red.

En el esquema de Base de Datos han definido ambientes de Desarrollo y de Producción, usándose el de desarrollo como prueba. Al primero acceden desarrolladores y testadores, con, permiso de escritura. En no así para producción, los permisos son de solo lectura

En el esquema de Redes cuenta con los mismos ambientes de trabajo: Desarrollo, y Producción, y en ellos se han creado diferentes grupos de usuarios que poseen permisos (lectura, escritura, modificación, acceso full control, etc), permitiendo al administrador de red, ofrecer una delimitación clara de las tareas entre los ambientes de desarrollo y mantenimiento de sistemas en su esquema.

Para el proceso de transitar y controlar estas etapas del ciclo de vida de un desarrollo, se cuenta con un procedimiento en uso, no aprobado y encontrándose formulada la Observación N° 7 del Informe UAI SRT N° 33/2012 "Ciclo de Vida del desarrollo de Sistemas"; que al día de la fecha sigue vigente.

Este proceso de control se soporta en un sistema propio, desarrollado por la Subgerencia de Sistemas (SiPro), el cual administra los módulos por los que va transitando el desarrollo, registrándose los resultados obtenidos en cada uno de los pasos, (análisis, desarrollo, pruebas, puesta en producción y aprobación final del usuario).

#### **4.10. Incidentes Informáticos**

En el apartado 2.2.8, de las Políticas de Seguridad de la Información de la SRT, define a un incidente de seguridad como *"un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes"*

El Responsable de Seguridad de la Información no solo es el encargado de supervisar el cumplimiento de la P.S.I. y asesorar a los integrantes de la S.R.T. en materia de seguridad de la información; sino que también del seguimiento de la documentación y del análisis de los incidentes de seguridad de la información reportados, así como el manejo de los reportes de incidentes y anomalías producidos en los datos y de los sistemas. Para que luego el Comité de Seguridad que es un cuerpo integrado por representantes de todas las áreas sustantivas de la S.R.T., destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad de seguridad de acuerdo a lo dispuesto en la Resolución S.R.T. N° 1343/06; será el encargado del seguimiento de la evolución e investigación, impulsando la resolución de los incidentes relativos a la seguridad informática.

De acuerdo a CobiT, los incidentes deben ser identificados, clasificados y categorizados; y como mínimo, la clasificación debe determinar la categoría, impacto, urgencia y prioridad. Los incidentes deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte, etc.).

Para ello la Subgerencia de Sistemas, implementó controles internos se realizan en forma manual y/o automáticos para prevenir, detectar y corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema e incluso una red informática. Entre ellos, se encuentran:

- El **firewall** (Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente, decidiendo si permite o bloquea dicho tráfico, en función de un conjunto de reglas de seguridad, previamente definidas.)
- El **servidor proxy** (equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor. Ofreciendo diversas funcionalidades, como ser: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, etc.)
- El **Antispam** (software que utiliza diferentes métodos para prevenir el correo basura o SPAM)

Entre estos controles también deben mencionarse los escaneos y monitoreo de red y equipos, mediante herramientas administrativas de red, las mismas se encuentran detallados en el punto 4.7 "Software de Monitoreo" del presente informe.

En el punto 8.1.3. "Procedimientos de Manejo de Incidentes", de las Políticas de Seguridad de la Información se establece la necesidad de tener procedimientos de manejo de los incidentes relativos a la seguridad, considerando diversos tipos probables de incidentes.

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.

En mayo del 2016 la Subgerencia de Sistemas implementó un libro de actas denominado "Acta de Incidentes", en el que han registrado los sucesos relacionados con ataques a la red, como ser escaneos, denegaciones de servicios, intentos de accesos remotos, entre otros; afectando la continuidad en alguno de los servicios tecnológicos.

Al día de la fecha se han detallado 10 episodios, los cuales 7 fueron incidentes informáticos internos del Organismo y 3 de los episodios por causas de terceros externos (2 servicio eléctrico y 1 del servicio de fibra óptica).

En todos los casos se ha detallado la fecha y hora de ocurrencia, como también la descripción del hecho, el motivo y solución del acontecimiento. Todos los incidentes tuvieron una solución rápida, que van de los 30 minutos hasta 1 día de demora. En ninguno de los casos se ha registrado la clasificación y/o categorización de la estimación de los riesgos ocurridos.

#### **4.11. Interconexión de la Red Informática**

La Superintendencia de Riesgos del Trabajo, suscribió un Convenio Marco con Provincia Net<sup>9</sup> para fortalecer los enlaces de conectividad críticos y mejorar la disponibilidad de las comunicaciones para el Procesamiento y los Servicios de Tecnología de la Información de la S.R.T.

<sup>9</sup> Convenio Marco N° 01/16 22 de Febrero 2016, Expediente S.R.T. N° 16564/16,

El presente trabajo únicamente abordará las cuestiones vinculadas al esquema de conectividad dispuesto, ya que el análisis global del Convenio y sus acuerdos complementarios excede su objeto y alcance.

En ese contexto, entre las actividades comprometidas según Anexo I del Convenio Específico Complementario N° 1<sup>10</sup>; se incluyó la conectividad entre ambas partes

En el Anexo I del Segundo Convenio Específico Complementario<sup>11</sup>, se enumeran 3 actividades:

- Conectividad entre Edificios y Sitios de la S.R.T. - Existencia de vínculos de comunicaciones entre los edificios de Bartolomé Mitre 751, Moreno 401, Reconquista 723 y Sarmiento 1230 de la S.R.T. en C.A.B.A. y la sede de Provincia Net en Bartolomé Mitre 430 en C.A.B.A.
- Conectividad entre Sitios de la S.R.T. y Comisiones Médicas. -Existencia de un vínculo de comunicación entre las CCMM, la S.R.T. y Provincia Net.
- Conectividad entre Sitios de la S.R.T. y Delegaciones del Interior del Ministerio de Trabajo y Seguridad Social.- Existencia de un vínculo de comunicación entre las Delegaciones del interior del país del Ministerio de Trabajo y Seguridad Social, la S.R.T. y Provincia Net.

La implementación de estos vínculos deviene de los compromisos asumidos en el Acuerdo Marco de Cooperación Institucional N° 56/16 (Expediente SRT N° 112858/16), suscripto con el citado Ministerio.

En el Anexo II de este convenio se establecen los Acuerdos de Niveles de Servicio (Disponibilidad – Indisponibilidad) y el Régimen de Penalidades por indisponibilidad del Servicio.

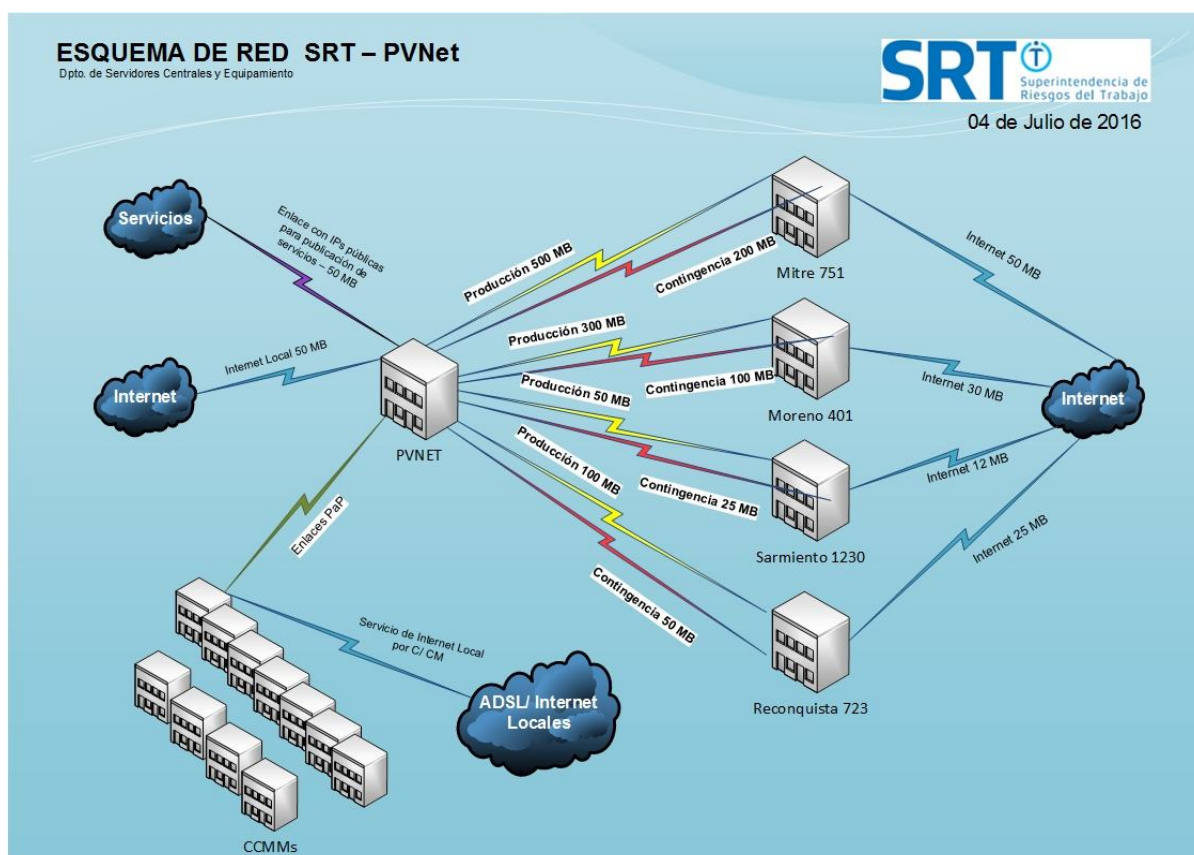
La Subgerencia de Sistemas ha informado que se encuentran operativos los siguientes enlaces.

- Edificio Mitre: Dos (2) enlaces hasta Provincia Net, ya que los enlaces de Producción (500 Mb) y contingencia (200 Mb) irán por caminos distintos.
- Edificio Moreno: Dos (2) enlaces hasta Provincia Net, Producción (300 Mb) y contingencia (100 Mb)
- Edificio Reconquista: Dos (2) enlaces hasta Provincia Net, Producción (100 Mb) y contingencia (50 Mb)
- Edificio Sarmiento: Dos (2) enlaces hasta Provincia Net, Producción (500 Mb) y contingencia (24 Mb)

<sup>10</sup> Convenio Complementario N° 10/16 18 de Marzo de 2016, Expediente S.R.T. N° 16564/16

<sup>11</sup> Convenio Interadministrativo N° 34/16 15 de Junio de 2016, Expediente S.R.T. N° 121202/16





Cuadro 4.11.a: Diagrama de interconectividad entre PVNET, SRT Y CCMM  
(Contempladas en el Anexo I del Convenio Interadministrativo N° 34/16).

Las Comisiones Médicas (CCMM) ubicadas fuera de la C.A.B.A. mantienen activo el esquema de conexión relevado oportunamente en el Informe UAI SRT N° 25/16 "Infraestructura Tecnológica"

En dicho esquema, dependiendo de la CCMM, se cuenta con un vínculo principal *Punto-Multipunto (P2MP)*<sup>12</sup> de 25 Mbps o de 3 Mbps, y otro de contingencia de tipo WAN-ADCL. Todos los enlaces se conectan con la Sede de Moreno 401.

La Subgerencia también ha informado que en las veinte CCMM<sup>13</sup> definidas en el Anexo I del Convenio Complementario antes mencionado se encuentra operativa la conectividad con la red de PvNet, mediante vínculos de 3 Mbps, por cable coaxial o fibra óptica (según disponibilidad local). Del mismo modo se encuentran conectados los 37

<sup>12</sup> **P2MP:** Las redes multipunto son redes en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos. En una red multipunto solo existe una línea de comunicación cuyo uso está compartida por todas las terminales en la red.

<sup>13</sup> CM31 Zarate; CM08 Entre Ríos; CM05 Córdoba; CM07 Rosario; CM11 La Plata; CM12 Mar del Plata; CM33 Rio Cuarto; CM06 Villa María; CM02 Resistencia; CM13 Bahía Blanca; CM09 Neuquén; CM23 Salta; CM17 Santa Rosa; CM03 – Posadas CM04 ,Mendoza, CM14 Junín; CM15 Paso del Rey; CM28 Formosa; CM30 Corrientes; CM35 General Roca.

vínculos entre el Organismo y las unidades desconcentradas del MTEySS contempladas en el Anexo I del Convenio Interadministrativo N° 34/16. En todas estas localizaciones se han instalado dispositivos RUTER CISCO 881, para los Servicios de Red de Datos.

En las veinte CCMM incluidas en el convenio, el vínculo operativo es provisto por PvNet. Este proveedor cuenta con certificación de las normas ISO/IRAM de Sistemas de Gestión ISO/IEC27001, como también la norma TIER II<sup>14</sup>.

Esta Unidad, estima concluir que los dispositivos de conectividad de la red informática del Organismo, son razonablemente seguros, dentro de los lineamientos incluidos en la Política por Seguridad Informática, tanto en el esquema preexistente, tal como se señaló en el mencionado Informe UAI SRT N° 25/16, como en las modalidades acordadas con ProvinciaNet

Al día de la fecha la conectividad de la red informática de la SRT - ProvinciaNet, se configura de acuerdo al diagrama del cuadro 4.11.a.

## **5. CONCLUSIÓN**

Como resultado de la tarea realizada, se estima concluir que existe un razonable nivel de control en los aspectos analizados dentro del alcance definido en el apartado 3, con las salvedades que se mencionan en los apartados 4.1, 4.2, relacionados con la actualización de las políticas y el funcionamiento del Comité de Seguridad de la Información.

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

Mediante correo electrónico con fecha 16/08/2017, la Subgerencia de Sistemas expresó su conformidad con la versión preliminar del presente trabajo.

**Buenos Aires, 17 de Agosto de 2017.**

<sup>14</sup> **TIER II:** Certificado otorgado por el organismo internacional Uptime Insistute. Este certificado garantiza que se trata de un data center redundante, con escasas probabilidades de sufrir interrupciones del servicio. Es decir, constituye todo un aval respecto a los compromisos establecidos en SLA (Service Level Agreement), que fija una disponibilidad del servicio de un 99,7%.