BOLETIN OFICIAL
DE LA REPUBLICA ARGENTINA

Buenos Aires,
jueves 2
de noviembre de 2006

Año CXIV
Número 31.024

Primera Sección
Legislación y Avisos Oficiales

Suplemento

Los documentos que aparecen en el BOLETIN OFICIAL DE LA REPUBLICA ARGENTINA serán tenidos por auténticos y obligatorios por el efecto de esta publicación y por comunicados y suficientemente circulados dentro de todo el territorio nacional (Decreto Nº 659/1947)

Sumario

DISPOSICIONES

Unidad de Coordinación Técnica

CONSEJO NACIONAL DE COORDINACION DE POLITICAS SOCIALES

Disposición 74/2006

Apruébase el Manual de Políticas de Seguridad de los Sistemas de Información del Sistema de Identificación Nacional Tributario y Social (SINTyS) y sus Procedimientos.

Bs. As., 30/8/2006

VISTO, el expediente Nº 19.301/06 de Secretaría General de Presidencia de la Nación, el Decreto Nº 357 de fecha 21 de febrero de 2002, el Decreto Nº 1195 de fecha 5 de julio de 2002, la Decisión Administrativa Nº 669 de fecha 20 de diciembre de 2004, la Disposición Nº 6 de fecha 3 de agosto de 2005, la Resolución C.N.C.P.S. Nº 325 de fecha 21 de noviembre de 2005 y la Disposición U.C.T – C.N.C.P.S. Nº 40 de fecha 22 de noviembre de 2005, y

CONSIDERANDO:

Que mediante el artículo 4 del Decreto Nº 357 de fecha 21 de febrero de 2002, se crea el Consejo Nacional de Coordinación de Políticas Sociales, en el ámbito de la Presidencia de la Nación.

Que a través de los artículos 12 y 13 del Decreto mencionado en el párrafo anterior, se transfieren al ámbito de este Consejo Nacional, el Programa Sistema de Información, Monitoreo y Evaluación de Políticas Sociales – Sistema de Identificación y Selección de Familias Beneficiarios Actuales y Potenciales de Programas Sociales (SIEMPRO-SISFAM), el Programa Sistema de Identificación Nacional Tributario y Social (SINTyS), el Centro Nacional de Organizaciones de la Comunidad (CENOC), la Comisión Nacional Asesora para la Integración de Personas Discapacitadas y el Consejo Nacional de la Mujer.

Que mediante la Decisión Administrativa Nº 669 de fecha 20 de diciembre de 2004, se establece que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8 de la Ley 24.156 y sus modificatorias, deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.

Que asimismo, dispone que las máximas autoridades de dichos organismos, deberán conformar en sus ámbitos un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes del organismo.

Que mediante Disposición Nº 6 de fecha 3 de agosto de 2005 el Sr. Director Nacional de Tecnologías de Información facultado por el Subsecretario de la Gestión Pública de la Jefatura de Gabinete de Ministros de la Nación, aprueba la “Política de Seguridad de la Información Modelo” que como Anexo I forma parte de la misma.

Que mediante Resolución C.N.C.P.S. Nº 325 de fecha 21 de noviembre de 2005, el Señor Secretario Ejecutivo del Consejo Nacional, aprueba la constitución del Comité de Seguridad de la Información, encomendando su coordinación a la titular de la Unidad de Coordinación Técnica del Consejo Nacional mencionado.

Que por el artículo 3 de la Resolución antes mencionada, se establece que la titular de la Unidad de Coordinación Técnica, podrá dictar las normas complementarias, aclaratorias y de aplicación, previendo las adecuaciones necesarias y permanentes para el mejor cumplimiento de los objetivos que se persiguen.

Que mediante la Disposición U.C.T. — C.N.C.P.S. Nº 40 de fecha 22 de noviembre de 2005, se crea el Area de Coordinación Informática del Consejo Nacional con la finalidad de coordinar y administrar los distintos componentes informáticos tendientes a optimizar un mejor aprovechamiento de los recursos existentes y definir criterios técnicos en materia de seguridad de la información, entendiendo, asistiendo y supervisando en los aspectos relativos a seguridad y privacidad de la información.

Que el artículo 4º de la referida Disposición designa al responsable del Area creada.

Que dicho responsable es el Coordinador del Componente de Infraestructura del Programa Sistema de Identificación Nacional Tributario y Social (SINTyS) y ha puesto a consideración de esta Unidad de Coordinación Técnica del Consejo Nacional un Manual de Política de Seguridad de los Sistemas de información del SINTyS y distintos Procedimientos adjuntos al mismo.

Que dichos documentos fueron elaborados en cumplimiento de las disposiciones legales vigentes con el objeto de proteger adecuadamente la información, los sistemas de procesamiento y almacenamiento informático y las comunicaciones del SINTyS.

Que en ese orden de ideas, corresponde elaborar un Manual sobre Políticas de Seguridad y los correspondientes Procedimientos en los demás Proyectos, Programas y Organismos que dependen del Consejo Nacional.

Que en virtud de todo lo expuesto, resulta necesario aprobar el Manual de Políticas de Seguridad de los Sistemas de información del SINTyS y los Procedimientos anexos, y encomendar al Coordinador del Area de Informática del Consejo Nacional elaborar un Manual sobre Política de Seguridad y los Procedimientos que correspondan con el alcance señalado en el párrafo precedente.

Que la presente medida se dicta en el ejercicio de las facultades conferidas por el artículo 4º del Decreto 1195 de fecha 5 de julio de 2002 y por el artículo 3º de la Resolución C.N.C.P.S. Nº 325 de fecha 21 de noviembre de 2005.

Por ello,

LA COORDINADORA TECNICA
DE LA UNIDAD DE COORDINACION TECNICA
DEL CONSEJO NACIONAL
DE COORDINACION DE POLITICAS SOCIALES
DE LA PRESIDENCIA DE LA NACION
DISPONE:

Artículo 1º — Apruébase el Manual de Políticas de Seguridad de los Sistemas de Información del Sistema de Identificación Nacional Tributario Y Social (SINTyS) y sus Procedimientos, que como Anexo I forma parte de la presente Disposición.

Art. 2º — Encomiéndase al Coordinador del Area de Informática del Consejo Nacional de Coordinación de Políticas Sociales la elaboración de un Manual de Política de Seguridad de los Sistemas de Información y los correspondientes Procedimientos en los demás Proyectos, Programas y Organismos que dependen del Consejo Nacional.

Art. 3º — Regístrese, publíquese y archívese. — Matilde Morales.

PRESIDENCIA DE LA NACION

SECRETARIA LEGAL Y TECNICA
DR. CARLOS ALBERTO ZANNINI
Secretario

DIRECCION NACIONAL DEL REGISTRO OFICIAL
JORGE EDUARDO FEIJOÓ
Director Nacional

www.boletinoficial.gov.ar

e-mail: dnro@boletinoficial.gov.ar

Registro Nacional de la Propiedad Intelectual
Nº 451.095

DOMICILIO LEGAL
Suipacha 767-C1008AAO
Ciudad Autónoma de Buenos Aires
Tel. y Fax 4322–4055 y líneas rotativas

Política de Seguridad
de los Sistemas de Información

SINTyS

Sistema de Identificación Nacional
Tributario y Social

Consejo Nacional de Coordinación de Políticas Sociales
Presidencia de la Nación

Indice

1 Alcance

La presente Política de Seguridad se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de proteger adecuadamente la Información, los sistemas de procesamiento y almacenamiento Informático y las comunicaciones del programa SINTyS, ya sea con internet o con otros organismos en el intercambio de información.

Debe ser conocida y cumplida por todos los consultores del programa, tanto se trate de funcionarios políticos como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista.

2 Términos y Definiciones

A los efectos de este documento se aplican las siguientes definiciones:

1. Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el programa SINTyS.

- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la Información**: Se refiere al hardware y software operados por el programa SINTyS o por un tercero que procese información en su nombre, para llevar a cabo una función propia del programa SINTyS, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2. Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

3. Administración de Riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.

4. Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del programa SINTyS, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

5. Responsable de Seguridad Informática

Es la persona que cumple la función de supervisión de todos los aspectos inherentes a los temas tratados en la presente Política y su correspondiente implementación en procedimientos de seguridad.

6. Incidente de Seguridad

Un incidente de seguridad es una violación de las políticas de seguridad que regulan el buen funcionamiento de un sistema informático.

3 Política de Seguridad de la Información

1 Generalidades

La información es un recurso que, al igual que el resto de los activos, tiene valor para el programa SINTyS y por consiguiente debe ser debidamente protegida. Pero en el caso particular del SINTyS, donde se administran gran cantidad de datos generados por otros organismos, muchos de ellos de alta sensibilidad, las bases de datos son indudablemente el activo más valioso y consecuentemente será el recurso al que mayor esfuerzo de protección deba dedicarse.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del programa SINTyS.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional del programa.

Para esto, se debe asegurar un compromiso manifiesto del las máximas Autoridades del programa SINTyS y de los coordinadores de los distintos componentes para la difusión, consolidación y cumplimiento de la presente Política.

2 Objetivo

Proteger los recursos de información del programa SINTyS y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad que se desprendan de esta Política, asignando los recursos y las partidas presupuestarias correspondientes.

Mantener la Política de Seguridad del programa SINTyS actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

3 Alcance

Esta Política se aplica en todo el ámbito del programa SINTyS (incluyendo UCSN y UCPS), a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados al programa a través de contratos o acuerdos con terceros.

4 Responsabilidad

Todos los Coordinadores de Componentes, SubComponentes, Areas específicas o UPCS, tanto se trate de autoridades políticas o técnicas y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de Información es de aplicación obligatoria para todo el personal del programa SINTyS, cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades del programa SINTyS suscriben esta Política y son responsables de la autorización de modificaciones posteriores.

El Comité de Seguridad de la Información del programa SINTyS, es quien procederá a realizar las actualizaciones y adaptaciones de esta Política que resulten necesarias y convenientes. Por otra parte, será responsable de implementar los medios y canales necesarios para los reportes de incidentes y anomalías de los sistemas (Ver 1 - “Seguridad del Personal”).

Asimismo, el Comité de Seguridad de la Información, el Responsable de Seguridad Informática y los coordinadores de componentes, son responsables de la elaboración y prueba de los procesos que garanticen la continuidad de la actividad del programa SINTyS, de participar en la elaboración de normas, procedimientos y prácticas de seguridad en este sentido, así como en su difusión y concientización de todo el personal del programa SINTyS (Ver 1 – “Administración de la Continuidad de las Actividades del programa”).

El Coordinador del Comité de Seguridad de la Información (Ver 1 – “Comité de la Seguridad de la Información”) será el responsable de impulsar la implementación de la presente Política.

El Responsable de Seguridad Informática tiene la responsabilidad de supervisar todos los aspectos inherentes a los temas tratados en la presente Política, lo cual incluye verificar el cumplimiento de la misma y orientar y asesorar a las dependencias del programa SINTyS respecto a su implementación. Asimismo es responsable de asegurar que la utilización de los recursos de la tecnología de información satisfaga todos los requerimientos de seguridad, de acuerdo a la criticidad de la información procesada y en relación con el nivel de clasificación establecido por su propietario.

Por otra parte, el Responsable de Seguridad Informática conjuntamente con los Responsables de Activos de la Información, son responsables por el cumplimiento de las disposiciones sobre seguridad de las instalaciones (Ver 1 – “Seguridad Física y Ambiental”) y el control de acceso de las áreas y recursos del programa SINTyS (Ver 1 – “Control de Accesos”).

Los propietarios de los sistemas y datos, es decir los Responsables de Activos de Información, son responsables de clasificar la información de su propiedad de acuerdo con el grado de sensibilidad y criticidad de la misma, y de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información. (Ver 1 - “Clasificación y Control de Activos”).

El Componente Administración, es responsable de informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Acuerdos de Confidencialidad y las tareas de capacitación continua en materia de seguridad (Ver 1 - "Seguridad del Personal").

El Responsable del Componente Infraestructuras es el responsable de cumplir los requerimientos de seguridad informática establecidos para las operaciones, administración y comunicaciones de los sistemas y recursos de la tecnología del programa SINTyS. (Ver 1 – "Gestión de Comunicaciones y Operaciones"). Por otra parte tendrá la responsabilidad de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología del ciclo de vida de sistemas aprobada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases (Ver 1 – "Desarrollo y Mantenimiento de Sistemas").

UNOPS, a cargo de la contratación de terceros será responsable de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de esta Política y de todas las normas, procedimientos y prácticas que de ella surjan.

La asesoría legal del programa SINTyS es responsable de determinar las sanciones que correspondieran por el incumplimiento de la presente Política.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de:

a) Acceder solamente a aquellos datos y recursos respecto a los cuales cuentan con la autorización respectiva.

b) Utilizar esos recursos según las funciones que le fueron asignadas y con los fines para los que dispone de autorización.

c) Mantener la confidencialidad de la información del programa SINTyS y la privacidad de la información de terceros.

d) Cumplir todos los procedimientos y controles previstos para la utilización de los sistemas y demás recursos de la tecnología de la información.

e) Cumplir y observar el cumplimiento por parte del resto del personal de los controles y medidas de seguridad orientadas a la protección física y lógica de los recursos del programa SINTyS.

f) Notificar al Responsable de Seguridad Informática las violaciones y riesgos que detecten relacionados con la seguridad de la información y de los recursos.

El área de auditoría interna será responsable de practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan (Ver 1 – "Cumplimiento").

La presente descripción de roles y responsabilidades, no exime a cada sector de la responsabilidad del cumplimiento de las funciones que le son propias, ni de las responsabilidades específicas que emanen de los próximos capítulos.

5 Política

1. Aspectos Generales

Esta Política incluye los siguientes tópicos:

1. Organización de la Seguridad
Orientado a administrar la seguridad de la información dentro del programa SINTyS y establecer un marco gerencial para controlar su implementación.

2. Clasificación y Control de Activos
Destinado a mantener una adecuada protección de los activos del programa SINTyS.

3. Seguridad del Personal
Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el programa SINTyS o uso inadecuado de instalaciones.

4. Seguridad Física y Ambiental
Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del programa SINTyS.

5. Gestión de las Comunicaciones y las Operaciones
Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

6. Control de Acceso
Orientado a controlar el acceso a la información.

7. Desarrollo y Mantenimiento de los Sistemas
Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información.

8. Administración de la Continuidad de las Actividades del programa SINTyS
Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

9. Cumplimiento
Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, el programa SINTyS asignará los recursos necesarios e indicará las partidas presupuestarias correspondientes formalmente, como anexo de la presente Política.

El Comité de Seguridad de la Información revisará anualmente la presente Política, a efectos de mantenerla actualizada.

6 Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido (Ver 1 – "Sanciones Previstas por Incumplimiento").

4 Organización de la Seguridad

Generalidades

La presente Política de Seguridad establece las medidas de seguridad de los sistemas de información, como parte fundamental de los objetivos y actividades del programa SINTyS.

Por ello, se definirá formalmente un ámbito de coordinación de las actividades de seguridad que se llevarán a cabo, identificando claramente los alcances y responsabilidades.

Por otro lado debe tenerse en cuenta que ciertas actividades del programa SINTyS pueden ser realizadas por terceros, contratados por éste a tal fin, por lo que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad.

Por lo tanto, cuando se trate de la tercerización de la administración y el control de los sistemas de información, se deberán contemplar los riesgos asociados y los controles de seguridad pertinentes, como así también los procedimientos de seguridad que deberán cumplir.

Objetivo

Administrar la seguridad de la información dentro del programa SINTyS y establecer un marco gerencial para su implementación.

Establecer un Comité de Seguridad integrado por los niveles directivos, a fin de coordinar la implementación de la Política en todo el programa SINTyS.

Alentar un enfoque multidisciplinario para la seguridad de la información, comprometiendo la cooperación y colaboración de los coordinadores de componentes, tanto se trate de autoridades Políticas o técnicas, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad.

Garantizar la aplicación de las medidas de seguridad establecidas, cuando la responsabilidad por el procesamiento de la información fuera tercerizada.

Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información del programa SINTyS a los que tuvieran acceso terceras partes (incluyendo procesos de tercerización del procesamiento de información).

Incluir en los contratos de tercerización, cláusulas relativas a los riesgos, a los controles de seguridad y a los procedimientos para sistemas de información y la tecnología involucrada.

Establecer contactos con la Coordinación de Emergencias en Redes Teleinformáticas (ArCERT) y con otros especialistas en materia de seguridad para disponer de información actualizada de las tendencias, estándares y métodos de evaluación y para obtener información para afrontar incidentes de seguridad.

Alcance

Esta Política se aplica a todos los recursos del programa SINTyS y a todas sus relaciones con terceros que impliquen el acceso a sus recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política.

El área del programa SINTyS a cargo de la contratación de terceros será responsable de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de esta Política y de todas las normas, procedimientos y prácticas que de ella surjan.

Política
1. Infraestructura de la Seguridad de la Información
1. Comité de la Seguridad de la Información

La seguridad de la información es una responsabilidad del programa SINTyS compartida por todas las Autoridades políticas y Directores Nacionales o Generales, Gerentes o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todos los Directores mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad, el que será presidido por la directora nacional del programa SINTyS, Matilde Morales, quien deberá asignar funciones y responsabilidades específicas relativas a la seguridad de la información para todo el programa SINTyS.

Conformación del Comité de Seguridad de la Información

Area / Componente	Representante
Coordinación General	Coordinador Técnico CNPCS
Componente Infraestructuras	Encargado de informatica del CNCPS
Area Seguridad	Encargado de seguridad del CNCPS, Coordinador de seguridad SINTyS
Asesor Legal	Asesor Legal del CNCPS
Area BBDD	Encargado del area BD de SINTyS
Area Intercambio de Información	Director SINTyS
Area Administración de Sistemas	Represente de Administración de sistemas del CNCPS
Area Desarrollo	Encargado área desarrollo de SINTyS

Este Comité tendrá entre sus funciones:

- Revisar y proponer a la máxima autoridad del programa SINTyS para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.
- Acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.

- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del programa SINTyS.
- Coordinar el proceso de administración de la continuidad del programa SINTyS.

El Secretario Ejecutivo de la CNCPS coordinará las actividades del Comité de Seguridad de la Información.

2. Asignación de Responsabilidades en Materia de Seguridad de la Información

La directora nacional del SINTyS, asigna las funciones relativas a la Seguridad Informática del programa SINTyS al coordinador del Componente Infraestructura, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Clasificación y Control de Activos	Coordinador Infraestructura
Seguridad del Personal	Coordinador Seguridad
Seguridad Física y Ambiental	Coordinador infraestructura
Seguridad en las Comunicaciones	Coordinador Seguridad y las Operaciones Responsable de comunicaciones
Control de Accesos	Coordinador Seguridad
Seguridad en el Desarrollo y Mantenimiento	Coordinador Seguridad de Sistemas Responsable área desarrollo de sistemas
Planificación de la Continuidad Operativa	Coordinador infraestructura Coordinador seguridad

3. Proceso de Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Coordinadores de los componentes involucrados, considerando su propósito y uso, así como por el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del programa SINTyS.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad informática y deberá ser autorizado por el Director Nacional (General, Gerente o equivalente en el programa SINTyS) responsable del área al que se destinen los recursos.

4. Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el programa SINTyS a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Este podrá obtener asesoramiento de otros programas semejantes u organismos gubernamentales (Ver 1 – "Cooperación entre Organizaciones").

5. Cooperación entre Organizaciones

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con las siguientes organizaciones especializadas en temas relativos a la seguridad informática:

- Oficina Nacional de Tecnologías de Información (ONTI), y particularmente con:
  - ArCERT – Coordinación de Emergencias en Redes Teleinformáticas.
  - Infraestructura de Firma Digital, si fuera el caso.
- Dirección Nacional de Protección de Datos Personales.

En los intercambios de información de seguridad, no se divulgará información confidencial perteneciente al programa SINTyS a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Acuerdo de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad informática cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

6. Seguridad Frente al Acceso por Parte de Terceros
Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de una conexión con un sitio externo, se llevará a cabo y se documentará una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido.
- El valor de la información.
- Los controles consultores por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del programa SINTyS.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro del SINTyS, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.
b) Limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados.
c) Pasantías y otras designaciones de corto plazo.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado acuerdo de confidencialidad que defina las condiciones para la conexión o el acceso.

1. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos con terceros, teniendo en cuenta la factibilidad de aplicar los siguientes controles, mediante su explícita exigencia a UNOPS:

I. Cumplimiento de la Política general de seguridad de la información del programa SINTyS.
II. Protección de los activos del programa SINTyS, incluyendo:
a. Procedimientos para proteger los bienes del programa SINTyS, abarcando los activos físicos, la información y el software.
b. Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
c. Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
d. Procedimientos para garantizar la integridad y disponibilidad de la información.
III. Restricciones a la copia y divulgación de información.
IV. Descripción de los servicios disponibles.
V. Nivel de servicio esperado y niveles de servicio aceptables.
VI. Permiso para la transferencia de personal cuando sea necesario.
VII. Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
VIII. Existencia de Derechos de Propiedad Intelectual.
IX. Acuerdos de control de accesos que contemplen:
a. Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
b. Proceso de autorización de accesos y privilegios de usuarios.
c. Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
X. Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
XI. Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
XII. Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
XIII. Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
XIV. Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
XV. Proceso claro y detallado de administración de cambios.
XVI. Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
XVII. Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
XVIII. Controles que garanticen la protección contra software malicioso.
XIX. Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
XX. Relación entre proveedores y subcontratistas.

5 Clasificación y Control de Activos

7 Generalidades

Las clasificaciones y los controles de protección de la información deben considerar las necesidades del SINTyS respecto a la distribución (uso compartido) y/o las restricciones de la información, y su incidencia en sus actividades.

En general, la clasificación asignada a la información es una forma sencilla de señalar cómo ha de ser tratada y protegida.

Se deben rotular según su valor y grado de sensibilidad para el programa SINTyS tanto la información como las salidas de los sistemas que administran datos clasificados. Asimismo, resulta conveniente rotular la información según su grado de criticidad, por ejemplo en términos de integridad y disponibilidad.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el programa SINTyS.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar el número de categorías de clasificación y los beneficios que se obtendrán con su uso. Los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos. Deben interpretarse cuidadosamente los rótulos de clasificación de los documentos de otras organizaciones que podrían tener distintas definiciones para rótulos iguales o similares.

La responsabilidad por la definición de la clasificación de un ítem de información, por ejemplo un documento, registro de datos, archivo de datos o disquete, y por la revisión periódica de dicha clasificación, debe ser asignada al responsable de la información.

La información adopta muchas formas, tanto en los sistemas como fuera de ellos. Puede estar en cualquiera de los siguientes estados: Almacenada, Transmitida o Procesada

- Almacenada, en los sistemas o en medios portátiles en formato digital; o en un medio físico, impresa o escrita en papel.
- Transmitida, a través de redes y enlaces de comunicaciones o entre sistemas.
- Información en estado de procesamiento, o almacenada temporalmente dentro de un proceso.

Bajo el punto de vista de Seguridad, las medidas de protección deben ser aplicadas a todas y cada una de las formas relacionadas con los sistemas de información del programa SINTyS.

8 Objetivo

Garantizar que los recursos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar la necesidad, prioridad y grado de protección requerido, definiendo niveles de protección y comunicando la necesidad de medidas de tratamiento especial.

9 Alcance

Esta Política se aplica a toda la información administrada en el programa SINTyS, cualquiera sea el soporte en que se encuentre.

10 Responsabilidad

Los propietarios de los sistemas y datos, es decir los Responsables de Activos de Información, son los encargados de clasificar la información de su propiedad de acuerdo con el grado de sensibili-

dad y criticidad de la misma, y de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que la utilización de los recursos de la tecnología de información satisfaga todos los requerimientos de seguridad de acuerdo a la criticidad de la información procesada en ellos, en relación al nivel de clasificación establecido por su propietario,

El Responsable de los procesos de Clasificación y Control de Activos supervisará que la presente Política sea aplicada por cada uno de los responsables de los activos de información.

11 Política

Generalidades

Para clasificar un Activo de Información, se utilizarán los criterios definidos en los siguientes niveles:

1 - SIN CLASIFICAR	Información de dominio público que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del programa SINTyS o no.
2 - RESERVADA - USO INTERNO	Información que puede ser conocida y utilizada por todos los consultores y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el programa SINTyS.
3 - CONFIDENCIAL	Información que sólo puede ser conocida y utilizada por un grupo de consultores, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas, materiales o serio perjuicio de imagen.
4 – SECRETA	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de consultores, generalmente de la alta dirección del programa SINTyS, y cuya divulgación o uso no autorizados podría ocasionar graves pérdidas materiales o grave perjuicio de imagen.

En adelante, se hablará de Información Clasificada refiriéndose exclusivamente a la descrita en los niveles 3 y 4 precedentes.

Sólo el Responsable de un Activo de Información puede asignar o cambiar el nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

1. Rotulado de la Información

El nivel de clasificación asignado tiene que estar rotulado en todas y cada una de las páginas de los impresos que contengan información clasificada, incluyendo la carátula, siendo opcional el rotulado en la cabecera o al pie de página, y siempre de forma que resulte fácilmente legible.

La información clasificada que aparezca en los terminales o estaciones de trabajo de usuario, tiene que reflejar su nivel de clasificación, como mínimo, en la pantalla inicial y siempre que sea posible, en todas y cada una de las pantallas o estar permanentemente en la cabecera de pantalla.

Cada medio de almacenamiento removible (cintas, CDs, cartuchos, disquetes, etc.), que contenga información clasificada, tiene que ser etiquetado con el nivel más alto de clasificación de la información que contenga. Los medios de almacenamiento no removibles no necesitan ser marcados con etiquetas de clasificación. La Información transmitida por medio de redes de comunicaciones (correo electrónico, teléfono, fax, etc.) debe ser rotulada de acuerdo con el nivel más alto de clasificación de la información que contenga.

Para la correcta administración de las Bases de Datos del programa SINTyS, se establecerá la clasificación de los registros de datos aislados así como del conjunto de los mismos, los cuales pueden corresponder a niveles de clasificación diferentes (por ejemplo un registro individual puede ser público o reservado, mientras que la base de datos es confidencial o secreta, siempre y cuando, sea baja la probabilidad de reconstrucción de la base de datos completa a partir de conjuntos de registros individuales).

2. Protección de la Información Clasificada

La principal regla de protección es que la información clasificada sea conocida o utilizada sólo por personas autorizadas a acceder a la misma y siempre con motivo del ejercicio de sus funciones.

Todos los consultores tienen que suscribir con el programa SINTyS, un Acuerdo de Confidencialidad en virtud del cual asuman la obligación de proteger y no divulgar la información clasificada que manejen (Ver 1 – “Acuerdos de Confidencialidad”). Este compromiso complementa las obligaciones del empleado público que emanan de la normativa vigente (Ver 1 – “Protección de Datos y Privacidad de la Información Personal” y Anexo II - “Política de Uso Aceptable”).

Guardar información clasificada en cualquier sistema o medio de almacenamiento supone:

- Tener los medios físicos y lógicos adecuados para protegerla.
- No permitir su acceso público o de personas con nivel de acceso inferior al de la información de mayor nivel allí contenida.
- Limitar el acceso a esta información.

3. Protección de Información Impresa

La información clasificada debe permanecer, en todo momento, lejos del alcance de consultores y personas que no tengan necesidad de conocerla.

La Información Clasificada, debe guardarse bajo llave permanentemente, y durante su uso debe evitarse que puedan tener acceso personas no autorizadas.

El empleo de cualquier dispositivo para generar salidas impresas que contengan Información Clasificada debe limitarse a aquellos que cumplan con las siguientes condiciones:

- Estén situados en áreas de acceso limitado o restringido.
- Tengan algún tipo de control de borrado de listados.
- Sean de uso exclusivo del usuario o componente al que pertenece.

Si ninguna de las opciones anteriores está disponible, se puede imprimir en cualquier otro dispositivo siempre que los listados sean esperados por el usuario y recogidos inmediatamente por el mismo.

En cualquier caso, la creación de salidas impresas de información clasificada estará siempre bajo la responsabilidad y el control del usuario que genera la impresión.

4. Divulgación de la Información Clasificada

La información clasificada se debe divulgar únicamente sobre la base de la necesidad de conocerla por motivos de trabajo y tiene que ser autorizada formalmente, caso a caso, por el Responsable de dicha información.

Cualquier divulgación a terceros, tiene que estar amparada por un Acuerdo de Confidencialidad previamente firmado entre el cedente y el cesionario.

El copiado y distribución de información clasificada debe contar previamente con la aprobación explícita del Responsable de dicha información, quien puede reservarse el derecho de aprobar personalmente cada caso, pudiendo añadir la leyenda **“Prohibida la Reproducción”** o bien numerar las copias aprobadas, para su control.

Para una correcta divulgación, la información clasificada no podrá ser transmitida a través de medios de comunicación inseguros, a menos que se encuentre cifrada con los algoritmos de encriptación adecuados (Ver 1 - “Transporte de la Información Clasificada”).

5. Transporte de la Información Clasificada

Siempre que la información clasificada sea transportada dentro del ámbito del programa SINTyS, bastará con ponerla en un sobre o contenedor cerrado y marcarlo con la clasificación más alta del contenido.

Si la información clasificada es enviada al exterior o por medio de correo ajeno al programa SINTyS, el sobre o contenedor cerrado y marcado deberá ser introducido en otro cerrado y NO marcado. Debe incluirse, como medida de protección adicional, el acuse de recibo por parte del destinatario. A su vez, la información enviada en formatos digitales (ópticos/ magnéticos/ electrónicos) se cifrará con algoritmos reconocidos de cifrado asimétrico (en el caso en que el destinatario tenga acceso a infraestructura PKI) o cifrado simétrico en su defecto.

Siempre que la información clasificada sea enviada a través de redes de comunicaciones, propias o ajenas debe utilizarse un método de cifrado seguro. Para ello se utilizará en orden de preferencia:

- Método de Cifrado Asimétrico (por ejemplo Certificado Digital)
- Método de Cifrado Simétrico, que incluya la protección de la clave de cifrado mediante el uso de Cifrado Asimétrico.
- Otro método de Cifrado Simétrico.

En este último caso, se enviará la información cifrada y por otra vía la clave correspondiente.

Fuera del ámbito del programa SINTyS, el personal evitará el transporte de información clasificada. Si esto no fuera posible, deberá conservar la información en su poder, no debiendo dejarla desatendida y, siempre que sea posible, manteniéndola cifrada.

6. Destrucción de la Información Clasificada

Cuando haya dejado de ser útil, la información clasificada debe ser destruida en la forma más adecuada al soporte que la contenga, conforme a la normativa vigente.

La información impresa y en papel deberá ser destruida mediante incineradores, trituradoras o bien colocada en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo la supervisión del Responsable del Control de Activos.

Respecto a los medios de almacenamiento, antes de ser desechados o reutilizados deben ser procesados para borrar su contenido en forma apropiada o hacerlo ilegible. En caso de que esto no sea posible, se procederá a la destrucción física del medio de almacenamiento.

El Responsable de Seguridad Informática o algún analista por él delegado, realizará un análisis de riesgo a fin de determinar si los medios de almacenamiento dañados, conteniendo datos clasificados, deben ser destruidos, reparados o desechados.

Se establecen los siguientes métodos de destrucción de información, para cada tipo de soporte:

Tipo de Soporte de Información	**Método de Destrucción**
Papel	Mediante Máquina de corte en cintas, o Incinerado y mezclado de restos
CD / DVD Cintas magnéticas	Cortado o Rotura Sobreescritura y borrado mediante Transformador con dispersión magnética (núcleo abierto)
Diskettes Discos Rígidos	Sobreescritura y Cortado o Rotura Sobreescritura, Apertura y Rotura

6 Seguridad del Personal

12 Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal, cualquiera sea su situación de revista, acerca de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es importante determinar la relevancia del papel que desempeña el personal en materia de seguridad, para lo cual se les debe comunicar la totalidad de las medidas de seguridad que afecten el desarrollo de sus funciones, en especial las que deben aplicar, y las consecuencias de su incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes, sin perjuicio de que éstos se presenten de todos modos. Es por ello que resulta necesario implementar un plan que permita reportar los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones de los mismos. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

13 Objetivo

Reducir los riesgos de error humano, comisión de ilícitos o uso inadecuado de instalaciones.

Seleccionar adecuadamente los candidatos a ocupar los puestos de trabajo críticos.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del programa SINTyS en el transcurso de sus tareas normales.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal, incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Establecer Acuerdos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas necesarias para minimizar el daño producido por incidentes y anomalías en materia de seguridad, monitorear dichos incidentes y aprender de los mismos.

Informar a todos los consultores los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos del programa SINTyS.

14 Alcance

Esta Política se aplica a todo el personal del programa SINTyS, cualquiera sea su situación de revista.

15 Responsabilidad

El Coordinador del Componente Administración es responsable de informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Acuerdos de Confidencialidad y las tareas de capacitación continuas en materia de seguridad.

El Comité de la Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, deberá tomar conocimiento, supervisar la investigación y monitorear los incidentes relativos a la seguridad.

16 Política

1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

1. Inclusión de la Seguridad en las Responsabilidades de los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Estas incluirán las responsabilidades generales por la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas por la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

2. Control y Política del Personal

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto, alcanzan al programa SINTyS.

3. Acuerdos de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los consultores, cualquiera sea su situación de revista, firmarán un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del programa SINTyS. La copia firmada del Acuerdo deberá ser retenida en forma segura por el Componente Administración.

El “Acuerdo de Confidencialidad” deberá advertir que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Acuerdo de Confidencialidad donde se incluirán aspectos sobre:

a) Suscripción inicial del Acuerdo por parte de la totalidad del personal.
b) Revisión periódica anual del contenido del Acuerdo.
c) Método de resuscripción en caso de modificación del texto del Acuerdo.

4. Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del empleado por la seguridad de la información.

Cada consultor al momento de vincularse contractualmente al proyecto SINTyS suscribirá la correspondiente Polïtica de Uso Aceptable (Anexo II)

Las responsabilidades y derechos legales del empleado, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo

También se incluirá la responsabilidad por la clasificación y administración de los sistemas y datos del programa SINTyS. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del programa SINTyS y del horario normal de trabajo.

2. Capacitación del Usuario

1. Formación y Capacitación en Materia de Seguridad de la Información

Todos los consultores del SINTyS y, cuando sea pertinente, los usuarios externos, recibirán una adecuada capacitación y actualización periódica en materia de las Políticas y procedimientos del programa SINTyS. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

Cada año se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación

Areas Responsables del Material de Capacitación
Informática
Gestión
Administración
Prensa

El personal que ingrese al SINTyS, recibirá el material indicando el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

3. Respuesta a Incidentes y Anomalías en Materia de Seguridad

1. Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este asignará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

Sin perjuicio de informar a otros programas gubernamentales de competencia, el Responsable de Seguridad Informática, comunicará a la Coordinación de Emergencias en Redes Teleinformáticas (Ar-CERT) todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los consultores deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

2. Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

Se prohíbe a los consultores ajenos al área seguridad informática, la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

3. Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
c) Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

4. Aprendiendo de los Incidentes

Se definirá un proceso que permita cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

5. Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Publica Nacional, para los consultores que violen las Políticas y procedimientos de seguridad del programa SINTyS (Ver 1 – “Sanciones Previstas por Incumplimiento”).

7 Seguridad Física y Ambiental

17 Generalidades

La seguridad Física y Ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del programa SINTyS. Asimismo, pretende evitar al máximo el riesgo de accesos no autorizados por medios físicos, mediante el establecimiento de perímetros de seguridad. Se distinguen tres temas a tener en cuenta: La protección física de accesos, la protección ambiental y el transporte y disposición final del equipamiento y documentación.

Mediante la protección física de acceso se intenta evitar la manipulación no autorizada de sistemas o documentos. El establecimiento de perímetros de seguridad facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del programa SINTyS.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del SINTyS como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas de los mismos mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

18 Objetivo

Impedir accesos no autorizados, daños e interferencia a los recursos e información del SINTyS.

Proteger las instalaciones de procesamiento de información crítica o clasificada del SINTyS ubicándolas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados.

Reducir el riesgo de acceso no autorizado o de daño a documentación en soporte papel, medios de almacenamiento e instalaciones de procesamiento de información.

Prevenir pérdidas, daños o exposiciones a riesgos, en los activos del programa SINTyS, e interrupción de sus actividades.

Proteger físicamente al equipamiento de las amenazas a la seguridad y los peligros del entorno.

Proporcionar protección proporcional a los riesgos identificados.

19 Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del SINTyS: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

20 Responsabilidad

El Responsable de Seguridad Informática, conjuntamente con los Responsables de Activos de la Información, son los encargados de verificar el cumplimiento de las disposiciones sobre seguridad de las instalaciones indicadas en la presente Política.

21 Política

1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de medidas de control físicas alrededor de las sedes del SINTyS y de las instalaciones de procesamiento de información.

El programa SINTyS utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada control de acceso estará definido por el Responsable de los Activos de Información de que se trate, conjuntamente con el Responsable del Area Informática y el Responsable de Seguridad Informática, quienes lo definirán de acuerdo a la evaluación de riesgos efectuada.

Se considerará la definición del perímetro en UCSN de la siguiente manera:

a) Se distinguen cuatro puertas a diferentes recintos: CPD (Centro de Procesamiento de datos), Oficina de Coordinadores, Entrada principal y Expedientes. Cada persona vinculada al proyecto tendrá definidos accesos a cada una de ellas de acuerdo al componente que integra y a las funciones inherentes al mismo.
b) Identificar claramente todas las puertas de incendio del perímetro de seguridad y del edificio en general

El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Area.
b) Principales elementos a proteger.
c) Medidas de protección física.

2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán definidos por el Responsable de Seguridad Informática, a fin de permitir el acceso solo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: Sistema de control de acceso por tarjeta magnética. Se mantendrá un registro protegido para permitir auditar todos los accesos.
c) Implementar el uso de una identificación (acceso con 3 factores de identificación) para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
d) Revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el coordinador del componente del que dependa.

Los controles definidos son los siguientes:

Cada puerta cuenta con distintos factores de autenticación de entrada y salida:

a) Oficina de Coordinadores: Huella y PIN para entrada; PIN para salida.
b) Entrada principal: Huella y PIN para entrada; PIN para salida.
c) CPD: Huella, PIN y Tarjeta para entrada; Tarjeta para salida.
d) Expedientes: Huella, PIN y Tarjeta para entrada; Tarjeta para salida.
e) Administración: Tarjeta para entrada; Tarjeta para salida.

Las personas que deban tener tarjeta; es decir, que tengan acceso al CPD y/o Expedientes, firmarán un remito interno (ver Anexo V) en el que se responsabilizan a notificarle al subcomponente Seguridad Informática del SINTyS ante robo y/o extravío de la misma, dentro de las 12 horas de notada su desaparición.

Al proceso de registrar la huella dactilar, el PIN y la Tarjeta junto con los datos de la persona, se lo denomina “enrolamiento”. Dicho enrolamiento se lleva a cabo por única vez antes de la puesta en marcha del sistema de control de acceso. De esta manera la persona queda debidamente registrada para poder ingresar y egresar de los accesos habilitados según su perfil de privilegio.

A los efectos del uso apropiado del sistema de control de accesos, se define la siguiente reglamentación de uso:

a) Para quienes posean tarjeta de acceso, es indispensable llevarla siempre consigo y que la misma esté en poder de su responsable directo (no delegarla a terceros) ya que toda acción de ingreso y/o egreso registrada con la misma responsabilizará exclusivamente al propietario de la misma, sin derecho alguno a la no-repudiación (con la notable excepción de haber notificado de su extravío, según lo discutido en el punto anterior).
b) El PIN y el Nº de tarjeta de cada persona, sólo debe ser conocida por el responsable y por el Administrador del sistema de control de acceso.
c) Se deberá adjuntar al Remito Interno de entrega de Tarjetas, la fotocopia de 1ra y 2da hoja del DNI.
d) Todos los datos descriptos a continuación deben ser almacenados en la base de datos al momento del enrolamiento.

1.- De la persona:
Nombre y apellido.
Documento de identidad.
Componente u organismo.
Area.
Nº de tarjeta
PIN (Personal Identification Number).

2.- Del acceso
Puerta/s.
Tipo de acceso (Temporal / Permanente). En el caso de ser temporal, el acceso se registra en un módulo llamado “Visitas”.
Motivo de la visita.
A quien visita.

Tanto las altas como las bajas de usuarios, se registrarán además mediante formularios diseñados a tal fin, para llevar un registro estricto de los accesos al SINTyS. Para el caso de las bajas, corresponderá asegurarse el proceso de inhibición del usuario, en el lapso de 24 horas hábiles a partir de la recepción de dicho formulario.

3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de las áreas protegidas se tendrá en cuenta la posibilidad de daño producido por incendio, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones o desde pisos superiores.

Se definen los siguientes sitios como áreas protegidas del programa SINTyS

Areas Protegidas
CPD
Despacho
Administración
Sala Expedientes

Se establecen los siguientes controles:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder el público. No se podrá ingresar a ninguno de los recintos sintys sin las correspondientes credenciales de ingreso, ya sean temporarias en el caso de visitas eventuales o de personal vinculado al proyecto.
b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información. Realizar una segmentación funcional de las impresoras, de manera de que exista una por componente y llevar un registro del material impreso por cada consultor habilitado. Requerir que el acceso a las fotocopiadoras requiera de un código de indentificación personal, de manera de permitir el registro auditable del volumen de material copiado por cada consultor habilitado a su uso.
d) Implementar los siguientes mecanismos de control para la detección de intrusos: control de acceso de factor múltiple, con alarma de ingreso simultáneo. Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores.
e) Separar las instalaciones de procesamiento de información administradas por el programa SINTyS de aquellas administradas por terceros.
f) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
g) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del programa SINTyS: Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.
h) Almacenar los equipos redundantes y la información de resguardo (back up) en el siguiente sitio seguro distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal: El sitio Redundante se encuentra en el Ministerio de Desarrollo Social, y los backups son resguardados en una caja de seguridad en el Banco Nación.

4. Trabajo en Areas Seguras. Desarrollo de Tareas en Areas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

f) Dar a conocer al personal la existencia del área protegida, o de las actividades que se llevan a cabo dentro de la misma, sólo si es necesario para el desarrollo de sus funciones (principio de la necesidad de saber)
g) Evitar la ejecución de trabajos por parte de terceros sin supervisión, en las áreas protegidas, tanto por razones de seguridad, como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.
h) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

i) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Para permitir su acceso, se emitirá una tarjeta de acceso de validez temporal (por la duración estimada de la visita) en un equipo destinado a tal fin, registrándose además del nombre del visitante, su afiliación profesional y su DNI o identificación válida. Se mantendrá un registro de todos los accesos de personas ajenas a las áreas protegidas.

j) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

k) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que el Responsable de Seguridad Informática o el Responsable del Activo de que se trate, lo autorice formalmente.

l) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

5. Aislamiento de las Areas de Recepción y Distribución

Se controlarán las áreas de Recepción, Distribución y Despacho, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de despacho, desde el exterior de la sede del programa SINTyS, sólo al personal previamente identificado y autorizado, mediante los mecanismos de control de acceso previamente establecidos.

b) Diseñar el área de despacho de manera tal que los suministros puedan ser entregados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de despacho hasta el lugar de uso.

d) Registrar tanto el material entrante al ingresar como el material saliente del sitio pertinente.

6. Ubicación y Protección del Equipamiento

El equipamiento será ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en el siguiente sitio donde se minimiza el acceso innecesario a las áreas de trabajo: CPD.

b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en el siguiente sitio a fin de reducir el riesgo de falta de supervisión de las mismas durante su uso: CPD

c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

d) Adoptar los siguientes controles para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales	Controles
Robo o hurto.	Policía o seguridad en edificio
Incendio.	Detectores y Sistema de Extinción por Gas en CPD Bomberos en edificio
Explosivos.	-
Sobretemperatura	Detectores en CPD
Humo.	Detectores en CPD
Inundaciones o filtraciones de agua. (o falta de suministro)	Personal de mantenimiento del Edificio
Polvo.	Limpieza de Filtros en instalaciones de aire acondicionado
Vibraciones.	-
Efectos químicos.	-
Interferencia en el suministro de energía eléctrica.	UPS con baterías
Radiación electromagnética.	Bandejas portacables metálicas, gabinetes metálicos y puesta a tierra
Derrumbes	Sitio de contingencia

e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará con la siguiente periodicidad: una vez por semana.

f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede del programa SINTyS.

7. Suministros de Energía.

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones más estrictas de los fabricantes o proveedores de los equipos. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del programa SINTyS. La autonomía de la UPS deberá ser tal que permita la operación de servidores críticos durante al menos una (1) hora. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que tienen la capacidad requerida.

c) Si el presupuesto y el espacio disponible así lo permitieran, montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Los generadores deberán ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor. Se deberá disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen 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. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra rayos en todos los edificios y se adaptarán filtros de protección contra rayos en todas las líneas de comunicaciones externas.

8. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.

b) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa: bandejas portacables metálicas.

c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles: el uso de conductos o canalizaciones metálicas y evitando trayectos que atraviesen áreas públicas sin supervisión de seguridad.

d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Para los sistemas sensibles o críticos, Redes Locales, Enlaces de Datos y Telefonía, se implementarán los siguientes controles adicionales:

a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.

b) Utilizar rutas o medios de transmisión alternativos.

9. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter al equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de los responsables de los activos. El Area de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo (ver formulario adjunto).

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

d) Registrar cuando se retiran equipos de la sede del programa SINTyS para su mantenimiento, el que estará a cargo del Responsable de los Activos de que se traten.

e) Eliminar la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de resguardo (Ver 1 – "Destrucción de la Información Clasificada").

10. Seguridad de los Equipos Fuera de las Instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del SINTyS, será autorizado por el Responsable del Activo, sin importar quien es el propietario del mismo. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del programa SINTyS para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

11. Desafectación o Reutilización Segura de los Equipos.

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material clasificado, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar (Ver 1 – "Destrucción de la Información Clasificada").

12. Políticas de Escritorios y Pantallas Limpias.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información sensible o crítica del programa SINTyS (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

c) Bloquear el acceso a máquinas de escritorio cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas, lectores de huellas dactilares u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

d) Bloquear puertos USB de máquinas de escitorio a fin de evitar la captura no autorizada de información. Se utilizarán tiras adhesivas que al ser violentadas dejan la marca de 'VOID'

e) Proteger los puntos de recepción y envío de correo y las máquinas de fax no atendidas.

f) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

g) Retirar inmediatamente la información clasificada, una vez impresa (Ver 1 – "Protección de Información Impresa").

13. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede del programa SINTyS sin autorización.

Periódicamente, el Componente Administración llevará a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del programa SINTyS. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Para retirar un software o un equipamiento se debe solicitar su permiso a

1) al responsable de área
2) al Componente Administración
3) a la guardia del edificio

8 Gestión de Comunicaciones y Operaciones

22 Generalidades

La proliferación de software malicioso, como virus, troyanos, etc, hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del SINTyS, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre si, tanto dentro del programa SINTyS en UCSN como con dependencias provinciales (UPCS) y en un futuro con otros organismos gubernamentales. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

23 Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

24 Alcance

Todas las instalaciones de procesamiento y transmisión de información del programa SINTyS.

25 Responsabilidad

El Responsable del Area de Informática es el encargado de cumplir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de la tecnología del programa SINTyS.

El Responsable de Seguridad Informática es el encargado de verificar que los procedimientos de aprobación de Software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico.

26 Política

1. Procedimientos y Responsabilidades Operativas

1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.
b) Requerimientos de programación, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
d) Restricciones en el uso de utilitarios del sistema.
e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
f) Instrucciones especiales para el manejo de “salidas”, como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

2. Control de Cambios en las Operaciones

El Responsable de Seguridad Informática controlará los cambios en los sistemas e instalaciones de procesamiento de información, implementando procedimientos y asignando responsabilidades para garantizar un control satisfactorio de todos los cambios en el equipamiento, software y procedimientos.

Se retendrá un registro de auditoría que contenga toda la información relevante.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Comunicación de detalles de cambios a todas las personas pertinentes.
e) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

En particular para el caso de necesidad de modificación de reglas en el firewall con la idea de atenuar potenciales impactos operativos, se definen dos tipos de ventanas de mantenimiento: ordinaria (VMO) y extraordinaria (VME). La primera se aplica cuando los cambios a aplicar no son urgentes. La segunda se aplica cuando existe urgencia en aplicar dichos cambios. En cualquier caso, se crearán sendas listas de distribución internas (vme@sintys.gov.ar y vmo@sintys.gov.ar) a fin de comunicar a todo el personal con incumbencia en los cambios de la implementación de los mismos.

3. Procedimientos de Manejo de Incidentes

Se establecerán responsabilidades y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

a) Contemplar todos los tipos probables de incidentes relativos a seguridad, incluyendo

1) Fallas en los sistemas de información y pérdida del servicio.
2) Denegación del servicio.
3) Errores ocasionados por datos incompletos o inexactos (baja calidad de datos).
4) Violaciones de la confidencialidad.

b) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

1) Análisis e identificación de la causa del incidente.
2) Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.

3) Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
4) Notificación de la acción a la autoridades del programa SINTyS.

c) Realizar registros de auditoría y evidencia similar para:

1) Análisis de problemas internos.
2) Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en el caso de un proceso judicial, por ejemplo por aplicación de legislación sobre protección de datos (Ver 1 – “Cumplimiento de Requisitos Legales”).
3) Negociación de compensaciones por parte de los proveedores de software y de servicios.

d) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

1) Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
2) Que todas las acciones de emergencia emprendidas son documentadas en forma detallada.
3) Que las acciones de emergencia se comuniquen al titular de la Unidad Organizativa y se revisen sistemáticamente.
4) Que la integridad de los controles y sistemas del programa SINTyS sea constatada en un plazo mínimo.

4. Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios.

Si este método de control no se pudiera cumplir en algún caso, se deberán implementar controles como:

a) Monitoreo de las actividades.
b) Llevar registros de auditoría y controlarlos periódicamente.
c) Supervisión de la autoridad que corresponda.

Se asegurará la independencia de la auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a) Separar actividades que requieren connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software en desarrollo y en operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en operación, cuando no sean indispensables para el funcionamiento del mismo.
d) Utilizar sistemas de autenticación y autorización independientes para los sistemas en prueba y en operación. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a que instancia se está realizando la conexión.
e) Las contraseñas para la realización de tareas de soporte por parte del personal de desarrollo, deberán generarse bajo estricto control, y deberán ser cambiadas una vez que finalicen las tareas para las cuales fueron generadas.

Para el caso que no puedan mantener separados los distintos ambientes, deberán implementarse los controles indicados en el punto 1 – “Separación de Funciones”.

6. Administración de Instalaciones Externas

En el caso de alojar equipos del programa SINTyS en dependencias que no estén bajo el control del programa, se acordarán controles con los responsables del CPD y se incluirán en el contrato o acuerdo, contemplando las siguientes cuestiones específicas:

a) Identificar las implicancias para la continuidad de los planes de las actividades del programa SINTyS.
b) Especificar los estándares de seguridad y el proceso de medición del cumplimiento.
c) Asignar responsabilidades específicas y procedimientos para monitorear con eficacia todas las actividades de seguridad.
d) Definir las responsabilidades y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

2. Planificación y Aprobación de Sistemas

1. Planificación de la Capacidad

El Responsable del Area Informática deberá monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de garantizar el poder de procesamiento y almacenamiento adecuados, tomando en cuenta los nuevos requerimientos de las actividades del programa SINTyS y sistemas, y las tendencias actuales y proyectadas en el procesamiento de la información del programa SINTyS. Deberá informar las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad del sistema o a los servicios del usuario, y puedan planificar una adecuada acción correctiva.

2. Aprobación del Sistema

El Responsable del Area Informática establecerá criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, realizando las prueba necesarias antes de su apro-

bación definitiva. El responsable de la implantación del sistema garantizará que los requerimientos y criterios de aprobación de nuevos sistemas estén claramente definidos, acordados con los Responsables de los Activos de información involucrados, documentados y probados. Se deben considerar los siguientes puntos:

a) Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
b) Garantizar la recuperación ante errores.
c) Preparar y poner a prueba los procedimientos operativos de rutina según estándares definidos.
d) Garantizar la implementación de un conjunto acordado de controles de seguridad.
e) Redactar procedimientos eficaces.
f) Confeccionar disposiciones relativas a la continuidad de las actividades del programa SINTyS.
g) Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
h) Considerar el efecto que tiene el nuevo sistema en la seguridad global del programa SINTyS.
i) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

3. Protección Contra Software Malicioso

1. Controles Contra Software Malicioso

El Responsable de la Administración de la Red y/o comunicaciones y el Responsable del Area Informática implementarán controles de detección y prevención para la protección contra software malicioso, y desarrollarán procedimientos adecuados de concientización de usuarios en materia de seguridad y en controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por el programa SINTyS (Ver 1 - Derecho de Propiedad Intelectual del Software).
b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, tanto como medida precautoria como rutinaria.
d) Revisar periódicamente el contenido de software y datos de los sistemas que sustentan procesos críticos del programa SINTyS investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
e) Verificar, antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
f) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.[EW]
g) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

4. Mantenimiento

1. Resguardo de la Información

El Responsable del Area Informática dispondrá la realización periódica de copias de resguardo de la información y el software esenciales para el programa SINTyS. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y el software critico del programa SINTyS. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del programa SINTyS, según el punto 1 – "Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del programa SINTyS." de esta política.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a) Almacenar en una 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, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el programa SINTyS.
b) Asignar a la información de resguardo un nivel de protección física y ambiental según los estándares aplicados en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
c) Probar periódicamente los medios de resguardo.
d) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones del punto 1 – "Clasificación y Control de Activos" y 1 – "Protección de los Registros del programa" de la presente Política.

Además, se almacenaran copias de resguardo en la caja de seguridad del Banco Nación, las cuales se probaran periódicamente en el sitio de contingencia.

2. Registro de Actividades del Personal Operativo

El Responsable del Area Informática llevará un registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.
b) Errores del sistema y medidas correctivas tomadas.
c) Confirmación del manejo correcto de archivos de datos y salidas.
d) El nombre de la persona que lleva a cabo la actualización del registro.

El Responsable de Auditoría contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

3. Registro de Fallas

El Responsable del Area Informática deberá desarrollar un procedimiento para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.

5. Administración de la Red

1. Controles de Redes

El Responsable de la Administración de la Red implementará controles para garantizar la seguridad de los datos y los servicios conectados en las redes del programa SINTyS, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto 1 – "Asignación de Responsabilidades en Materia de Seguridad de la Información".
b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
d) Encomendar a proveedores externos la realización de pruebas de penetración perimetrales con una frecuencia no mayor a la semestral.

6. Administración y Seguridad de los Medios de Almacenamiento

1. Administración de Medios Informáticos Removibles

El Responsable del Area Informática implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al capítulo 1 – "Control de Accesos".

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Borrar los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el programa SINTyS, siguiendo los lineamientos expuestos en el punto 1 – "Destrucción de la Información Clasificada".
b) Requerir autorización para retirar cualquier medio del programa SINTyS y realizar un registro de todos los retiros a fin de mantener un registro de auditoría.
c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización., en concordancia con el capítulo 1 – "Clasificación y Control de Activos".

2. Eliminación de Medios Informáticos

El Responsable del Area Informática, junto con el Responsable de Seguridad implementarán procedimientos para la eliminación segura de los medios informáticos de acuerdo a los lineamientos del punto 1 – "Destrucción de la Información Clasificada".

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos o casetes removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.

Asimismo, se debe considerar que podría ser mas fácil disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítem sensibles.

3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a las pautas del capítulo 1 – "Clasificación y Control de Activos".

Se contemplarán en los procedimientos las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
b) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se aplica la validación de salidas.
c) Proteger los datos en espera ("colas").
d) Almacenar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

4. Seguridad de la Documentación del Sistema

La documentación del sistema deberá considerarse información clasificada, y como tal deberán tomarse las medidas requeridas por el capítulo 1 – "Clasificación y Control de Activos".

7. Intercambios de Información y Software

1. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, estos especificarán el grado de sensibilidad de la información del programa SINTyS involucrada y las consideraciones de seguridad sobre la misma. Se deberán tener el cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
c) Estándares técnicos mínimos para el empaquetado y la transmisión.
d) Pautas para la identificación del prestador del servicio de correo.
e) Responsabilidades y obligaciones en caso de pérdida de datos.
f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

g) Términos y condiciones de la licencia bajo la cual se suministra el software.
h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
i) Estándares técnicos para la grabación y lectura de la información y del software.
j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

2. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. Acordar con el Responsable del Activo informático una lista de servicios de mensajería autorizados e incluir un procedimiento para verificar la identificación de los mismos.
b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
c) Adoptar controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
1) Uso de recipientes cerrados.
2) Entrega en mano.
3) Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
4) En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

3. Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto 1 – "Aprobación del Sistema" incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

a) Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y el programa SINTyS.
b) Autorización: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave. Cómo conoce este punto el otro participante de la transacción electrónica.
c) Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
d) Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios.
e) Cierre de la transacción: Forma de interacción más adecuada para evitar fraudes.
f) Ordenes: Protección que requiere para mantener la confidencialidad, integridad y no repudio de la información sobre trámites y para evitar la pérdida o duplicación de transacciones.
g) Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Las consideraciones mencionadas se implementarán mediante la aplicación de las técnicas criptográficas enumeradas en 1 – "Política de Utilización de Controles Criptográficos." y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente.

Se documentarán los acuerdos de gobierno electrónico entre partes que comprometan a las mismas a respetar los términos y condiciones acordados, incluyendo los detalles de autorización, requiriéndose otros acuerdos con proveedores de servicios de información y de redes que aporten beneficios adicionales.

Se darán a conocer a los usuarios, los términos y condiciones aplicables.

4. Seguridad del Correo Electrónico

7.4.1 Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
c) El impacto de un cambio en el medio de comunicación en los procesos del programa SINTyS, por ejemplo, el efecto del incremento en la velocidad de envío o el efecto de enviar mensajes formales de persona a persona en lugar de mensajes entre organizaciones.
d) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
e) Las implicancias de la publicación externa de listados de personal, accesibles al público.
f) El control del acceso de usuarios remotos a las cuentas de correo electrónico.

7.4.2 Política de Correo Electrónico

Se elaborará una política clara con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.
b) Protección de archivos adjuntos de correo electrónico.
c) Lineamientos sobre cuando no utilizar correo electrónico como medio de comunicación.
d) Responsabilidad del empleado de no comprometer al programa SINTyS, por ejemplo enviando correos electrónicos difamatorios, llevando a cabo prácticas de hostigamiento, o realizando acciones no autorizadas. En caso de permitir el uso personal de direcciones de correo, al pie de cada mensaje deberá haber una advertencia que diga que los dichos vertidos en el mail no representan la posición oficial del programa SINTyS.
e) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 1 – "Controles Criptográficos").
f) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
g) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

5. Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los medios de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias del programa SINTyS, incluyendo:

a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.
c) Exclusión de categorías de información sensible del programa SINTyS, si el sistema no brinda un adecuado nivel de protección.
d) Limitación del acceso a la información de agenda de personas determinadas, por ejemplo el personal que trabaja en proyectos sensibles.
e) La aptitud del sistema para dar soporte a las aplicaciones del programa SINTyS, como la comunicación de órdenes o autorizaciones.
f) Categorías de personal, contratistas o socios a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
h) Identificación de la posición o categoría de los usuarios, por ejemplo consultores del programa SINTyS a beneficio de otros usuarios.
i) Retención y resguardo de la información almacenada en el sistema.
j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

6. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del programa SINTyS que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con leyes, normas y estatutos de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público.

Todos los sistemas de acceso público deberán prever que:

i) La información se obtenga de acuerdo con la legislación de protección de datos.
j) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
k) La información sensible sea protegida durante el proceso de recolección y su almacenamiento.
l) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.

7. Otras Formas de Intercambio de Información

Se implementarán procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo, contemplando las siguientes acciones:

a) Concientizar al personal sobre la toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:

1) Personas cercanas, en especial al utilizar teléfonos móviles.
2) Terceros que tengan acceso a la comunicación mediante la Intervención de la línea telefónica, y otras formas de escucha subrepticias, a través del acceso físico al aparato o a la línea telefónica, o mediante equipos de barrido de frecuencias al utilizar teléfonos móviles análogos.
3) Terceros en el lado receptor.

b) Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.
c) No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado.
d) Recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular:

1) El acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos.
2) La programación deliberada o accidental de equipos para enviar mensajes a determinados números.
3) El envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado.

9 Control de Accesos

27 Generalidades

El acceso, por medio de un sistema de restricciones y excepciones, a la información y al hardware y a las aplicaciones que la procesan, es la base de todo sistema de seguridad informática, en cuanto a la utilización de las computadoras por parte del personal autorizado.

Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

28 Objetivo

Impedir el acceso no autorizado a los sistemas de información.

Proteger los servicios de red, tanto internos como externos.

Restringir el acceso a los recursos del computador mediante los mecanismos de seguridad a nivel del sistema operativo.

Se deben generar procedimientos de acceso que permitan:

a) Identificar y verificar la identidad y, si fuera necesario, la terminal o ubicación de cada usuario autorizado.

b) Registrar los accesos exitosos y fallidos al sistema.
c) Suministrar medios de autenticación apropiados; por ejemplo si se utiliza un sistema de administración de contraseñas, éste debe asegurar la calidad de las mismas.
d) Restringir los tiempos de conexión de los usuarios, según corresponda.

Detectar actividades no autorizadas en los sistemas del programa SINTyS.

Monitorear los sistemas para detectar desviaciones respecto de la Política y registrar eventos que suministren evidencia en caso de producirse incidentes relativos a la seguridad.

Comprobar la eficacia de los controles de acceso adoptados y verificar la conformidad con la Política correspondiente.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

29 Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los servicios o sistemas de información del programa SINTyS, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y los que administran la seguridad de las mismas.

30 Responsabilidad

El Responsable de Seguridad Informática, conjuntamente con los Responsables de Activos de la Información, son responsables del cumplimiento de las disposiciones establecidas para el control de acceso de las áreas y recursos del programa SINTyS.

31 Política

1. Requerimientos Políticos y de las Actividades del programa SINTyS

1. Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver 1 – "Clasificación y Control de Activos").
d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

2. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

a) Indicar expresamente si las reglas son obligatorias u optativas
b) Establecer reglas sobre la premisa "Todo debe estar generalmente prohibido a menos que se permita expresamente" y no "Todo está generalmente permitido a menos que se prohíba expresamente".
c) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario (Ver 1 – "Clasificación y Control de Activos").
d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
e) Controlar las reglas que requieren la aprobación del administrador o del Responsable del Activo de Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

2. Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado en los sistemas de información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.

1. Registración de Usuarios

Se definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de identificadores grupales sólo debe ser permitido cuando son convenientes para el trabajo a desarrollar debido a razones operativas.
b) Verificar que el usuario tiene autorización del propietario del sistema para el uso del sistema o servicio de información. Puede resultar necesaria una aprobación adicional de derechos de acceso por parte del Responsable de la Unidad Organizativa.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del programa SINTyS, por ejemplo que no compromete la separación de tareas.
d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
e) Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso.
f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización o se desvincularon del programa SINTyS.
i) Verificar periódicamente, y cancelar identificadores y cuentas de usuarios redundantes.
j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multiusuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones), debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

m) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
n) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
o) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.
p) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

3. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
b) Garantizar, cuando se requiera que los usuarios mantengan sus propias contraseñas, que se les provea inicialmente de una contraseña provisoria segura, que deberán cambiar de inmediato. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben acusar recibo de la recepción de la misma.
d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
e) Utilizar otras tecnologías de identificación y autenticación de usuarios, como la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma y uso de autenticadores de hardware (como las tarjetas de circuito integrado). Para ello, el Comité de Seguridad de la Información dispondrá, cuando el análisis de riesgo correspondiente lo determine, el uso de estas herramientas.
f) Configurar los sistemas operativos de red de tal manera que: las contraseñas tengan 8 (ocho) caracteres de longitud mínima, suspendan o bloqueen temporalmente al usuario al 3er (tercer) intento de entrar con una contraseña incorrecta (si corresponde, deberá pedir la rehabilitación al responsable de administración de seguridad), solicitar el cambio de la contraseña cada 30 (treinta) dias e impedir que una contraseña se repita durante un lapso de 3 (tres cambios).

4. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Responsable de los Activos de Información de que se trate llevará a cabo un proceso formal, a intervalos regulares cada mes, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos de 1 (un) mes y después de cualquier cambio.
b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 15 (quince) dias.
c) Revisar las asignaciones de privilegios a intervalos de 15 (quince) días, a fin de garantizar que no se obtengan privilegios no autorizados.

3. Responsabilidades del Usuario

III. Aspectos Generales

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. También permiten la identificación de las actividades realizadas en los sistemas de información.

1. Uso de Contraseñas

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
1. sean fáciles de recordar.
2. no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
3. no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema operativo de red se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquéllas almacenadas en una tecla de función o macro.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel razonable de protección de las contraseñas almacenadas.

2. Equipos Desatendidos en Areas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos durante un período extenso de tiempo.

El Responsable de Seguridad Informática debe disponer las tareas de concientización a todos los usuarios, acerca de los requerimientos y procedimientos de seguridad, para la protección de

equipos desatendidos, así como de sus responsabilidades por la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantallas protegido por contraseña.
b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

4. Control de Acceso a la Red

III. Aspectos Generales

Las conexiones no seguras a los servicios de red pueden afectar a todo el programa SINTyS, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

Para ello se deberán garantizar:

a) Interfaces adecuadas entre la/s red/es del programa SINTyS y las de otras organizaciones, o redes públicas.
b) Mecanismos de autenticación apropiados para usuarios y equipamiento.
c) Control de acceso de usuarios a los servicios de información.

1. Política de Utilización de los Servicios de Red

El Responsable de la Administración de la Red del programa SINTyS otorgará acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal de un titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad del programa SINTyS.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar procedimientos de autorización para determinar las personas y, las redes y servicios de red a los cuales tienen permitido el acceso.
c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Control de Accesos del programa SINTyS (Ver 1 – "Política de Control de Accesos").

2. Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del programa SINTyS, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

a) Asignar, números telefónicos o líneas, en forma dedicada.
b) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
c) Limitar las opciones de menú y submenú de cada uno de los usuarios.
d) Evitar la navegación ilimitada por la red.
e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls.
g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera del programa SINTyS.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos del programa SINTyS (Ver 1 – "Política de Control de Accesos"). El Responsable de Seguridad Informática, conjuntamente con el Responsable de los Activos de Información de que se trate, realizarán una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

3. Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del programa SINTyS. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad Informática, conjuntamente con el Responsable de los Activos de Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:

- Asignación de la herramienta de autenticación.
- Registro de los poseedores de autenticadores.
- Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
- Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:

- Establecimiento de las reglas con el usuario.
- Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de re-llamada o dial-back, pueden brindar protección contra conexiones no autorizadas y no deseadas a las instalaciones de procesamiento de información del programa SINTyS. Al aplicar este tipo de control, el programa SINTyS no debe utilizar servicios de red que incluyan desvío de llamadas o, si lo hacen, deben inhabilitar el uso de dichas herramientas para evitar las debilidades asociadas con la misma. Asimismo, es importante que el proceso de re-llamada garantice que se produzca una desconexión real del lado del programa SINTyS.

4. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación del programa SINTyS. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del programa SINTyS. En el punto anterior se enumeran algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

5. Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto 1 – "Autenticación de Usuarios para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto 1 - "Camino Forzado".

6. Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall", para filtrar el tráfico entre los dominios (Ver 1 – "Control de Conexión a la Red" y 1 – "Control de Ruteo de Red") y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos (Ver 1 – "Requerimientos Políticos y de las Actividades del programa").

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso (Ver 1 – "Requerimientos Políticos y de las Actividades del p"), el Responsable del Area Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados (Ver 1 – "Control de Conexión a la Red" y 1 - Control de Ruteo de Red") para subdividir la red.

7. Control de Conexión a la Red

En base a lo definido en el punto 1 - "Requerimientos Políticos y de las Actividades del p", se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red (Ver 1 – "Subdivisión de Redes").

Algunos ejemplos de las aplicaciones a las que deben aplicarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red restringido por hora o fecha.

8. Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden de los límites del programa SINTyS, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos (Ver 1 – "Política de Control de Accesos"). Estos controles se basarán en la verificación positiva de direcciones de origen y destino. Para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

9. Seguridad de los Servicios de Red

Se dispondrá de una clara documentación de las propiedades de seguridad de todos los servicios de red utilizados, sean públicos o privados. Estos atributos serán evaluados por el Responsable de Seguridad Informática.

5. Control de Acceso al Sistema Operativo

1. Identificación Automática de Terminales

El Responsable del Area Informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado del acceso al Sistema Operativo. Este análisis contará con la aprobación del Comité de Seguridad de la Información.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a) El método de identificación automática de terminales utilizado.
b) El detalle de transacciones permitidas por terminal.

2. Procedimientos de Conexión de Terminales

El acceso a los servicios de información solo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:

a) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.

c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
e) Limitar el número de intentos de conexión no exitosos permitidos y:
- Registrar los intentos no exitosos.
- Implementar una demora obligatoria antes de permitir otros intentos de identificación, o rechazar otros intentos sin autorización especifica.
- Desconectar conexiones de comunicaciones de datos.

f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
g) Desplegar la siguiente información, al completarse una conexión exitosa:
- Fecha y hora de la conexión exitosa anterior.
- Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

3. Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el programa SINTyS, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea especifica. Para casos de esta índole, se documentará la aprobación del Responsable de los Activos de Información de que se trate.

Si se utilizara un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.
b) Registrar los poseedores de autenticadores.
c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

4. Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Imponer una selección de contraseñas de calidad según lo señalado en el punto 1 – “Uso de Contraseñas”.
d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto 1 – “Uso de Contraseñas”.
e) Obligar a los usuarios a cambiar las contraseñas temporarias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
f) Mantener un registro de las últimas contraseñas del usuario, y evitar la reutilización de las mismas.
g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc).

5. Uso de Utilitarios de Sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas al programa SINTyS tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

6. Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable del Area Informática, con aprobación del Comité de Seguridad de la Información. En este caso, se definirán y asignarán responsabilidades y procedimientos para responder a la activación de una alarma silenciosa.

7. Desconexión de Terminales por Tiempo Muerto

Las terminales inactivas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad del programa SINTyS, o que sirven a sistemas de alto riesgo, se apagarán después de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red, después de un periodo definido de inactividad. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de los usuarios de la terminal.

Para algunas PC’s, puede suministrarse una herramienta limitada de desconexión de terminal por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

8. Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad del programa SINTyS.

Entre los controles que se deben aplicar, se enuncian:

a) Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
b) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
c) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando se autoricen excepciones para una extensión horaria ocasional.

6. Control de Acceso a las Aplicaciones

1. Restricción del Acceso a la Información.

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política del programa SINTyS para el acceso a la información, (Ver 1 – “Requerimientos Políticos y de las Actividades del p”).

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación.
b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

2. Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación (Ver 1 – “Clasificación y Control de Activos”).
b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
c) Coordinar con el Responsable del Area informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

7. Monitoreo del Acceso y Uso de los Sistemas

1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Dichos registros serán mantenidos durante un período que será definido por el Comité de Seguridad de la Información, para acceder en futuras investigaciones y en el monitoreo de control de accesos.

Los registros de auditoría deberán incluir:

a) Identificación del usuario.
b) Fecha y hora de inicio y terminación.
c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma (Ver 1 – “Identificación Automática de Terminales”).
d) Registros de intentos exitosos y fallidos de acceso al sistema.
e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados conforme los requerimientos de la Política de Retención de Registros (Ver 1 – “Recolección de Evidencia”).

2. Monitoreo del Uso de los Sistemas

7.2.1 Procedimientos y Areas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios solo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los consultores deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo (Ver 1 – “Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información”).

El alcance de estos procedimientos deberá corresponderse a la evaluación de riesgos que realice el Responsable del Area Informática y el Responsable de las Aplicaciones con aprobación del Comité de Seguridad de la Información.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) Acceso no autorizado, incluyendo detalles como:
1. Identificación del usuario.
2. Fecha y hora de eventos clave.
3. Tipos de eventos.
4. Archivos a los que se accede.
5. Utilitarios y programas utilizados.

b) Todas las operaciones con privilegio, como:
1. Utilización de cuenta de supervisor.
2. Inicio y cierre del sistema.
3. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.

c) Intentos de acceso no autorizado, como:
1. Intentos fallidos.
2. Violaciones de la Política de Accesos y notificaciones para “gateways” de red y “firewalls”.
3. Alertas de sistemas de detección de intrusiones.

d) Alertas o fallas de sistema como:
1. Alertas o mensajes de consola.
2. Excepciones del sistema de registro.
3. Alarmas del sistema de administración de redes.

7.2.2 Factores de Riesgo

Se desarrollará un procedimiento donde se establezca la periodicidad de revisión de las actividades de monitoreo, determinada de acuerdo a la evaluación de riesgos efectuada por el Responsable del Area Informática y el Responsable del Activo de que se trate.

Entre los factores de riesgo que se deben considerar se encuentran:

e) La criticidad de los procesos de aplicaciones.
f) El valor, la sensibilidad o criticidad de la información involucrada.
g) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
h) El alcance de la interconexión del sistema (en particular las redes públicas).

7.2.3 Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas realizadas contra el sistema y los métodos utilizados.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el Responsable del Area Informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los archivos.

En la asignación de responsabilidades en materia de seguridad de la información (Ver 1 – “Infraestructura de la Seguridad de la Información”), se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

a) La desactivación de la herramienta de registro.
b) La alteración de mensajes registrados.
c) La existencia de archivos de registro editados o suprimidos.
d) La saturación de un medio de soporte de archivos de registro.
e) La falla en los registros de los eventos.
f) La sobre escritura de los registros.

A los registros de eventos tendrán acceso las Unidades de Auditoría Interna, a fin de colaborar en el control y recomendaciones sobre modificaciones a los aspectos de seguridad. Adicionalmente podrían evaluar las herramientas, pero no tendrán libre acceso a ellas.

3. Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, de acuerdo con algún estándar establecido al respecto o, en su defecto, acordado entre el Responsable de Informática y el Comité de Seguridad de la Información. Este procedimiento indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección de cualquier variación significativa.

8. Computación Móvil y Trabajo Remoto

1. Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información del programa SINTyS.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital),Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales.

Esta lista no es taxativa, y deberán incluirse todos los dispositivos que pudieran contener información confidencial del programa SINTyS, y por lo tanto ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria
b) El acceso seguro a los dispositivos
c) La utilización de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios del programa SINTyS a través de dichos dispositivos.
e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
f) Los mecanismos de resguardo de la información contenida en los dispositivos.
g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia deberá entrenarse especialmente al personal que los utilice. Se desarrollarán procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.
b) No dejar desatendidos los equipos.
c) No llamar la atención acerca de portar un equipo valioso.
d) No poner identificaciones del programa SINTyS en el dispositivo.
e) No poner datos de contacto técnico en el dispositivo.
f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del programa SINTyS, los que incluirán:

a) Revocación de las credenciales afectadas
b) Notificación a grupos de Trabajo donde potencialmente se comprometan recursos.

2. Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al programa SINTyS.

A los efectos de autorizar el trabajo remoto, éste sólo será autorizado por el Responsable de los Activos de que se trate, conjuntamente con el Responsable del Area Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las presentes normas.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y urgencia del mismo tales como horarios del programa SINTyS, solicitudes de la Superioridad, etc.

Para ello, se establecerán procedimientos para el trabajo remoto, que consideren los siguientes aspectos.

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
b) El ambiente de trabajo remoto propuesto.
c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del programa SINTyS, la sensibilidad de la información a la que se accederá y que pasará a través del vinculo de comunicación y la sensibilidad del sistema interno.
d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
e) Evitar la instalación / desinstalación de software no provisto por el programa SINTyS.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.
b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del programa SINTyS y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
d) Incluir seguridad física.
e) Definir reglas y orientación para cuando familiares y visitantes accedan al equipo e información.
f) Proveer el hardware y el soporte y mantenimiento del software.
g) Definir los procedimientos de backup y de continuidad de las operaciones.
h) Efectuar auditoría y monitoreo de la seguridad.
i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

10 Desarrollo y Mantenimiento de Sistemas

32 Generalidades

El desarrollo de las aplicaciones, tanto comerciales como propias, es uno de los puntos más críticos de la seguridad.

Dado que los analistas y programadores tienen el conocimiento total de la lógica del proceso, se deben implementar validaciones y controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas y la plataforma de software de base (en el sentido de operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, encontrar rápidamente al responsable.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se debe identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación.

Asimismo, una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, asegura una correcta implementación de la seguridad ya que en general los aplicativos se asientan sobre este tipo de software.

33 Objetivo

Asegurar la inclusión de controles de seguridad en el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en los cuales éstos se apoyan.

34 Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios como contratados a proveedores, y a todos los sistemas operativos y/o de base que integren cualquiera de los ambientes administrados por el programa SINTyS en donde residan los desarrollos mencionados.

35 Responsabilidad

El Responsable del Area Informática es el encargado de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología del ciclo de vida de sistemas aprobada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

36 Política

1. Requerimientos de Seguridad de los Sistemas

1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información, sean estos sistemas nuevos, mejoras a los existentes o paquetes comerciales.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán las necesidades de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos de sistemas, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación y análisis de riesgo previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes de los productos a utilizar.

b) Evaluar los requerimientos de seguridad y los controles requeridos, en términos que éstos deben ser proporcionales en costo y esfuerzo, al valor del bien que se quiere proteger y al daño potencial a las actividades realizadas.

c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

2. Seguridad en los Sistemas de Aplicación

Para evitar la pérdida, modificaciones o uso inadecuado de los datos en los sistemas de información, se establecerán controles y registros de auditoría, controlando:

a) La validación de datos de entrada.
b) La validación de datos de salida.
c) El procesamiento interno.

1. Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

a) Control de secuencia.
b) Control de monto límite por operación y tipo de usuario.
c) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
d) Control de paridad.
e) Control contra valores cargados en las tablas de datos.
f) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

α) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quienes deberán ser informados del resultado, etc.

β) Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.

χ) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

2. Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

a) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos. Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
b) Procedimiento que establezca la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
c) Procedimiento que realice la validación de los datos generados por el sistema.
d) Procedimiento que verifique la integridad de los datos o software cargados o descargados entre computadoras.
e) Procedimiento que controle la integridad de registros y archivos.
f) Procedimiento que verifique la ejecución de los aplicativos en el momento adecuado.
g) Procedimiento que asegure el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

3. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensaje que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto 1 – “Controles Criptográficos”.

4. Validación de Datos de Salidas

Se establecerá un procedimiento para validar la salida de los datos de una aplicación, incluyendo:

a) Verificaciones físicas de la información que brinda el sistema, que actúen como un control por oposición.
b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos, etc..

3. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección de la confidencialidad, autenticidad e integridad.

1. Política de Utilización de Controles Criptográficos.

El programa SINTyS determina la presente Política de uso de controles criptográficos, a fin de determinar el correcto uso de los mismos. Para ello se establece que:

a) Se utilizarán controles criptográficos en las siguientes ocasiones:
1) Para la protección de claves.
2) Para la transmisión de información clasificada, fuera del ámbito del programa SINTyS.
3) Para el resguardo de información, cuando así surja del análisis de riesgos correspondiente, que será realizado por el Responsable del Area Informática.

b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

c) Se designa a los siguientes responsables:

Función	Cargo
Implementación de la Política de Controles Criptográficos	Encargado de seguridad del CNCPS, Coordinador de seguridad SINTyS
Administración de Claves	Encargado de seguridad del CNCPS, Coordinador de seguridad SINTyS

d) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

1) Cifrado Simétrico

Algoritmo	Longitud de Clave
AES	128/192/256
3DES	168 bits
IDEA	128 bits
RC4	128 bits
RC2	128 bits

2) Cifrado Asimétrico

Utilizar Para	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
	ECDSA	190 bits

2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Responsable del Area Informática, conjuntamente con el responsable de la implementación de la Política de Controles Criptográficos, se identificará el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política del programa SINTyS en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica (Ver 1 – “Regulación de Controles para el Uso de Criptografía”).

3. Firma Digital

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Los algoritmos de firma utilizados, como así también la longitud de clave a emplear, son las enumeradas en el punto 1 – “Política de Utilización de Controles Criptográficos”, en el cuadro de cifrado asimétrico.

Se recomienda que las claves criptográficas utilizadas para realizar firmas digitales no sean empleadas en procedimientos de cifrado de información y sean resguardadas bajo el control exclusivo del titular.

Al utilizar firmas digitales, se considerará la legislación pertinente (Ley 25.506, el Decreto Nº 2628/02 y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos) que describa las condiciones bajo las cuales una firma digital es legalmente vinculante. Por ejemplo, en el caso del comercio electrónico, es importante conocer la situación jurídica de las firmas digitales.

Podría ser necesario establecer contratos de cumplimiento obligatorio u otros acuerdos para respaldar el uso de las mismas, cuando el marco legal es inadecuado. Se deberá obtener asesoramiento legal con respecto a las leyes y normas que podrían aplicarse al uso de firmas digitales que pretende realizar el programa SINTyS (Ver 1 – "Cumplimiento").

4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia o no de un evento o acción.

5. Administración de Claves

3.5.1 Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar su uso por parte del programa SINTyS de los dos tipos de técnicas criptográficas, los cuales son:

a) Técnicas de clave secreta, cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla.
b) Técnicas de clave publica, cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Las técnicas criptográficas enumeradas en el punto 1 – "Política de Utilización de Controles Criptográficos", serán aplicadas con este propósito.

Se proveerá de protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

3.5.2 Normas, Procedimientos y Métodos

Se redactarán los procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de clave publica.
c) Distribuir claves a los usuarios que corresponda, incluyendo cómo deben activarse las claves cuando se reciben.
d) Almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados.
e) Cambiar o actualizar claves, incluyendo reglas sobre cuando y como deben cambiarse las claves.
f) Ocuparse de las claves comprometidas.
g) Revocar claves, incluyendo como deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del programa SINTyS (en cuyo caso las claves también deben archivarse).
h) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades del programa SINTyS, por ejemplo la recuperación de la información cifrada.
i) Archivar claves, por ejemplo, para la información archivada o resguardada.
j) Destruir claves.
k) Registrar (logging) y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de entrada y fin de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de 1 año.
Además de la administración segura de las claves secretas y privadas, también deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Estos certificados se generarán de forma que vincule de manera única la información relativa al propietario del par de claves pública / privada con la clave pública.

En consecuencia es importante que el proceso de administración que genera estos certificados sea confiable. Normalmente, este proceso es llevado a cabo por una autoridad de certificación, la cual deberá residir en una organización reconocida, con adecuados controles y procedimientos implementados, para ofrecer el nivel de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicios o contratos con proveedores externos de servicios criptográficos, por ejemplo con una autoridad de certificación, deben comprender los tópicos de responsabilidad legal, confiabilidad del servicio y tiempos de respuesta para la prestación de los mismos.

4. Seguridad de los Archivos del Sistema

Se garantizará que los proyectos y actividades de soporte al sistema se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

1. Control del Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada internamente o adquirida a un proveedor tendrá un único Responsable designado formalmente por el Responsable del Area Informática.

- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

- El Responsable del Area Informática, asignará formalmente la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones y responsabilidades principales:

a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, son los autorizados y aprobados de acuerdo a los procedimientos vigentes.
c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.
b) Llevar un registro de auditoría de las actualizaciones realizadas.
c) Retener las versiones previas del sistema, como medida de contingencia.
d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
e) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
f) Evitar, cuando fuera posible, que la función de implementador sea ejercida por alguna persona que pertenezca al sector de desarrollo o mantenimiento.

2. Protección de los Datos de Prueba del Sistema

Para proteger los datos de prueba se establecerá un procedimiento que contemple lo siguiente:

a) Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
b) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal actuación.
c) Registrar formalmente, tanto el uso como la copia de la información de bases de datos operativas.
d) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

3. Control de Acceso a las Bibliotecas de Programas Fuentes.

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) Asignar formalmente, al Responsable del Area Informática, la función de "Administrador de Fuentes", quien tendrá en custodia los programas fuentes y deberá:

- Proveer al Area de Desarrollo de los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
- Llevar un registro actualizado de todos los programas fuentes que estén en producción, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación, y fecha / hora de compilación y estado (en modificación, en producción).
- Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario.
- Administrar las distintas versiones de una aplicación.

b) Denegar al Administrador de Fuentes permisos de modificación sobre los programas fuentes bajo su custodia.
c) Establecer que todo programa objeto o ejecutable en producción tendrá un único programa fuente asociado que garantice su origen.
d) Establecer que la generación del programa objeto o ejecutable que estará en producción (compilación) la hará el Administrador de Fuentes o el implementador de producción, a fin de garantizar tal correspondencia.
e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
f) Evitar, cuando fuera posible, que la función de administrador de fuentes sea ejercida por alguna persona que pertenezca al sector de desarrollo y/o mantenimiento.
g) Prohibir la guarda de programas fuentes en el ámbito de producción.
h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el programa SINTyS.

5. Seguridad de los Procesos de Desarrollo y Soporte

Esta Política provee seguridad del software y de la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte a los mismos.

1. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Estos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones

e) Mantener un registro de los niveles de autorización acordados.
f) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
g) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
h) Obtener aprobación formal para las propuestas detalladas antes que comiencen las tareas, por parte del Responsable de Sistemas.
i) Obtener la aprobación por parte del usuario autorizado y del área de testing.
j) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
k) Mantener un control de versiones para todas las actualizaciones de software.
l) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y no alterando los procesos involucrados.

2. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b) Incluir las revisiones y pruebas del sistema operativo dentro del plan de tareas y presupuesto del programa SINTyS.
c) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
d) Asegurar la actualización del Plan de Continuidad de las Actividades del programa SINTyS.

3. Restricción del Cambio de Paquetes de Software

Se prohíbe la modificación de paquetes de software suministrados por proveedores.

En caso de considerarlo esencial, y previa autorización del Responsable del Area Informática, se tendrá en cuenta:

a) Obtener el consentimiento del proveedor en caso de ser necesario.
b) Intentar que sea el proveedor quien realice los cambios requeridos generando una actualización estándar de los programas.
c) Evaluar el impacto que se produce si el programa SINTyS se hace cargo del mantenimiento.
d) Retener el software original y los cambios deberán realizarse sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

4. Canales Ocultos y Código Troyano

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código troyano está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

Para revisar este tópico, se redactará un procedimiento que incluya:

a) Comprar programas a proveedores acreditados o productos ya evaluados.
b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
c) Controlar el acceso y las modificaciones al código instalado.
d) Efectuar tareas de monitoreo.

5. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerá un procedimiento que contemple los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos de propiedad intelectual (Ver 1 – “Derechos de Propiedad Intelectual”).
b) Requerimientos contractuales con respecto a la calidad del código.
c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código troyano, etc.
d) Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto – “”.
e) Acuerdos de custodia en caso de quiebra de la tercera parte.

37 Anexo

Para cumplir con esta Política, en lo referente a los puntos “Seguridad de los Archivos del Sistema y “Seguridad de los Procesos de Desarrollo y Soporte”, se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados.

Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalan programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A continuación se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de cada programa SINTyS, con las limitaciones de recursos y equipamiento correspondientes.

- **Ambiente de Desarrollo**

Es donde se desarrollan los programas fuentes. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el administrador de fuentes.
El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

- **Ambiente de Pruebas**

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote al efecto, junto con el usuario de ser posible.
El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

- **Ambiente de Producción**

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el administrador de fuentes y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El programa fuente se compila dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de fuentes.

Procedimientos de la misma naturaleza y alcance deberían aplicarse a las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deberían cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

11 Administración de la Continuidad de las Actividades del programa SINTyS

38 Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del programa SINTyS.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del programa SINTyS puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

39 Objetivo

Minimizar los efectos de las interrupciones de las actividades normales del programa SINTyS y proteger los procesos críticos de dichas actividades, de las fallas significativas o desastres.

Reducir a un nivel aceptable, la discontinuidad de las actividades (sea ésta resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del programa SINTyS con el establecimiento de planes de contingencia que incluyan al menos las siguientes etapas:

a) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Identificar las actividades, los recursos, y los procedimientos necesarios para cumplir los requisitos de procesamiento de la Organización durante una interrupción prolongada de las operaciones normales.

Asignar responsabilidades al personal designado del programa SINTyS y proporcionar una guía para la recuperación de los sistemas durante períodos prolongados de interrupción de las operaciones normales.

Asegurar la coordinación con el personal del programa SINTyS que participará en las estrategias de planificación de contingencias.

Asegurar la coordinación con los contactos externos al programa SINTyS que participarán en las estrategias de planificación de contingencias.

40 Alcance

Esta Política se aplica a todos los procesos críticos identificados del programa SINTyS.

41 Responsabilidad

El Comité de Seguridad de la Información, el Responsable de Seguridad Informática y los coordinadores de todos los componentes, son responsables de la elaboración y prueba de los procesos que garanticen la continuidad de la actividad del programa SINTyS, de participar en la elaboración de normas, procedimientos y prácticas de seguridad en este sentido, así como en su difusión y concientización de todo el personal del programa SINTyS.

42 Política

1. Proceso de la Administración de la Continuidad del programa SINTyS

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de la actividad del programa SINTyS.

Este Comité tendrá a cargo las siguientes funciones, además de las definidas en el punto 1 – “Comité de la Seguridad de la Información”:

a) Definir los objetivos organizacionales de las herramientas de procesamiento de información.
b) Garantizar que la administración de la continuidad de los negocios esté incorporada a los procesos y estructura del programa SINTyS.
c) Identificar y priorizar los procesos críticos de las actividades del programa SINTyS.
d) Asegurar que todos los integrantes del programa SINTyS comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto, así como los efectos que una interrupción puede tener en la actividad del programa SINTyS.
e) Elaborar y documentar una estrategia de continuidad de los negocios consecuente con los objetivos y prioridades acordados.
f) Elaborar y documentar planes de continuidad de las actividades del programa SINTyS de conformidad con la estrategia de continuidad acordada.
g) Efectuar pruebas y actualizaciones periódicas de los planes y procesos implementados.
h) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio.

2. Continuidad de las Actividades y Análisis de los Impactos

Con el fin de establecer un Plan de Continuidad de las Actividades del programa SINTyS se deben contemplar los siguientes puntos:

- Identificar los eventos que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, robo o hurto, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo 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.

Esto será llevado a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate. Esta evaluación considerará todos los procesos de las actividades del programa SINTyS y no se limitará a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de los negocios. Una vez que se ha creado este plan, el mismo debe ser aprobado por el Comité de la Seguridad de la información.

3. Elaboración e Implementación de los Planes de Continuidad de las Actividades del programa SINTyS

Los propietarios de procesos y recursos de información elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del programa SINTyS. Estos procesos deberán ser aprobados por el Comité de Seguridad de la Información.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las responsabilidades y procedimientos de emergencia.
b) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de negocios externos y a los contratos vigentes.
c) Documentar los procedimientos y procesos acordados.
d) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
e) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
1) Objetivo del plan.
2) Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
3) Procedimientos de divulgación.
4) Requisitos de la seguridad.
5) Procesos específicos para el personal involucrado.
6) Responsabilidades individuales.
f) Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades del programa SINTyS requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

4. Marco para la Planificación de la Continuidad de las Actividades del programa SINTyS

Se mantendrá un solo marco para los planes de continuidad de las actividades, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas responsables de ejecutar cada componente del mismo. Cuando se identifican nuevos requerimientos, deben modificarse de conformidad con los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

Estas modificaciones deberán ser aprobadas por el Comité de Seguridad de la Información.

El marco para la planificación de la continuidad de las actividades del programa SINTyS, tendrá en cuenta los siguientes puntos:

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del programa SINTyS y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del programa SINTyS o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos.
d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del programa SINTyS.
e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
f) Efectuar actividades de concientización e instrucción que estén diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces.
g) Documentar las responsabilidades de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda.

Los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de los recursos o procesos pertinentes. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del programa SINTyS.

Debido a que los planes de continuidad de las actividades del programa SINTyS pueden fallar, debido a suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplos de interrupciones).
b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
d) Realizar ensayos completos probando que el programa SINTyS, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del programa SINTyS se tomarán en cuenta, además, los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del programa SINTyS en paralelo, con operaciones de recuperación fuera del sitio principal).
b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído).

Los planes de continuidad de las actividades del programa SINTyS serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del programa SINTyS para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

Cada uno de los propietarios de los procesos y recursos de información, es el responsable de las revisiones periódicas de cada uno de los planes bajo su responsabilidad, como así también de la identificación de cambios en las disposiciones relativas a las actividades del programa SINTyS aún no reflejadas en los planes de continuidad.

Todas las modificaciones efectuadas serán aprobadas por el Comité de la Seguridad de la Información

Por otra parte, el resultado de este proceso será distribuido a fin de que todo el personal involucrado tenga conocimiento de los cambios.

Deberá prestarse atención, especialmente, a los cambios de:

a) Personal.
b) Direcciones o números telefónicos.
c) Estrategia del programa SINTyS.
d) Ubicación, instalaciones y recursos.
e) Legislación.
f) Proveedores y clientes críticos.
g) Procesos, o procesos nuevos / eliminados.
h) Tecnologías.
i) Requisitos operacionales.
j) Requisitos de seguridad.
k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
l) Requerimientos de los sitios alternativos.
m) Registros de datos vitales.

12 Cumplimiento

43 Generalidades

El diseño, operación, uso y administración de los sistemas de información está regulado por disposiciones legales y contractuales que se tienen que respetar.

Los requisitos legales, normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

Es necesario contar con el respaldo de los asesores jurídicos del programa SINTyS, quienes se encargarán de informar las conductas que no se ajustan a derecho.

44 Objetivos

Cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas y legales al programa SINTyS y/o al empleado.

Garantizar que los sistemas cumplan con las Políticas y estándares de seguridad del programa SINTyS.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de las Políticas y estándares de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del programa SINTyS.

45 Alcance

Esta Política se aplica a todo el personal del programa SINTyS, cualquiera sea su situación de revista.

Asimismo se aplica a los sistemas de información, procedimientos, documentación y plataformas técnicas del programa SINTyS, y a las auditorías efectuadas sobre los mismos.

46 Responsabilidad

Todos los consultores de los mandos medios y superiores deberán conocer, dar a conocer, cumplir y hacer cumplir la presente Política y la normativa vigente.

47 Políticas

1. Cumplimiento de Requisitos Legales

1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades individuales para cumplir con dichos requisitos.

2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los consultores únicamente podrán utilizar material autorizado por el programa SINTyS.

El programa SINTyS solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por quien lo haya desarrollado, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deberán tener presentes las siguientes normas:

- *Ley de Propiedad Intelectual Nº 11.723:* Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

- *Ley de Marcas Nº 22.362:* Protege la propiedad de una marca y la exclusividad de su uso.
- *Ley de Patentes de Invención y Modelos de Utilidad Nº 24.481:* Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

1.2.1 Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual.

Esta ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos a máquinas específicas y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad Informática analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir un procedimiento para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
c) Mantener un adecuado registro de activos.
d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f) Verificar que sólo se instalen productos con licencia y software autorizado.
g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
i) Utilizar herramientas de auditoría adecuadas.
j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

3. Protección de los Registros del programa SINTyS

Los registros importantes del programa SINTyS se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del programa SINTyS.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

Tipo de Registro	Sistema de Información	Período de Retención	Medio de Almacenamiento
expedientes	No informático	5 años	Papel
VUO	Informático	6 meses Logs de auditoría	magnético
RUBAD	Informático	6 meses Logs de auditoría	magnético
Base desarrollo	Informático	6 meses Logs de auditoría	magnético
Base producción	Informático	1 año Logs de auditoría	magnético
Base Registración Personas	Informático	6 meses Logs de auditoría	magnético
Bases Recibidas	informático	5 años	CD, DKT, cinta

Las claves criptográficas asociadas con archivos cifrados o firmas digitales se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario.(Ver 1 – "Controles Criptográficos")

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante.(Ver 1 – "Política de Utilización de Controles Criptográficos.")

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el programa SINTyS.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Mantener un inventario de fuentes de información clave.
d) Implementar adecuados controles para proteger los registros y la información esenciales contra pérdida, destrucción y falsificación.

En particular, se deberán tener presente las siguientes normas:

- *Etica en el Ejercicio de la Función Pública. Ley 25.188:* Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- *Código de Etica de la Función Pública:* Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.
- *Código Penal Art. 255:* Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.
- *Ley Nº 24.624. Artículo 30:* Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorgar valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.
- *Decisión Administrativa 43/96:* Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquellos.

4. Protección de Datos y Privacidad de la Información Personal

Todos los consultores deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El programa SINTyS redactará un "Acuerdo de Confidencialidad", el cual deberá ser suscrito por todos los consultores. La copia firmada del acuerdo será retenida en forma segura por el programa SINTyS.

Mediante este acuerdo se comprometerá al empleado a usar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. El "Acuerdo de Confidencialidad" deberá advertir que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado (Ver 1 – "Seguridad del Personal").

En particular, se deberán tener presente las siguientes normas:

- *Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164*: Establece que los Funcionarios Públicos deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera.
- *Convenio Colectivo de Trabajo General*: Dispone que todos los agentes deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueran asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.
- *Etica en el Ejercicio de la Función Pública. Ley 25.188:* Obliga a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.
- *Código de Etica de la Función Pública:* Establece que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes, ni la debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.
- *Protección de Datos Personales. Ley 25.326:* Establece responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.
- *Confidencialidad. Ley Nº 24.766:* Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.
- *Código Penal:* Sanciona a aquel que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (Art. 156), al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (Art. 157), al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223).

Asimismo, deberá considerarse lo establecido en el Decreto 1172/03, que regula el acceso a la información pública por parte de los ciudadanos.

5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del programa SINTyS se suministran con un propósito determinado. La utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos, sin la aprobación del Responsable de la Unidad Organizativa, debe ser considerada como uso indebido.

Todos los consultores deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

En particular, se debe respetar lo dispuesto por las siguientes normas:

- *Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164*: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.
- *Convenio Colectivo de Trabajo General*: Obliga a los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal.
- *Etica en el Ejercicio de la Función Pública. Ley 25.188*: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.
- *Código de Etica de la Función Pública*: Obliga al funcionario público a proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

6. Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales, se deberá considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/02, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Respecto a la comercialización de controles criptográficos, nuestro país ha suscrito el acuerdo Wassennar, que establece un listado de materiales y tecnologías de doble uso, cuya comercialización puede ser considerada peligrosa.

El Decreto 603/92 regula el Régimen de Control de las Exportaciones Sensitivas y de Material Bélico, estableciendo un tratamiento especial para la exportación de determinados bienes que pueden ser comprendidos dentro del concepto de material bélico.

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección General de Política, de la Secretaría de Asuntos Militares, Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

7. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el programa SINTyS garantizará que sus sistemas de información cumplen con los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.
b) Copiar la información en medios informáticos removibles y la información en discos rígidos o en memoria, para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal. Por consiguiente, existe el riesgo de que la evidencia necesaria sea destruida accidentalmente antes de que se advierta la gravedad del incidente.

El Comité de la Seguridad de la Información, encargado del monitoreo de los incidentes de seguridad, deberá involucrar a un asesor letrado y/o a la policía, en la primera etapa de cualquier acción legal contemplada y procurar asesoramiento acerca de la evidencia requerida, a fin de precisar todas las circunstancias y reunir los elementos de prueba tendientes a esclarecer la comisión de irregularidades e individualizar a los responsables.

Se deberá tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley Nº 19.549 (Ley de Procedimiento Administrativo) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente (Art. 255).

2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

1. Cumplimiento de la Política de Seguridad

Cada coordinador de componente, deberá garantizar la correcta implementación y cumplimiento de los procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del programa SINTyS a efectos de garantizar el cumplimiento de las Políticas y estándares de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información y de recursos de información.
d) Usuarios.
e) Gerentes.

Los propietarios de los sistemas de información brindarán apoyo a la revisión periódica del cumplimiento de las Políticas, estándares y otros requisitos de seguridad aplicables.

2. Verificación de la Compatibilidad Técnica

El Responsable de Seguridad Informática verificará periódicamente que los sistemas de información cumplan los estándares de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración, las cuales podrán contar con la asistencia de especialistas independientes contratados a ese efecto. Esta verificación tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes y formalmente autorizadas o bajo la supervisión de las mismas.

3. Consideraciones de Auditorías de Sistemas

1. Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a) Acordar con el Area que corresponda los requerimientos de auditoría.
b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

- Eliminar archivos transitorios.
- Eliminar entidades ficticias y datos incorporados en archivos maestros.
- Revertir transacciones.

d) Identificar claramente los recursos de TI para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, el Responsable de la Auditoría completará el siguiente formulario, el cual deberá ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a utilizar en la Verificación	
Sistemas de información	
Base de datos	
Hardware	
Software de Auditoría	
Medios Magnéticos	
Personal de Auditoría	
Interlocutores de las Areas de Informática	
Interlocutores de las Areas Usuarias	
Conexiones a Red	

e) Identificar y acordar los requerimientos de procesamiento especial o adicional.

f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

- Fecha y hora.
- Puesto de trabajo.
- Usuario.
- Tipo de acceso.
- Identificación de los datos accedidos.
- Estado previo y posterior.
- Programa y/o función utilizada.

g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

2. Protección de los Elementos Utilizados Durante la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

4. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Publica Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los programa SINTySs pertinentes.

1 Anexo I: Planilla Control de Acceso de Visitas

Control de Acceso de visitas.

Sistema de Identificación Nacional Tributario y Social
Consejo Nacional de Coordinación de Políticas Sociales
Presidencia de la Nación

SINTyS

Fecha: Dia: del Mes del Año

Nombre	Apellido	Tipo	N° Documento	Razón Social	Ing/Egr	Hora	Firma	Autoriza	Firma	Motivo de la visita

2. Anexo II: Política de Uso Aceptable

Objetivo

El objetivo del presente documento es el de definir la política de uso aceptable para que toda persona vinculada al proyecto SINTyS sea debidamente informada del uso considerado como aceptable de los recursos informáticos y de infraestructura de comunicaciones asociados al proyecto.

Introducción

Este documento describe la política del proyecto SINTyS en lo que respecta al uso, acceso, revisión y difusión de las comunicaciones en formato digital o electrónico, incluyendo en las mismas tanto a las comunicaciones recibidas como a las emitidas por personas vinculadas al proyecto.

Para los fines de este documento, el término *comunicaciones electrónicas* incluye (pero no se limita a) el envío, la recepción y el uso de información a través de la red de información corporativa, Internet, red de telefonía (privada y pública), los servicios de fax y videoconferencia y todo otro tipo de servicios de información en línea.

Para los fines de este documento, el término *persona vinculada al Proyecto*, se refiere a toda persona que desarrollando actividades en el marco del Proyecto SINTyS, independientemente de la relación jurídica que los vincule, que use, acceda, revise y difunda comunicaciones electrónicas en el ejercicio de esas actividades, e incluyendo a toda persona que utilice los sistemas informáticos y de comunicaciones del proyecto.

Contenido

Implicancia en las actividades relacionadas con el SINTyS

Los sistemas de información y comunicaciones son puestos a disposición de las personas vinculadas al Proyecto para su uso exclusivo de sus actividades.

El uso personal está restringido y no debería interferir con el desempeño de la persona vinculada al proyecto en el normal desenvolvimiento de sus actividades. El acceso a cuentas de correo electró-

nico personal está sujeto a la aprobación de la jerarquía inmediata superior. Los mensajes personales no pueden ser retransmitidos a grupos de individuos u otras personas vinculadas al proyecto, con la posible excepción de foros apropiados. La difusión multitudinaria de mensajes involucrando a toda la organización debe ser previamente autorizada por la Coordinación General del Proyecto.

1 Monitoreo y Privacidad

Las comunicaciones electrónicas efectuadas desde los sistemas de información y comunicaciones del SINTyS son propiedad del SINTyS y están destinadas a facilitar la operatoria del proyecto. El SINTyS tratará a todas las comunicaciones electrónicas emitidas, recibidas y/o almacenadas como mensajes de la organización, incluyendo los mensajes de índole personal. Ninguna persona vinculada al proyecto debería esperar tratamiento de privacidad en ninguna de las comunicaciones electrónicas establecidas en dependencias del SINTyS. Aún si no se monitorearán comunicaciones electrónicas en forma rutinaria, el SINTyS se reserva el derecho de monitorear, consultar, revisar, copiar, almacenar o borrar todo tipo de comunicación electrónica, incluidos mensajes personales para cualquier propósito y sin previo aviso. Asimismo, SINTyS se reserva el derecho de divulgación de dicha información a quien lo considere apropiado.

2 Retención de Información

SINTyS se reserva el derecho a retener copias de respaldo de toda comunicación cursada y de todo documento generado y/o modificado en dependencias del SINTyS por el plazo que se considere apropiado.

3 Actividades Prohibidas y Empleo del Buen Juicio

Está terminantemente prohibida la consulta no autorizada de información en las bases de datos de los organismos participantes del proyecto, así como la divulgación de ésta y toda otra información de carácter confidencial del proyecto SINTyS a terceros, que no se encuentre debidamente autorizada por la Coordinación General del Proyecto. (ver saneamiento).

Está expresamente prohibido el acceso a recursos informáticos y de comunicaciones que no se correspondan con los autorizados a las personas vinculadas al proyecto en sus roles respectivos, según descriptos en el Anexo "A" (*Perfiles de Usuarios del Proyecto SINTyS*). Los derechos de acceso a recursos de una persona vinculada al proyecto deben ceñirse a lo estrictamente delineado por su correspondiente perfil de usuario, estando éste en la obligación de reportar inmediatamente a su jerarquía inmediata superior cualquier violación de las políticas de control de acceso derivada de un mal uso o incorrecta configuración de mecanismos de control de acceso que el individuo perciba en su operatoria habitual.

Toda comunicación electrónica que resulte amenazante, discriminatoria (basada en raza, credo, color de piel, edad, sexo, condiciones físicas o mentales, orientación sexual, etc), difamatoria u ofensiva está expresamente prohibida. Las comunicaciones electrónicas no deberían revelar información de carácter personal sin la debida autorización. La alteración o destrucción de comunicaciones electrónicas con la intención de causar daño a la organización o a una persona vinculada al proyecto de la misma está estrictamente prohibida. Las comunicaciones electrónicas no deben emplearse con propósitos ilegales o para violar propiedad intelectual de terceros. Las personas vinculadas al proyecto no deben acceder en forma ilegal a sistemas de otras personas vinculadas al proyecto o terceros o interceptar comunicaciones entre otros individuos, a menos que cuente con la correspondiente aprobación de la Coordinación General del Proyecto (enmarcado en las operaciones descriptas en el item *Monitoreo y Privacidad*).

Los individuos vinculados contractualmente con el SINTyS deberán usar su mejor juicio y tomarán las mismas precauciones para preparar comunicaciones electrónicas que tomarían para elaborar un documento de acceso público tal como un memorando. El contenido de las comunicaciones electrónicas puede tener un impacto negativo significativo cuando es sacado del contexto apropiado (con posibles consecuencias económicas, financieras y legales). Deberá tomarse el mayor recaudo para evitar el envío de información sin la apropiada revisión final, para evitar que presiones de índole temporal hagan incurrir al remitente en errores de significativo perjuicio para el SINTyS.

Las personas vinculadas al proyecto deberán prestar atención para garantizar que las comunicaciones electrónicas sean cursadas a los destinatarios adecuados, evitando difundir información a terceros no incluidos en el contexto apropiado de la comunicación. A los efectos de minimizar riesgos, se aconseja mantener un tono profesional, respetuoso y cordial en todas las comunicaciones electrónicas efectuadas desde y hacia SINTyS.

4 Propiedad Intelectual. Protección de datos personales.

Las facilidades de replicación de información protegida que ofrece la tecnología digital, plantea un serio riesgo para la violación de propiedad intelectual. Las personas vinculadas al proyecto serán informadas respecto de la propiedad intelectual de los desarrollos y productos elaborados en el SINTyS, a través de un convenio de confidencialidad adjuntado al presente como Anexo "B".

El convenio de confidencialidad, diseñado por el Componente Gestión, establece los términos legales que regulan el tratamiento de los datos personales, y es suscripto por las personas vinculadas al proyecto en dos ejemplares, uno para el que suscribe y otro para ser depositado en la Coordinación General del Proyecto.

5 Uso de Licencias

El software sindicado como *libre*, de *dominio público* o de *uso público*, podría ser gratuito para uso personal, pero no necesariamente así para uso corporativo. Al descargar software de Internet, el uso de cierto tipo de software podría violar derechos de *copyright* o de *licencias,* además de constituir riesgo de violación del perímetro de seguridad (ver *Protección contra Malware*). Las personas vinculadas al proyecto no deberán copiar software licenciado al SINTyS, a menos que cuenten con autorización expresa para ello de su jerarquía inmediata superior. Las personas vinculadas al proyecto no deberán instalar ningún tipo de software en sus computadoras personales. Ante la necesidad de requerir aplicaciones que no se encuentren pre-instaladas en su sistema, deberán cursar pedido formal (autorizado por su jerarquía inmediata superior), al área de soporte de infraestructura. Queda terminantemente prohibido quitar u ocultar en forma deliberada las notificaciones de restricciones de licencias del software utilizado por el proyecto SINTyS.

6 Protección contra Malware

Las personas vinculadas al proyecto no deberán en forma consciente crear, ejecutar, reenviar o introducir ningún tipo de código diseñado para auto-replicarse, propagarse en la infraestructura de comunicaciones y violar las políticas de seguridad en cualquiera de sus aspectos.

Los archivos adosados al correo electrónico y en general todos los archivos que procedan de infraestructura ajena al SINTyS y se ingresen al sistema por diversos perfiféricos (Floppies, CDs, Dispositivos USBs, descargas de internet, etc) deberán ser monitoreados con el software antivirus puesto a disposición de la plataforma de cómputo personal del individuo por el SINTyS (el cual deberá encontrarse debidamente actualizado) previo a su apertura para visualización, modificación o reenvío a terceros, independientemente de si éstos pertenecen o no al proyecto.

Esta terminantemente prohibido desactivar la plataforma de monitoreo de malware del proyecto SINTyS, tanto sea en servidores como en estaciones de trabajo.

Acciones Disciplinarias

La Coordinación General del Proyecto se reserva el derecho a revocar los privilegios de acceso de los usuarios a los recursos informáticos del sistema ante violaciones a esta política, conductas que sean de carácter disruptivo hacia el normal desenvolvimiento de procesos informáticos o desvinculación temporal o permanente del proyecto SINTyS. Cualquier conducta que afecte negativamente la disponibilidad de la infraestructura informática y de comunicaciones de la organización o que pueda dañar u ofender a terceros o perjudicar los intereses del proyecto SINTyS será considerada como indeseable y por ende no será permitida. Violaciones de cualquier tipo a esta política podrán ocasionar sanciones y medidas disciplinarias sin notificación previa de la Coordinación General del Proyecto.

Aceptación

Con mi firma y aclaración como prueba de conformidad, manifiesto haber leído y comprendido los términos del presente documento y me comprometo a velar por su cumplimiento.

3. Anexo III: Convenio de Confidencialidad

Entre el SISTEMA DE IDENTIFICACION NACIONAL TRIBUTARIO Y SOCIAL (SINTyS), Préstamo BIRF Nº 4459-AR, representado por la Coordinadora General del SINTyS, Doctora Matilde Morales, por una parte, en adelante EL SINTyS; y …… con D.N.I. …….. por la otra, celebran el presente convenio de confidencialidad, el que se regirá por las cláusulas siguientes:

PRIMERA: EL/LA CONSULTOR/A cede en su totalidad al SINTyS, en los términos de la ley 11.723, los derechos de propiedad de autor y de reproducción, así como cualquier otro derecho intelectual que pudiera corresponderle, sobre los informes, estudios u obra producidos, como consecuencia de la relación que rige entre EL SINTyS y EL/LA CONSULTOR/A. Las partes declaran que bajo ningún concepto serán objeto del derecho de propiedad intelectual, los datos personales contenidos en las bases de datos, en concordancia con lo que establece la ley 25.326 de Protección de la Datos Personales y su Decreto Reglamentario Nº 1558/2001.

SEGUNDA: Las partes acuerdan otorgar a todos los datos referidos a personas físicas o jurídicas, ya sea que consten en informes, formularios, documentación, publicaciones, estudios o en cualquier otro tipo de información, impresos en papel u obrantes en medios electrónicos o magnéticos, discos, ópticos, microfilmes, películas u otros medios similares a los cuales EL/LA CONSULTOR/A tenga o pudiera llegar a tener acceso, el carácter de CONFIDENCIAL, por lo que está obligada a guardar SECRETO PROFESIONAL, del que sólo podrá ser relevado/a por expresa autorización de EL SINTyS, o mediante resolución judicial, y/o por mediar fundadas razones relativas a la seguridad pública, la defensa nacional o la salud pública. Además, EL/LA CONSULTOR/A se compromete a no utilizar los datos, a los que tenga acceso, en beneficio propio, de familiares o terceros en general, ni utilizarlos con finalidades distintas o incompatibles con aquellas que motivaron su obtención.

TERCERA: EL/LA CONSULTOR/A se compromete en forma personal, a adoptar las medidas técnicas, administrativas u organizativas que individualmente pudieran corresponderle, para garantizar la seguridad y confidencialidad de los datos personales, y evitar de ese modo su adulteración, pérdida, consulta o tratamiento no autorizado.

CUARTA: La violación por parte del/la CONSULTOR/A del secreto profesional especificado en la cláusula SEGUNDA u omisión en la toma de las medidas previstas en la cláusula TERCERA, la hará pasible de las sanciones administrativas correspondientes, en los términos de la ley Nº 25.326, su Decreto Reglamentario Nº 1558/2001, la Disposición DNPDP 1/2004 que prevé multas de entre pesos UN MIL ($ 1000) y pesos CIEN MIL ($ 100.000).

QUINTA: Está prohibido insertar o hacer insertar a sabiendas datos falsos en un archivo de datos personales; proporcionar a un tercero a sabiendas información falsa contenida en un archivo de datos personales; acceder de cualquier forma, a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, a un banco de datos personales; o relevar a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. La ejecución de esas acciones están penadas por el Código Penal de la Nación en los términos de los artículos 117 bis y 157 bis, cuyos textos se transcriben a continuación:

ARTICULO 117 bis .—

1º. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2º. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3º. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4º. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena.

ARTICULO 157 bis. -Será reprimido con la pena de prisión de un mes a dos años el que:

1º. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2º. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años

SEXTA: La obligación de EL/LA CONSULTOR/A a que se refiere el artículo anterior seguirá vigente aún después de la finalización de la relación que lo rige con EL SINTyS, y sólo puede ser relevado/a de la misma, por las causales previstas en la cláusula SEGUNDA, haciéndose responsable EL/LA CONSULTOR/A de los daños y perjuicios que pudiera irrogar la violación de dicha obligación. El transcurso del tiempo desde que se interrumpa la relación que la vincula con EL SINTyS, no es causal de relevamiento de la obligación de guardar secreto profesional.

En prueba de conformidad se firman dos ejemplares de un solo tenor y al mismo efecto, en Buenos Aires, a los ..... días del mes de.....de ……..-

4. Anexo IV: *Perfiles de Usuarios del Proyecto SINTyS*

Grupo	Subgrupo	Accesos Permitidos
Secretaria		Acceso a servidor de archivos, carpeta secretaria, agenda y utilidades
Coordinación		Acceso a servidor de archivos, componentes A,B,C,D y E. Acceso a intranet con herramientas comunes, navegación por Internet y correo electrónico.
Componente A		Acceso a servidor de archivos, componentes A,B,C y D. Intranet a herramientas comunes, navegación por Internet y correo electrónico.
Componente B		Acceso a servidor de archivos, componentes A,B,C y D. Intranet a herramientas comunes, navegación por Internet y correo electrónico.
Componente C	Usuario Expedientes	Acceso a servidor de archivos, componente A,B,C y D, Unidad J. Expedientes, Base de datos esquemas varios sintys, pad, inventario, acceso a intranet herramientas comunes, herramientas infraestructura, VUO, navegación por Internet y correo electrónico.
	Usuario Integración	Acceso a servidor de archivos, componentes A,B,C y D, Intranet, herramientas comunes, infraestructura tablas, base de datos a esquema propio, navegación por Internet y correo electrónico.
	Usuario Administración de equipos	Acceso administración de equipos servidores de base de datos, servidores WH, servidor de correo, servidor intranet, navegación por Internet, correo electrónico, descargas de Internet.
	Usuario DBA	Acceso a servidor BD, clave DBA, navegación por Internet y correo electrónico.
	Usuario Interconexión	Acceso a servidor de archivos, componentes A,B,C y D, navegación por Internet y correo electrónico.
	Usuario Desarrollo	Acceso a Intranet herramientas comunes e infraestructura, servidor Intranet, navegación por Internet, correo electrónico, descargas e instalación de programas.
	Usuario Soporte	Navegación por Internet, correo electrónico, descargas e instalación de programas.
Componente D		Acceso a servidor de archivos, componentes A,B,C y D, Intranet a herramientas comunes.

5. Anexo V: Entrega de Tarjetas de Control de Acceso

SINTyS – Sistema de Identificación Nacional Tributario y Social –

REMITO INTERNO SINTyS Nº /05

FECHA:

Recibí la Tarjeta de Control de Acceso que abajo se detalla, responsabilizándome a notificar al SINTyS ante cualquier desperfecto técnico, pérdida y/o robo que ocurra con la misma.

Tarjeta

- Responsable:
- Componente:
- Nivel de Acceso (*****):
- Nº de Tarjeta:

Firma:

Aclaración:

Fecha:

(*) Referencias:
A= Centro de Procesamiento de Datos.
B= Expedientes.
C= Entrada Principal.
D= Coordinadores.

Recomendaciones de Instalación y Configuración de MS Windows XP

Fecha: 09/02/2005

Versión: 10

Fecha de Act.: 02/06/2006

1. Objetivo

Proponer a soporte informático una serie de recomendaciones para la instalación y configuración segura de PCs con sistema operativo MS Windows XP (sistema operativo estándar para PCs de escritorio, alineadas con las políticas de seguridad del programa SINTyS).

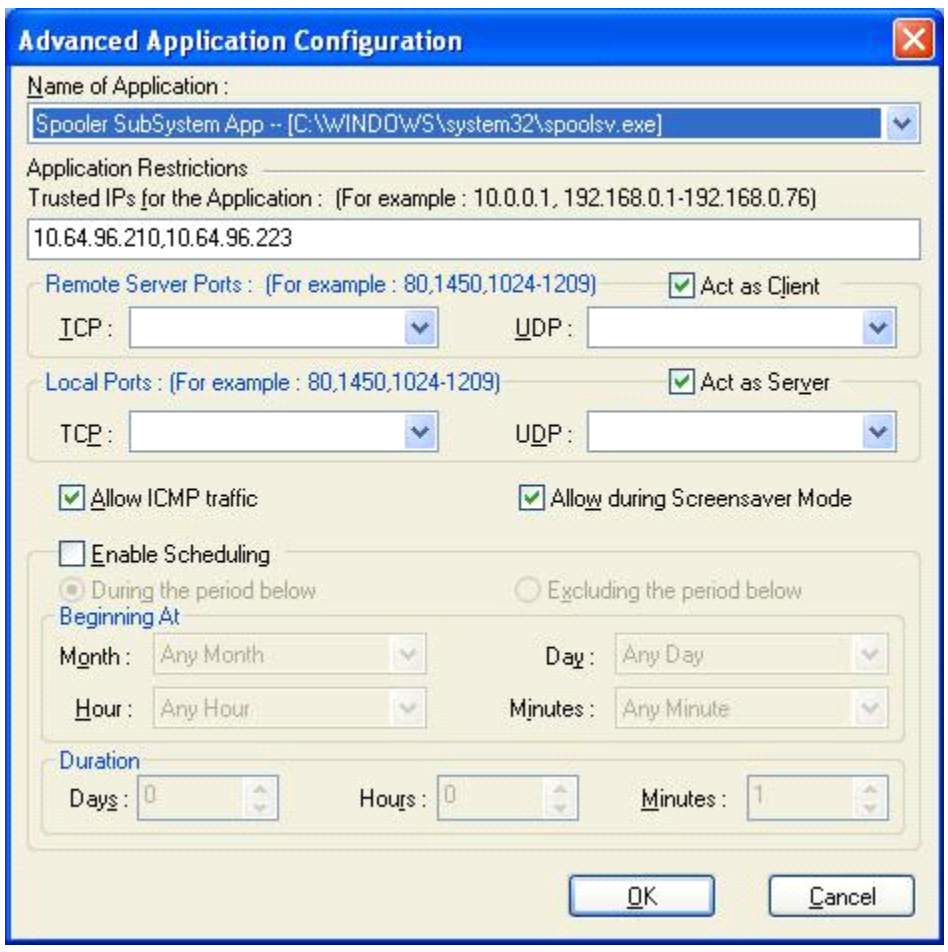
2. Recomendaciones

Instalación y Configuración Inicial

- Instalar el sistema operativo sin conexión a red.
- Particionar el disco en C: y D: una para el S.O (c:\xp) y los Archivos de programa, y otra para Aplicaciones y datos. Por ejemplo: 15 GB para el primero y el resto para el segundo. De esta manera al modificar los directorios de instalación por defecto se evitan ciertos ataques automatizados. Por otro lado si se necesita formatear por alguna razón, se formatea la unidad C: y la otra permanece intacta con todos sus datos, y así evitar que se pasen los archivos por la red para hacer backup en la máquina que tiene la grabadora o que se pongan en un servidor.
- Para evitar escrituras desde el equipo a dispositivos USB, crear la siguiente entrada en el registro (si es que no existe) y configurarle el valor 1:

Nombre de configuración: WriteProtect**, Ubicación**: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies**, Valor predeterminado**: DWORD=1 Habilitado.

- Instalar Sygate personal firewall última versión y habilitar el firewall personal de WinXP, ambos con los settings tradicionales (settings por defecto). En el caso de Sygate se debe configurar una regla para permitir que los lectores de huella funcionen al momento de autenticarse al dominio, ver pantalla ejemplo:



- Instalar plataforma anti-virus y anti-spyware seleccionadas por seguridad informática.
- Browser y Cliente de correo predeterminados: Mozilla Firefox y Mozilla Thunderbird respectivamente. Eliminar los accesos a Internet Explorer y Outlook Express desde el Menú Inicio – Programas.
- Analizar y eliminar servicios que se ejecutan innecesariamente. Ejemplo: Compartir archivos e impresoras, protocolos NetBIOS & NetBEUI (asumiendo que todas las máquinas Windows son XP), y todo otro servicio de red innecesario listado con el comando netstat –ano
- Habilitar conexión a red
- Actualizar el sistema con todas las actualizaciones críticas sugeridas por Microsoft.
- Actualizar plataforma anti-virus y anti-spyware de manera tal que al iniciar sesión en el dominio jefatura haga ambas cosas automáticamente.
- Instalar office, y aplicaciones autorizadas por el Coordinador del componente.

Administración de Usuarios

- Renombrar el usuario *administrador* en todos los equipos como *sintys-host-admin.*
- Deshabilitar el usuario *guest.*
- Reservar la cuenta *sintys-host-admin* para propósitos de administración, resguardando su contraseña en poder del personal de soporte informático, Coordinador Infraestructura y Seguridad Informática.
- Crear una cuenta con perfil de operador de backup: *sintys-host-backup.*
- Utilizar perfiles de usuarios predefinidos. Crear un usuario único del tipo **no-privilegiado** (restringido) para el usuario del equipo, asegurándose de que pida contraseña en la pantalla de logon.
- Habilitar bloqueo de pantalla con contraseña al cabo de cinco minutos de inactividad.
- Seguir una nomenclatura estándar para la definición de usuarios. La misma es: YZZZZZ, donde Y es la primera letra del nombre y las Z el apellido).
- Salvo casos excepcionales, asegurarse que por equipo no existan más de 3 usuarios definidos: *sintys-host-admin*, *sintys-host-backup y* YZZZZZ.

Administración de Perfiles de Usuarios y Grupos a nivel local

- Definir nomenclatura estándar de grupos según áreas. Por ej.: Grupo: Infraestructura-Soporte, integrantes: JEFATURA\smansilla, JEFATURA\mkuceski. El grupo se deberá agregar a la directiva de seguridad “Inicio de sesión local”. Ver página 4.
- Restringir permisos para compartir shares a usuarios no privilegiados

Administración de Perfiles de Usuarios y Grupos a nivel dominio

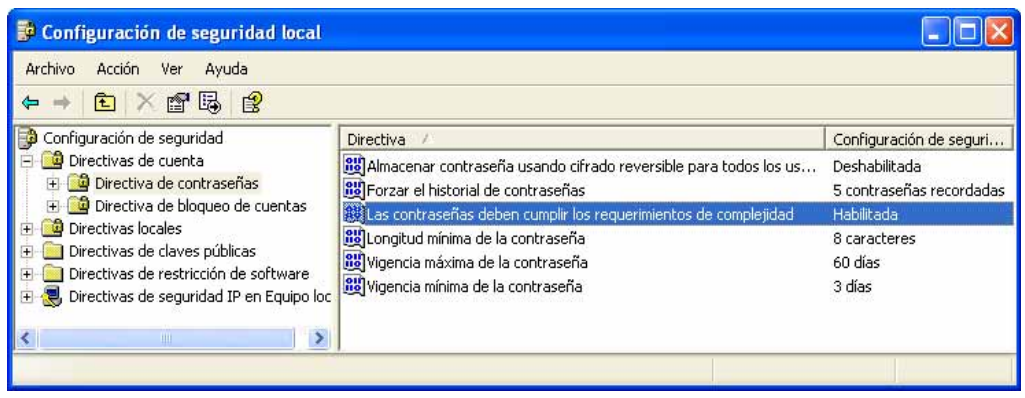
- Asignación de permisos basados en perfiles de usuarios de acuerdo al Formulario de ABM Nº 105, autorizado por su correspondiente coordinador.
- Restringir accesos a lo estrictamente necesario (*principio del mínimo privilegio*)

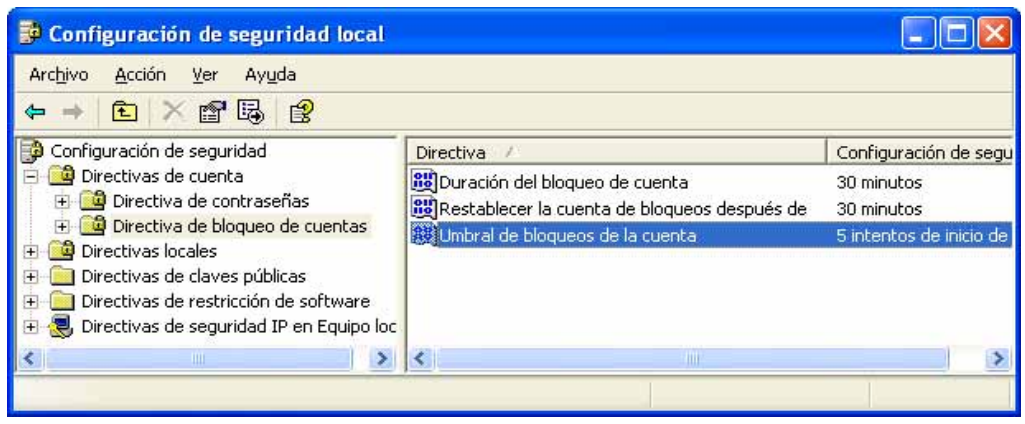
Administración de Aplicaciones

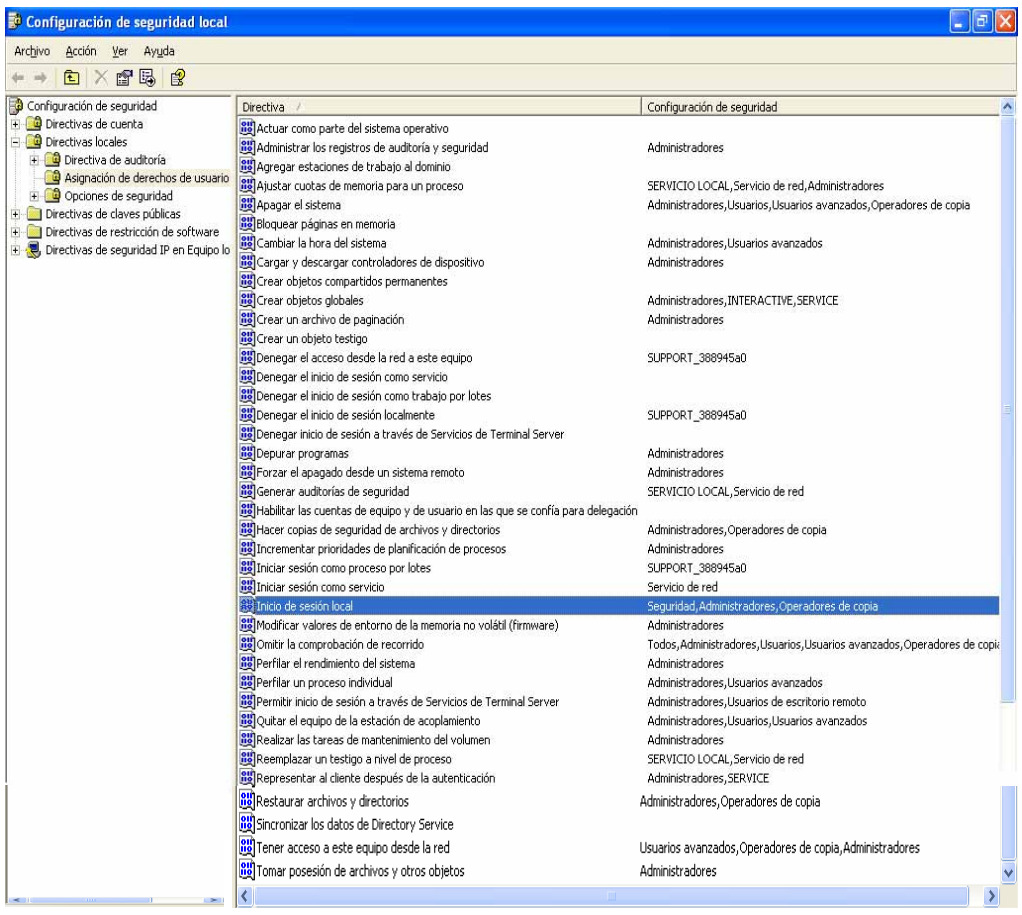
- Se contará con una lista de aplicaciones estándares del proyecto SINTyS de probada integridad criptográfica con Checksum.
- Restringir las aplicaciones a instalar que no se encuentren listadas en los estándares a aquellas que cumplan con el triple requisito: aprobación por coordinador componente infraestructura, aprobación por coordinador componente del usuario correspondiente, aprobación por Area de seguridad informática.

Configuración de Política de Seguridad Local

Desde Panel de Control – Rendimiento y Mantenimiento – Herramientas Administrativas – Directiva de Seguridad Local:







Notas importantes

▪▪ El texto completo de la directiva “Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión”, es el siguiente:

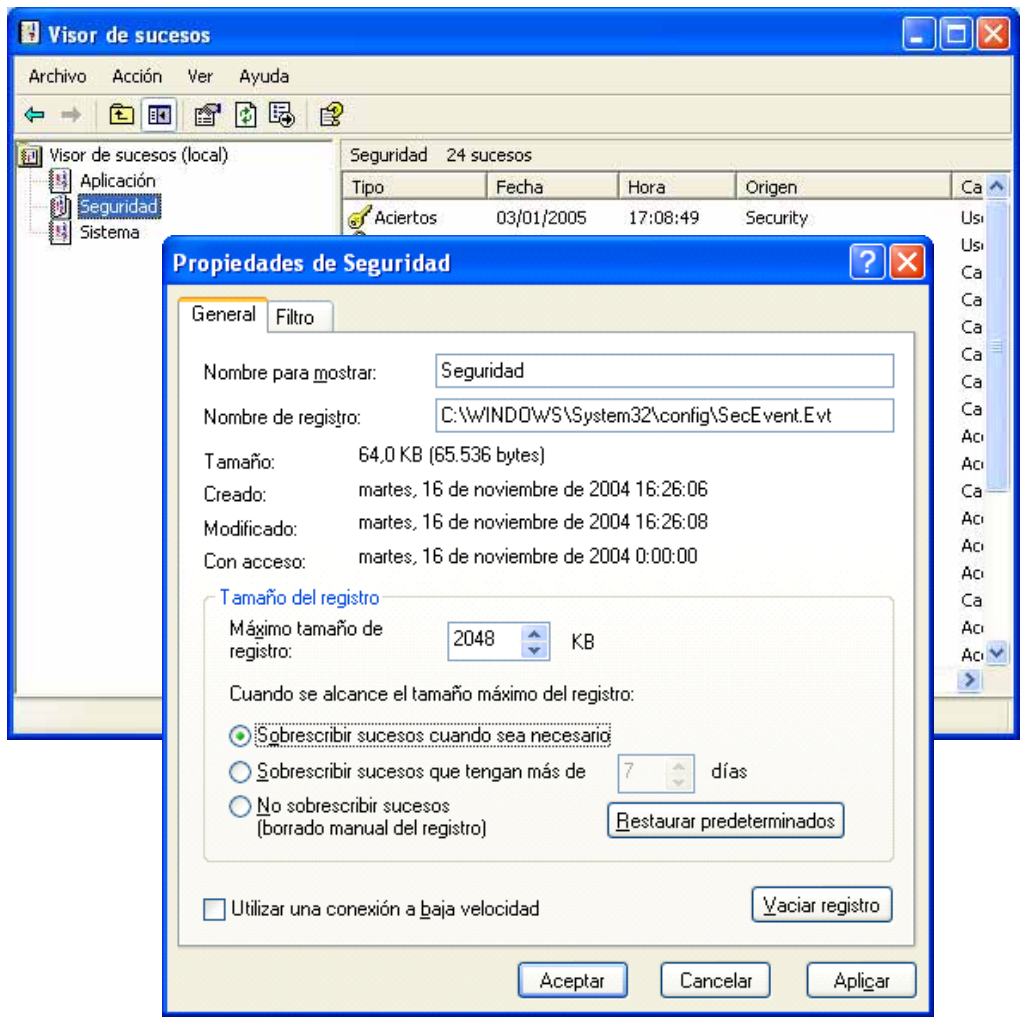
El uso de su cuenta de usuario es de uso exclusivo para las tareas habituales en relación con los objetivos del programa SINTyS. Usted es responsable de mantener la confidencialidad tanto de su cuenta de usuario como de sus contraseñas. Todas las actividades de los usuarios en los sistemas pueden ser monitoreadas y auditadas.

Accediendo a este sistema Usted acepta cumplir con las condiciones arriba expuestas.

▪▪ La directiva “Miembro de dominio: requerir clave de sesión protegida (Windows 2000 o más reciente)” presenta una incompatibilidad con dominios NT; por lo tanto, aunque es aconsejable que su valor sea “habilitado”, en nuestro caso deberá permanecer como “Deshabilitado” mientras tengamos dominio NT.

Editar Visor de Eventos y reconfigurar política de ciclado de logs

Desde Panel de Control – Rendimiento y Mantenimiento – Herramientas Administrativas – Visor de sucesos



Replicar settings de ciclado de logs para aplicaciones y sistema.

Configuración de Política de Seguridad en Dominio

- Replicar settings de política de seguridad local

Configuración Servicio Syslog

- Volcar logs relevantes de seguridad a servidor syslog centralizado

Procedimientos de Asignación de Accesos a VUO para Usuarios Internos y Externos.

Fecha: 19/09/2005

Versión: 1.1

1. Objetivo

Definir un método satisfactorio de registración de usuarios habilitados al sistema VUO (Ventanilla Unica de Organismos). Mantener un inventario de permisos de accesos vigentes al sistema, diferenciando entre usuarios SINTyS y usuarios externos (pertenecientes a organismos autorizados).

2. Introducción

Existen dos tipos de usuarios, internos y externos, ambos deberán completar según corresponda el formulario 110e (para usuarios externos) y 110i (para usuarios internos) previo a la habilitación, y se deberá renovar el acceso a usuarios existentes mediante los mismos formularios (ver anexo).

3. Funciones y responsabilidades en el procedimiento

3.1. Areas intervinientes y funciones:

3.1.1. Coordinador General

3.1.1.1. Aprobar, con su firma las solicitudes de alta y baja al VUO.

3.1.1.2. Ordenar la revocatoria de las autorizaciones ante el uso indebido del acceso.

3.1.2. Componente de Gestión – Area Legal

3.1.2.1. Analizar la competencia del funcionario que solicita la información.

3.1.2.2. Analizar la procedencia de la consulta a la información solicitada.

3.1.2.3. Establecer el nivel de acceso en los términos del documento. Establecimiento de los Niveles de Acceso a la Información por parte de las jurisdicciones y organismos de la Administración Pública Nacional Central y Descentralizada. Julio 2004.

3.1.3. Componente Infraestructura y Servicios Comunes

3.1.3.1. Area Seguridad Informática

3.1.3.1.1. Recepción de las solicitudes de altas y bajas.

3.1.3.1.2. Control de documentación.

3.1.3.1.3. Impulsar el procedimiento para acceso y baja del VUO.

3.1.3.1.4. Apertura de legajo, donde se ingresará la documentación que llegue con la solicitud.

3.1.3.1.5. Ejercer funciones de control del correcto uso del sistema VUO.

3.1.3.1.6. Interrumpir preventivamente el acceso, ante la detección de posibles irregularidades.

3.1.3.1.7. Mantener informado al Coordinador General, respecto de todas las circunstancias que puedan ser relevantes para el adecuado funcionamiento del Sistema.

3.1.3.2. Area Administración de cuentas VUO

3.1.3.2.1. Otorgar las claves de altas.

3.1.3.2.2. Establecer las bajas de usuarios.

4. Funcionarios autorizados a solicitar Acceso a VUO

4.1. Funcionarios y agentes externos al SINTyS.

4.1.1 Funcionarios de la administración pública nacional central y descentralizada, que participen de los servicios de intercambio de información del SINTyS.

4.1.1 Funcionarios provinciales, de la Ciudad Autónoma de Buenos Aires y municipales, en los términos de los respectivos acuerdos de institucionalización.

4.2. Funcionarios y consultores del SINTyS.

4.2.1. Coordinador General del SINTyS

4.2.2. Coordinadores del SINTyS

4.2.3. Consultores del SINTyS, en los términos de la autorización de su Coordinador respectivo.

5. Recaudos para el Acceso a VUO

5.1. Funcionarios y agentes externos al SINTyS.

5.1.1. La solicitud deberá ser por nota formal de solicitud de acceso del Usuario suscripta por ministro, secretario, subsecretario, director y/o máxima autoridad de organismo descentralizado (Este recaudo no es necesario para los funcionarios que revistan estos cargos).

5.1.1.1. La nota deberá adjuntar el Formulario 110e por duplicado, debidamente completado con letra imprenta y suscrito.

5.1.1.2. Asimismo, deberá adjuntar fotocopia de la 1ra y 2da hoja del DNI de Usuario.

5.2. Funcionarios y consultores del SINTyS.

5.2.1. Deberá ser solicitado por nota formal de solicitud de acceso del Usuario suscripta por el Coordinador de Componente. Deberán adjuntar el Formulario 110i por duplicado, debidamente completado con letra imprenta y suscrito.

5.2.1.1. La nota, deberá adjuntar el Formulario 110i, debidamente completado con letra imprenta y suscrito.

6. Secuencia Operativa

6.1. Tramitación de Acceso para funcionarios y agentes externos al SINTyS.

6.1.2. La nota de solicitud es recibida por despacho.

6.1.2.1. Despacho gira la nota que contiene la solicitud al Componente Infraestructura y Servicios Comunes – Area Seguridad.

6.1.3. El Componente Infraestructura y Servicios Comunes – Area Seguridad, recibe la solicitud.

6.1.3.1. Verifica que esté debidamente confeccionado el formulario y adjuntadas las copias del Documento Nacional de Identidad.

6.1.3.1.1. En caso que esté correctamente confeccionado y adjuntadas las copias, se remite al área legal.

6.1.3.1.2. En el caso que la información esté incompleta, la solicitud se haya elaborado de manera inadecuada, o se haya omitido adjuntar la documentación el Componente Infraestructura – Area Seguridad devolverá al remitente, en el término de 48 horas, la solicitud, a los efectos de que se subsanen los errores, se integren las omisiones o en su caso se adjunte la documental.

6.1.4. El Componente Gestión – Area Legal, recibe la solicitud.

6.1.4.1. Evalúa la solicitud de acceso a la información.

6.1.4.1.1. Analiza la competencia del funcionario que solicita la información.

6.1.4.1.2. Analiza la procedencia de la consulta a la información solicitada.

6.1.4.2. Establece el nivel de acceso según el informe 04/04.

6.1.4.3. Gira la solicitud al Componente Infraestructura – Area Seguridad.

6.1.5. El Componente Infraestructura – Area Seguridad, recibe la solicitud, con el nivel de acceso definido.

6.1.5.1. El Componente Infraestructura – Area Seguridad, eleva la solicitud al Coordinador General para su aprobación.

6.1.6. El Coordinador General recibe la solicitud.

6.1.6.1. El Coordinador General puede recabar información adicional de los distintos componentes y áreas intervinientes.

6.1.6.2. En caso que apruebe la solicitud se devuelve al Componente Infraestructura - área Seguridad, sirviendo la firma de instrucción para el otorgamiento del Acceso al VUO.

6.1.7. Instruido por el Coordinador General, el Componente Infraestructura – Area Seguridad Informática gira el expediente al Componente Infraestructura – Area Administrador de cuentas VUO.

6.2.8. El Componente Infraestructura – Area Administrador de cuentas VUO, asigna la cuenta de usuario, informándola al Componente Infraestructura – Area Seguridad Informática.

6.2.9. El Componente Infraestructura – Area Seguridad Informática notifica al consultor, el alta y su clave de usuario.

6.2. Tramitación de Acceso para agentes funcionarios y consultores del SINTyS.

6.2.1. La nota de solicitud es recibida formalmente por despacho.

6.2.1.1. Despacho gira la nota de solicitud al Componente Infraestructura y Servicios Comunes – Area Seguridad.

6.2.2. El Componente Infraestructura y Servicios Comunes – Area Seguridad, recibe la solicitud.

6.2.2.1. Verifica que esté debidamente confeccionado el formulario.

6.2.3.1.1. En caso que esté correctamente confeccionado, se remite el formulario al área legal.

6.2.3.1.2. En el caso que la información esté incompleta o la solicitud se haya elaborada de manera inadecuada el Componente Infraestructura – Area Seguridad devolverá al remitente, en el término de 48 horas, la solicitud, a los efectos de que se subsanen los errores o se integren las omisiones.

6.2.4. El Componente Gestión – Area Legal, recibe la solicitud.

6.2.4.1. Evalúa la solicitud de acceso a la información.

6.2.4.2. Establece el nivel de acceso según las funciones del componente.

6.2.4.3. Gira la solicitud al Componente Infraestructura – Area Seguridad.

6.2.5. El Componente Infraestructura – Area Seguridad, recibe la solicitud, con el nivel de acceso definido.

6.2.5.1. El Componente Infraestructura – Area Seguridad, eleva la solicitud al Coordinador General para su aprobación.

6.2.6. El Coordinador General recibe la solicitud.

6.2.6.1. El Coordinador General puede recabar información adicional de los distintos componentes y áreas intervinientes.

6.2.6.2. En caso que apruebe la solicitud se devuelve al Componente Infraestructura - Area Seguridad, sirviendo la firma de instrucción para el otorgamiento del Acceso al VUO.

6.2.7. Instruido por el Coordinador General, el Componente Infraestructura – Area Seguridad Informática gira el expediente al Componente Infraestructura – Area Administrador de cuentas VUO.

6.2.8. El Componente Infraestructura – Area Administrador de cuentas VUO, asigna la cuenta de usuario, informándola al Componente Infraestructura – Area Seguridad Informática.

6.2.9. El Componente Infraestructura – Area Seguridad Informática notifica al consultor, el alta y su clave de usuario.

7. Bajas de Acceso a VUO.

7.1. Causales

7.1.1. Expiración del plazo de Acceso, cualquiera sea el sujeto autorizado.

7.1.2. Para Coordinador/Consultor, desde su desvinculación con el SINTyS.

7.1.3. Para funcionarios públicos, desde que dejan de ejercer el cargo.

7.2. Recaudos

7.2.1 En el caso de consultores del SINTyS, se deberá presentar una nota solicitando la baja por el Coordinador del Componente en el que presta servicios, adjuntando el Formulario 110i,

7.2.2. En el caso de Coordinadores del SINTyS, se presenta el Formulario 110i.

7.2.3. En el caso de Funcionarios y agentes externos al SINTyS, se deberá presentar una nota suscrita por el funcionario dado de alta, en la que adjunte el Formulario 110e.

7.3. Secuencia Operativa

7.3.1. Todas las solicitudes son remitidas desde despacho, hacia el Componente Infraestructura – Area Seguridad.

7.3.2. Recibida la solicitud de baja, el Componente Infraestructura – Area Seguridad, gira la solicitud de baja al administrador de cuentas VUO quien deberá inhibir al usuario, en un lapso de 24 horas hábiles a partir de la recepción de dicho formulario.

7.3.3. El administrador de cuentas VUO deberá notificar por correo electrónico a seguridad@sintys.gov.ar la fecha y hora de realización de los cambios.

Anexo A: Formulario 110i

El formulario consigna los siguientes datos:

1.- Del Consultor:
- Nombre y apellido:
- C.U.I.T./C.U.I.L./C.D.I.:
- Componente:
- Area

3.- Del acceso
- Tipo de Solicitud (alta o baja).
- Tipo de información:
- Identificación de personas
- Social - Empleo Público – Programas sociales - Obras sociales -
- Fiscal – Impuestos - Patrimonial
- Permisos de acceso:
- C: Si tiene alta o no en una base
- D: Acceso a toda la información
- S/N: Posibilidad de ver si tiene ingresos mayores a determinado monto: S: positivo/ N: negativo
- Tipo de acceso (temporal / permanente)
- Motivo de la solicitud.

4.- De autorización
- Firma de Coordinador General.
- Firma de ministro, secretario, subsecretario, director y/o máxima autoridad de organismo descentralizado.
- Firma de Usuario.
- Firma de Responsable de Seguridad Informática.

NÂde Formulario:		
Apellido y Nombre:		
DNI:		
Componente:		
Ãrea:		

Tipo de solicitud de acceso a VUO:

Alta	Baja

Permisos

Consulta Total	Consulta Binaria	Consulta Fiscal

Consulta Total Sin Montos	Completo

Tipo de acceso

Temporal	Permanente

Temporal

Desde	Hasta

Motivo de solicitud de acceso:

FIRMAS:

Coordinador General _____ Fecha: _____

Coordinador Sustantivo _____ Fecha: _____

USUARIO _____ Fecha: _____

Seguridad InformÃtica _____ Fecha: _____

Coordinador Infraestructura _____ Fecha: _____

Infraestructura- Administracion cuentas VUO _____ Fecha: _____

Nota: Adjuntar fotocopia 1ra y 2da hoja del DNI y Nota formal de la persona a dar de alta.

Anexo B: Formulario 110e

El formulario consigna los siguientes datos:

1.- De la jurisdicción u organismo:
- Nacional/provincial/municipal
- Centralizados
- Ministerio
- Secretaría
- Subsecretaria
- Dirección
- Descentralizados
- Denominación

2.- Del funcionario:
- Nombre y apellido:
- C.U.I.T./C.U.I.L./C.D.I.:
- Cargo:
- Superior Jerárquico

3.- Del acceso
- Tipo de Solicitud (alta o baja).
- Tipo de información:
- Identificación de personas
- Social - Empleo Público – Programas sociales - Obras sociales -
- Fiscal – Impuestos - Patrimonial
- Permisos de acceso:
- C: Si tiene alta o no en una base
- D: Acceso a toda la información
- S/N: Posibilidad de ver si tiene ingresos mayores a determinado monto: S: positivo/ N: negativo
- Tipo de acceso (temporal / permanente)
- Motivo de la solicitud.

4.- De autorización
- Firma de Coordinador General.
- Firma de ministro, secretario, subsecretario, director y/o máxima autoridad de organismo descentralizado.
- Firma de Usuario.
- Firma de Responsable de Seguridad Informática.
- Firma de Coordinador de Infraestructura.

Otorgada en forma la autorización para el funcionamiento de una institución universitaria extranjera por los procedimientos indicados en el artículo anterior, la misma quedará sujeta a las exigencias, condiciones y mecanismos de control y seguimiento establecidos por la normativa aludida, gozando a partir de ese momento de los mismos derechos y facultades de las instituciones universitarias legalmente autorizadas por dicho mecanismo.

NÂºde Formulario:		
Apellido y Nombre:		
DNI:		
Nombre Organismo		
Ãrea:		

Tipo de solicitud de acceso a VUO:	Alta	Baja

Permisos	Consulta Total	Consulta Binaria	Consulta Fiscal
	Consulta Total Sin Montos		Completo

Tipo de acceso	Temporal	Permanente

Temporal	Desde	Hasta

Motivo de solicitud de acceso:

FIRMAS:

Coordinador General		Fecha:
Jefe inmediato superior		Fecha:
USUARIO		Fecha:
Seguridad InformÃ¡tica		Fecha:
Coordinador Infraestructura		Fecha:
Infraestructura- Administracion cuentas VUO		Fecha:

Nota: Adjuntar fotocopia 1ra y 2da hoja del DNI y Nota formal de la persona a dar de alta.

Procedimiento de Instalación y Configuración Checkpoint Secure-Client (Tokens).

Fecha: 07/06/2005

Versión: 0.2

1. Objetivo

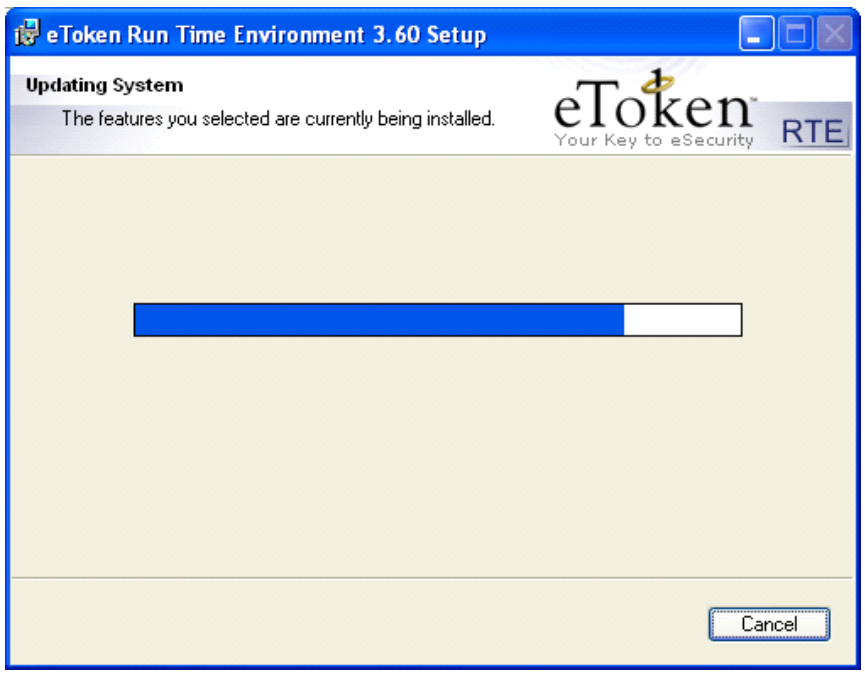
Proveer a las personas autorizadas a poseer Tokens, la documentación necesaria para la instalación, configuración y utilización de los mismos. Esta última dependerá de las políticas asignadas a cada persona en el Policy Server administrado por Seguridad Informática.

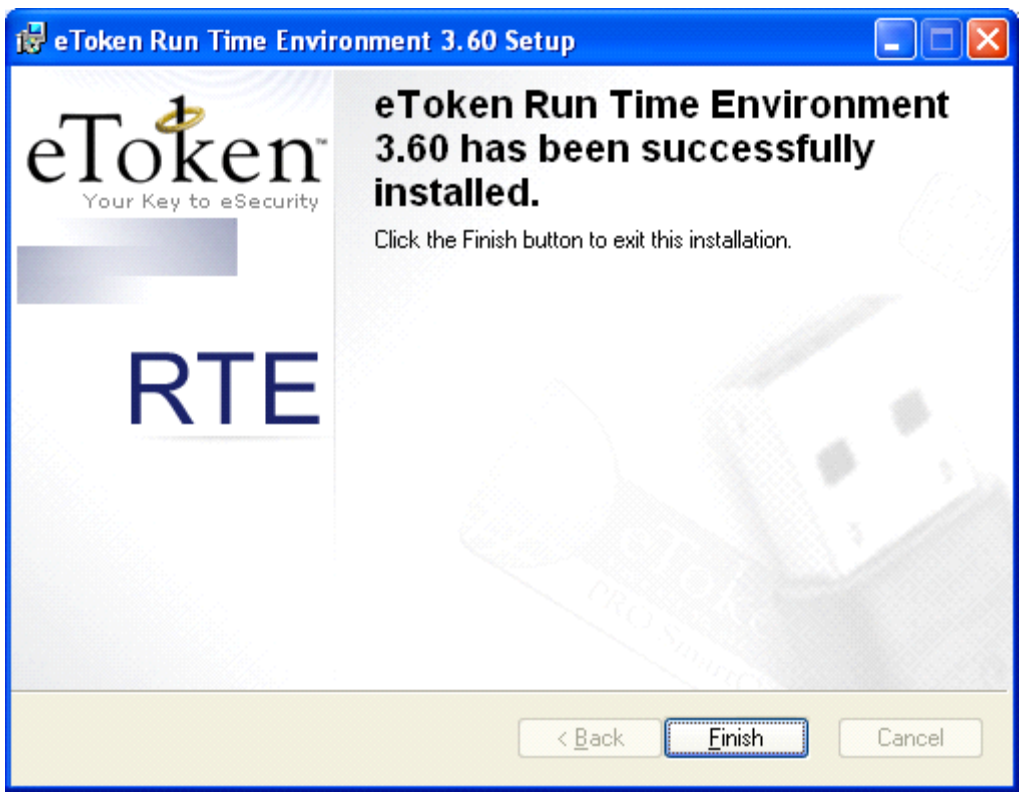
2. Introducción

Un Token es un dispositivo USB que se conecta a la PC que accede a los recursos de SINTyS remotamente, es decir, a distancia. Para su correcto funcionamiento, es necesario instalar un driver y un programa denominado Secure-Client. Una vez hecho esto, los pasos a seguir se describen detalladamente en este documento.

3. Instalación Driver eToken Run Time Environment (RTE)

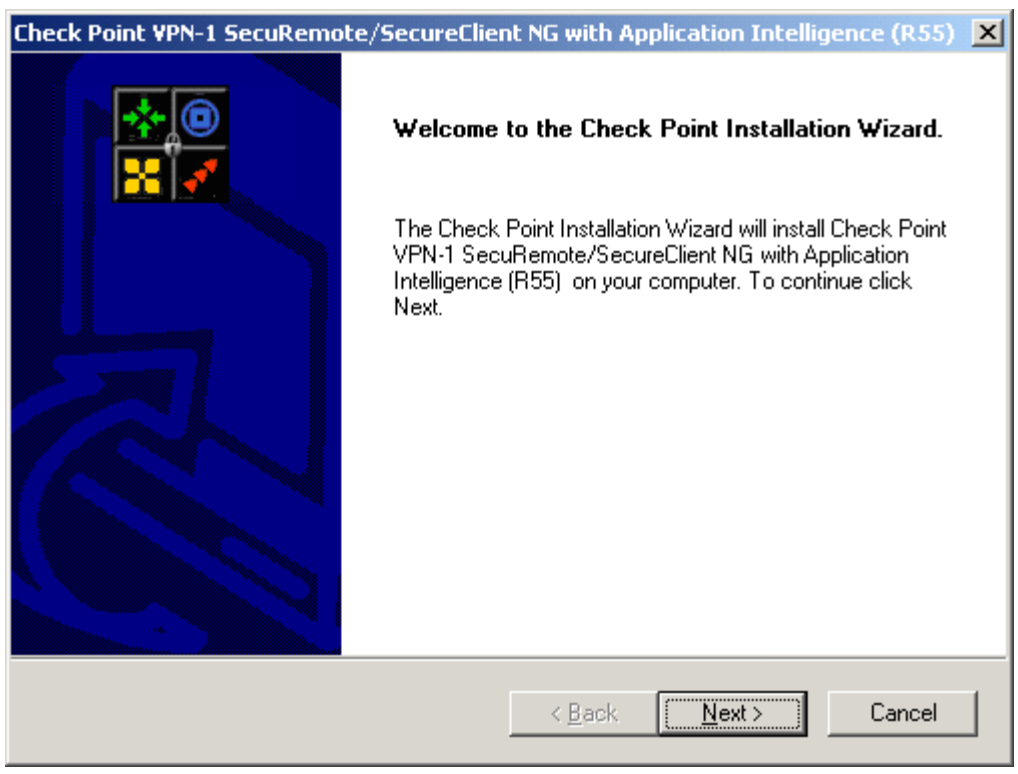
Desde el CD correr \TokensInstallers\RTE_3_60.msi, aparece el asistente como se muestra a continuación:

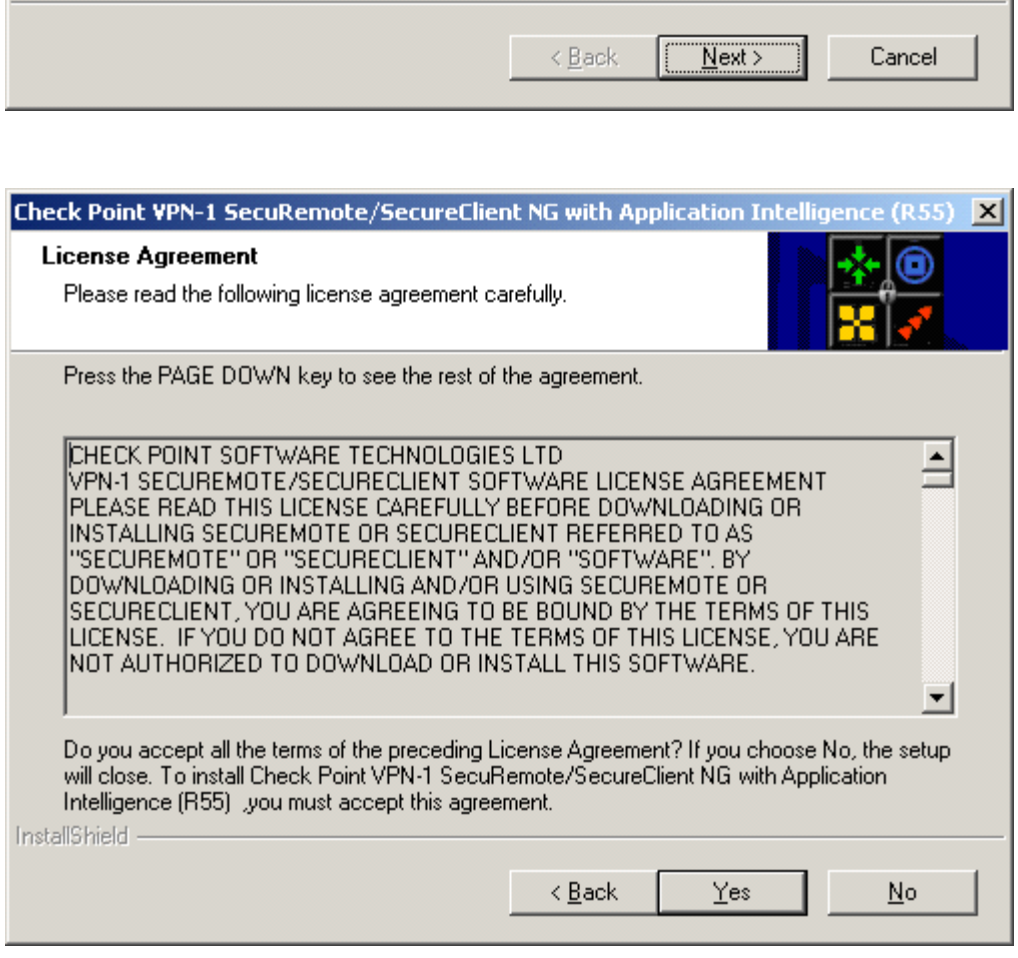


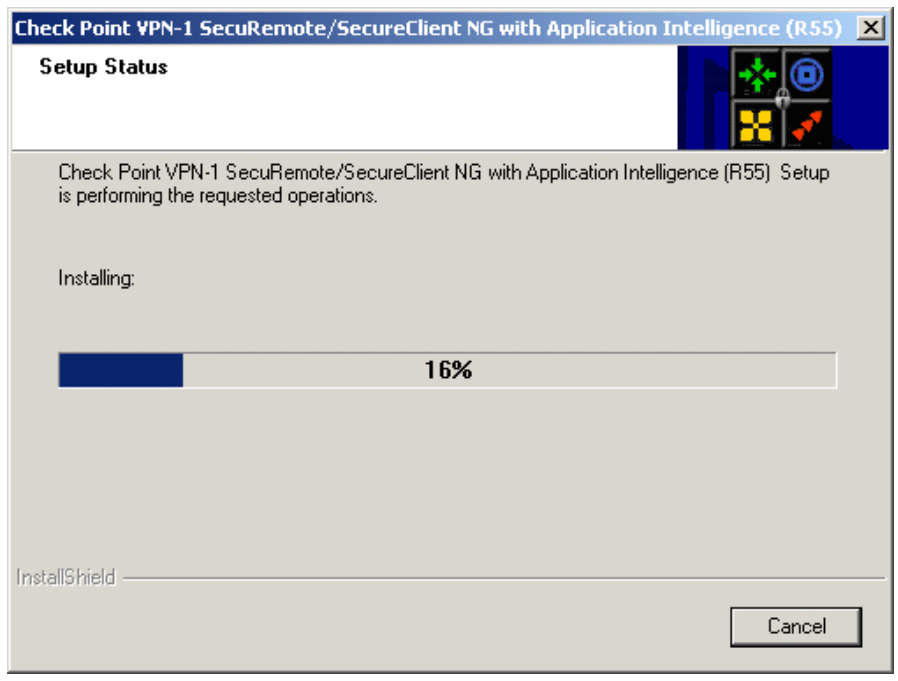


4. Instalación Secure Client

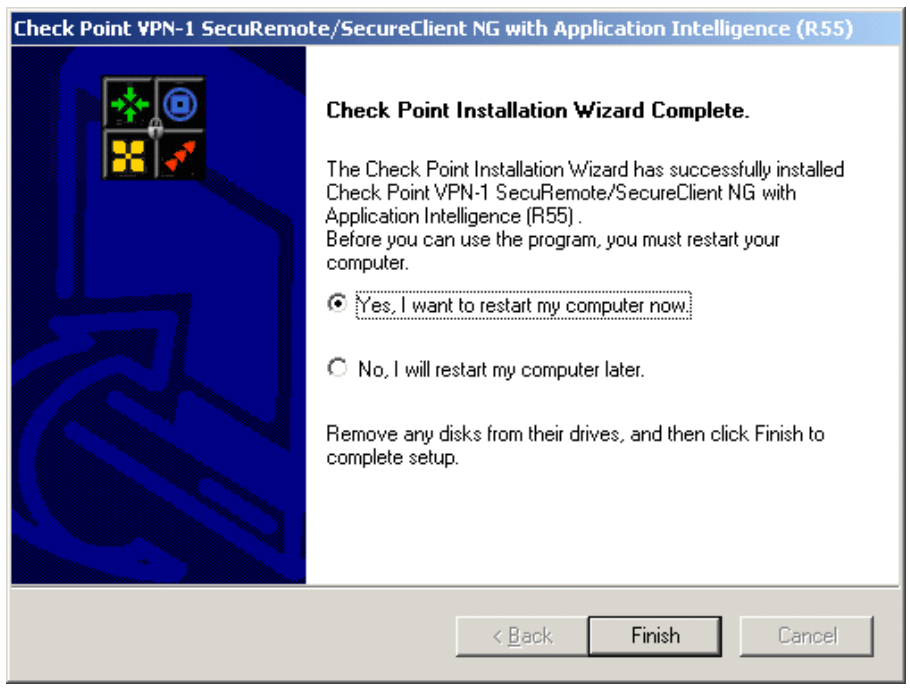
Al finalizar la instalación del RTE, el próximo paso es instalar SecureClient. A continuación se muestran las pantallas que se irán sucediendo.



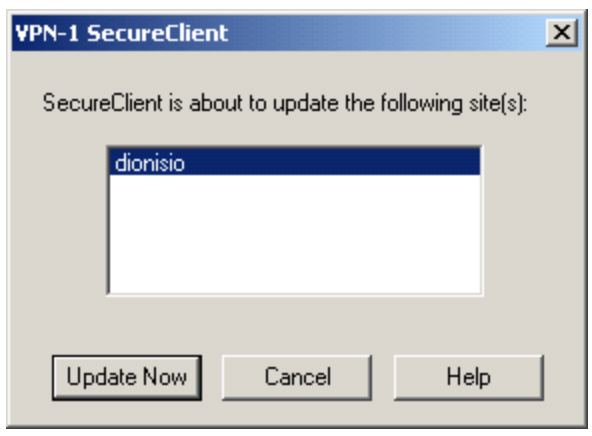




Es necesario reiniciar el equipo para que funcione correctamente

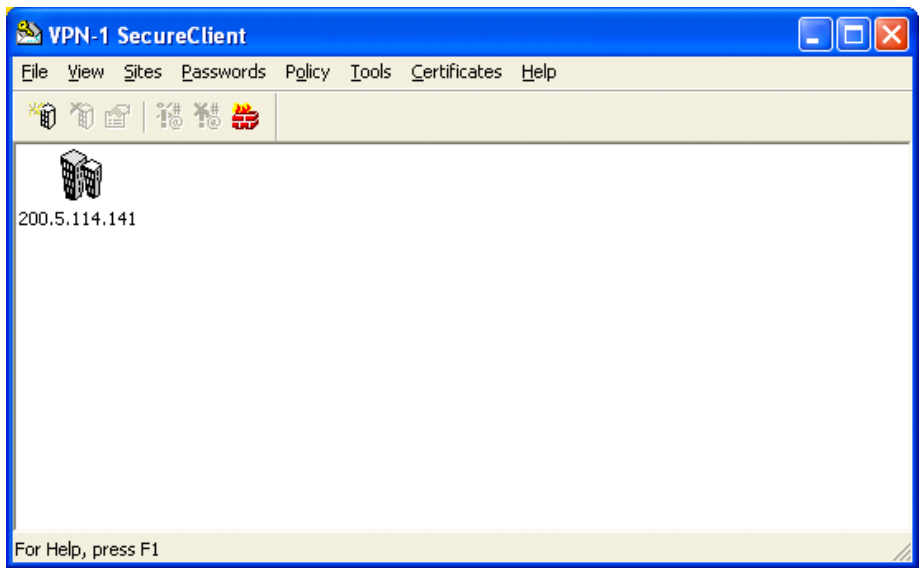


Al reiniciar aparece la siguiente pantalla, seleccionamos Dionisio y elegimos Update Now.

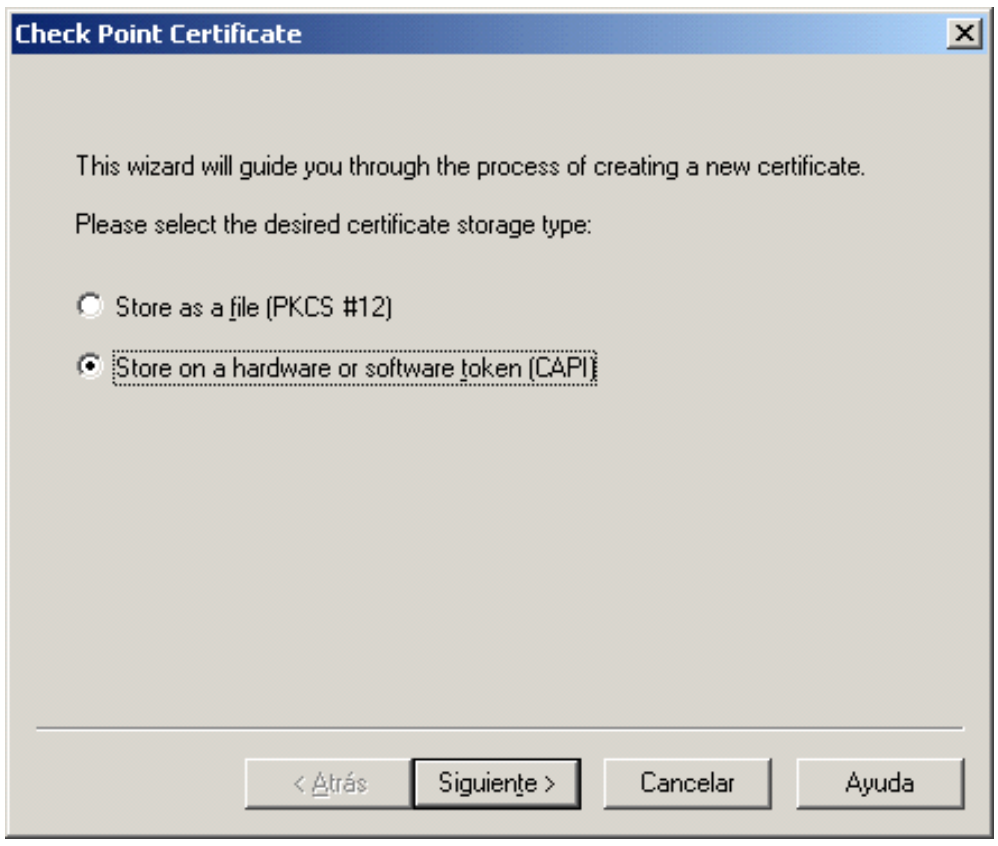


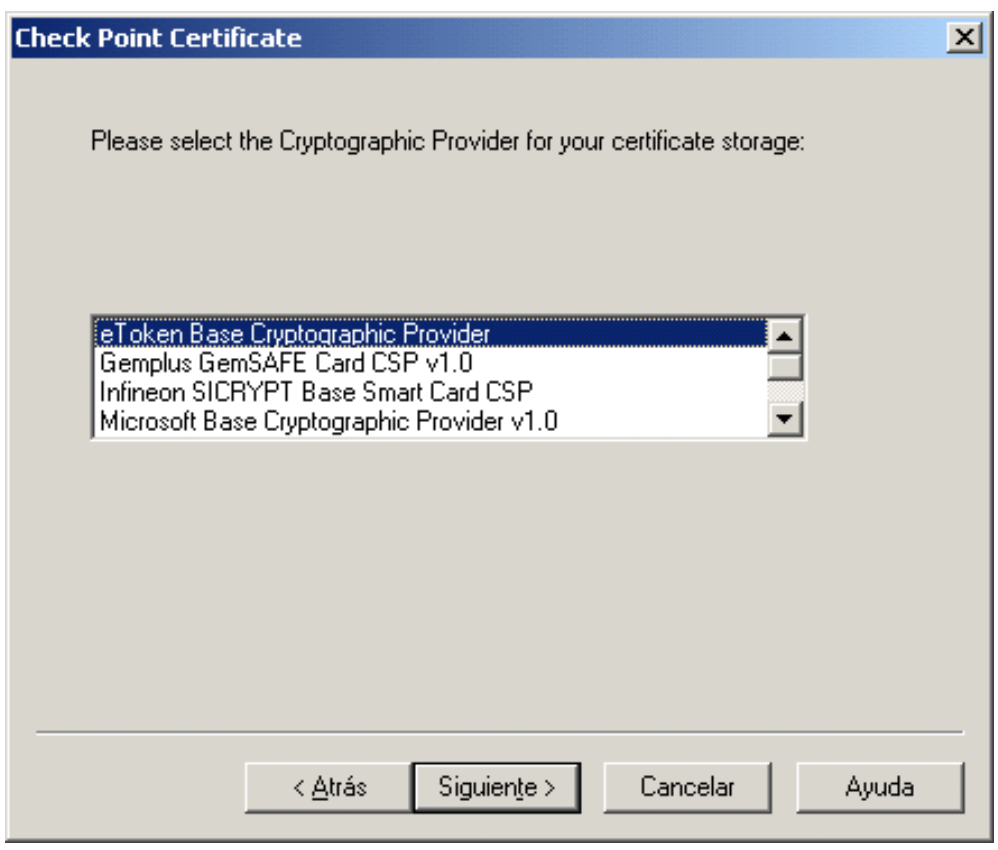
5. Creación del Certificado mediante Secure Client

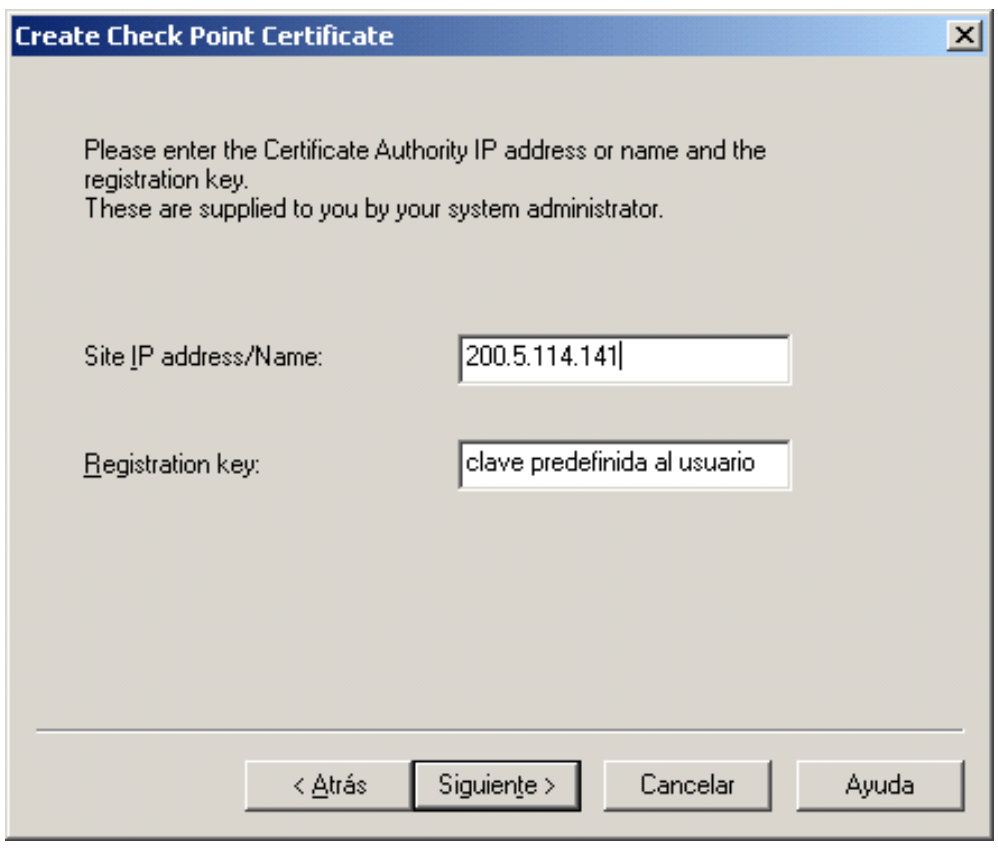
Podemos ver que se nos creó un icono en la barra de tareas en forma de sobre con una llave. Sobre éste, hacemos botón derecho y elegimos Configurar. Una vez dentro vemos que ya tenemos el Sitio creado, entonces dentro del menú Certificates elegimos Check Point Certificates – Create.



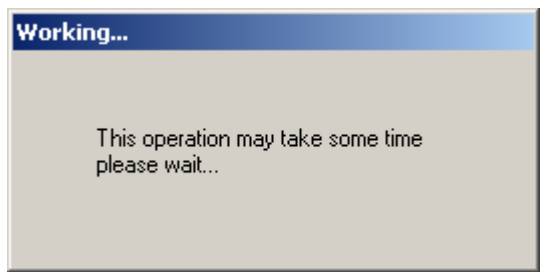
Nos aparece un asistente que nos guía durante la creación de nuestro certificado. Vamos siguiendo las pantallas tildando todo tal y como se muestra a continuación.

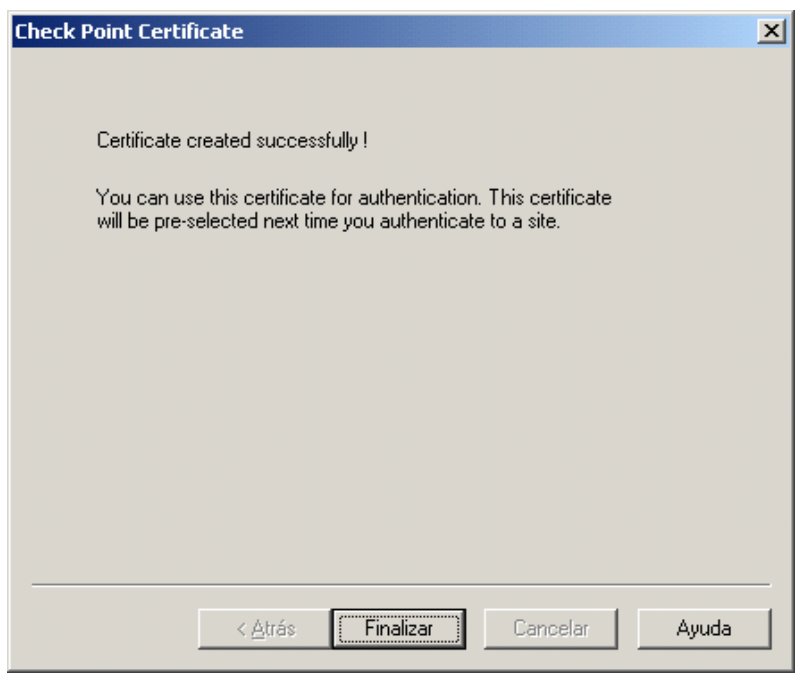






En el campo Registration key, ingresar la clave que les entregó en un sobre cerrado y click en siguiente.





6. Conectándonos al Sitio a través de Secure Client

Por último, conectamos el Token al puerto USB de la PC que accederá al sitio. Sobre el icono del SecureClient (en la barra de tareas) hacemos botón derecho y elegimos Connect aceptando el default Profile.

Luego, Secure Client nos dice que debemos autenticarnos. Para esto, tildamos Use Certificate, desplegamos el combo, elegimos nuestro certificado como se ve en la siguiente figura y hacemos clic en OK:

Validamos el Token con la password correspondiente.

Click en OK y luego de un corto proceso, si todo está bien, ya estaríamos conectados al sitio.

Recién ahora estamos en condiciones de empezar a usar los recursos del sitio que nos corresponde según nuestro perfil. Ej.: Intranet, VUO, etc.

Procedimiento Instalación y Configuración de GnuPT (incluye WinPT y GPGrelay).

Fecha: 02/06/2005

Versión: 0.4

1. Objetivo

Proveer la documentación necesaria para la instalación, configuración y utilización de una herramienta robusta y Freeware de criptografía como lo es GnuPT; garantizando así que el cruce de datos con los distintos organismos sea haga en forma segura preservando la Confidencialidad de los mismos.

2. Introducción – Criptografía y Firma digital

Criptografía (o Cifrado): es una técnica que permite transformar cierta información en una serie de datos ininteligibles o "datos cifrados".

Cuando se desea transmitir un mensaje, antes de su envío, se le aplica un algoritmo criptográfico, generándose como resultado un mensaje cifrado, que sólo podrá ser descifrado por aquellos que conozcan el algoritmo y la clave correcta.

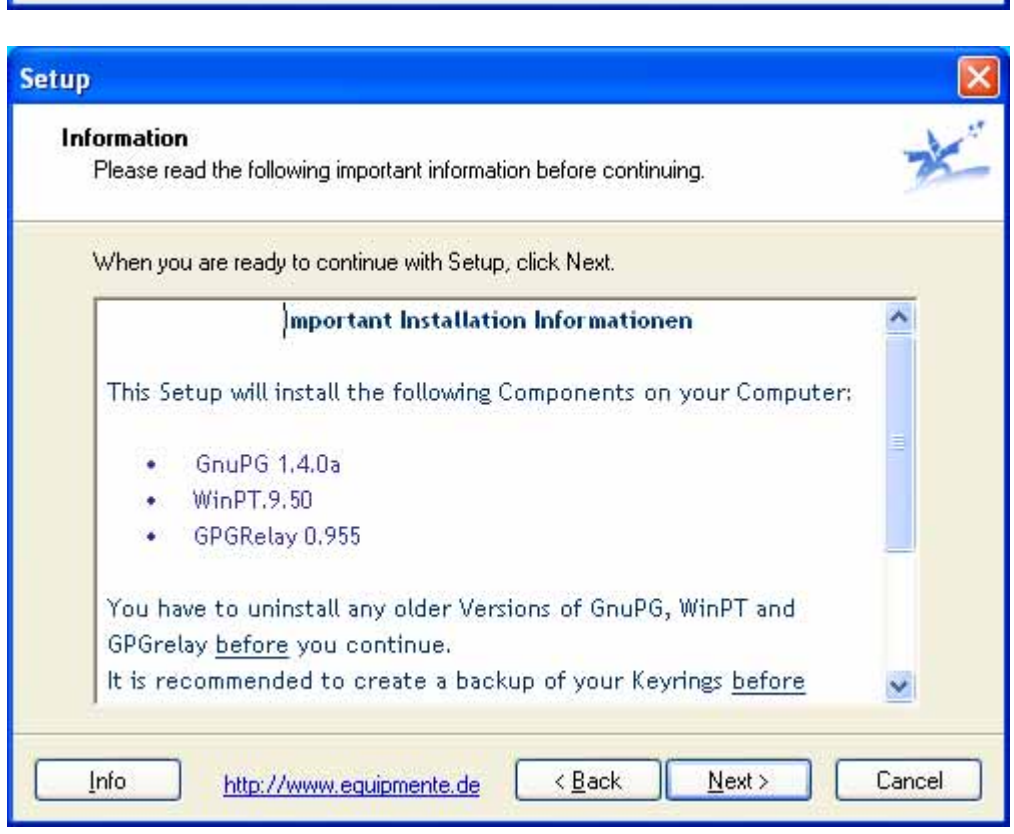
Firma digital: permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la autenticación e integridad de los datos así como para el no repudio en origen, ya que el receptor de un mensaje firmado digitalmente no puede argumentar que no lo es.

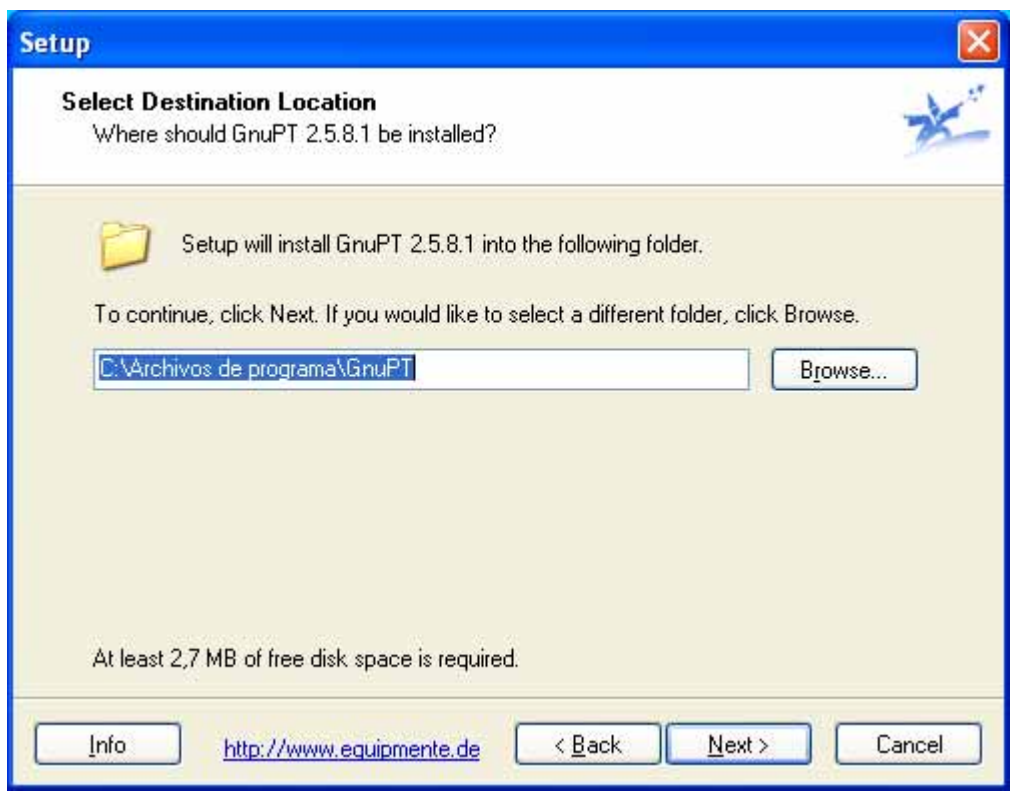
3. Instalación

La instalación de GnuPT consiste en un asistente que nos va guiando durante todo el proceso. Básicamente lo que hace es preguntarnos el directorio de instalación del programa y el directorio donde van a residir las claves. El último paso es la creación de nuestro par de claves y para ello nos pide una frase secreta.

Importante: Para poder intercambiar archivos y correos cifrados y verificar las Firmas digitales, es necesario que el destinatario se encuentre en nuestro "Anillo de Claves" y nosotros también lo estemos en el suyo. Esto se logra obteniendo su clave pública ya sea porque nos la pasó en un archivo o porque la bajamos de un servidor de claves (keyserver).

A continuación veremos las pantallas que se irán sucediendo durante la instalación de GnuPT:



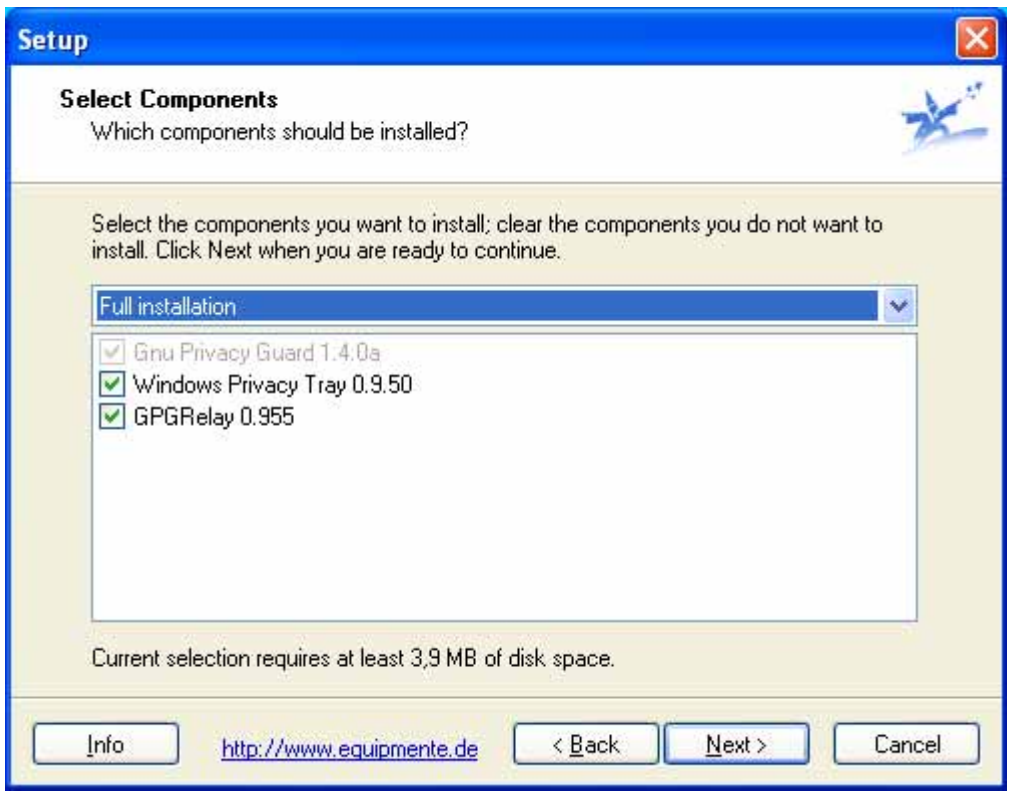


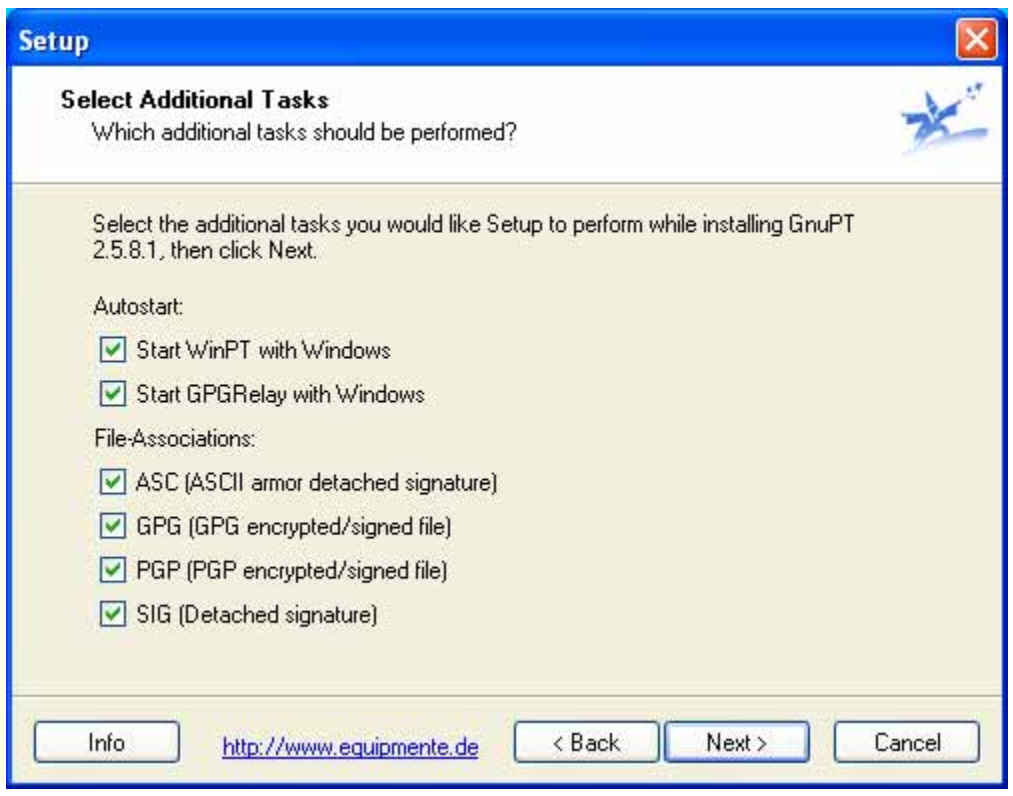
Se necesita crear una carpeta donde se almacenarán todas las claves públicas que, por razones de unificación de nomenclatura, las guardaremos de la siguiente manera: ***usuario@servidor.pub***. Ej.: **mlivachof*@sintys.pub***.

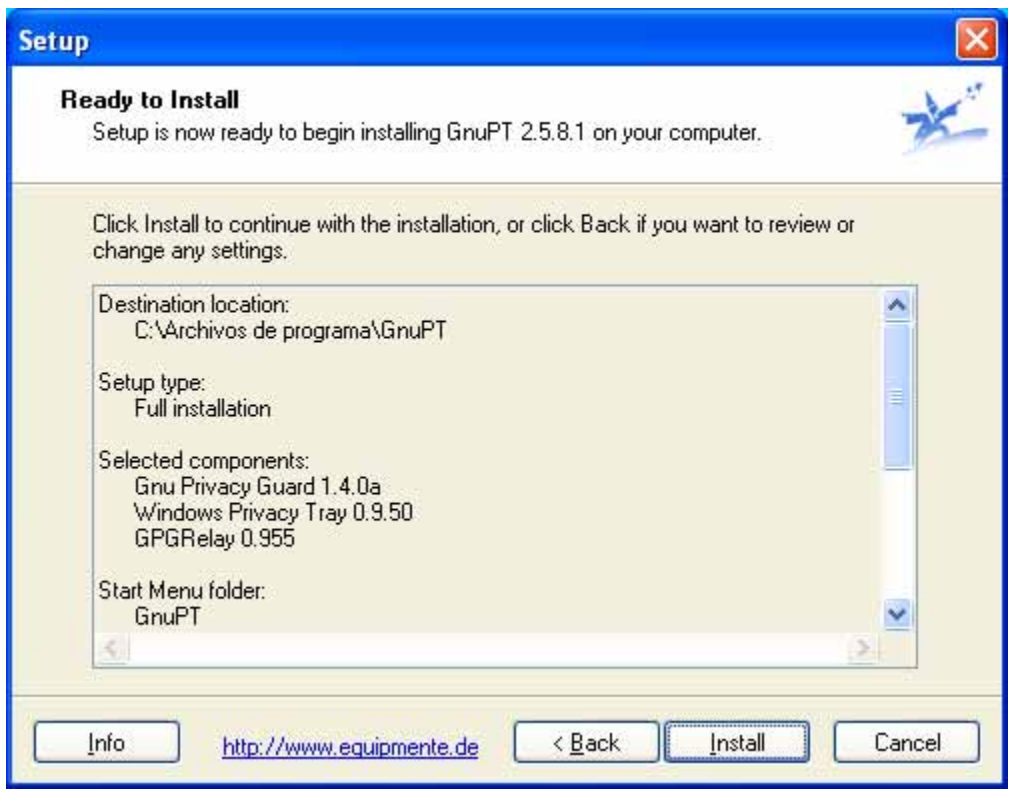
A esta carpeta la llamaremos GnuPG y la crearemos dentro de *C:\Documents and Settings\Usuario\Application Data\GnuPG*. Donde *Usuario* es el que inicia sesión en el equipo.

Una vez creada la carpeta hay que agregarla en el siguiente paso.

Se requiere la instalación completa del producto (Full Installation)







4. Configuración

Para corroborar que todo salió bien, debemos ver en Windows Privacy Tray (botón derecho en la barra de herramientas) / Preferences / GPG, todos los directorios que le fuimos indicando durante la instalación.

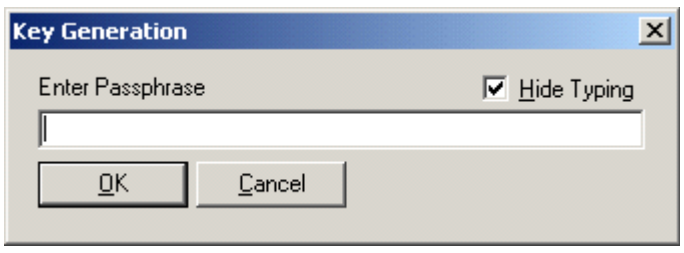
Cómo crear nuestro par de claves.

Como primer paso es necesario que creemos nuestro par de claves: clave pública y clave privada.

En Windows Privacy Tray (botón derecho en la barra de herramientas) / Key Manager, ir al menú Key / new / normal y se nos abre el siguiente wizard:

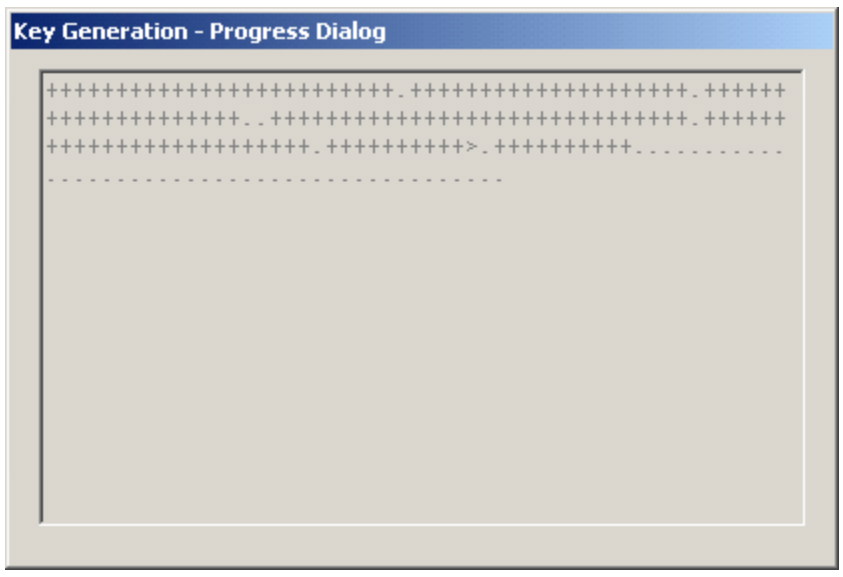
Escribir el nombre real del usuario, su e-mail y tildar Prefer RSA keys.

Luego nos va a pedir una frase. Es aconsejable que esta frase posea cierta complejidad pero por supuesto que podamos recordarla fácilmente. Ej.: mayúsculas, minúsculas, más de 5 caracteres, etc.



Aclaración!: La frase que ingresamos nos permite **crear** y **usar** nuestro par de claves (privada y pública). Nuestra clave privada ni nosotros mismos la sabemos, ya que la administra el programa exclusivamente, y la pública si queremos la podemos exportar a un archivo o verla desde un servidor de claves.

Luego, como vemos a continuación, comienza la generación de nuestro par de claves.

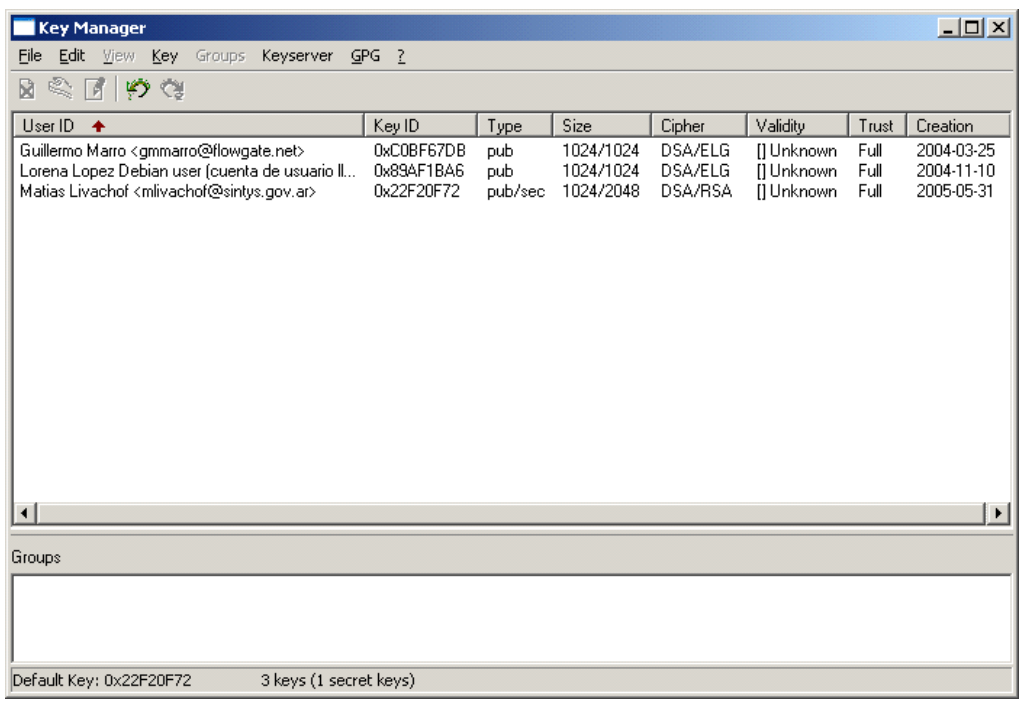


Y finalmente hacemos click en Si.

Publicar nuestra clave pública en un servidor de claves.

Botón derecho sobre nuestra clave, luego “Send to Keyserver”, y elegir de la lista que nos aparece a random.sks.keyserver.penguin.de.

A continuación vemos un ejemplo de un Key manager, también llamado Anillo de claves o KeyRing.

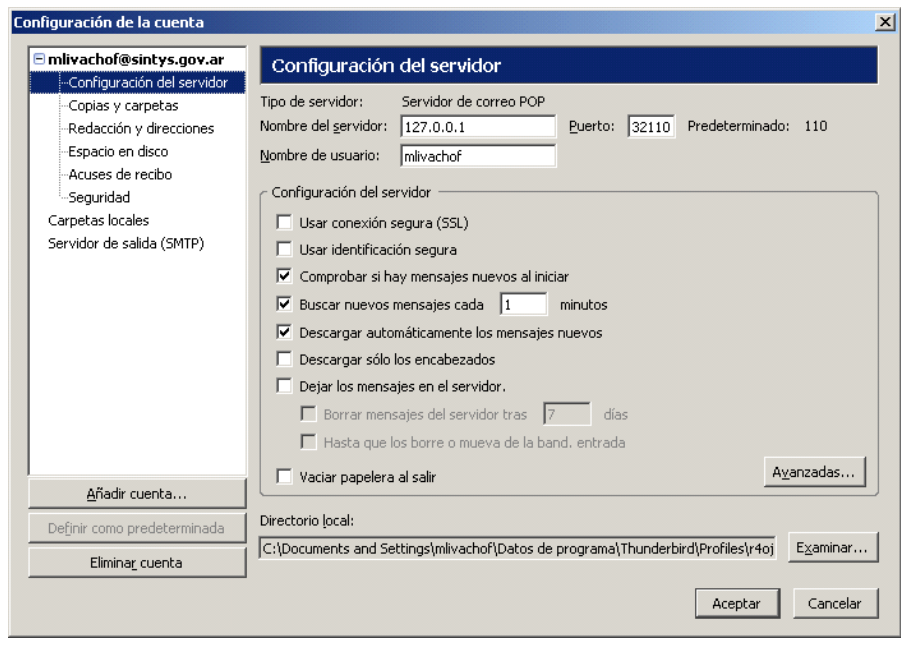


Y por último, una vez que hemos incorporado una clave pública a nuestro anillo, ya sea desde un archivo o desde un servidor de claves, tenemos que indicar nuestra confianza sobre la misma. Con el botón derecho sobre la clave importada hacer click en Ownertrust y seleccionar “I trust fully” o la que creamos apropiada para esa persona.

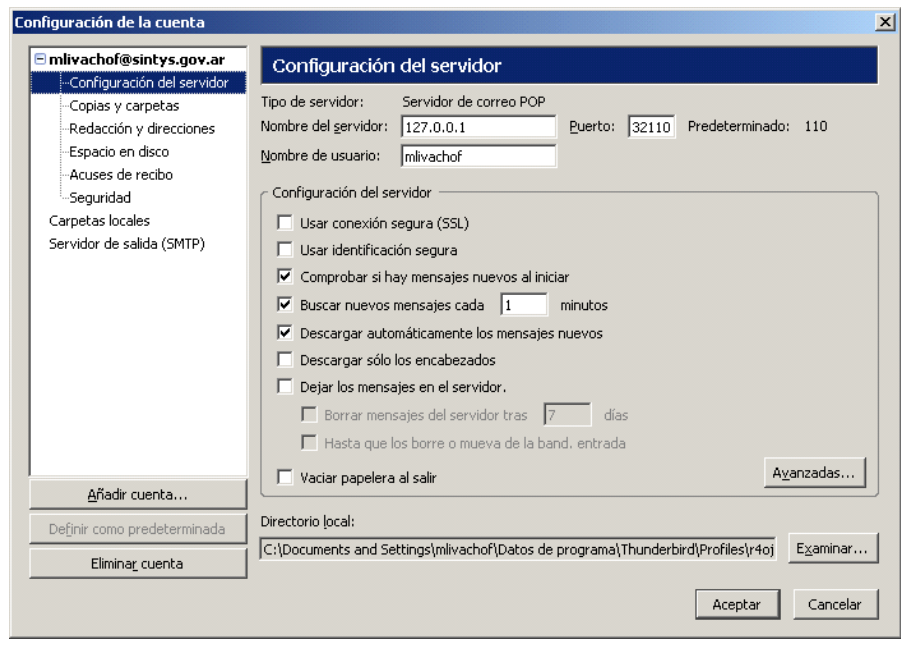
5. Configuración de Thunderbird, GPGrelay y WinPT:

GPGrelay, será el encargado de estar escuchando qué sucede entre el cliente de correo y el servidor. Todos los e-mails atravesarán GPGrelay desde donde se detectará si se envía o se recibe de un usuario incluido en nuestro anillo de claves. De ser así procederá a encriptar, firmar, desencriptar (según sea el proceso a realizar). Cabe aclarar que si queremos enviar un mail encriptado a algún destinatario que no se encuentre en nuestro anillo de claves, obtendremos un error.

Desde el Thunderbird, en herramientas / configuración de cuentas / configuración del servidor:

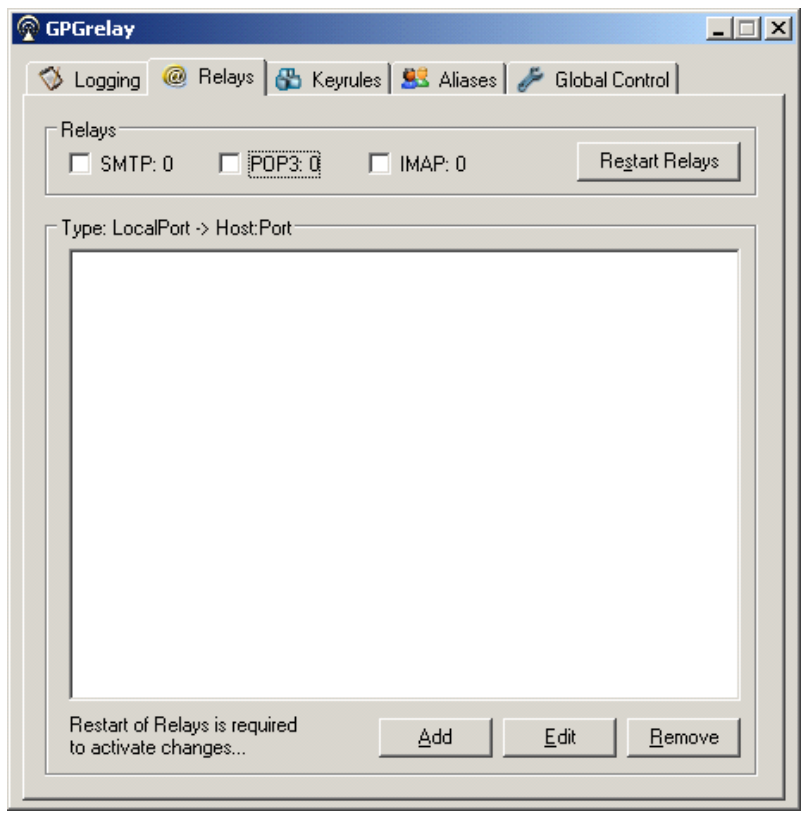


Debemos modificar la dirección del servidor por 127.0.0.1 y puerto 32110.
Luego en la misma ventana, pero en Servidor de salida (SMTP) configuramos lo siguiente:

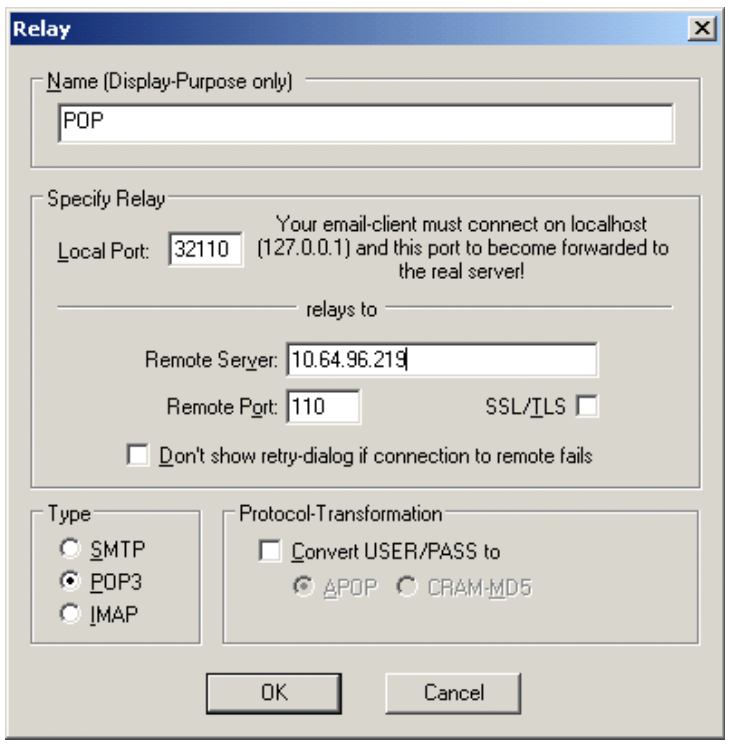


Cambiamos el nombre del servidor por 127.0.0.1 y puerto 32110.

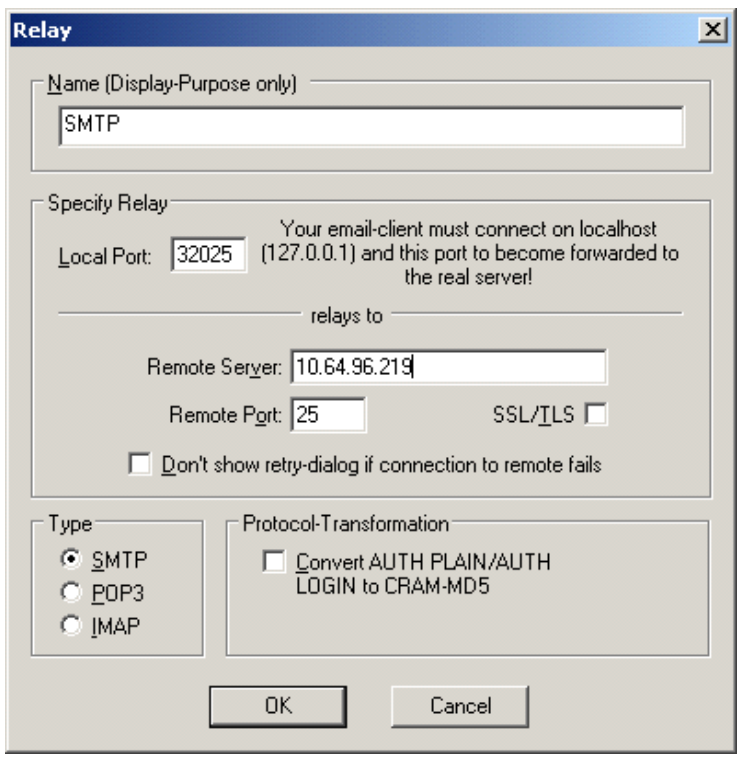
Ahora pasamos a configurar el GPGrelay. Hacemos doble clic en GPGrelay en la barra de herramientas y se despliega la siguiente ventana:



En la solapa Relays elegimos Add. Ingresamos un nombre, por ejemplo POP, en Remote Server colocamos la IP o el nombre del servidor de correo, puerto 110 (por defecto) y en Type seleccionamos en nuestro caso POP3.

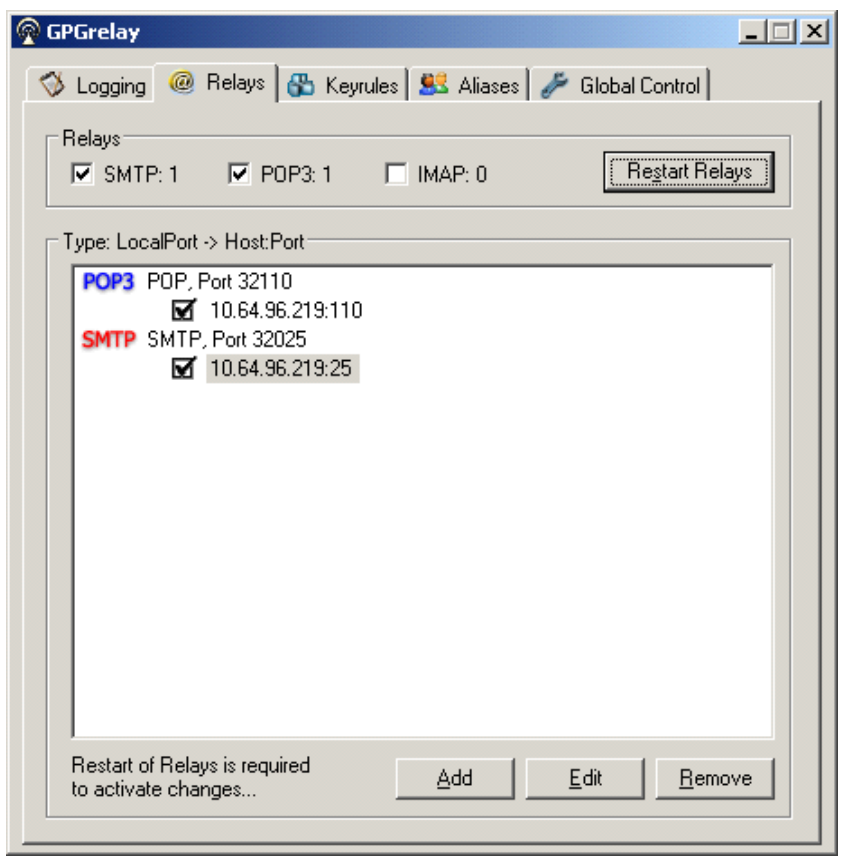


Aceptamos con OK, volvemos a la pantalla anterior y otra vez clickemos en Add, ahora para la configuración saliente de los correos.

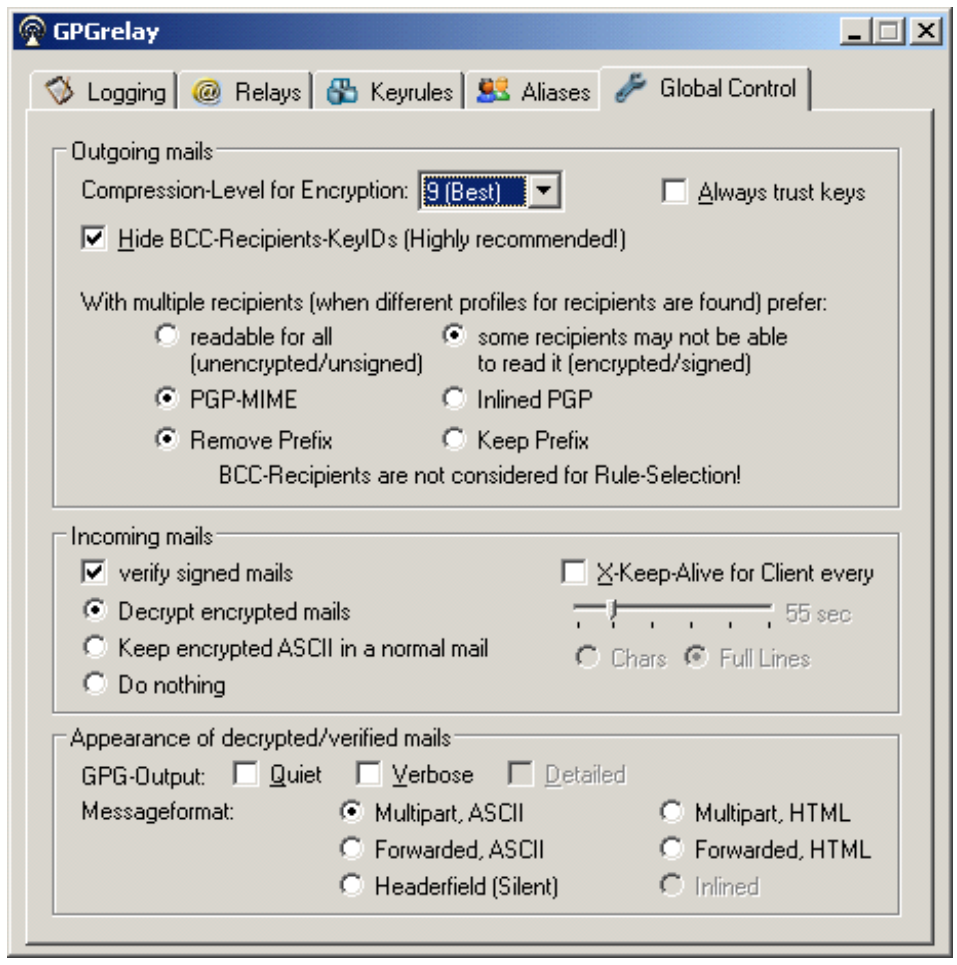


Y le indicamos un nombre, ejemplo SMTP, en Remote Server ingresamos la IP o el nombre del servidor de correo, puerto 25 (por defecto) y en Type seleccionamos SMTP.

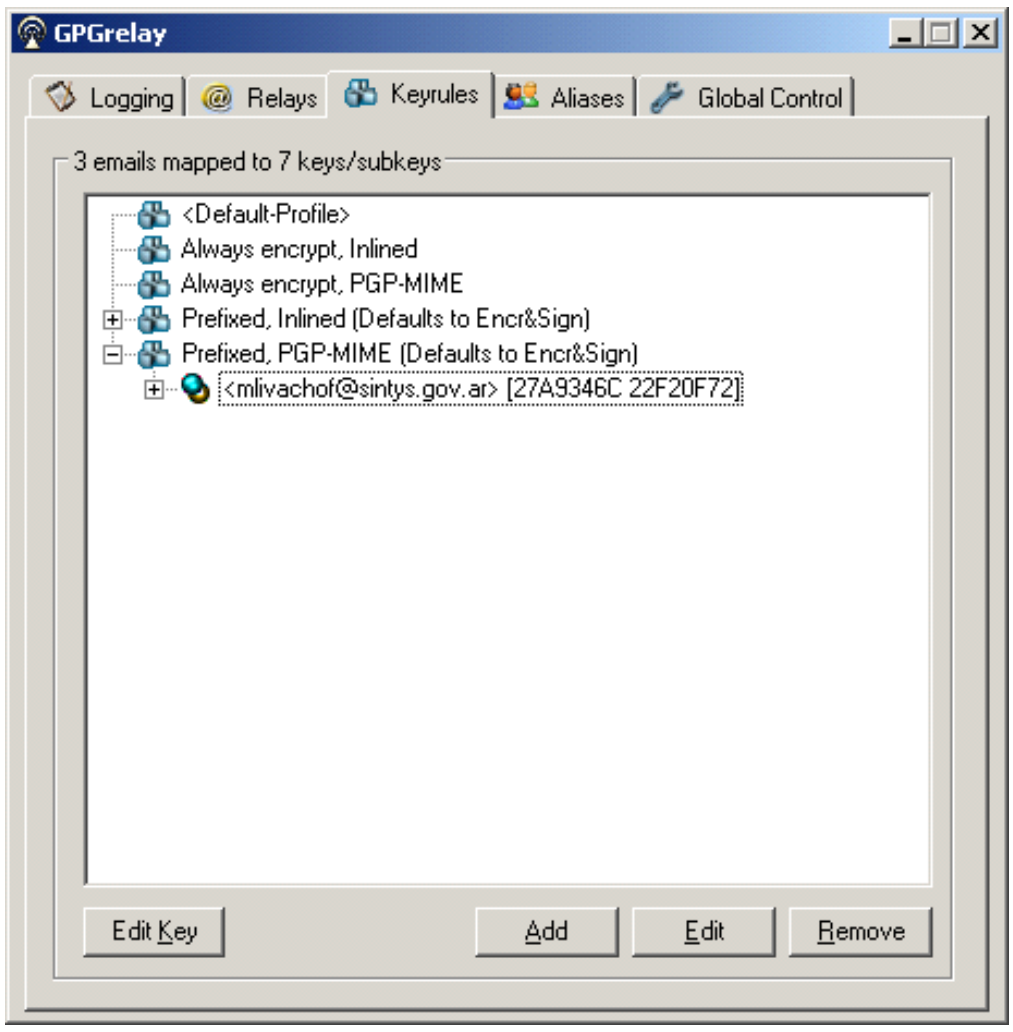
Al aceptar, si hicimos todo bien, nos debe quedar una vista como la siguiente.



Verificamos que coincida la configuración en la solapa Global Control.



En la solapa Keyrules lo que podemos configurar es cómo se van a tratar los mails que se envíen a usuarios de nuestro anillo de claves.



Automáticamente se incorporará nuestro usuario al perfil por defecto, y por cada usuario que agreguemos a nuestro anillo de claves.

Luego lo podremos arrastrar al perfil deseado para que cumpla con las reglas predefinidas.

Los diferentes perfiles funcionan de la siguiente manera: Cuando creamos un email nuevo con thunderbird, si el destinatario de correo es un participante de nuestro anillo, ese email se enviará siguiendo las reglas del perfil asociado.

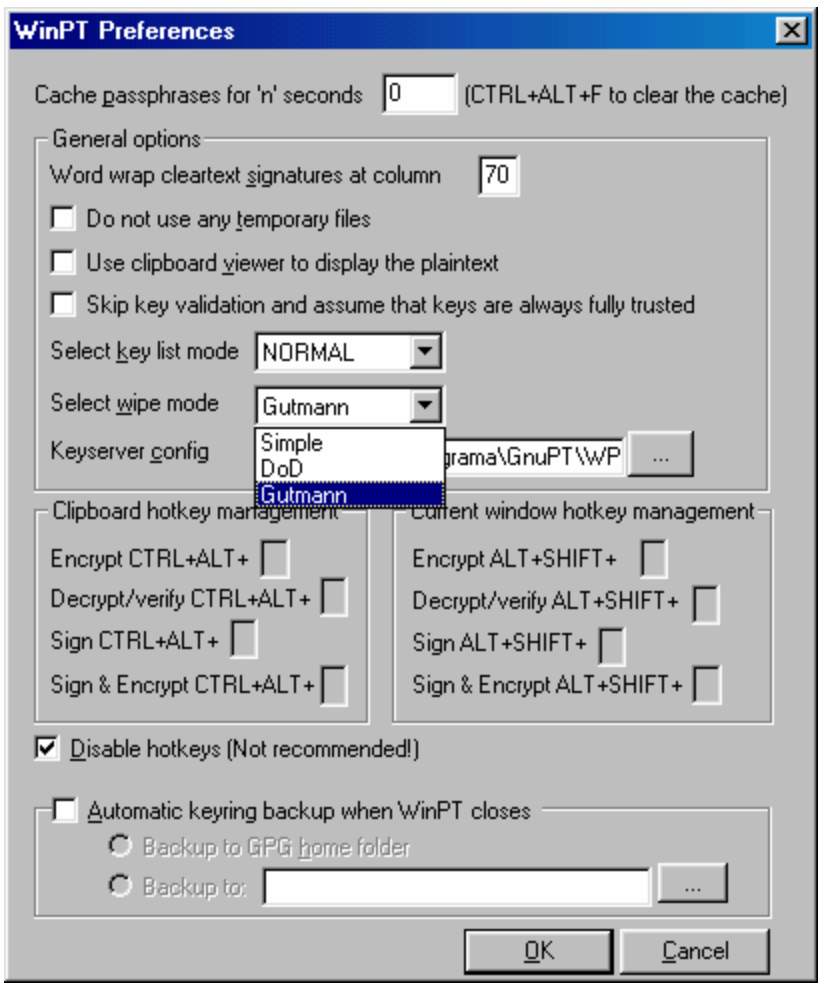
Always encrypt, Inlined: Encriptará el email enviado al usuario, con el texto encriptado en el cuerpo del email.

Always encrypt, PGP-MIME: Encriptará el email enviado al usuario, con el texto encriptado en un archivo adjunto.

Prefixed, Inlined (Defaults to Encr&Sign): Encriptará y firmará digitalmente el email enviado al usuario, con el texto encriptado en el cuerpo del email.

Prefixed, PGP-MIME(Defults to Encr&Sign): Encriptará y firmará digitalmente el email enviado al usuario, con el texto encriptado en un archivo adjunto.

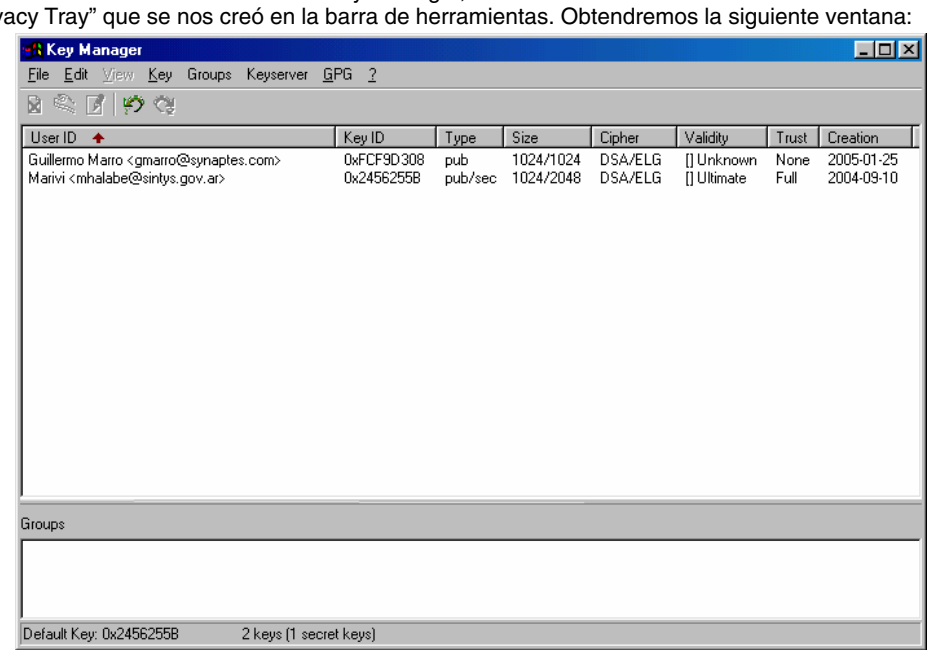
Configuración de WinPT
Desde la barra de herramientas, Windows Privacy Tray / Preferentes / WinPT verificamos que coincida la siguiente configuración.
Para el borrado seguro, en “Select wipe mode”, elegir Gutmann.



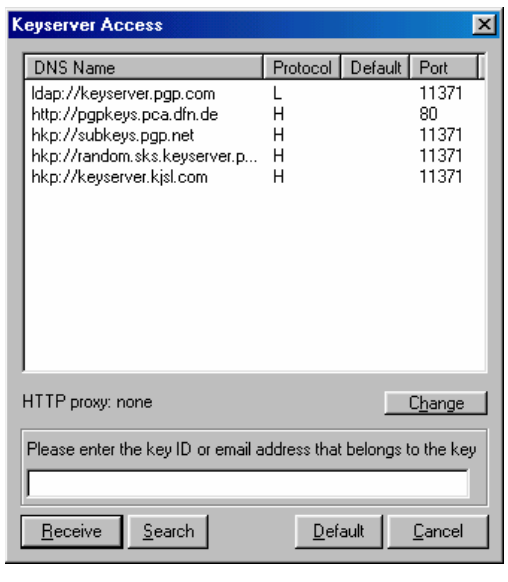
Administrador de claves (Key Manager)

Esta es la ventana que más utilizaremos, ya que además de ver nuestro par de claves (creado al finalizar la instalación de GnuPT), podemos importar las claves públicas de quienes correspondan, exportar nuestra clave PUBLICA a un keyserver, exportar las claves en archivos, asignar niveles de confianza a las claves públicas incorporadas a nuestro keyring y buscar claves en los keyserver por nombre de la persona a incorporar o número de ID.

Podemos acceder entonces al Key Manager, haciendo botón derecho sobre el ícono “Windows Privacy Tray” que se nos creó en la barra de herramientas. Obtendremos la siguiente ventana:

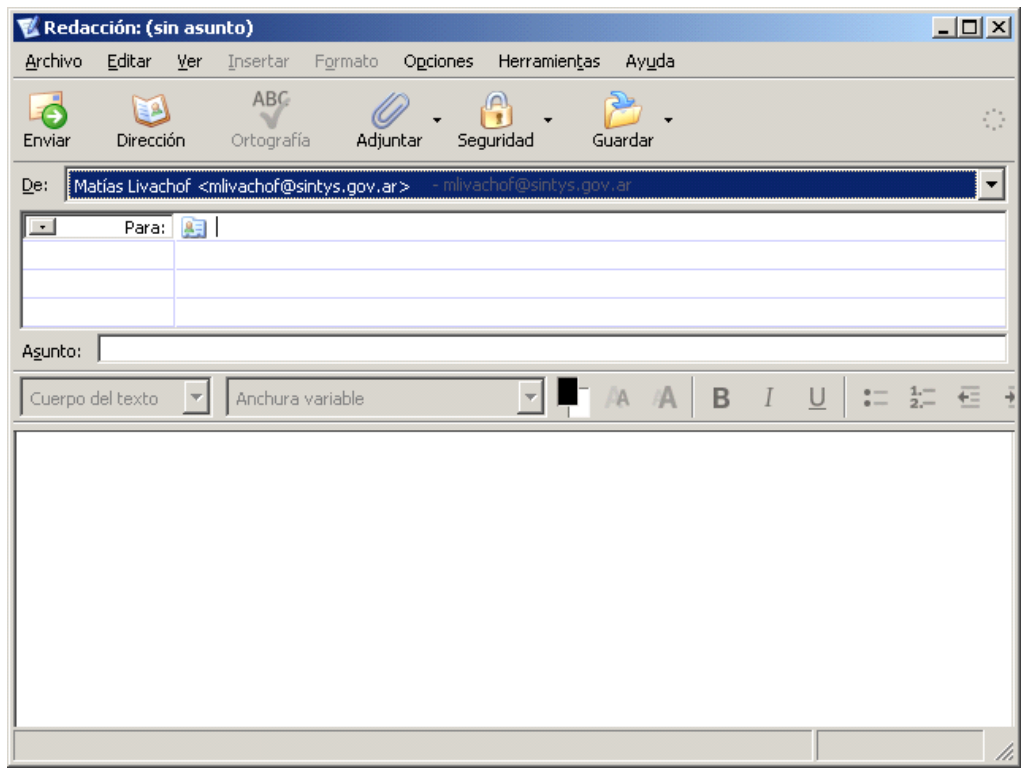


DDesde el menú “Keyserver” vemos los servidores que almacenan las claves públicas en los que se pueden hacer las búsquedas de determinadas claves y adonde podemos exportar la pública nuestra.

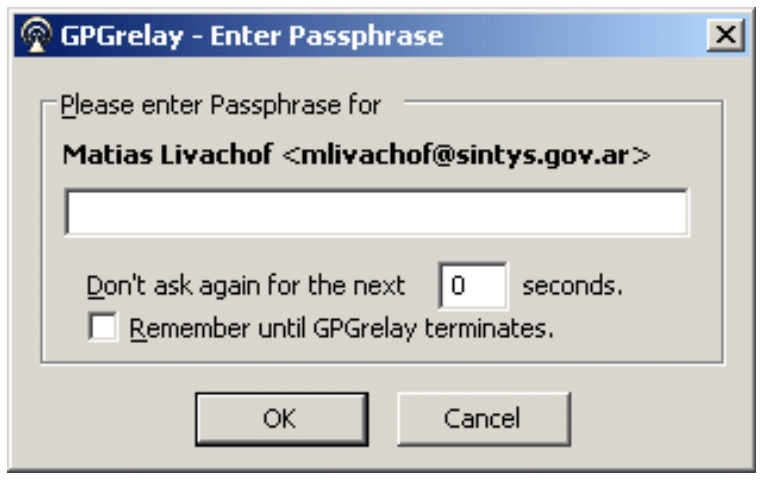


Envío de e-mails con PKI.

Cuando creamos un nuevo email en nuestro cliente de correo Thunderbird nos aparece la siguiente pantalla:

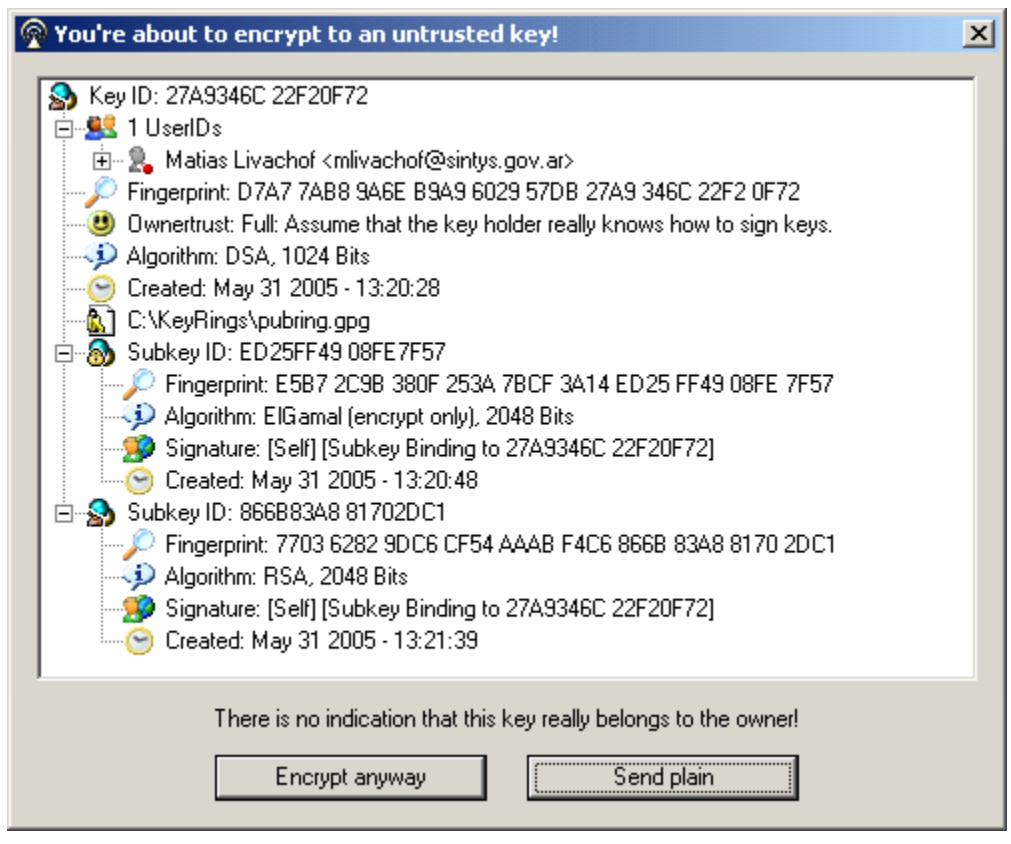


En el campo asunto, si agregamos direcciones que están dentro de nuestro anillo de claves antes de ser enviado, aparecerán las siguientes pantallas:



Ingresamos nuestra frase, la cual creamos en el punto 4.

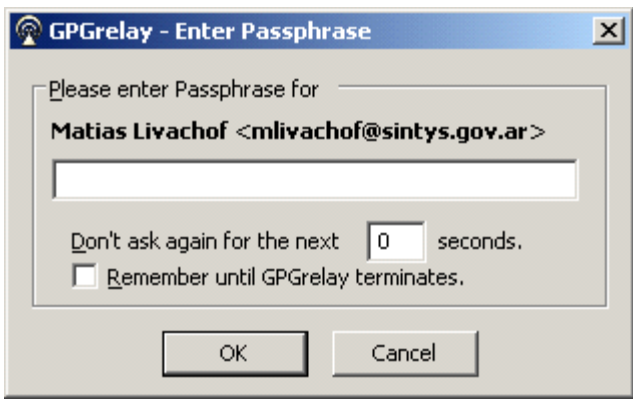
Sólo en caso de que la clave del destinatario no le hayamos configurado la confianza, antes de enviarse el e-mail, aparecerá esta pantalla:



Elegimos “Encrypt anyway” y el e-mail se enviará encriptado. Si ya le habíamos configurado la confianza, este paso por supuesto se obvia.

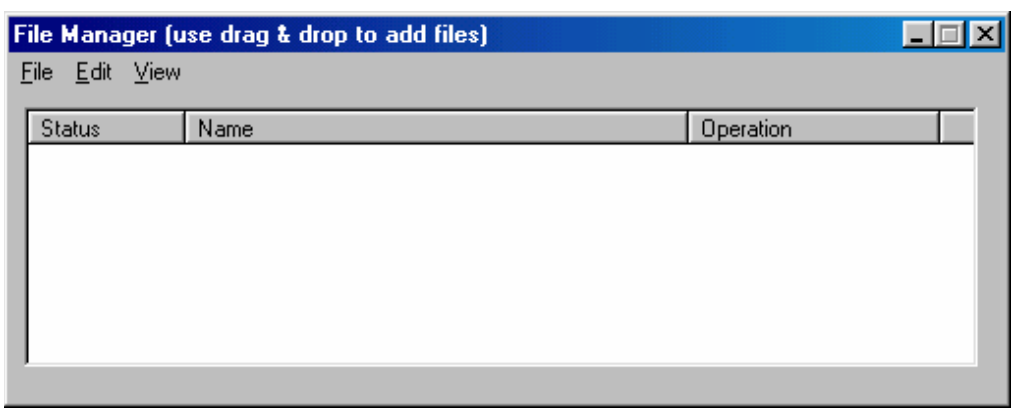
Recepción de e-mail con PKI.

Cuando recibimos un e-mail encriptado y/o firmado digitalmente, también nos pide ingresar nuestra frase:



6. Administrador de archivos (File Manager)

Las funciones que ofrece esta opción de GnuPT, son varias: firmar, encriptar, firmar y encriptar, verificar, borrado seguro (wipe), etc. Podemos acceder al File Manager, haciendo botón derecho sobre el icono “Windows Privacy Tray” que se nos creó en la barra de herramientas.



Esta ventana permite arrastrar un determinado archivo y desde el menú File elegir la función que deseemos realizar con el mismo.

Hardenización de Servidores Debian Linux.

Fecha: 02/09/2005

Versión: 0.4

1. Objetivo

Proponer a soporte informático una serie de recomendaciones para la instalación y configuración segura de Servidores con sistema operativo Debian Linux (sistema operativo alineado con las políticas de seguridad del programa SINTyS).

2. Procedimiento de asignación de contraseñas

a.- Instalar con apt libpam-cracklib

b.- editar el archivo /etc/pam.d/common-password

c.- comentar la siguiente línea:

password required pam_unix.so nullok obscure min=4 max=8 md5

d.- y agregar las siguientes líneas al archivodescomentar las siguientes 2 líneas

password required pam_cracklib.so type=Linux retry=5 minlen=8 difok=3 ucredit=2 dcredit=2

password required pam_unix.so use_authtok nullok md5

Con esto se permite lo siguiente:

1.- 5 reintentos de cambio de password por vez

2.- Que el largo sea por lo menos de 8 caracteres

3.- Que al menos 3 dígitos sean distintos del password anterior

4.- Que al menos haya 2 letras mayúsculas

5.- Que haya dos caracteres numéricos

6.- Al menos una letra minúscula.

7.- Se permite que el usuario cambie su password desde un password en blanco (nuevo usuario)

8.- Se guardan los passwords en /etc/shadow encriptados en md5

3. Recomendaciones

1. Antes de la instalación ingresar una contraseña de BIOS según los pasos de creación de password citados en el punto anterior.

Después de la instalación modificar desde el BIOS la secuencia de arranque del sistema para impedir el arranque desde el disco flexible, el CD-ROM y otros dispositivos desde los que no se debería arrancar.

2. Separar los directorios en que un usuario tiene acceso de escritura así como /home y /tmp una partición separada.

3. Cualquier partición que pueda variar, p.e. /var (especialmente /var/log) también debe estar en una partición separada.

4. Cualquier partición donde haya que instalar un software fuera de la distribución debe estar en una partición separada. De acuerdo con la jerarquía estándar de archivos, serían /opt o /usr/local.

5. No conectarse a internet hasta que se hayan revisado los servicios instalados.

6. Colocar una contraseña de root difícil de resolver. Según los pasos de creación de password citados en el punto anterior.

7. Al final de la instalación se le preguntará si las contraseñas shadow deben ser habilitadas. Responda con un SI a esta pregunta, y así las contraseñas se mantendrán en el archivo /etc/shadow. Sólo el usuario root y el grupo shadow tienen acceso de lectura a este archivo.

8. Instalar la menor cantidad de servicios posibles.

Ejecutar un nmap -sTU -P0 (ip del host a checkear) desde una pc de la red para saber que puertos se están escuchando e identificar servicios innecesarios.

Para deshabilitar los demonios innecesarios modificar los archivos que se encuentran en /etc/rc#.d (donde # es el número del runlevel [0-6]). Cada archivo que comienza con S es que se ejecuta al inicio del sistema, de ser innecesario renombrar el archivo para que no contenga la letra S como primer carácter, agregando la letra K al nombre original

Revisar la lista de servicios en /etc/init.d. En caso de haber un servicio que no debería estar ejecutándose utilizar /usr/sbin/update-inetd -- disable (service), este comando comentará la línea correspondiente al servicio en /etc/initd.conf

9. Instalar la menor cantidad de software posible, basándose en estricta necesidad de uso.. El paquete de Debian contiene una gran cantidad de software que puede no ser necesario, inclusive herramientas de programación y compilación que podrían ayudar a comprometer el equipo.

El siguiente listado son algunos programas que no deben instalarse si no son requeridos específicamente:

Package
---
gdb

gcc- 3.3

dpkg-dev

libc6-dev

cpp- 3.3

manpages-dev

flex

g++ (virtual package)

linux-kernel-headers

bin86

cpp

gcc (virtual package)

g++- 3.3

bison

make

libstdc++5- 3.3-dev

10. Colocar contraseña a Grub

Editar /boot/grub/menu.lst y agregar las siguientes dos líneas al inicio. Esto previene a los usuarios de editar los ítems de entrada. ‘timeout3’ especifica tres segundos antes del arranque del sistema por defecto. (Reemplazar contraseña por el password deseado).

timeout 3
password -md5 [contraseña]

11.Restringir reboot a través de la consola.

Para hacer esto hay que editar /etc/inittab y comentar la siguiente línea:

ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a - r now

12. Para permitir algunos usuarios a que puedan reiniciar el equipo, hay que crear el archivo /etc/shutdown.allow e incluir ahí la lista de los usuarios que podrán hacer el reboot con *ctrl+alt+del.*

13. Acciones de login de usuarios:

Editar el archivo /etc/login.defs
y verificar que estén habilitadas las siguientes variables:

FAIL_DELAY 10

FAILLOG_ENAB yes

LOG_UNKFAIL_ENAB yes

PASS_MAX_DAYS 120

PASS_MIN_DAYS 10

PASS_WARN_AGE 7

14. Instalar timeoutd y configurar /etc/timeouts.

Incluir los usuarios del equipo y consensuar con administrador del equipo un tiempo razonable de uso del equipo. los rangos de tiempo en los que se permitirá el acceso a cada usuario

15. Instalar autolog y configurarlo para remover usuarios *idle.*

Exepto en casos especiales donde se dejan sesiones abiertas por transferencia de archivos entre servidores, configurar autolog para que a los 10 minutos de inactividad, se cierre la sesión.

16. Deshabilitar acceso de administración remota.

Se debe descomentar la siguiente línea

-:wheel:ALL EXCEPT LOCAL
en /etc/security/access.conf

De esta forma los usuarios necesitarán usar su o sudo para tener poderes administrativos y de este modo las trazas de auditoría se generarán.

17. Utilizar acct.

Con apt- get install acct automáticamente se configura el inicio de la aplicación desde el arranque.

Para utilizarlo manualmente, con el comando -acct start- comienza a auditarse todos los comandos que ejecutan los usuarios. Debido a la gran capacidad requerida por este tipo de log, debe generarse algún script para rotar los archivos de log. Los datos se envían a var/account/, más específicamente en el pacct.

sa, ac y lastcomm son aplicaciones que nos permiten el acceso a los archivos de log, ya que éstos no son archivos de texto.

18. Instalación de libsafe para evitar buffer overflows

Descargar el paquete debian desde:

http://packages.debian.org/cgi-bin/download.pl?arch=i386&file=pool%2Fmain%2Flibs%2Flibsafe%2Flibsafe_2.0-16-6_i386.deb&md5sum=df859c153f258f2b4332699c07be8119&arch=i386&type=main

Instalación

Para que esté disponible para todo el sistema debemos añadir al fichero */etc/ld.so.preload* el nombre de la librería (libsafe.so.2) que deseamos cargar nada más se inicie el sistema. La siguiente manera es un forma de hacerlo:

echo “/lib/libsafe.so.2” >> /etc/ld.so.preload

Para evitar que un programa pase por libsafe debemos añadir el programa con path completo a */etc/libsafe.exclude*, en cada línea un programa diferente. Esta opción puede sernos útil si tenemos algún programa que esté compilado con libc5 o bien que desborda la pila intencionadamente (poca utilidad en un servidor, pero es posible). Debido a lo que esto implica */etc/libsafe.exclude* sólo debería poderse modificar por root.

Para saber con qué se ha linkado un programa podemos usar la herramienta *ldd* sobre el programa que queramos averiguar de la siguiente manera:

# ldd /sbin/init
libc.so.6 => /lib/libc.so.6 (0x4001d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)

La segunda situación donde no funciona libsafe es si el programa se ha compilado con la opción *gcc-fomit-frame-pointer*, ya que al compilarlo de esta manera libsafe no puede controlar correctamente el tamaño del frame, y no sabe si se está saltando fuera del frame. Pero esta opción de compilación es extraña, así que la mayoría de programas que nos interesa (servidores principalmente). Y en el caso de no ser así el programa libsafe simplemente no busca si hay violaciones, es decir no modificará el funcionamiento del programa.

19. Segurizando las interfaces de red

Debe crearse el siguiente script con un nombre cualquiera (en el ejemplo es /etc/network/interface-secure)

#!/bin/sh -e

Script-name: /etc/network/interface-secure

Modifies some default behavior in order to secure against

some TCP/IP spoofing & attacks for all interffaces

Contributed by Dariusz Puchalak

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

broadcast echo protection enabled

echo 0 > /proc/sys/net/ipv4/conf/all/forwarding

ip forwarding disabled

echo 1 > /proc/sys/net/ipv4/tcp_syncookies # TCP syn cookie protection enabled

echo 1 >/proc/sys/net/ipv4/conf/all/log_martians # Log strange packets

(this includes spoofed Packets, source routed Packets, redirect Packets)

but be careful with this on heavy loaded web servers

echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

bad error message protection enabled

now ip spoofing protection

echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter

and finally some more things:

Disable ICMP Redirect Acceptance

echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects

echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects

Disable Source Routed Packets

echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route

exit 0

Para llamar al script editaremos el archivo /etc/network/interfaces

Y se agrega la última línea:

auto eth0

iface eth0 inet static

address xxx.xxx.xxx.xxx

netmask 255.255.255.xxx

broadcast xxx.xxx.xxx.xxx

gateway xxx.xxx.xxx.xxx

pre-up /etc/network/interface-secure

20. Ataques ARP

Para evitar los ataques ARP (Cache poisoning, ARP spoofing...) utilizar entradas estáticas en el cache arp con:

arp -s host_name hdwr_addr

para cada host importante en nuestra red para asegurarnos de que nadie pueda crear o modificar el destino de los paquetes.

21. Tripwire

a.- Instalar con apt el paquete tripwire

b.- Seguir el procedimiento de instalación propio y configurar las clave de sitio (site-key pass-phrase) que se utilizará para proteger los archivos de configuración.

c.- Configurar la clave local (local-key pass-phrase) que se utilizará para proteger los archivos en el host, por ejemplo la base de datos de tripwire.

d.- La configuración por defecto cubre los archivos y directorios más importantes. Se puede utilizar esta configuración.

e.- Para agregar más archivos o directorios, se debe editar el archivo twpol.txt y agregar los archivos necesarios de la siguiente manera:

(archivo o directorio) (atributos)

Los atributos pueden ser:

+a; # hora/fecha de acceso

+b; # número de bloques

+c; # hora/fecha de creación/modificación de inodo

+g; # ID de grupo

+i; # número de inodo

+m; # hora/fecha de modificación

+n; # número de enlaces

+p; # permisos

+s; # tamaño del archivo

+t; # tipo del archivo

+u; # ID de usuario

f.- Ejecutar la siguiente línea:

tripwire –init

Nos solicitará la clave de paso local y comenzará a generar la base de datos guíandose en los archivos y directorios que se describen en twpol.txt

Esto demora aproximadamente 20 minutos.

La base de datos estará en /var/lib/tripwire/(nombre de host).twd y debe ser guardada en un medio de sólo lectura, como un floppy o cd.

g.- Para verificar posteriormente el estado del sistema contra este cambio se utiliza el siguiente comando.

tripwire –check -d (ruta del archivo de la base de datos en el medio seguro)

22. Segurizando SSH

• ListenAddress xxx.xxx.xxx.xxx
elegir la interfaz o interfaces que escuchará el demonio ssh.

• PermitRootLogin no
Siempre y cuando sea posible, evitar logins de root remotas. De esta manera se evita conseguir acceso de root por fuerza bruta, ya que se necesitarán dos logins para convertirse en root.

• PermitEmptyPasswords no
Simplemente no permitir passwords en blanco.

• AllowUsers user@somewhere
Para incrementar la seguridad describir los usuarios/ip que tendrán acceso permitido.

• PasswordAuthentication yes
Es posible elegir si utilizar usuario y password para ingresar, o ssh-keys. A definir. Las llaves deben estar alojadas en ~/.ssh/authorized_keys file. Para utilizar las llaves elegir NO.

• Deshabilitar cualquier tipo de login que no utilicemos, por ejemplo RhostsRSAAuthentication, Hostbased Authentication, KerberosAuthentication or RhostsAuthentication. Debemos deshabilitarlo, aún si vienen habilitadas por default,

• Protocol 2
Deshabilita la versión 1 del protocolo debido a la facilidad que permite esa versión a crackear los passwords.

• Banner /etc/*some_file*
Escribir en /etc/banner_legal el siguiente texto

El uso de este sistema está reservado a personal debidamente autorizado.

Todas las actividades de este sistema se registran y están sujetas a revisiones frecuentes.

La información disponible en este sistema es de exclusiva propiedad del SINTyS, que se reserva el derecho a interceptarla, registrarla, leerla o hacerla pública. Los usuarios no deberán esperar privacidad de ningún tipo sobre la información utilizada o intercambiada, independientemente de si ésta se encuentra cifrada o protegida por contraseñas. El uso de este sistema implica el acuerdo implícito con los términos aquí descriptos.

This system is to be used only by authorized personnel. All others will be prosecuted under local and international laws. Activities on this system are automatically logged and subject to review. All data on this system is the property of SINTyS, which reserves the right to intercept, record, read or disclose it at the sole discretion of authorized personnel. Specifically, system or security administrators may disclose any information on or about this system to law enforcement or other appropriate individuals. Users should not expect privacy from system review for any data, whether business or personal, even if encrypted or password-protected. Use of this system constitutes consent to these terms.

23. X Window System

Si no es necesario conectarse vía remota al servidor X iniciar el mismo del siguiente modo:

$ startx -- -nolisten tcp

24. chroot a los servicios más importantes (ejemplo con apache)

1. Loguearse como root y crear el directorio jaula:

mkdir -p /var/chroot/apache

2. Crear un nuevo usuario y un nuevo grupo. El chroot Apache va a correr con este usuario/grupo, y no deben usarse para nada más en el servidor. En este ejemplo se van a llamar ambos (usuario y grupo) chrapach.adduser -- home /var/chroot/apache --shell /bin/false --no-create-home \-- system -- group chrapach

3. Instalar el Apache de modo normal en Debian:

apt-get install apache

4. Configurar Apache (ej. definir lso subdominios, etc). En /etc/apache/httpd.conf, setear las opciones *User* y *Group* con chrapach. Luego reiniciar el Apache y asegurarse de que funcione correctamente. Ahora, detener el demonio.

User chrapach
Group chrapach

/etc/init.d/apache restart
...
/etc/init.d/apache stop

5. Instalar makejail. También instalar wget y lynx ya que se usarán junto con makejail para testear el chroot server.

apt-get install makejail wget lynx

6. Copiar el archivo de configuración ejemplo que brinda makejail para Apache. (hay ejemplos también para sshd, etc...)

cp /usr/share/doc/makejail/examples/apache.py /etc/makejail/

7. Editar /etc/makejail/apache.py. Necesitamos setear las opciones chroot, users y groups. El archivo quedaría como este.

```
chroot="/var/chroot/apache"

testCommandsInsideJail=["/usr/sbin/apachectl start"]

processNames=["apache"]

testCommandsOutsideJail=[--"wget -r --spider http://localhost/",
                         "lynx --source https://localhost/"]

preserve=   ["/var/www",
             "/var/log/apache",
             "/dev/log"]

users=["chrapach"]

groups=["chrapach"]

packages=["apache", "apache-common"]

userFiles=  ["/etc/password",
             "/etc/shadow"]

groupFiles= ["/etc/group",
             "/etc/gshadow"]

forceCopy=   ["/etc/hosts",
              "/etc/mime.types"]
```

8. Crear el directorio de chroot:

makejail /etc/makejail/apache.py

9. Si /etc/password y /etc/group se copiaron enteros, ejecutar las siguientes líneas:

grep chrapach /etc/passwd > /var/chroot/apache/etc/passwd

grep chrapach /etc/group > /var/chroot/apache/etc/group

para reemplazar estos archivos por copias filtradas.

10. Copiar las páginas webs y logs a la jaula. Estos archivos no se copian automáticamente.

cp -Rp /var/www /var/chroot/apache/var

cp -Rp /var/log/apache/*.log /var/chroot/apache/var/log/apache

11. Editar el script de startup del demonio de log de sistema para que también escuche los logs que se generarán dentro de la jaula

/var/chroot/apache/dev/log . En /etc/init.d/sysklogd, reemplazar:

SYSLOGD=" "

Por

SYSLOGD=" -a /var/chroot/apache/dev/log"

y reiniciar el demonio (/etc/init.d/sysklogd restart).

12. Editar el script de inicio de Apache (/etc/init.d/apache). Se deben modificar las siguientes opciones por defecto para que se ejecute adecuadamente en un directorio chroot:

• Setear una nueva variable CHRDIR al inicio del archivo;
CHRDIR=/var/chroot/apache

• editar las secciones start, stop, reload, etc. con los valores actuales de la jaula;

• agregar una línea para montar y desmontar un directorio /proc en la jaula.

```
case "$1" in

 start)

 echo -n "Starting web server: $NAME"

 mount -t proc proc /var/chroot/apache/proc

 start-stop-daemon --start --pidfile $PIDFILE --exec $DAEMON \

       --chroot $CHRDIR

 ;;

stop)

 echo -n "Stopping web server: $NAME"

 start-stop-daemon --stop --pidfile "$CHRDIR/$PIDFILE" --oknodo

 umount /var/chroot/apache/proc

 ;;

reload)

 echo -n "Reloading $NAME configuration"

start-stop-daemon --stop --pidfile "$CHRDIR/$PIDFILE" \
      --signal USR1 --startas $DAEMON --chroot $CHRDIR

 ;;

reload-modules)

 echo -n "Reloading $NAME modules"

 start-stop-daemon --stop --pidfile "$CHRDIR/$PIDFILE" --oknodo \

--retry 30

 start-stop-daemon --start --pidfile $PIDFILE \

--exec $DAEMON --chroot $CHRDIR
```

```
 ;;
restart)
 $0 reload-modules
 exit $?
 ;;
force-reload)
 $0 reload-modules
 exit $?
 ;;
 *)
 echo “Usage: /etc/init.d/$NAME {start/stop/reload/reload-modules/force-reload/ restart}”
 exit 1
 ;;
esac
```

13. En /etc/logrotate.d/apache, reemplazar

/var/log/apache/*.log

con

/var/chroot/apache/var/log/apache/*.log

14. Iniciar Apache (/etc/init.d/apache start) y revisar que se reportó en el log de la jaula (/var/chroot/apache/var/log/apache/error.log).

En caso de que la configuración sea más compleja (por ejemplo si se usa PHP y MySQL), van a faltar archivos. Se puede editar el archivo

/etc/makejail/apache.py y agregar estos archivos en la opción forceCopy.

15. Un poco más de seguridad.

Setear el bit immutable en los archivos passwd, group, htpd.conf, resolv.conf, hosts, nsswitch.conf:

cd /chroot/httpd/etc/
chattr +i passwd

cd /chroot/httpd/etc/
chattr +i group

cd /chroot/httpd/etc/httpd/conf/
chattr +i httpd.conf

cd /chroot/httpd/etc/
chattr +i resolv.conf

cd /chroot/httpd/etc/
chattr +i hosts

cd /chroot/httpd/etc/
chattr +i nsswitch.conf

Copiar el archivo localtime a la jaula para que las entradas de log se ajusten adecuadamente a nuestro timezone.

cp /etc/localtime /chroot/httpd/etc/

16. Asegurarse de que el Apache esté corriendo chrooted:

Para probarlo...
ls -la /proc/‘cat /var/chroot/apache/var/run/apache.pid‘/root/.

25. Inhabilitar a los usuarios a publicar contenido html

En caso de que el servidor utilice el servidor apache, en el archivo /etc/apache/http.conf comentar la siguiente línea:

LoadModule userdir_module /usr/lib/apache/1.3/mod_userdir.so

26. Deshabilitar o limitar el servicio RPC (portmap)

Para deshabilitar el servicio, renombrar el archivo

/etc/rcS.d/S43portmap por /etc/rcS.d/K43portmap

En caso de que sea necesario para servicios locales (por ejemplo GNOME) se puede configurar el package portmap para que sólo escuche servicios locales. Para esto se debe modificar el archivo /etc/default/portmap, y no cometar la siguiente línea:

#OPTIONS=”-i 127.0.0.1"

En caso de que no sea posible deshabilitarlo, más adelante se verá como hacerlo ajustar el servicio a través del firewall.

27. Firewall IpTables

```
#!/bin/sh

# Caveats:
# - This configuration applies to all network interfaces
# if you want to restrict this to only a given interface use
# ‘-i INTERFACE’ in the iptables calls.
# - Remote access for TCP/UDP services is granted to any host,
# you probably will want to restrict this using ‘--source’
# description: Activates/Deactivates the firewall at boot time
PATH=/bin:/sbin:/usr/bin:/usr/sbin
# Services that the system will offer to the network
TCP_SERVICES=”” # SSh only
UDP_SERVICES=””
SSH_PORT=”22"
POP3_PORT=”110"
SMTP_PORT=”25"
EUCLIDES=”10.64.96.201"
# MTA & apt-proxy
APT_PROXY=”10.64.96.219"
# Services the system will use from the network
REMOTE_TCP_SERVICES=”3128" # web browsing
REMOTE_UDP_SERVICES=”53" # DNS
# Network that will be used for remote mgmt
# (if undefined, no rules will be setup)
NETWORK_MGMT=10.64.0.0/16
if ! [ -x /sbin/iptables ]; then
exit 0
fi
fw_start () {
# Input traffic:
/sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Services
if [ -n “$TCP_SERVICES” ] ; then
for PORT in $TCP_SERVICES; do
/sbin/iptables -A INPUT -p tcp --dport ${PORT} -j ACCEPT
done
fi
if [ -n “$UDP_SERVICES” ] ; then
for PORT in $UDP_SERVICES; do
/sbin/iptables -A INPUT -p udp --dport ${PORT} -j ACCEPT
done
fi
# Remote management
if [ -n “$NETWORK_MGMT” ] ; then
/sbin/iptables -A INPUT -p tcp --src ${NETWORK_MGMT} --dport ${SSH_PORT} -j ACCEPT
else
/sbin/iptables -A INPUT -p tcp --dport ${SSH_PORT} -j ACCEPT
fi
# Remote testing
/sbin/iptables -A INPUT -p icmp -m limit --limit 3/s -j ACCEPT
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -P INPUT DROP
/sbin/iptables -A INPUT -j LOG
# Output:
/sbin/iptables -A OUTPUT -j ACCEPT -o lo
/sbin/iptables -A OUTPUT -m state  - - state NEW,ESTABLISHED,RELATED -j ACCEPT
# ICMP is permitted
```

```
/sbin/iptables -A OUTPUT -p icmp -j ACCEPT
# So are security package updates
/sbin/iptables -A OUTPUT -p tcp -d ${APT_PROXY} --dport 9999 -j ACCEPT
# So are mail ports
/sbin/iptables -A OUTPUT -p tcp -d ${APT_PROXY} --dport ${POP3_PORT} -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -d ${APT_PROXY} --dport ${SMTP_PORT} -j ACCEPT
# As well as the services we have defined
if [ -n “$REMOTE_TCP_SERVICES” ] ; then
for PORT in $REMOTE_TCP_SERVICES; do
/sbin/iptables -A OUTPUT -p tcp --dport ${PORT} -j ACCEPT
done
fi
if [ -n “$REMOTE_UDP_SERVICES” ] ; then
for PORT in $REMOTE_UDP_SERVICES; do
/sbin/iptables -A OUTPUT -p udp --dport ${PORT} -d ${EUCLIDES} -j ACCEPT
done
fi
# All other connections are registered in syslog
/sbin/iptables -A OUTPUT -j LOG
/sbin/iptables -A OUTPUT -j DROP
/sbin/iptables -P OUTPUT DROP
# Anti-flooding syn packages
/sbin/iptables -N syn-flood
/sbin/iptables -A INPUT -p tcp --syn -j syn-flood
/sbin/iptables -A syn-flood -m limit --limit 2/s --limit-burst 4 -j RETURN
/sbin/iptables -A syn-flood -j DROP
# Other network protections
# echo 1 > /proc/sys/net/ipv4/tcp_syncookies
echo 0 > /proc/sys/net/ipv4/ip_forward
#ignore ping
#echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo 1 >/proc/sys/net/ipv4/conf/all/log_martians
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route
}
fw_stop () {
/sbin/iptables -F
/sbin/iptables -t nat -F
/sbin/iptables -t mangle -F
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT ACCEPT
}
fw_clear () {
/sbin/iptables -F
/sbin/iptables -t nat -F
/sbin/iptables -t mangle -F
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -P OUTPUT ACCEPT
}
```

```
case “$1” in

start/restart)

echo -n “Starting firewall..”

fw_stop

fw_start

echo “done.”

;;

stop)

echo -n “Stopping firewall..”

fw_stop

echo “done.”

;;

clear)

echo -n “Clearing firewall rules..”

fw_clear

echo “done.”

;;

*)

echo “Usage: $0 {start/stop/restart/clear}”

exit 1

;;

esac

exit 0
```

28. Tcpwrappers (libwrap)

Si bien Tcpwrappers nos provee resultados similares a iptables, trabaja de manera diferente ya que intercepta el intento de conexión, examina sus archivos de configuración, y decido si aceptar o no. Tcpwrappers controla el acceso a nivel de aplicación.

Primero consulta el archivo hosts.allow

Tcpwrappers consiste de archivos de configuración /etc/hosts.allow y /etc/hosts.deny. La funcionalidad está provista por la librería libwrap.

Tcpwrappers se utiliza para proteger los servicios que se inician en inetd. Asumimos que la mayoría de las aplicaciones no están compiladas con soporte para libwrap por lo tanto, sólo usaremos tcpwrappers para los servicios que se inician en inetd y IpTables para los servicios que no sean parte del inetd.

Tcpwrappers primero mira si se permite el acceso en /etc/hosts.allow, y si está incluido en el archivo, el acceso es otorgado, sino, se mira en /etc/hosts.deny para ver si el acceso no está permitido. Si está, se niega el acceso, sino, el acceso es otorgado, por eso se recomienda negar cualquier acceso que no esté permitido.

Un ejemplo del archivo inetd.conf:

```
# Pop and imap mail services et al

#

#pop-2 stream tcp nowait root /usr/sbin/tcpd ipop2d

#pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d

#imap stream tcp nowait root /usr/sbin/tcpd imapd

#
```

Desde la segunda hasta la última columna, configuran el demonio tcpwrappers -- **/usr/sbin/tcpd**.

La política default será negar todo y abrir agujeros para permitir la mínima cantidad de tráfico necesario.

Editar /etc/hosts.deny y sólo debe contener la siguiente línea.

```
ALL: ALL
```

Ahora se abren los servicios necesarios tan restrictivo como se pueda.

```
ALL: 127.0.0.1

sshd, ipop3d: 192.168.1.

sshd: .myworkplace.com, hostess.mymomshouse.com
```

La formato es: $Nombre_Servicio: $Quien

Para verificar la configuración de tcpwrappers se incluye la utilidad **tcpdchk**

Procedimientos de tratamiento de Expedientes en UPCS

Fecha: 08/11/2005

Versión: 0.1

1. Objetivos

El propósito de este procedimiento es el de sentar los mecanismos generales de tratamiento de información sensible contenida en expedientes que se utilicen en nodos SINTyS provinciales (UPCS). A tal efecto se presentan dos esquemas, mínimo y óptimo, dentro de los cuales deberán enmarcarse el manejo de expedientes en dependencias UPCS.

2. Responsabilidades

El responsable del área de seguridad informática junto al coordinador del componente Infraestructura tienen responsabilidad sobre la confección y actualización del presente procedimiento y de gestionar la implementación de las medidas protectivas que se desprenden del mismo, basados en el análisis de riesgos sobre el manejo de información sensible en las distintas UPCS y su contexto. Asimismo, ambos responsables o personal por ellos delegado, deberán efectuar visitas no anunciadas con una frecuencia no mayor a la semestral por las distintas UPCS, a fin de auditar el cumplimiento del presente procedimiento.

El responsable informático de la UPCS, junto al coordinador de la UCPS serán los/las encargados/as de velar por el cumplimiento de la presente política y deberán notificar con carácter de urgencia al área de seguridad informática (seguridad@sintys.gov.ar) sobre violaciones a la misma.

Los consultores asignados en las distintas UPCS deberán cumplir el presente procedimiento, informando a los responsables de la UPCS o al área de seguridad informática sobre violaciones al mismo.

4. Procedimiento

Información recibida en UPCS

Esquema Mínimo

Toda información confidencial que se reciba en formato CD o DVD se ingresará por despacho en la UPCS. Inmediatamente se le asignará un código de inventario respetando la siguiente nomenclatura:

Fecha de Recepción|Código de Origen|ID de Disco

Donde:

- *Fecha de recepción* es la fecha en la que se da ingreso por despacho al CD/DVD correspondiente
- *Código de Origen* es el código con el que ha sido rotulado el CD/DVD en cuestión
- *ID de disco* es un número secuencial generado en la UPCS ante la llegada de un nuevo disco o soporte magnético

Ejemplo:

08/11/2005|10450-1877|28

El código así generado, junto al código de barras equivalente se imprimirán en una etiqueta inviolable que se adosará al medio en cuestión (CD o DVD). Asimismo, una vez procesada la información allí contenida (integrado en BBDD, etc), se lo conservará en un armario ad-hoc bajo llave en poder del coordinador de la UPCS.

El coordinador informático de la UPCS será el responsable del resguardo del acceso físico y lógico de la información allí contenida, hasta su almacenamiento en el armario correspondiente.

Los backups que abarquen dicha información deberán preservarse con las mismas medidas de resguardo físico y lógico de manera de preservar las mismas premisas de seguridad que en el caso de la información disponible on-line.

Esquema Optimo

Se sigue el mismo proceso de ingreso por despacho y asignación de código identificatorio único.

Adicionalmente, se guardarán los archivos correspondientes junto a un checksum criptográfico generado con la utilidad tripwire sobre los mismos. Toda esta información se protegerá a su vez con los permisos de grupo del sistema de archivos, restringidos exclusivamente a los usuarios que tengan necesidad estricta de acceso a la misma. Si, al cabo de un cierto tiempo dicha información no necesita procesarse más, se procederá al borrado seguro de la misma, preservando no obstante el registro de ingreso a despacho de dicha información como comprobante de procesado de la misma.

Los backups que abarquen a dicha información deberán respaldarse con control de integridad y confidencialidad según la criticidad de la misma. A tal efecto, se sugiere la creación de tres claves criptográficas para cifrar información de categoría *pública*, *confidencial* o *secreta*.

Información emitida en UPCS destinada a otros Organismos / Dependencias

Esquema Mínimo

Toda información confidencial que se genere en la UPCS destinada a distintos organismos o dependencias SINTyS, se grabará en medios ópticos (CD o DVD) y se nomenclará de la siguiente manera:

Fecha de Generación| Nota de Pedido|Repartición Destino|UPCS|ID de Disco

Donde:

- *Fecha de generación* es la fecha en la que se finaliza el proceso de compilación de la información, y se graba en el CD/DVD correspondiente

• *Nota de pedido* es la identificación única de la nota de pedido de la información correspondiente

• *Repartición Destino* es el organismo o dependencia destinataria del CD o DVD con la información generada

• *UPCS* es la dependencia provincial SINTyS desde donde se genera dicha información

• *ID de disco* es un número secuencial generado en la UPCS ante la generación de un nuevo disco o soporte magnético

Ejemplo:

16/11/2005|18492|RENAPER|UPCS-Salta|31

El código así generado junto al código de barras equivalente se imprimirán en una etiqueta inviolable que se adosará al medio en cuestión (CD o DVD). Asimismo, una vez procesada la información allí contenida (integrado en BBDD, etc), se lo conservará en un armario ad-hoc bajo llave en poder del coordinador de la UPCS.

Esquema Optimo

Toda información confidencial que se genere en la UPCS destinada a distintos organismos o dependencias SINTyS se distribuirá respetando los siguientes pasos:

• Se nomenclarán los archivos siguiendo el siguiente formato:

Fecha de Generación| Nota de Pedido|Repartición Destino|UPCS

Donde:

• *Fecha de generación* es la fecha en la que se finaliza el proceso de compilación de la información.

• *Nota de pedido* es la identificación única de la nota de pedido de la información correspondiente

• *Repartición Destino* es el organismo o dependencia destinataria del CD o DVD con la información generada

• *UPCS* es la dependencia provincial SINTyS desde donde se genera dicha información

• En segundo lugar se compactará el archivo y se usará criptografía de clave pública (PGP o GPG) para cifrar y firmar los archivos generados. De esta manera se preservarán las premisas de confidencialidad (al cifrar con la clave pública del destinatario), integridad (al firmar con la clave secreta del operador a cambio de la UPCS), y no repudiación (cifrando para que sólo el destinatario en poder de la clave privada correspondiente a la clave pública empleada pueda recuperar la información)

• Finalmente se trasmitirá el archivo cifrado y firmado mediante VPN permanente o virtual hacia el destino, usando cualquiera de los protocolos siguientes: IPSec, SSL, SSH, acordando previamente con el destinatario la modalidad escogida.

• Finalizado dicho proceso se borrará de manera segura (sobreescritura siguiendo lo aconsejado por las buenas prácticas) el archivo original, preservando únicamente el archivo cifrado.

4. Incumplimiento

El incumplimiento del presente procedimiento puede derivar en cualquiera de las siguientes medidas

1. Revocación de privilegios de acceso sobre consultores SINTyS, proveedores o soporte técnico autorizados por el SINTyS.

2. Sanciones disciplinarias para consultores del SINTyS, pudiendo llegar a la desvinculación contractual immediata y eventual procesado legal.

3. Procesado legal a terceras partes según lo indicado en la legislación vigente.

5. Terminología

UCSN: Unidad Coordinadora SINTyS Nación

UPCS: Unidad Provincial Coordinadora SINTyS

Procedimiento de Utilización de GnuPT (WinPT y GPGrelay).

Fecha: 11/05/2005
Autor: Lorena López (llopez@sintys.gov.ar), Guillermo Marro (gmmarro@sintys.gov.ar)
Versión: 0.4

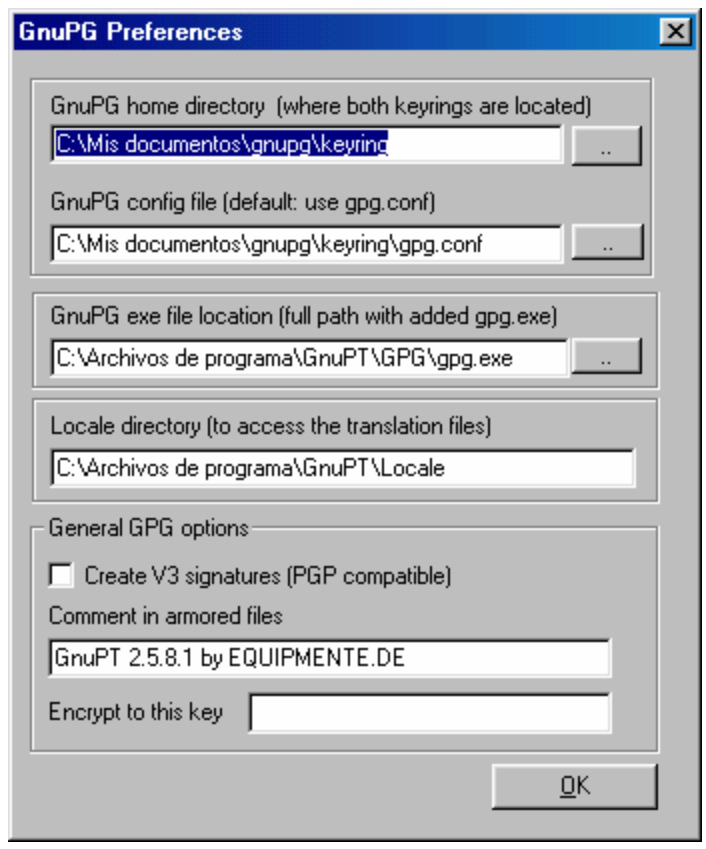
1. Objetivo

Proveer al Area Expedientes, de la documentación necesaria para la utilización de una herramienta Freeware de criptografía como lo es GnuPT, garantizando así que el cruce de bases de datos con los distintos organismos se haga en forma segura, preservando la confidencialidad e integridad de los mismos y en particular, asegurando la no repudiación.

2. Instalación y configuración

La instalación de GnuPT se apoya en un asistente que nos va guiando durante todo el proceso. Básicamente lo que hace es preguntarnos: el directorio de instalación del programa y el directorio donde van a residir las claves. El último paso es la creación de nuestro par de claves.

Para corroborar que todo salió bien, debemos ver en la ventana Preferencias (a la cual accedemos con botón derecho sobre el icono “Windows Privacy Tray-GPG” que se nos creó en la barra de herramientas), algo como lo siguiente:



3. Procedimiento para la Distribución de expedientes

Una vez instalado y configurado el GnuPT, se recomienda seguir los siguientes pasos para la distribución segura de los expedientes:

i) Compaginación del expediente.

ii) Zipeo del archivo.

iii) Cifrado con clave pública del destinatario (que previamente deberá cargarse en el keyring).

iv) Generación del archivo **.zip.gpg**.

v) Borrado seguro del archivo .zip y .txt desde el explorador de archivos, con botón derecho sobre el archivo a borrar, seleccionando la opción PGP – Wipe.

vi) Se quema el **.zip.gpg** en el CD a distribuir.

vii) Se envía el CD al destinatario.

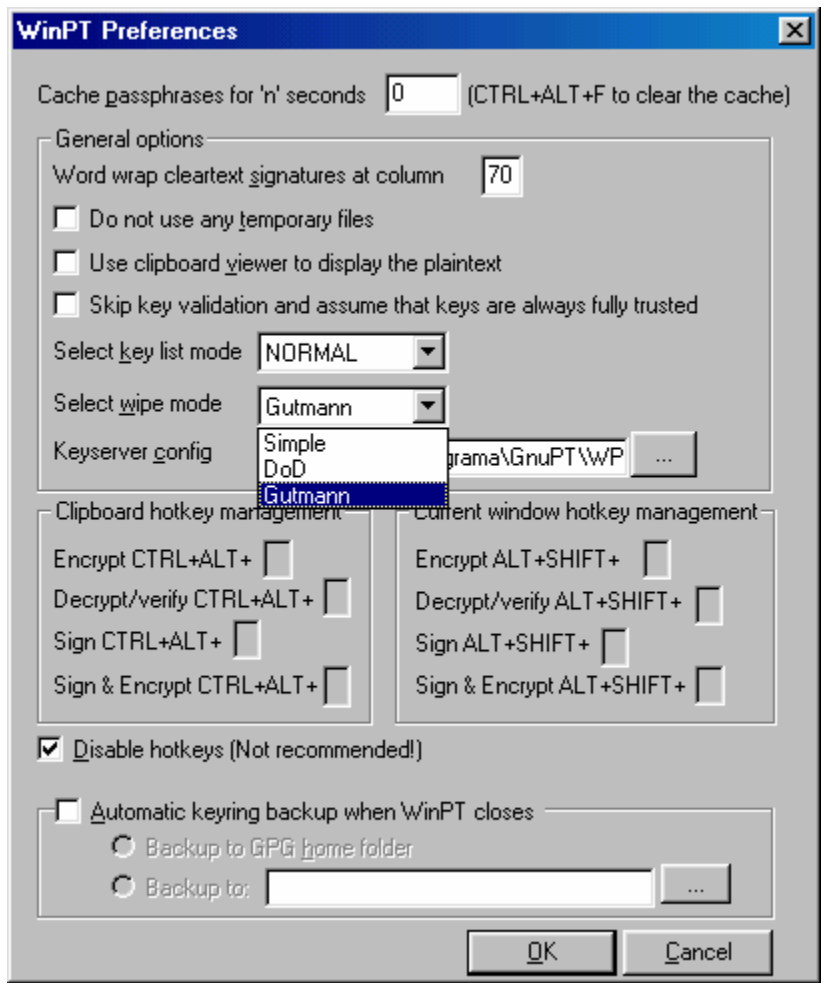
Notas MUY Importantes:

a) Debemos asegurarnos que el destinatario tenga GnuPT (o PGP), con la clave pública del SINTyS en su Keyring. Caso contrario no podrá descifrar el archivo.

b) Cuando el Area de Expedientes hace el cifrado (punto **iii**) deberá asegurarse de que sólo se cifre para la **clave pública del destinatario** (esto es, quitar la clave pública del SINTyS que estará por defecto). Esto permite deslindar toda futura responsabilidad del SINTyS de los datos contenidos en el CD (no-repudiación).

c) No es necesario que el destinatario tenga acceso a Internet.

d) Para el borrado seguro con Wipe, debemos chequear que el modo esté en “*Gutmann*” en las Preferencias de WinPT.



Procedimiento de Instalación y Configuración Checkpoint Secure-Client.

Fecha: 07/06/2005

Versión: 1

1. Objetivo

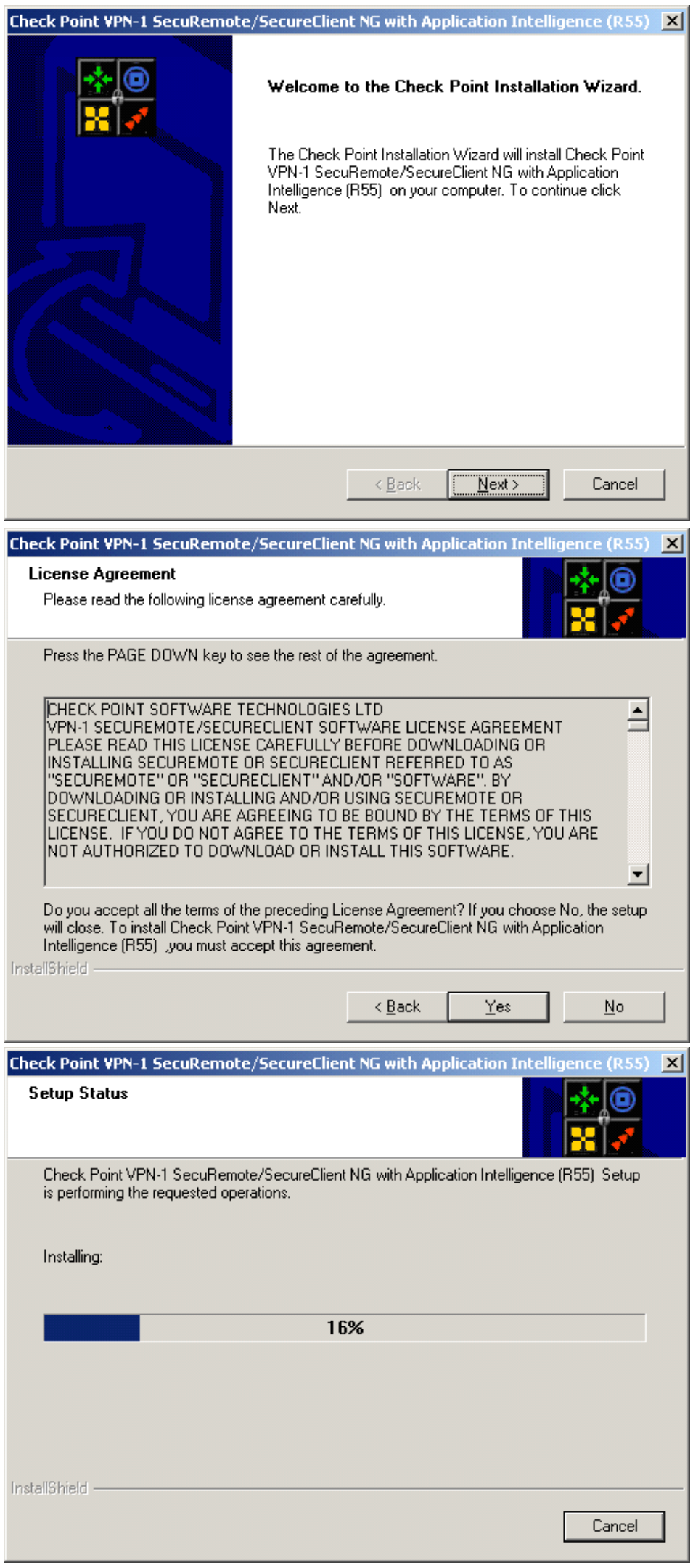
Proveer a las personas autorizadas, la documentación necesaria para la instalación, configuración y utilización de la red privada virtual. Esta última dependerá de las políticas asignadas a cada persona en el Policy Server administrado por Seguridad Informática.

2. Introducción

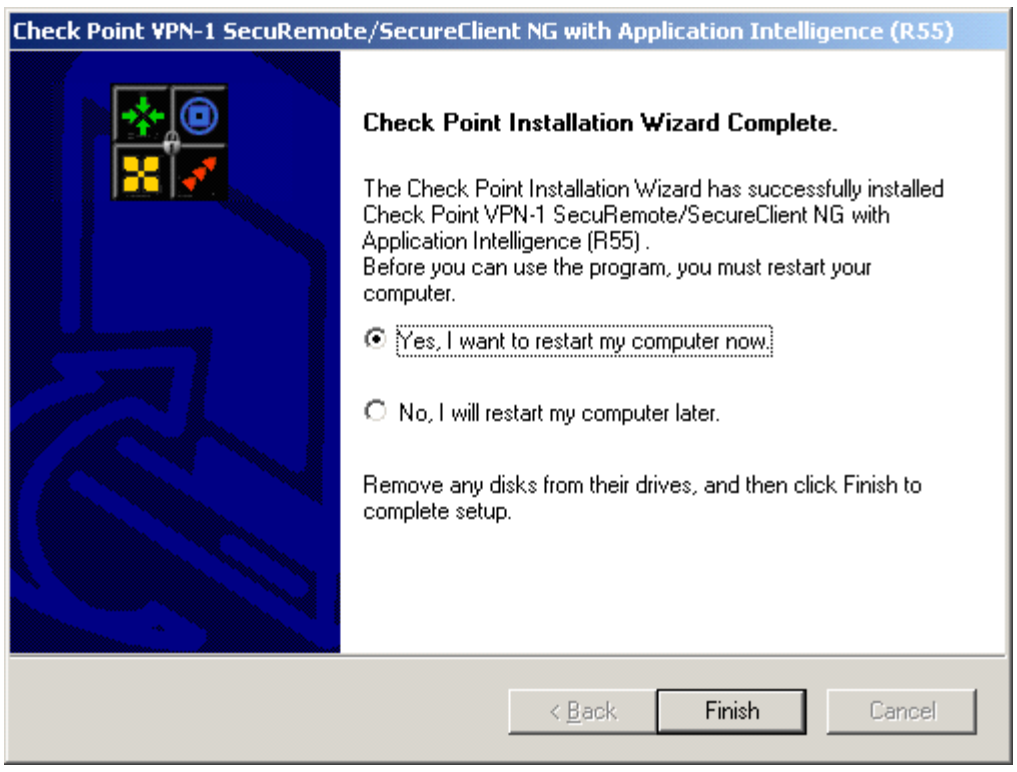
Es necesario instalar un programa denominado Secure-Client. Una vez hecho esto, los pasos a seguir se describen detalladamente en este documento.

3. Instalación Secure Client

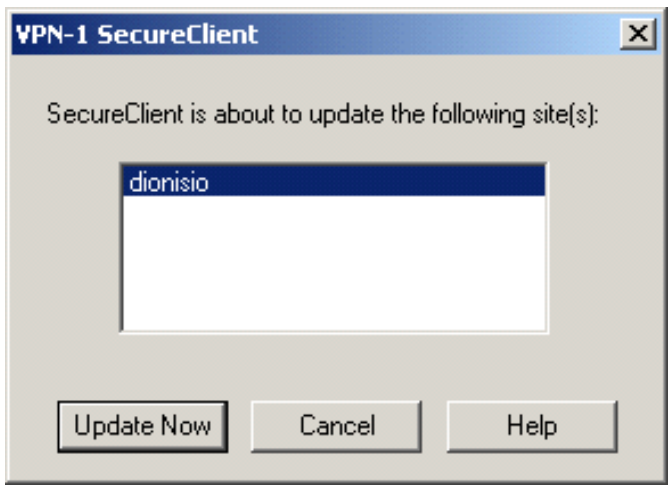
A continuación se muestran las pantallas que se irán sucediendo.



Es necesario reiniciar el equipo para que funcione correctamente



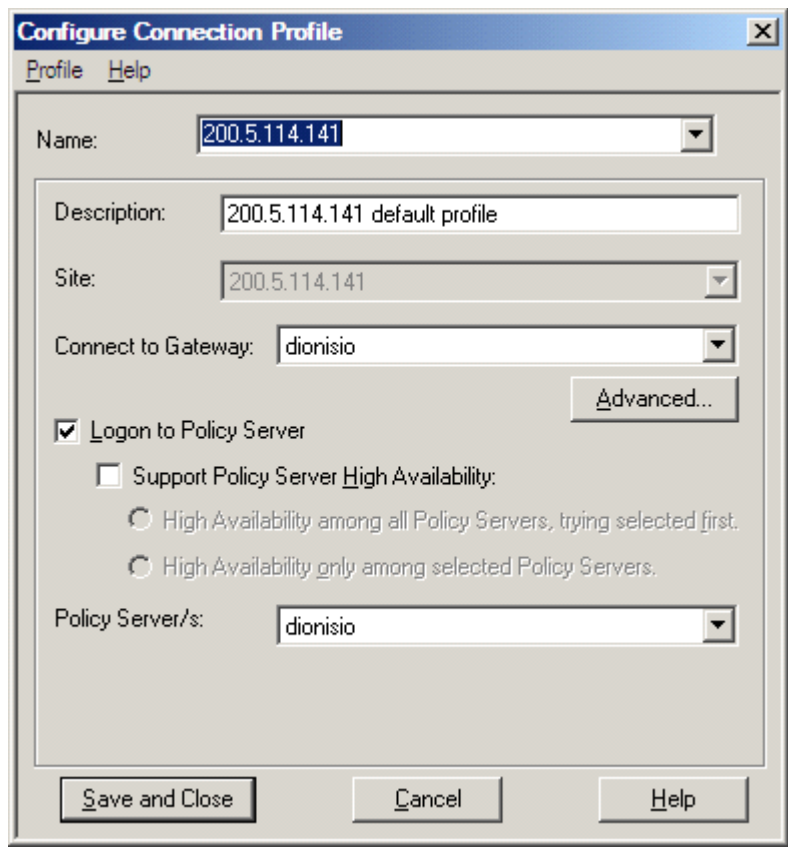
Al reiniciar aparece la siguiente pantalla, seleccionamos Dionisio y elegimos Update Now.



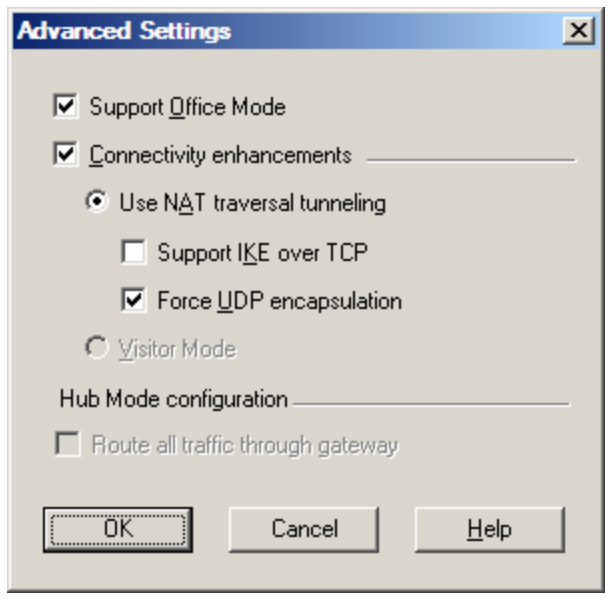
4. Conectándonos al Sitio a través de Secure Client

Sobre el icono del SecureClient (en la barra de tareas) hacemos botón derecho y elegimos Connect.

Luego, hacemos elegimos Properties.. y aparecerá esta pantalla.



Elegimos Advanced y verificamos que las opciones estén definidas como aparece en la siguiente imagen.



Marcamos las opciones que hagan falta para que quede de manera idéntica y elegimos ok. Automáticamente vuelve a la pantalla anterior y elegimos Save and Close.

Ahora estamos en la primer pantalla pero esta vez elegimos Connect.

Y aparecerá la siguiente pantalla.

Donde dice User name debe ir el nombre de usuario suministrado y donde dice Type in password now, se debe escribir el password suministrado.

Por último hacer click en Ok y en segundos estará conectado.

Procedimiento de Hardening de entornos Oracle

Fecha: 25/10/2005

Versión: 0.2

1. Objetivo

Definir los pasos a seguir ante el despliegue seguro de un nuevo sistema DBMS Oracle, para cumplir con las premisas de seguridad descriptas en la política de seguridad del SINTyS.

2. Introducción

Existe la necesidad de proteger el entorno de Bases de Datos (BBDD), tanto el de UCSN como en UPCS, ya que los datos allí contenidos constituyen los activos de información de mayor valor del programa SINTyS. Esto implica que deberían destinarse los mayores esfuerzos en mitigar riesgos en dichos entornos.

La aplicación exitosa de este documento para el programa SINTyS asume que se cuenta con un estudio BIA (Análisis de Impacto al Negocio) actualizado y que el consultor que hará la configuración inicial del DBMS está familiarizado con la clasificación de activos que se desprende de dicho BIA.

El presente documento no incluye una explicación de como implementar cada medida propuesta, sino tan sólo intenta ser un checklist de ayuda al/los consultor/es encargada/o/s de llevar a cabo la instalación segura del entorno Oracle.

3. Checklist

Las medidas a tomar pueden agruparse en distintos grupos según se ocupen de la seguridad física, la seguridad lógica del SO sobre el que se monta el servidor Oracle o la seguridad del entorno DBMS.

Seguridad Física

1. Garantizar las premisas básicas de seguridad física sobre la máquina sobre la que se instalará el servidor Oracle. Alojando dicho servidor en el CPD, tanto en UCSN o UPCS, dichas premisas deberían quedar garantizadas, de acuerdo a las consignas de diseño de dichos recintos CPD

2. Almacenar copias de los soportes de instalación y configuración de Oracle en depósito seguro remoto (off-site)

Seguridad Lógica de SO

Asumiendo el SO a emplear es Solaris 8 (o más moderno):

5. No instalar Oracle con el usuario *root*

6. Antes de instalar, setear la umask a *022*

7. No usar */tmp* como directorio de instalación. Usar un directorio ad-hoc con permisos tipo *700*

8. Bloquear la cuenta del usuario bajo el cual se instala Oracle. No usarla para administrar la BD. No nombrar dicha cuenta como *oracle*

9. Verificar que el usuario *oracle* es el propietario de todos los archivos en $ORACLE_HOME/bin. Verificar que los permisos sean *0750* o inferiores. Verificar que el grupo sea adecuado. Asegurarse que el usuario *oracle* no tenga privilegios de *root*.

10. Usar diferentes propietarios para componentes Oracle distintos: *listener*, *intelligent agent* y *database*

11. Chequear los integrantes del grupo OSDBA (rol de SO que permite controlar logins de DBAs usando autenticación del SO- contiene todos los privilegios de sistema con WITH ADMIN OPTION, permite CREATE DATABASE, etc)

12. No usar el nombre dba para el grupo OSDBA

13. Chequear los permisos de los archivos de datos

14. Seguir -cuando sea posible- las pautas de hardening descriptas en:

http://www.boran.com/security/sp/Solaris_hardening4.html

Seguridad Lógica de la Aplicación

1. Instalar sólo la funcionalidad de Oracle que vaya a utilizarse. No instalar paquetes innecesarios.

2. Aplicar los patches de seguridad recomendados por el fabricante con periodicidad adecuada

3. Cambiar la password de SYS Y SYSTEM en la base.

4. Chequear passwords por default al estilo de "*change_on_install*"

5. Chequear que las contraseñas elegidas para usuarios de privilegio (en particular usuarios SYS y SYSTEM) satisfacen las buenas prácticas en tal sentido (i.e.: longitud mínima de 8 caracteres, no basada en palabras de diccionarios, utilización obligatoria de minúsculas, mayúsculas, símbolos y números, cambios mínimos de 3 caracteres respecto a última contraseña, etc.)

6. Utilizar profiles de contraseñas:

FAILED_LOGING_ATTEMPS: 3

PASSWORD_LOCK_TIME 1 día

PASSWORD_LIFE_TIME 90 días

PASSWORD_GRACE_TIME 5 días

PASSWORD_REUSE_TIME 900 días

PASSWORD_REUSE_MAX 10

7. Asegurarse que los permisos del archivo *init.ora* sean limitados

8. Chequear que el parámetro *07_dictionary_accesibility* esté seteado a *false*

9. Crear una cuenta para cada persona con rol DBA que deba acceder al sistema DBMS y ninguna más. No usar una única cuenta con rol DBA compartida entre dos o más personas.

Query relacionado:

select distinct(username) from sys.dba_user_privs where rolename='DBA' and username not in ('SYS','SYSTEM').

(Listado: DBA_ROLES)

10. Chequear los permisos del *trace file*

11. Quitar *tkprof* de BBDD en producción

12. Quitar la utilidad *otrace* de BBDD en producción

13. Verificar que los siguientes archivos tengan un set de permisos limitados: webcache.xml, snmp_ro.ora, snmp_rw.ora, sqlnet.ora, htaccess, wdbsvr.app y xsqlconfig.xml

14. Setear los passwords para acceso HTTP

15. Inhibir iSQL*Plus para servidores en producción

16. Inhibir cuentas default que no se utilicen (en particular SNMPAGENT)

Query relacionado:

select * from dba_users

where username IN ('CTXSYS','DBSNMP','MDSYS','OUTLN','PERFSAT','SCOTT')

17. Asegurar que los siguientes valores están configurados en init.ora:

trace_files_public=FALSE

global_names=TRUE

remote_os_authent=FALSE

remote_listener=" "

sql92_security=TRUE

18. Limitar al extremo la asignación de permisos que incluyen el modificador *ANY*

19. Limitar al extremo privilegios para *ALTER SESSION*, *ALTER SYSTEM* y *BECOME USER*

20. No setear los parámetros *default_tablespace* o *temporary_tablespace* a *SYSTEM* para cuentas ordinarias de usuarios

21. No colapsar *OSDBA/SYSDBA, OSOPER/SYSOPER* y *DBA* en un único rol. Los mapeos de grupo a *OSDBA, OSOPER* y el usuario propietario del software deberían de ser distintos

22. Restringir usuarios que tienen privilegios del tipo *WITH ADMIN* (esto restringe usuarios habilitados a cambiar schemas y otros atributos de sistema)

23. Restringir asignaciones del tipo *WITH GRANT* (esto restringe la aplicación transitiva de permisos)

24. Setear *dblink_encrypt_login = true* (server) y *ora_encrypt_login* (cliente) para garantizar el cifrado de claves via dblinks

25. Controlar que el acceso por DBLINK no sea al usuario dueño de los objetos de la base destino.

Query relacionado:

SELECT * FROM DBA_DB_LINKS

Listado: SYSTEM_DBLINKS

26. Controlar que los accesos por medio de dblinks no se realicen con privilegios DBA, SYSTEM, SYS

Query relacionado:

SELECT * FROM DBA_DB_LINKS

Listado: SYSTEM_DBLINKS

27. Comprender y auditar privilegios asignados a usuarios y roles. En particular controlar que los privilegios otorgados a cada grupo de usuario mediante roles esté acorde a la función del grupo

Queries relacionados:

```
CREATE OR REPLACE VIEW DBA_USER_PRIVS (USERNAME, ROLENAME, PRIVILEGE) AS
SELECT DECODE(SA1.GRANTEE#, 1, 'PUBLIC', U1.NAME), SUBSTR(U2.NAME,1,20),
SUBSTR(SPM.NAME,1,27)
FROM SYS.SYSAUTH$ SA1, SYS.SYSAUTH$ SA2, SYS.USER$ U1,
SYS.USER$ U2, SYS.SYSTEM_PRIVILEGE_MAP SPM
WHERE SA1.GRANTEE# = U1.USER#
AND SA1.PRIVILEGE# = U2.USER#
AND U2.USER# = SA2.GRANTEE#
AND SA2.PRIVILEGE# = SPM.PRIVILEGE
UNION
SELECT U.NAME, NULL, SUBSTR(SPM.NAME,1,27)
FROM SYS.SYSTEM_PRIVILEGE_MAP SPM, SYS.SYSAUTH$ SA, SYS.USER$ U
WHERE SA.GRANTEE#=U.USER#
AND SA.PRIVILEGE#=SPM.PRIVILEGE
/
SELECT * FROM SYS.DBA_USER_PRIVS WHERE USERNAME NOT IN ('DBA', 'SYS',
'SYSTEM', 'IMP_FULL_DATABASE', 'RECOVERY_CATALOG_OWNER', 'OUTLN')
AND USERNAME NOT IN
(SELECT ROLE FROM DBA_ROLES)
SELECT 'USUARIO/ROLE: '||GRANTEE||' TIENE PERMISO DE '||PRIVILEGE||' SOBRE LA TA-
BLA '||TABLE_NAME||'.'
FROM DBA_TAB_PRIVS WHERE GRANTEE NOT IN
('SYS','SYSTEM','MARIVI','GCORRADO','GCORRADO1')
ORDER BY GRANTEE,PRIVILEGE
```

Listado: PRIV_ROLE_OBJECT_TO_USER

Listados de Roles otorgados a los usuarios:

```
SELECT GRANTEE USUARIO,GRANTED_ROLE ROLE
FROM DBA_ROLE_PRIVS
ORDER BY GRANTEE,GRANTED_ROLE
```

Listado: ROLE_TO_USER

Listado de Roles comunes existentes:

```
SELECT * FROM DBA_ROLES WHERE ROLE NOT IN ('CONNECT', 'RESOURCE', 'DBA',
'SELECT_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE', 'DELETE_CATALOG_ROLE',
'SQLNAV_ADMIN', 'IMP_FULL_DATABASE', 'RECOVERY_CATALOG_OWNER',
'AQ_ADMINISTRATOR_ROLE',
'AQ_USER_ROLE', 'SNMPAGENT', 'EXP_FULL_DATABASE');
```

Listado: USER_ROLES

28. Asegurarse que el parámetro *ut_file_dir* en *V$PARAMETER* no está seteado a *, o al mismo valor que el parámetro *user_dump_dest*

29. Restringir tanto como sea posible los permisos sobre las tablas y vistas SGA. Los usuarios ordinarios no deberían acceder a las tablas *X$*, *DBA_ views* o *V$ views* y las mismas contienen información sensitiva

30. Limitar tanto como sea posible el acceso a *ALL_USERS* y *ALL_% views*

31. Restringir acceso a SYS.AUD$, SYS.USER_HISTORY$, SYS.LINK$, SYS_USER$, SYS.RESOURCES$, PERFSTAT.STAT$SQLTEXT,

PERFSTAT.STATS$SQL_SUMMARY, ALL_SOURCE, DBA_ROLES,

DBA_SYS_PRIVS, DBA_ROLE_PRIVS, DBA_TAB_PRIVS, DBA_USERS,

ROLE_ROLE_PRIVS, USER_TAB_PRIVS y USER_ROLE_PRIVS

32. Asegurar el acceso a *catalog roles* y d*ba roles views*.

33. Revocar privilegios de ejecución pública a: *utl_file, utl_tcp, utl_http, utl_snmp, dbms_random, dbms_lob, dbms_job, dbms_scheduler, owa_util, dbms_sql* y *dbms_sys_sql*

34. Revocar los roles de *CONNECT* y *RESOURCE* de todos los usuarios

35. Chequear todos los *links* de la BD y comprobar que no se almacenen contraseñas en texto claro

36. Configurar una contraseña segura para el *listener*

37. Quitar el parámetro *EXTPROC* y prevenir la administración no autorizada del listener en *listener.ora* seteando

ADMIN_RESTRICTIONS_LISTENER_NAME= ON

38. Emplear la tabla PRODUCT_PROFILES para hardenizar SQL*Plus

39. Setear tcp.validnode_checking, tcp.invited_nodes y tcp.excluded_nodes en protocol.ora (Oracle 8.i) o sqlnet.ora (Oracle 9.i, 10g)

40. Revocar tantos paquetes de PUBLIC como sea posible

41. Definir entornos de producción y desarrollo, usuarios y privilegios en cada entorno, procesos y responsables del pasaje de datos, estructura de datos y programas del entorno de producción a desarrollo, definir solicitud de pasaje de datos y accesos, definir control de los pasajes.

42. Los siguientes privilegios no deberían otorgarse a usuarios comunes ya que permiten el acceso a los objetos del usuario sys

SELECT_CATALOG_ROLE

EXECUTE_CATALOG_ROLE

DELETE_CATALOG_ROLE

SELECT ANY TABLE

Listado de usuarios que poseen el role:

```
select grantee Usuario,granted_role Role
from dba_role_privs
where granted_role in
('SELECT_CATALOG_ROLE','DELETE_CATALOG_ROLE','EXECUTE_CATALOG_ROLE',
'SELECT ANY TABLE')
and grantee not in ('DBA','SYS','SYSTEM', 'EXP_FULL_DATABASE','IMP_FULL_DATABASE')
order by grantee,granted_role
```

Listado: USUARIO_SEL_CATALOG

43. Auditar que el entorno de desarrrollo no pueda acceder al entorno de producción

44. Habilitar auditing según lo sugerido en la siguiente tabla:

Action	Description	Severity Level	O/S	Oracle Version	Default Install
4.	**Auditing**				
4.1.1	Configure audit and storage.	2	ALL	ALL	
4.2.1	Audit insert failures on critical objects	2	ALL	ALL	
4.2.2	Use triggers to capture login events	2	ALL	ALL	YES
4.3.1	Audit create session	2	ALL	ALL	YES
4.3.2	Audit use of all grant privileges.	2	ALL	ALL	YES
4.3.3	Audit the use of all drop statements	3	ALL	ALL	
4.3.4	Audit the use of all alter statements	2	ALL	ALL	
4.3.5	Audit the use of create user	3	ALL	ALL	YES
4.3.6	Audit use of create role	3	ALL	ALL	
4.3.7	Audit all create statements	3	ALL	ALL	
4.3.8	Establish procedures to review audit logs	3	ALL	ALL	YES
4.3.9	Use Log Miner to audit in the case of forensics	4	ALL	ALL	
4.4.1	Configure basic audit	2	ALL	ALL	
4.4.2	Limit users who can change the audit trail	2	ALL	ALL	YES
4.4.3	Protect the audit trail	2	ALL	ALL	YES
4.4.4	Backup the audit trail	3	ALL	ALL	YES
4.4.5	Purge the audit trail	4	ALL	ALL	YES
4.4.6	Audit all SYS operations	1	ALL	>=9iR2	YES
4.5.1	Check date / time stamps on database objects	3	ALL	ALL	
4.6.1	Ensure reports and alerts are in place to deal with irregularities found through audit	3	ALL	ALL	YES
4.7.1	Use triggers for row level auditing	3	ALL	ALL	
4.7.2	Use VPD, RLS and label security for full data protection	3	ALL	>= 8	
4.8.1	Be aware of possible failure to be alerted of suspicious activities	2	ALL	ALL	YES
4.9.1	Be aware of possible failure to audit the security profile.	2	ALL	ALL	
4.10.1	Audit and review the Oracle generated log files	2	ALL	ALL	

4. Referencias

1) http://www.petefinnigan.com/orasec.htm

2) http://www.boran.com/security/sp/Solaris_hardening4.html

3) http://www.dba-oracle.com/articles.htm#burleson_arts

4) http://www.dbasupport.com

5) http://www.appsecinc.com/techdocs/whitepapers.html

6) Implementing Database Security and Auditing. Ron Ben Natan, Elsevier Digital Press 2005.

Política standard para el uso compartido del servidor de archivos.

Fecha: 14/07/2005

Versión: 1.0

1. Objetivo

Utilizar bajo las mismas normas el servidor de archivos con el objeto de reglamentar los nombres de archivos que se alojan en el mismo y facilitar el procedimiento de back up de todos los archivos.

2. Introducción

Cada vez que se guarde un archivo en el servidor de archivos, se debe seguir esta guía para no generar incompatibilidades a la hora de realizar un back up.

A su vez, evitar malformaciones en los nombres de archivo debido a las limitaciones del equipo de back up.

3. Reglamentación

- No utilizar tildes, acentos u otros símbolos o caracteres especiales.
- Sólo utilizar números, letras minúsculas sin la «ñ» y letras mayúsculas sin «Ñ».
- Utilizar una nomenclatura con un máximo de 32 caracteres.

4. Implementación

Se brindará a los usuarios del servidor de archivos 2 semanas de tiempo para verificar que sus archivos se adapten a las normas mencionadas. Luego de dos semanas de la fecha de entrega de esta política, se reemplazarán los archivos que no cumplan con estas condiciones de la siguiente manera:

Se recortará el largo del nombre a 32 caracteres.

Se cambiarán todos los acentos, tildes y caracteres especiales por un guión medio "-".

Procedimiento de Instalación y Configuración Checkpoint Secure-Client para conexión a aplicativos vía VPN.

Fecha: 10/01/2006

Versión: 1

1. Objetivo

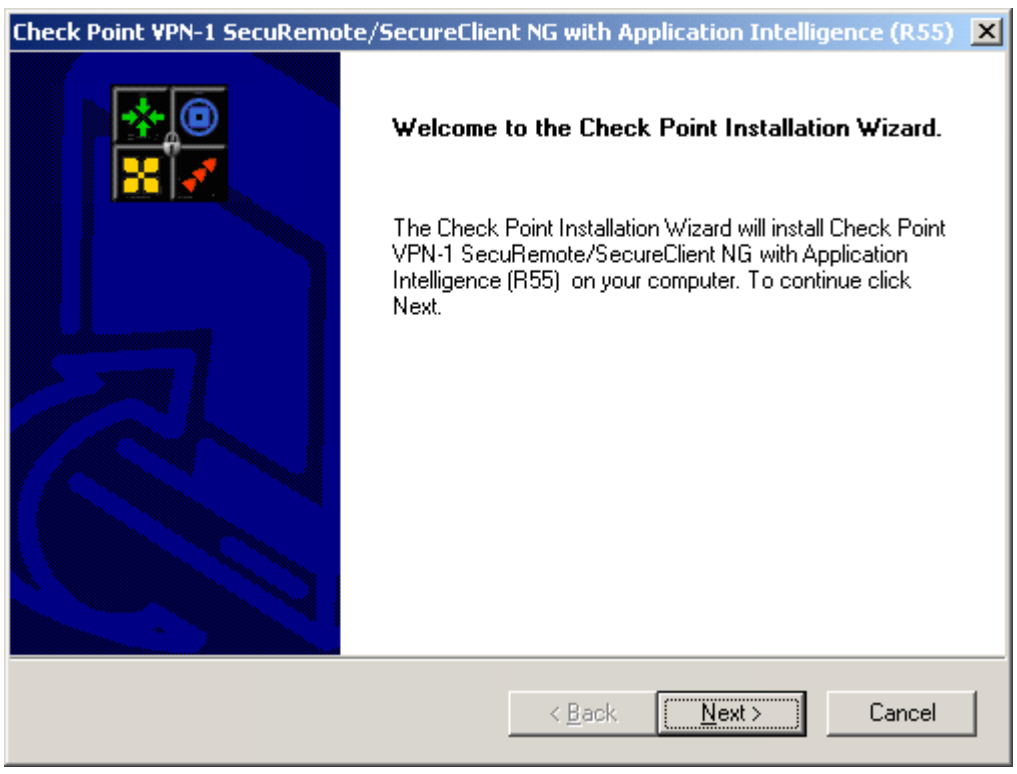
Proveer a las personas autorizadas, la documentación necesaria para la instalación, configuración y utilización de la red privada virtual. Esta última dependerá de las políticas asignadas a cada persona en el Policy Server administrado por Seguridad Informática.

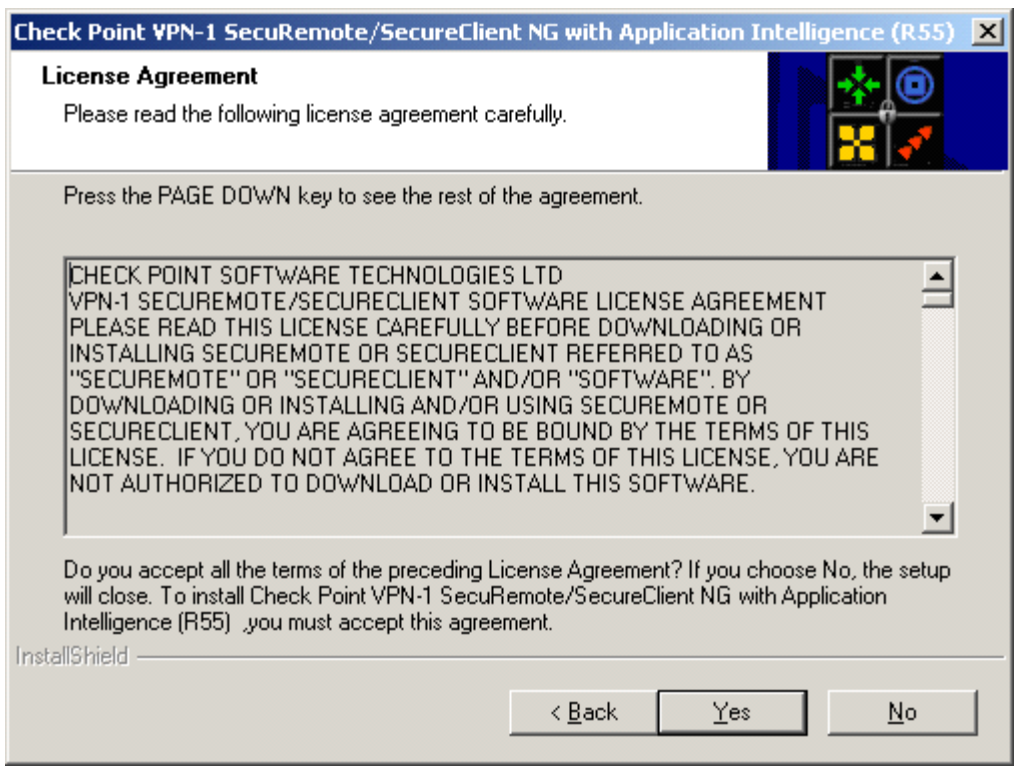
2. Introducción

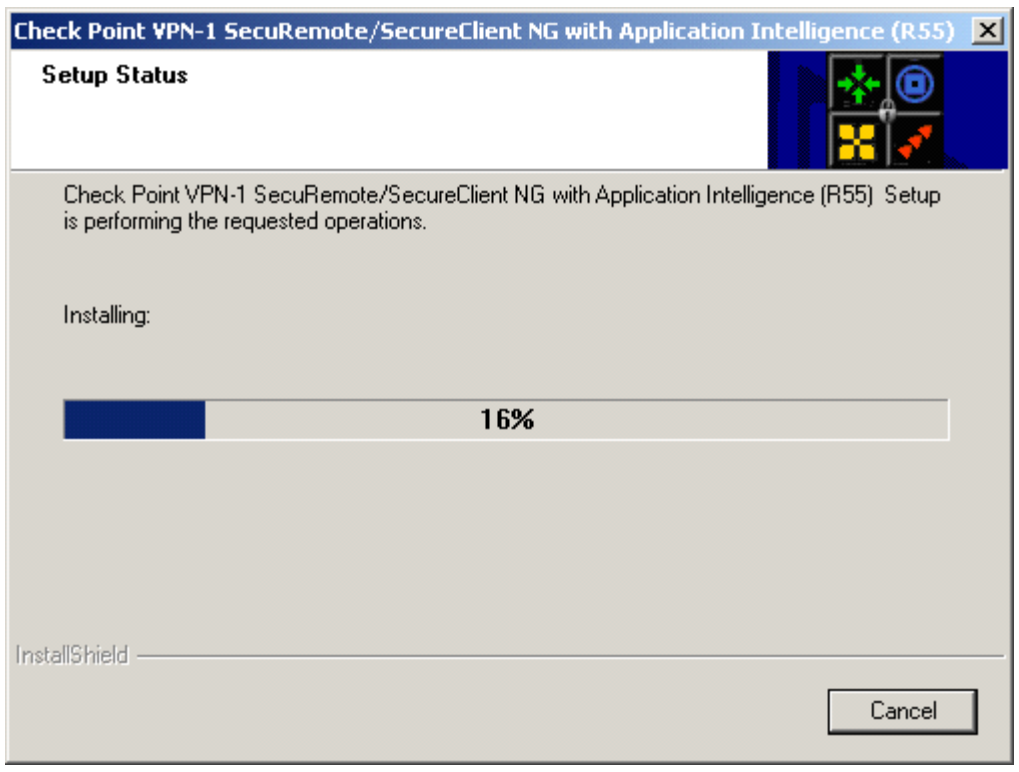
Es necesario instalar un programa denominado Secure-Client para poder acceder al aplicativo Rubad. Los pasos a seguir se describen detalladamente en este documento.

3. Instalación Secure Client

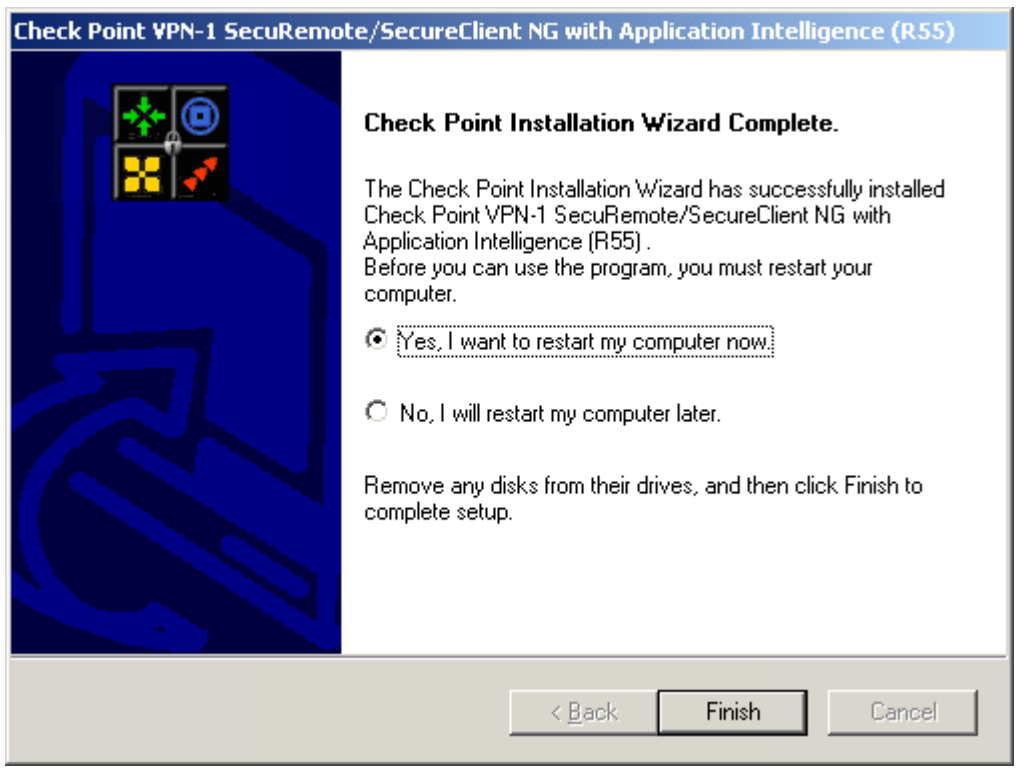
A continuación se muestran las pantallas que se irán sucediendo.







Es necesario reiniciar el equipo para que funcione correctamente

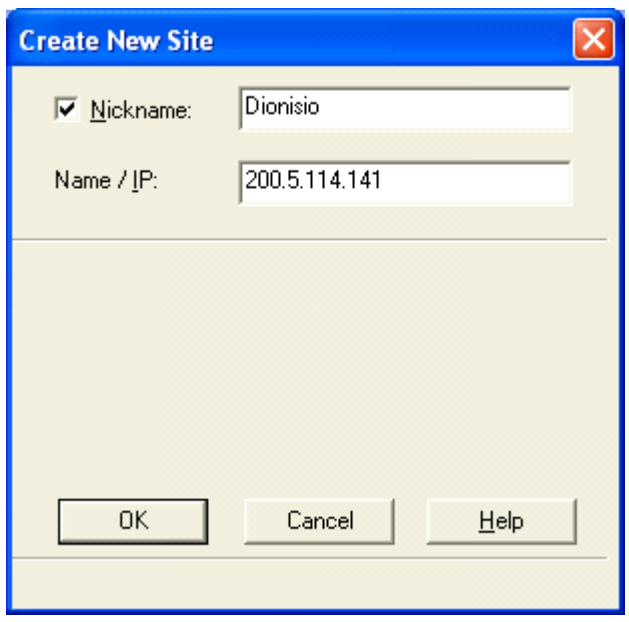


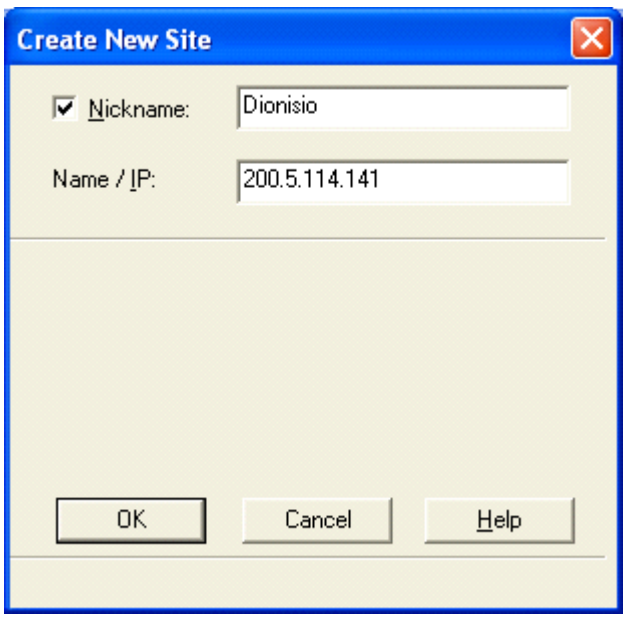
4. Conexión al Sitio a través de Secure Client

Luego de reiniciar aparecerá un nuevo icono en la barra de tareas, el mismo hace referencia al SecureClient. Con botón derecho seleccionar Open.

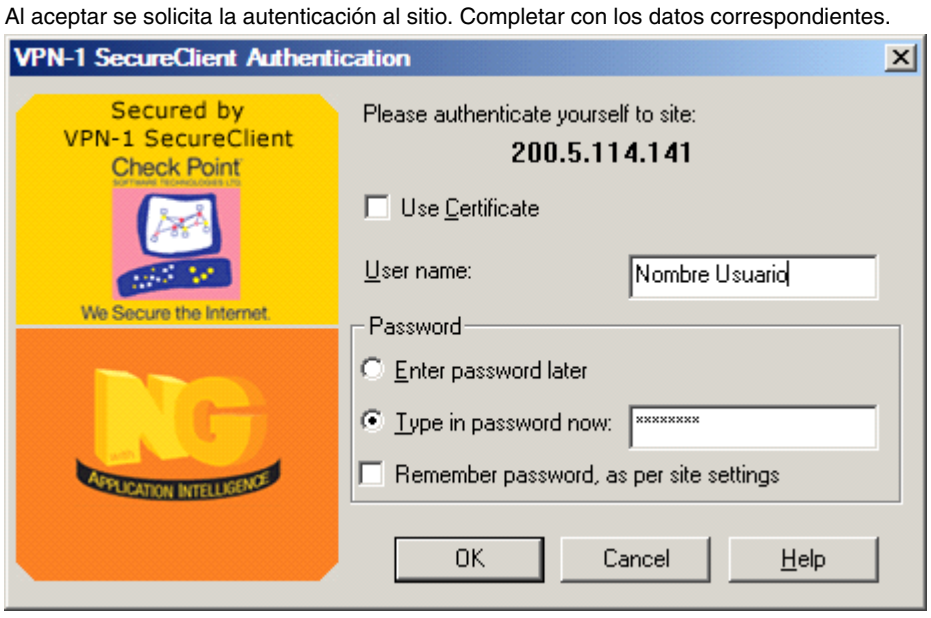
Ir al menú Tools-Configure Client Mode y elegir Connect Mode.

Una vez realizado esto, ir al menú Sites-Create New y completar la ventana que se abre tal y como se muestra a continuación:

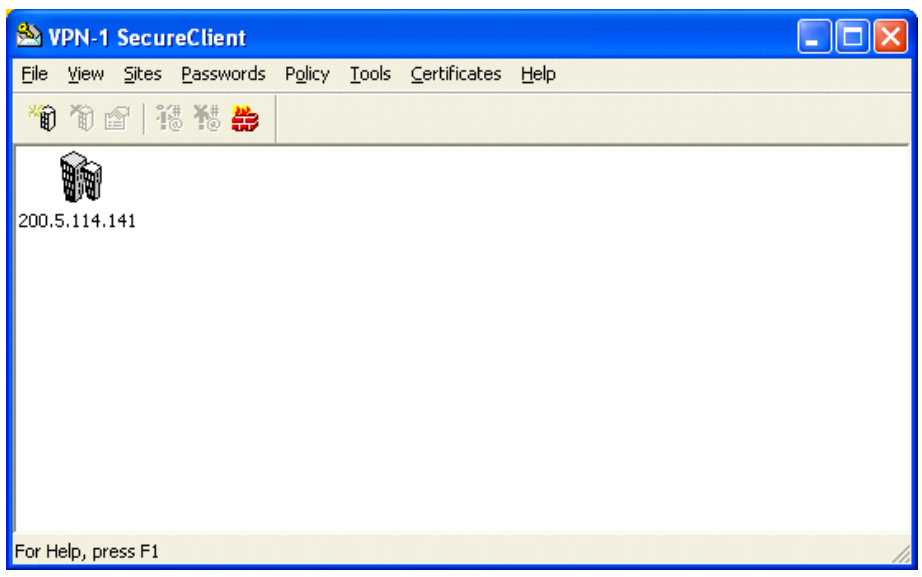




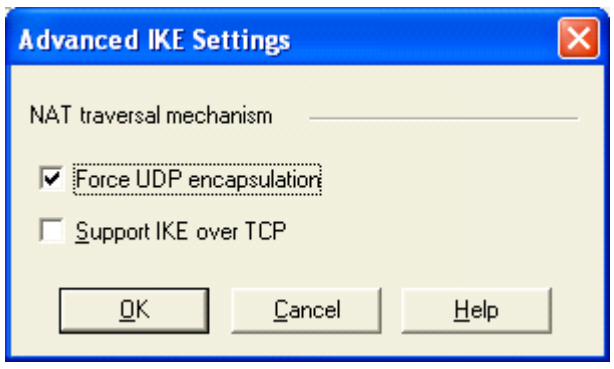
Al aceptar se solicita la autenticación al sitio. Completar con los datos correspondientes.



Hacer click en Ok y en segundos quedará establecida la conexión al sitio:

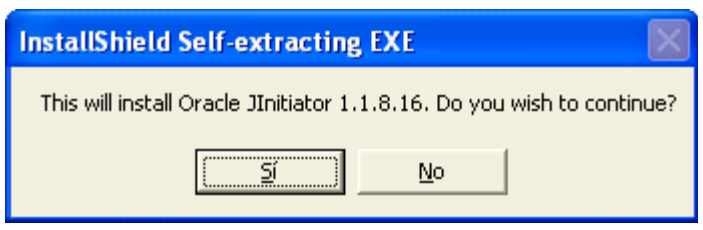


Por último en el menú Tools-Advanced IKE Settings, tildar la opción Force UDP Encapsulation.

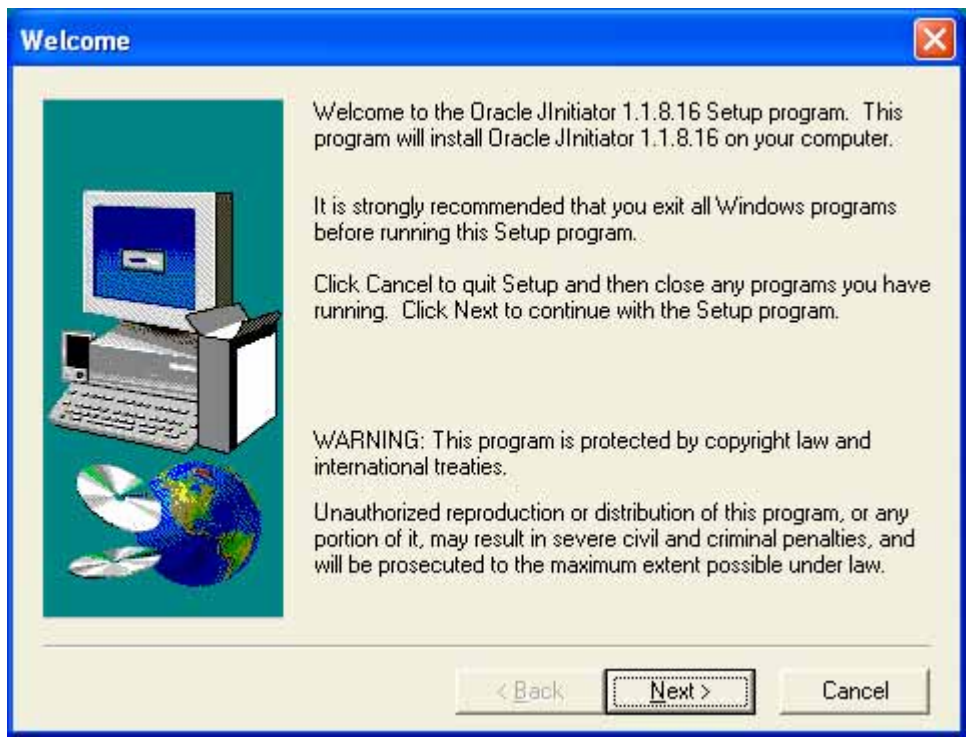


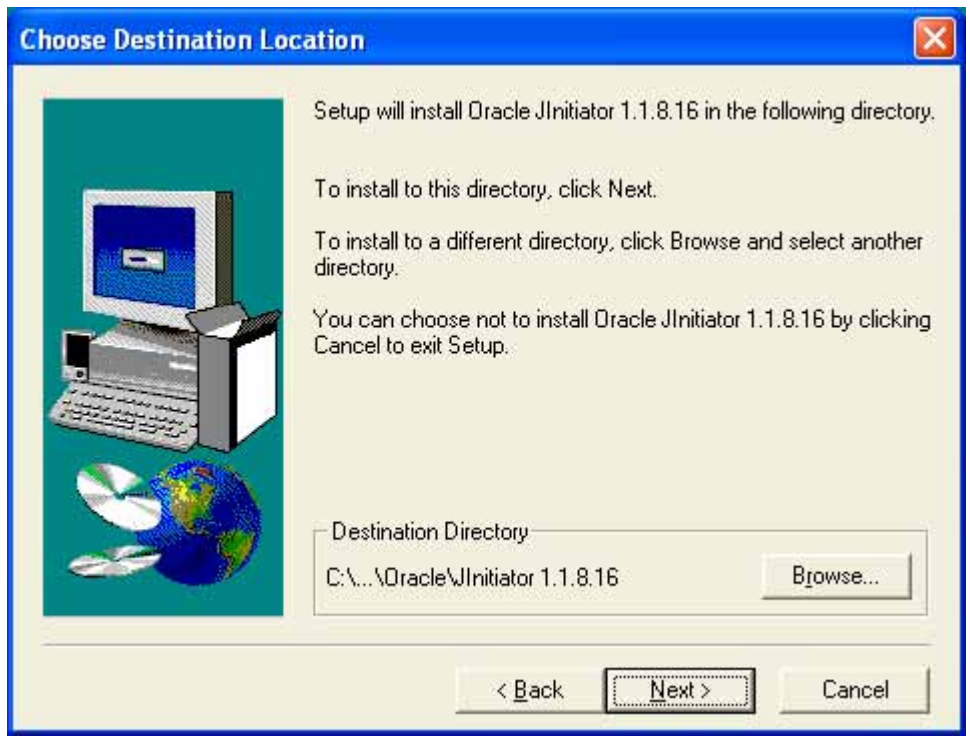
5. Instalación Jinitiator

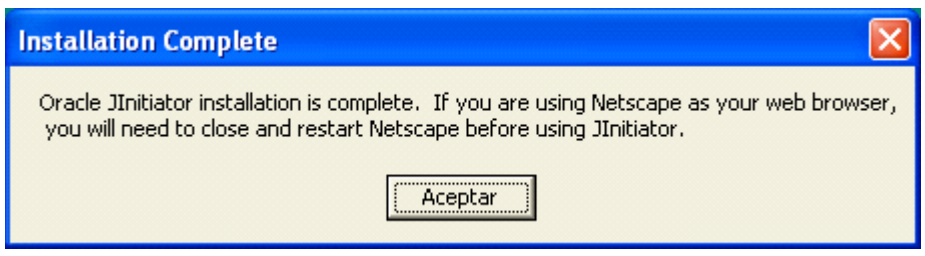
Dentro del CD provisto ejecutar el archivo “jinit11816.exe”, aparece un aviso diciendo que se instalará el Oracle JInitiator y aceptar.



Seguir las pantallas del asistente tal y como se indica a continuación:







Completada la instalación del JInitiator, se deberá editar el archivo c:\windows\system32\drivers\etc\hosts para agregarle la siguiente línea al final:

10.64.96.220 oraser oraser.sintys.gov.ar

Guardar y cerrar el archivo hosts.

Procedimiento de administración de usuarios externos.

Fecha: 23/08/2005

Autor: Matías Livachof (mlivachof@sintys.gov.ar), Lorena López (llopez@sintys.gov.ar), Guillermo Marro (gmmarro@sintys.gov.ar)

Versión: 1.1

1. Objetivo

Administrar y otorgar ordenadamente permisos de acceso externo a través de las reglas del Firewall a usuarios que utilizan el servicio ssh para transferir datos al servidor SFTP de SINTyS.

2. Introducción

Se cuenta con dos tipos de usuarios externos:

Usuarios externos con dirección IP estática.

Usuarios externos con dirección IP dinámica.

A ambos se le asignan los mismos permisos, pero al ser distinta la modalidad de acceso al sistema, las medidas a tomar serán diferentes.

3. Implementación

Usuarios externos con dirección IP estática:

Se creará el usuario como un objeto de nuestra plataforma de filtrado y se le permitirá utilizar el servicio ssh hacia el servidor SFTP, empleando dichos objetos para la semántica de las reglas.

Usuarios externos con dirección IP dinámica:

Se creará como usuario de Secure Client.

Se crearán las reglas de Desktop Security correspondientes a los servicios que el usuario requiera.

Se iniciará el proceso de creación de un certificado y el usuario deberá completar el trámite al momento de la primera conexión con la contraseña que será enviada en sobre sellado por correo postal ordinario.

Se le asignará y enviará al usuario un e-token "Aladdin" en donde almacenará el certificado una vez finalizado el trámite.

Procedimiento de prueba y escaneo de vulnerabilidades de equipos servidores.

Fecha: 19/08/2005
Autor: Matías Livachof (mlivachof@sintys.gov.ar), Lorena López (llopez@sintys.gov.ar), Guillermo Marro (gmmarro@sintys.gov.ar).
Versión: 1.1

1. Objetivo

Revisar periódicamente los servidores críticos del proyecto SINTyS en busca de posibles vulnerabilidades de software, de manera tal que se puedan llevar a cabo las correcciones del mismo en forma proactiva.

Analizar la respuesta a ataques internos y externos de los servidores de datos críticos del syntys.

2. Introducción

Se definirá un régimen de controles específicos donde se verificará:

Servicios que atiende el servidor.

Puertos abiertos indebidamente.

Vulnerabilidades de software detectables en forma remota.

3. Herramientas

Se utilizarán las siguientes herramientas de software:

Nessus

nmap

tcpdump

ethereal

xprobe2

4. Implementación

Se consensuará un día y horario de prueba [semanal/mensual/bimestral] entre las áreas equipos, comunicaciones, bases de datos y seguridad.

Se efectuarán los test correspondientes con una de las herramientas listadas en el punto 3.

Se analizarán los resultados obtenidos en busca de vulnerabilidades que posea el equipo respecto a posibles ataques y amenazas externas e internas.

Se enumerarán soluciones y medidas para prevenir que estos equipos sean comprometidos. Se comunicará de dichos resultados a los responsables del mantenimiento operativo de dichos sistemas.

Procedimiento de ABM de usuarios.

Fecha: 11/10/2005

Versión: 0.1

1. Introducción

Para controlar y mantener una base de datos formal, se documentarán los pasos necesarios para las tareas referidas a la administración de usuarios (Altas, bajas y modificaciones).

2. Objetivo

Se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información para impedir el acceso no autorizado a la información

3. Implementación

Alta de usuario:

1. El coordinador del área que incorporará un nuevo usuario deberá completar el formulario Form-105 y será el responsable de solicitar la asignación y uso de privilegios para que el nivel de acceso otorgado sea el adecuado y no comprometa las políticas de seguridad de Sintys. Luego debe firmar el formulario y entregarlo al área de equipos (componente infraestructura)

2. El responsable de equipos deberá asignarle una dirección IP y asocialar con la dirección MAC del equipo que utilizará.

3. El responsable de equipos asignará una cuenta de correo electrónico con una contraseña provisoria que el usuario deberá modificar antes de comenzar a utilizar el correo. Deberá ser dado de alta en las listas de correo correspondientes. También asignará los permisos requeridos para el servidor de archivos compartido.

4. El responsable de equipos debe completar los datos del equipo y la dirección de correo en el formulario Form-105, firmarlo y entregar el formulario al administrador del servidor Proxy de internet.

5. El administrador del Proxy de internet, ingresará a la dirección IP del equipo del usuario para que pueda utilizarlo. Luego entregará el formulario a Bases de Datos.

6. El responsable de Base de Datos deberá ingresar el usuario a las bases de datos solicitadas, verificar que los accesos requeridos sean adecuados para el perfil de usuario que se incorpora y asignarle los permisos requeridos. Luego debe firmar el formulario Form-105 y entregarlo a área de seguridad informática.

7. El responsable de seguridad informática ingresará el usuario en el Firewall. Otorgará los permisos correspondientes a cada solicitud de acceso y los servicios necesarios. Luego debe firmar el formulario Form-105, verificar que todos los campos del formulario hayan sido completados y firmados y lo almacenará bajo llave.

Modificación de usuario:

1. El coordinador del área del usuario que necesita una modificación de accesos respecto de los que fueron asignados al momento del alta, o en modificaciones anteriores, deberá completar el formulario Form-105 y será el responsable de solicitar la asignación y uso de privilegios para que el nivel de acceso otorgado sea el adecuado y no comprometa las políticas de seguridad de Sintys. Luego debe firmar el formulario y entregarlo al área que corresponda el cambio:

Dirección de mail, Servidor de archivos, corresponde al área Equipos.

Datos de equipo, corresponde al área equipos y seguridad informática.

Acceso a base de datos, corresponde al área de base de datos y seguridad informática.

2. El formulario debe contar con las firmas de:

Coordinador sustantivo.

Coordinador infraestructura

Usuario.

Seguridad Informática.

Y de las áreas a las que aplique la modificación.

3. Las tareas de cada responsable de área, corresponden a las descriptas en el procedimiento de alta.

El responsable de seguridad informática almacenará el formulario bajo llave.

Baja de usuario:

1. El responsable de administración iniciará el trámite de baja de usuario al presentarse un retiro.

Deberá completar el formulario Form-105 con el nombre y datos personales del usuario y su correspondiente firma. Luego entregará el formulario a seguridad informática.

2. El responsable de seguridad informática verificará los accesos ya otorgados al usuario y hará circular el formulario a las áreas correspondientes. Eliminará al usuario del firewall. En el caso de que el usuario tuviese acceso a bases de datos, utilizará la aplicación de baja de usuarios de bases de datos.

3. Verificará que todas las firmas estén en el formulario y se almacenará bajo llave.

Política de ABM de usuarios.

Fecha: 14/10/2005

Versión: 0.1

1. Introducción

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del Organismo, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

2. Alcance

1.- Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos (Servidor Proxy).

2.- Limitar las opciones de menú y submenú de cada uno de los usuarios.

3.- Evitar la navegación ilimitada por la red.

4.- Controlar activamente las comunicaciones con origen y destino autorizados a través del firewall.

5.- Restringir el acceso a redes, estableciendo dominios lógicos separados.

3. Implementación

El Responsable de Seguridad Informática y los responsables de cada área de infraestructura tendrán a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del Coordinador del componente que lo solicite para personal de su incumbencia.

Política de resguardo y correlación de logs de seguridad de servidores en equipo dedicado Syslog.

Fecha: 23/08/2005

Versión: 1.1

1. Objetivo

Centralizar la recepción de logs de seguridad de los equipos críticos de SINTyS por las siguientes razones:

1.- Resguardar los archivos de log.

2.- Mantener una secuencia cronológica de las actividades que se efectúen en los equipos.

2. Introducción

Se identificarán los logs de seguridad que realicen los equipos para obtener información y enviarla al equipo Syslog acerca de:

Accesos a recursos críticos del sistema

Mensajes de error o anomalías

Eventos de interés en seguridad informática

3. Implementación

Debe identificarse los equipos que deben estar resguardados por el Syslog basándose en los datos que éstos contienen. Deben estar incluidos los servidores de base de datos, servidor de correo, firewall perimetral, firewall propio de los equipos (en caso de que éstos lo posean), servidores de control de acceso, proxy y todo servidor de misión crítica.

Se deberá editar el archivo /etc/syslog.conf e indicar que los logs de seguridad sean reenviados al equipo Syslog.

A los efectos de segmentar lógicamente la red para mitigar el riesgo de sniffing de tráfico, se diseñará un canal fuera de banda para aislar el tráfico syslog de posibles intrusos. En principio, se creará una VLAN especial a tal fin.

Política de Asignación de Accesos a VUO para Usuarios Internos y Externos.

Fecha: 05/08/2005

Versión: 1.0

1. Objetivo

Definir un método satisfactorio de registración de usuarios habilitados al sistema VUO (Ventanilla Unica de Organismos). Mantener un inventario de permisos de accesos vigentes al sistema, diferenciando entre usuarios SINTyS y usuarios externos (organismos autorizados).

2. Introducción

Existen dos tipos de usuarios, internos y externos, ambos deberán completar según corresponda el formulario 110e (para usuarios externos) y 110i (para usuarios internos) previo a la habilitación, y se deberá renovar el acceso a usuarios existentes mediante el mismo formulario.

3. Reglamentación

Todos los elementos descriptos a continuación deben ser cumplimentados, de no ser así, la habilitación no podrá llevarse a cabo.

El formulario lleva los siguientes datos:

1.- De la persona:

Nombre y apellido.

Documento de identidad.

Componente u organismo.

Area.

2.- Del acceso

Tipo de Solicitud (alta o baja).

Permisos de acceso:

a.- Completo.

b.- Consulta Total.

c.- Consulta Binaria.

d.- Consulta Fiscal.

e.- Consulta Total sin Montos.

Tipo de acceso (temporal / permanente) En el caso de ser temporal de deberá especificar la fecha de inicio y finalización del acceso.

Motivo de la solicitud.

3.- De autorización

Firma de Jefe inmediato superior o Coordinador.

Firma de Usuario.

Firma de Responsable de Seguridad Informática.

Firma de Coordinador de Infraestructura.

Firma de Administrador de cuentas VUO (Infraestructura) (al completar la solicitud)

Se deberá adjuntar fotocopia de la 1ra y 2da hoja del DNI de Usuario

Se deberá adjuntar nota formal de solicitud de acceso del Usuario.

Una vez recibido un formulario de baja de usuario debidamente completo (con la excepción de la firma del Administrador de cuentas VUO, la cual se realizará al completarse la solicitud), deberá asegurarse el proceso de inhibición del usuario en cuestión en el lapso de 24 horas hábiles a partir de la recepción de dicho formulario.

El administrador de cuentas VUO deberá notificar por correo electrónico a seguridad@sintys.gov.ar la fecha y hora de realización de los cambios.

Política de Ventanas de Mantenimiento para Actualización de Reglas de Firewall.

Fecha: 03/08/2005

Versión: 1.0

1. Objetivo

Limitar y regularizar las operaciones de cambio de reglas de servicios del Firewall perimetral para evitar posibles inconvenientes que pudieran surgir al momento de compilación e instalación de las mismas.

Mejorar la disponibilidad en el ambiente de producción. Reducir el impacto sobre la operatoria normal que los cambios en la configuración del Firewall pudieran causar.

Formalizar los pasos a producción de un nuevo set de reglas del Firewall, restringidos a ventanas de mantenimiento ordinaria y extraordinaria, dependiendo de la urgencia en la necesidad de los cambios pertinentes.

2. Introducción

Se definirán dos tipos de ventana de mantenimiento:

• Ventana de Mantenimiento Ordinaria (VMO), en donde se agruparán los pedidos ordinarios que no revistan urgencia en su implementación.

• Ventana de Mantenimiento Extraordinaria (VME), para tareas de necesidad inmediata y/o crítica

3. Reglamentación

VMO: Ventana de Mantenimiento Ordinaria:

Consiste de 2 horas semanales distribuidas en horarios de bajo impacto productivo para poder compilar e implementar cambios en el set de reglas del FW. Se elige en principio los días lunes y jueves de 19:00 a 20:00 hs, para minimizar el posible (aunque no tan probable) impacto que estos cambios puedan tener en producción.

VME: Ventana de Mantenimiento Extraordinaria:

Pensada para casos de excepción, donde los cambios necesarios en el set de reglas del FW no puedan esperar hasta la próxima VMO para implementarse. Se utilizará esta lista de distribución (VME@sintys.gov.ar) para comunicar con antelación mínima de 15 minutos la próxima implementación de un VME, comunicando además en forma verbal a las DBA de la actuación pertinente, a fin de que puedan tomarse los recaudos necesarios para evitar trastornos indeseables.

Política de uso de Redes Privadas Virtuales (VPN)

Fecha: 10/10/2005

Versión: 0.1

1. Objetivo

El propósito de esta política es el de sentar los lineamientos generales de acceso vía VPN a los recursos corporativos del SINTyS.

2. Alcance

Esta política aplica a todos los consultores vinculados al SINTyS, así como también a terceras partes que cuentan con la apropiada autorización y que acceden remotamente a algún recurso informático del SINTyS vía VPN.

3. Política

Los consultores contractualmente vinculados al programa y terceras partes autorizadas por la dirección del SINTyS pueden hacer uso de un subconjunto de los recursos informáticos del SINTyS a través del acceso remoto vía VPN. Las terceras partes autorizadas son responsables de seleccionar un proveedor ISP y un enlace de conexión apropiados. El SINTyS por su parte otorgará el software cliente necesario para hacer uso de la plataforma VPN, como así también en ciertos casos y a sólo criterio de la dirección del programa SINTyS, tokens de autenticación vía certificados digitales.

Adicionalmente:

1. Es responsabilidad de los usuarios (consultores o terceras partes) con privilegio de acceso a VPN impedir el acceso no autorizado a la red del SINTyS empleando las credenciales de autenticación a ellos/as otorgadas.

2. La operación de los nodos concentradores VPN en UCSN y UPCS serán entera responsabilidad del subcomponente Seguridad Informática.

3. El esquema de autenticación para acceso a la red VPN será escogido por el SINTyS, y cuando los recursos así lo permitan, se basará en certificados digitales administrados por el subcomponente Seguridad Informática y almacenados en tokens electrónicos.

4. Durante el acceso a la red VPN del SINTyS, se bloqueará acceso a otro tipo de red WAN en el cliente remoto vía la instalación de políticas de escritorio que se gestionan desde UCSN y se aplican en los clientes remotos.

5. Un único túnel VPN puede establecerse por cliente remoto por vez. Intentos de establecer otros túneles simultáneos se prohibirán y se registrarán como actividad maliciosa.

6. Es exclusiva responsabilidad de los usuarios de VPN asegurarse que las medidas de seguridad informática mínimas discutidas en los documentos de hardening de sistemas operativos para máquinas de escritorio están aplicadas en los terminales desde los cuales se intenta acceder a la red VPN. Toda actividad maliciosa registrada en el concentrador VPN proveniente del terminal remoto VPN será exclusiva responsabilidad del usuario remoto, ya que al conectarse en forma remota, dicho terminal pasa a ser parte integrante de la infraestructura informática del SINTyS y por ende debe regirse bajo las mismas políticas de seguridad.

7. Los túneles VPN se desconectarán unilateralmente desde UCSN al cabo de 10 minutos de inactividad.

8. La utilización de software no suministrado por el SINTyS para intentar acceder a la plataforma VPN será considerado actividad maliciosa.

9. La disponibilidad de la red VPN es responsabilidad exclusiva del SINTyS, quien compromete su mejor esfuerzo para garantizar la operación adecuada. De ninguna manera puede asumirse que la red VPN estará disponible en modalidad 24/7/12.

10. El SINTyS se reserva el derecho unilateral a terminar la operación de la red VPN en cualquier momento sin previa notificación a terceras partes, no pudiendo ser objeto por ello de reclamos de ninguna índole.

11. El SINTyS se reserva el derecho a auditar todo tipo de acceso VPN a su sólo criterio

4. Incumplimiento

El incumplimiento de esta política puede derivar en cualquiera de las siguientes medidas

1. Revocación de privilegios de acceso

2. Sanciones disciplinarias para consultores del SINTyS, pudiendo llegar a la desvinculación contractual immediata y eventual procesado legal.

3. Procesado legal a terceras partes según lo indicado en la legislación vigente.

5. Terminología

VPN: Redes Privadas Virtuales

UCSN: Unidad Coordinadora SINTyS Nación

UPCS: Unidad Provincial Coordinadora SINTyS

ISP: Internet Service Provider

Política de seguridad física en UPCS

Fecha: 08/11/2005

Versión: 0.3

1. Objetivos

El propósito de esta política es el de sentar los lineamientos generales de protección física en nodos SINTyS provinciales (UPCS). A tal efecto se presentan dos esquemas, mínimo y óptimo, dentro de los cuales deberán enmarcarse las dependencias UPCS.

La protección física comprende los siguientes aspectos:

• Prevenir e impedir accesos no autorizados, daños e interferencias en las dependencias UPCS

• Proteger el equipamiento de procesamiento de información crítica de la UPCS ubicándolas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

• Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento de procesamiento de información.

• Implementar medidas para proteger la información manejada por los consultores, en el marco normal de sus actividades naturales.

2. Alcance

Esta política aplica a la protección de todos los recursos informáticos (los equipos de procesamiento de la información, instalaciones, cableado, expedientes, medios de almacenamiento, etc) destinados en dependencias provinciales (UPCS), tanto sea en las oficinas de los consultores como en el CPD propio o ajeno donde se alojan los equipos servidores y de comunicación del SINTyS,

3. Responsabilidades

El responsable del área de seguridad informática junto al coordinador del componente Infraestructura tienen responsabilidad sobre la confección y actualización de la presente política y de gestionar la implementación de las medidas protectivas que se desprenden de la misma, basados en el análisis de riesgos sobre las distintas UPCS y su contexto. Asimismo, ambos responsables o personal por ellos delegado, deberán efectuar visitas no anunciadas con una frecuencia no mayor a la semestral por las distintas UPCS, a fin de auditar el cumplimiento de la presente política.

El responsable informático de la UPCS, junto al coordinador de la UCPS serán los/las encargados/as de velar por el cumplimiento de la presente política y deberán notificar con carácter de urgencia al área de seguridad informática (seguridad@sintys.gov.ar) sobre violaciones a la misma.

Los consultores asignados en las distintas UPCS deberán cumplir la presente política, informando a los responsables de la UPCS o al área de seguridad informática sobre violaciones a la misma.

4. Políticas

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las salas donde se albergan las estaciones de trabajo del personal de la UPCS y de las instalaciones de procesamiento de información (de aquí en adelante, recintos SINTyS). Todos los recintos SINTyS deberán ser de uso exclusivo de la UPCS.

La UPCS utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Area Informática con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.

b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

Recinto\Esquema	*Optimo*	*Mínimo*
CPD	Mecanismo de control de acceso basado en sistemas de doble factor, con alarma antiviolación.	Area de recepción con atención permanente de personal de custodia, que registrará ingresos y egresos de terceros autorizados por el personal informático del SINTyS
Sala de Consultores	Area de recepción con atención permanente de personal de custodia, que registrará: • ingresos y egresos de terceros autorizados por el personal informático del SINTyS • Bolsos, carteras, maletines o equipaje en general del personal de la UPCS, para evitar el hurto de material del trabajo del SINTyS	Mecanismo de control de acceso basado en cerraduras convencionales (llaves exclusivamente en poder de responsables designados por el coordinador de la UPCS)

Tabla 1: Control de Acceso a Recintos SINTyS

c) Identificar claramente todas las puertas de incendio de un perímetro de seguridad. El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

i) Identificación del Edificio y Area.

ii) Principales elementos a proteger.

iii) Medidas de protección física.

Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el Responsable del Area Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los controles de autenticación para autorizar y validar todos los accesos definidos en la tabla 1. Se mantendrá un registro protegido para permitir auditar todos los accesos.

d) Revisar y actualizar cada 6 meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la UPCS de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Protección de Recintos, Oficinas e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la UPCS

Areas Protegidas:

CPD

Salas de Consultores

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

e) Separar las instalaciones de procesamiento de información administradas por la UPCS de aquellas administradas por terceros.

f) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

g) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas de la UPCS. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.

h) Almacenar los equipos redundantes en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

i) Almacenar los resguardos de datos (backup) y toda otra información sensible como expedientes, CDs de datos y programas, etc en un armario bajo llave en poder exclusivo del coordinador de la UPCS.

Desarrollo de tareas en áreas protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.

c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el coordinador de la UPCS o personal de Seguridad Informática

g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

Aislamiento de las áreas de Recepción y Distribución

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la UPCS, sólo al personal previamente identificado y autorizado.

b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.

d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

e) Registrar el material entrante al ingresar al sitio pertinente.

Ubicación y Protección de Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.

c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

d) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada 6 meses

f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la UPCS

Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la UPCS. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

Para el esquema óptimo, se contempla la siguiente medida adicional:

c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto. Asimismo, se procurará que los interruptores de emergencia se ubiquen 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. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.

b) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa cable canal fijado a la pared.

c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles: uso de ductos que eviten áreas públicas

d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Area Informática. El Area de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

d) Registrar el retiro de equipamiento de la UPCS para su mantenimiento.

e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

Seguridad de los Equipos Fuera de las Instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la UPCS, será autorizado por el coordinador de la UPCS. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Coordinador del Componente Infraestructura.

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la UPCS para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la UPCS, cuando sea conveniente.

Desafectación o Reutilización de Equipamiento

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

Políticas de Escritorio

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información sensible o crítica de la UPCS (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

c) Desconectar de la red/sistema/servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de la UPCS sin autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la UPCS, las que serán llevadas a cabo por personal del componente Infraestructura. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

4. Incumplimiento

El incumplimiento de esta política puede derivar en cualquiera de las siguientes medidas

1. Revocación de privilegios de acceso sobre consultores SINTyS, proveedores o soporte técnico autorizados por el SINTyS.

2. Sanciones disciplinarias para consultores del SINTyS, pudiendo llegar a la desvinculación contractual inmediata y eventual procesado legal.

3. Procesado legal a terceras partes según lo indicado en la legislación vigente.

5. Terminología

UCSN: Unidad Coordinadora SINTyS Nación

UPCS: Unidad Provincial Coordinadora SINTyS

BOLETIN OFICIAL
DE LA REPUBLICA ARGENTINA

Presidencia de la Nación
Secretaría Legal y Técnica
Dirección Nacional del Registro Oficial

→ Nuevo servicio para la publicación de avisos comerciales y edictos judiciales
(excepto edictos sucesorios)

Trámite Urgente y Trámite Semi Urgente

Horario de recepción:

Sede Central
Suipacha 767
desde 11.30 hasta 13.30 hs.

Delegación Tribunales
Libertad 469
desde 8,30 hs. hasta 13.30 hs.

Delegación Colegio Público de Abogados
Avda. Corrientes 1441
desde 10.00 hasta 13.30 hs.

Delegación Inspección General de Justicia
Moreno 251
desde 9.30 hasta 12.30 hs.

Ciudad Autónoma de Buenos Aires

www.boletinoficial.gov.ar