2017

Presidencia de la Nación
Secretaría Legal y Técnica

Dirección General de Sistemas Informáticos

Procedimientos inherentes a la administración y control de los recursos informáticos.

INFORME FINAL N° 05/2017

Índice

"Procedimientos inherentes a la Administración y control de los Recursos Informáticos"

INFORME EJECUTIVO

SECRETARÍA LEGAL Y TÉCNICA
DE LA PRESIDENCIA DE LA NACIÓN

UNIDAD DE AUDITORÍA INTERNA
INFORME FINAL N° 05/2017

"PROCEDIMIENTOS INHERENTES A LA ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS INFORMÁTICOS"

1.- OBJETO

Verificar el cumplimiento de la responsabilidad primaria de la DGSI consistente en "Entender en la administración y control de los recursos informáticos de la Secretaría".

2- OBSERVACIONES Y RECOMENDACIONES:

Del análisis efectuado, surgen las observaciones que a continuación se exponen en orden decreciente, según el riesgo potencial que cada una representa:

2.1 Observación: Se observa la existencia de usuarios que permanecen activos, correspondientes a agentes desvinculados de esta Secretaría. Puntualmente, respecto del sistema PSA, sobre un total de 246 (doscientos cuarenta y seis) usuarios activos se detectaron 73 (setenta y tres) casos que corresponden a agentes desvinculados de esta SLYT, lo que representa el 29,67%. Ver Anexo III – 1. Procedimientos – 1.1 Alta, Baja y Modificación de Usuarios.

Opinión del Auditado: Se implementó un procedimiento recurrente mediante el cual se dan de baja todos los usuarios que no se hayan logueado al Active Directory/VPN por un plazo de 90 días. De esta forma se evitará volver a la situación mencionada, en paralelo se solicitará que RRHH informe de las Bajas correspondientes en tiempo y forma. De todas formas, al dar de baja al usuario en el Active Directory, el mismo no puede acceder a la red de la SLYT con lo cual, en el caso de los 73 usuarios mencionados, no hubieran podido acceder al sistema PSA, que por otro lado dejará de funcionar durante el corriente año.

Recomendación: Se recomienda revisar el procedimiento ABM, aplicable a la administración de usuarios (alta/baja/modificaciones) y al propio tiempo realizar una depuración de usuarios de los distintos sistemas a fin de dejar activos sólo aquellos que correspondan.

Grado de Impacto: Medio

2.2 Observación: Se observa que en el ámbito de la SLyT no se encontraría conformado el Comité de Seguridad de la Información que prescribe la Disposición 01/2015 de la ONTI. Ello, en razón de que la mayoría de los miembros designados oportunamente por Resolución 64/2014 - SLyT, no pertenecerían actualmente a esta Secretaría. Ver Anexo III. Punto 2. Análisis de la Política de Seguridad de la Información.

Opinión del Auditado: La conformación del comité de Seguridad de la Información es una competencia que no se encuentra dentro del alcance de la DGSI.

Recomendación: Se recomienda conformar un "Comité de Seguridad de la Información" en el ámbito de esta Secretaría, siguiendo para ello las pautas previstas a tal fin en la Disposición 1/2015 de la ONTI.

Grado de Impacto: Medio

2.3 Observación: Se observa que la Política de Seguridad de la Información de esta Secretaría que fuera aprobada el 12/8/2014, se habría fundamentado en prescripciones normativas que a esa fecha ya habrían sido derogadas. Ello, según se desprende de lo manifestado por el Comité de Seguridad de la Información, quien en el acápite "Introducción", menciona como fundamentos de la Política de Seguridad aprobada, a la Disposición Nº 6/2005 de la ONTI que a esa fecha habría sido derogada por la Disposición Nº 3/2013. Corresponde agregar que esta última norma, a su vez fue posteriormente derogada por la Disposición 1/2015 del mismo Organismo. Ver Anexo III. Punto 2. Análisis de la Política de Seguridad de la Información.

Opinión del Auditado: Se remite a la respuesta a la observación 2.2.

Recomendación: Se recomienda adecuar y actualizar la Política de Seguridad de la Información en función de la normativa vigente al momento de su adecuación.

Grado de Impacto: Medio

2.4 Observación: Se observa que en el ámbito de la SLyT no se estarían cumpliendo los parámetros relativos a compromisos de confidencialidad de la información del organismo, requeridos por las normas respectivas, para el caso la Disposición 1/2015 de la ONTI. Ver Anexo III. Punto 2. Análisis de la Política de Seguridad de la Información.

Opinión del Auditado: Se remite a la respuesta a la observación 2.2.

Recomendación: Se recomienda revisar el procedimiento aplicable para que los agentes de cualquier situación de revista acuerden formalmente respetar el compromiso de confidencialidad de la información del organismo y al propio tiempo formalizar los casos que se encuentren incumplidos.

Grado de Impacto: Medio

3. CONCLUSIÓN:

En base a las tareas de auditoría realizadas en el presente trabajo, esta UAISLYT concluye que la DGSI ha cumplido satisfactoriamente con su responsabilidad primaria consistente en "Entender en la administración y control de los recursos informáticos de la Secretaría". No obstante es dable resaltar que en nuestra opinión el cumplimiento de las recomendaciones aquí formuladas coadyuvará a fortalecer el nivel de control imperante en la órbita de esta Secretaría Legal y Técnica en materia de administración y aplicación de las políticas de seguridad, toda vez que las observaciones formuladas se relacionan específicamente con dicha materia.

INFORME ANALÍTICO

SECRETARÍA LEGAL Y TÉCNICA
DE LA PRESIDENCIA DE LA NACIÓN

UNIDAD DE AUDITORÍA INTERNA
INFORME FINAL N° 05/2017

"PROCEDIMIENTOS INHERENTES A LA ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS INFORMÁTICOS"

En uso de las atribuciones conferidas por la Ley N° 24156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y el Decreto 172/2008, esta Unidad de Auditoría Interna de la Secretaría Legal y Técnica de la Presidencia de la Nación, en adelante UAISLyT-, efectuó un examen en el ámbito de la Dirección General de Sistemas Informáticos de la Secretaría Legal y Técnica de la Presidencia de la Nación, en adelante DGSI, con el objeto que se detalla a continuación:

1.- OBJETO

Verificar el cumplimiento de la responsabilidad primaria de la DGSI consistente en "Entender en la administración y control de los recursos informáticos de la Secretaría".

2.- ALCANCE DEL TRABAJO

2.1. Tareas de Campo (cronograma – ubicación física, temporal y geográfica):

Las tareas de campo fueron realizadas durante los meses de abril y mayo del año 2017 en las distintas sedes de la DGSI, ubicadas en Juncal 865 PB, Suipacha 767 piso 1 y Balcarce 24 PB de la Ciudad Autónoma de Buenos Aires.

El presente relevamiento se encuentra previsto en el Plan Anual de Trabajo 2017 de esta UAISLyT.

2.2. Procedimientos aplicados.

2.2.1. Requerimiento de documentación e información cursada al auditado a través de Nota NO-2017-04540507-APN-UAI#SLYT, solicitando:

- *Detalle de Sistemas en uso utilizados por el área*
- *Detalle de Sistemas instalados en la SLyT, con detalle de: Nombre, Función del Sistema, Cantidad de Usuarios, Vigencia de la Licencia*

- *.Estadística de incidencias informáticas*
- *Normativa aplicable a la presente auditoría.*
- *Estructura vigente conteniendo nómina de los responsables durante el año 2016 de cada unidad organizativa.*
- *Manual de Procedimientos.*
- *Detalle de los procedimientos inherentes al resguardo de datos.*
- *Detalle de los procedimientos inherentes a la seguridad de la información.*
- *Detalle de los procedimientos inherentes a la organización del área, indicando las tareas y responsabilidades de cada uno de los agentes del área.*
- *Información de contacto del responsable asignado a asistir a los auditores durante la ejecución de la presente auditoría.*

2.2.2. Recopilación y análisis de la normativa vigente, aplicable a la presente auditoría (Anexo I – 1.2 Análisis de Normativa)

2.2.3. Compulsa y análisis efectuados entre la documentación e información brindadas por el área auditada, detalladas en el punto 2.2.1. y las recabadas dentro del marco de las tareas de campo.

2.2.4. Relevamiento y verificación de los procedimientos inherentes a altas, bajas y modificaciones de perfiles de Usuarios (Anexo III – 1. Procedimientos - 1.1 Alta, Baja y modificación de Usuarios)

2.2.5. Verificación de las políticas de seguridad del centro de cómputos (Data Center – DC). (Anexo III –3.- Data Center)

2.2.6. Relevamiento y verificación del proceso de Back Up. (Anexo III – 1 Procedimientos - 1.2 Proceso de Backup)

2.2.7. Análisis de las Políticas de Seguridad y constatación de su efectivo cumplimiento. (Anexo III – 2 Análisis de la Política de Seguridad de la Información)

3.- ACLARACIONES PREVIAS

El criterio de auditoría adoptado para la realización del presente informe implica relevar los procedimientos llevados a cabo por la DGSI a efectos de cumplir con las acciones inherentes a la responsabilidad primaria establecida en la Planilla Anexa al Artículo 2° del Decreto N° 950/2012, consistente en "Administrar y controlar los recursos informáticos de la Secretaría". Ello, a partir de una medición de los mismos en términos de economía, eficiencia y eficacia; teniendo en cuenta los recursos humanos y tecnológicos con que contaba el auditado en el período bajo revisión.

El nombrado Decreto 950/12 crea la DGSI, modificando en consecuencia la estructura oportunamente establecida para la Subsecretaría Técnica de la SLyT por Decreto 78/00 y sus modificatorios.

La DGSI depende de la Subsecretaría Técnica, su Director General es el Lic. Gerardo M. Osterrieth, designado por Decreto Nº 248 de fecha 23 de diciembre de 2015.

De esta Dirección General dependen 4 (cuatro) Direcciones de área: la Dirección de Seguridad Informática cuyo responsable es el Ing. Rodrigo G. Jiménez, la Dirección de Informática cuyo responsable es el Lic. Martin Federico Rouaux, la Dirección de Procesos y Certificaciones cuyo responsable es el Ing. German E. Vigne y la Dirección de Administración de Sistemas de Información cuyo responsable es el Sr. Hernán P. Piscicelli.

De la lectura del Anexo IIb de la Resolución 56/2013 de la SLyT de fecha 26/9/2013 se desprende que el objeto de la presente auditoría concuerda mayoritariamente con la acciones encomendadas a la Dirección de Administración de Sistemas de Información - DGSI.

En esta instancia resulta pertinente concretar que el alcance del presente trabajo de auditoría abarcó:

a) Procesos inherentes a la administración de perfiles de usuarios. Se compulsaron los procedimientos aplicados para la administración de perfiles de usuarios, es decir para la generación de "Altas, Bajas, y Modificaciones" con los procesos delineados y aprobados por el Comité de Seguridad de la Información de la SLyT mediante Acta Nº 4 de fecha 7 de noviembre de 2012. Ver anexo III – 1.Procedimientos – 1.1 Alta, baja, y modificación de usuarios.

b) aspectos normativos y de ejecución de los procedimientos relativos a la seguridad y resguardo de la información:

- Se relevó el procedimiento de “Backup” realizado en las Sedes Balcarce 24 y Suipacha 767, verificando que la frecuencia y guarda de los respaldos de la información sean concordantes con lo establecido en el Anexo Resguardo de Información aprobado por el Comité de Seguridad de la Información –SLyT-, mediante acta de fecha 12/8/2014. Ello, en consonancia con la Disposición 1/2015 de la ONTI. (Ver anexo III – 1.2 Proceso de Backup)

- Se procedió a analizar el “Manual de Normas y Procesamientos para el Acceso Físico al Data Center” emitido el 2 de marzo de 2016, verificando el cumplimiento de algunas pautas incluidas en el mismo, tales como: control de acceso restringido al DC; que el NOC (Network Operations Center o Centro de Operaciones de Red) incluyera el monitoreo del Data Center (DC) mediantes alarmas de Humedad, temperatura, cámaras de video; que se cumpliera con los mantenimientos preventivos del aire acondicionado, de UPS y del grupo electrógeno. Cabe destacar que en el ámbito de la Secretaría Legal y Técnica existen 2 Data Center, uno ubicado en la sede de Suipacha y otro en la sede de Balcarce. (ver anexo III – 3.Data Center)

Con referencia al análisis normativo se procedió a analizar Disposición Nº 1/2015 de la ONTI vs la Política de Seguridad de la SLyT aprobada el 12 de agosto de 2014 por el Comité de Seguridad de la Información –SlyT-. (Ver anexo III – 2.- Análisis de la Política de Seguridad de la Información)

A efectos de un mejor entendimiento de la lectura de este informe, cabe incorporar definiciones de algunos términos que se reiterarán a lo largo de la presente:

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 Organismo o por un tercero que procese información en su nombre, para llevar a cabo*

una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Propietario de la Información: *Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.*

En esta instancia, corresponde transcribir conceptos incorporados en la Disposición 1/2015 de la Oficina Nacional de Tecnologías de Información (ONTI) que esta Unidad de Auditoría considera pertinente:

Toda vez que la información es un activo que, como otros activos importantes, es esencial, necesita ser protegido adecuadamente.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y la operación normal del organismo.

La seguridad de la información se logra implementando un adecuado conjunto de controles, incluyendo políticas, procesos, procedimientos, estructura organizativa y funciones de software y hardware.

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, deben considerarse los conceptos de:

- ***Autenticidad:*** *busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.*
- ***Auditabilidad:*** *define que todos los eventos de un sistema deben poder ser registrados para su control posterior.*
- ***Protección a la duplicación:*** *consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se*

grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- ***No repudio:*** *se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.*
- ***Legalidad:*** *referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.*
- ***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.*

En síntesis, la Política de Seguridad de la información es una herramienta que utilizada eficazmente protege a la misma de una amplia gama de amenazas, garantiza la continuidad de los sistemas de información, minimiza los riesgos de daño y asegura el eficiente cumplimiento de los objetivos del organismo. Ello, bajo efectivos estándares de confidencialidad, integridad, disponibilidad y legalidad de la información.

4- OBSERVACIONES Y RECOMENDACIONES:

4.1. OBSERVACIÓN:

Del análisis efectuado, surgen las observaciones que a continuación se exponen en orden decreciente, según el riesgo potencial que cada una representa:

4.1 Observación: Se observa la existencia de usuarios que permanecen activos, correspondientes a agentes desvinculados de esta Secretaría. Puntualmente, respecto del sistema PSA, sobre un total de 246 (doscientos cuarenta y seis) usuarios activos se detectaron 73 (setenta y tres) casos que corresponden a agentes desvinculados de esta SLYT, lo que representa el 29,67%. Ver Anexo III – 1. Procedimientos – 1.1 Alta, Baja y Modificación de Usuarios.

Opinión del Auditado: Se implementó un procedimiento recurrente mediante el cual se dan de baja todos los usuarios que no se hayan logueado al Active Directory/VPN por un plazo de 90 días. De esta forma se evitará volver a la situación mencionada, en paralelo se solicitará que RRHH informe de las Bajas correspondientes en tiempo y forma. De todas formas, al dar de baja al usuario en el Active Directory, el mismo no puede acceder a la red de la SLYT con lo cual, en el caso de los 73 usuarios mencionados, no hubieran podido acceder al sistema PSA, que por otro lado dejará de funcionar durante el corriente año.

Recomendación: Se recomienda revisar el procedimiento ABM, aplicable a la administración de usuarios (alta/baja/modificaciones) y al propio tiempo realizar una depuración de usuarios de los distintos sistemas a fin de dejar activos sólo aquellos que correspondan.

Grado de Impacto: Medio

4.2 Observación: Se observa que en el ámbito de la SLyT no se encontraría conformado el Comité de Seguridad de la Información que prescribe la Disposición 01/2015 de la ONTI. Ello, en razón de que la mayoría de los miembros designados oportunamente por Resolución 64/2014 - SLyT, no pertenecerían actualmente a esta Secretaría. Ver Anexo III. Punto 2. Análisis de la Política de Seguridad de la Información.

Opinión del Auditado: La conformación del comité de Seguridad de la Información es una competencia que no se encuentra dentro del alcance de la DGSI.

Recomendación: Se recomienda conformar un "Comité de Seguridad de la Información" en el ámbito de esta Secretaría, siguiendo para ello las pautas previstas a tal fin en la Disposición 1/2015 de la ONTI.

Grado de Impacto: Medio

4.3 Observación: Se observa que la Política de Seguridad de la Información de esta Secretaría que fuera aprobada el 12/8/2014, se habría fundamentado en prescripciones normativas que a esa fecha ya habrían sido derogadas. Ello, según se desprende de lo manifestado por el Comité de Seguridad de la Información, quien en el acápite "Introducción", menciona como fundamentos de la Política de Seguridad aprobada, a la Disposición Nº 6/2005 de la ONTI que a esa fecha habría sido derogada por la Disposición Nº 3/2013. Corresponde agregar que esta última norma, a su vez fue posteriormente derogada por la Disposición 1/2015 del mismo Organismo. Ver Anexo III. Punto 2. Análisis de la Política de Seguridad de la Información.

Opinión del Auditado: Se remite a la respuesta a la observación 2.2.

Recomendación: Se recomienda adecuar y actualizar la Política de Seguridad de la Información en función de la normativa vigente al momento de su adecuación.

Grado de Impacto: Medio

4.4 Observación: Se observa que en el ámbito de la SLyT no se estarían cumpliendo los parámetros relativos a compromisos de confidencialidad de la información del organismo, requeridos por las normas respectivas, para el caso la Disposición 1/2015 de la ONTI. Ver Anexo III. Punto 2. Análisis de la Política de Seguridad de la Información.

Opinión del Auditado: Se remite a la respuesta a la observación 2.2.

Recomendación: Se recomienda revisar el procedimiento aplicable para que los agentes de cualquier situación de revista acuerden formalmente respetar el compromiso de confidencialidad de la información del organismo y al propio tiempo formalizar los casos que se encuentren incumplidos.

Grado de Impacto: Medio

5. CONCLUSIÓN:

En base a las tareas de auditoría realizadas en el presente trabajo, esta UAISLYT concluye que la DGSI ha cumplido satisfactoriamente con su responsabilidad primaria consistente en “Entender en la administración y control de los recursos informáticos de la Secretaría”. No obstante es dable resaltar que en nuestra opinión el cumplimiento de las recomendaciones aquí formuladas coadyuvará a fortalecer el nivel de control imperante en la órbita de esta Secretaría Legal y Técnica en materia de administración y aplicación de las políticas de seguridad, toda vez que las observaciones formuladas se relacionan específicamente con dicha materia.

SECRETARÍA LEGAL Y TÉCNICA
DE LA PRESIDENCIA DE LA NACIÓN

UNIDAD DE AUDITORÍA INTERNA
INFORME FINAL N° 05/2017

"PROCEDIMIENTOS INHERENTES A LA ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS INFORMÁTICOS"

ANEXO I

1. NORMATIVA

1.1. Normativa consultada

- Resolución Administrativa 669/04
- Disposición 1/2015 de la Oficina Nacional de Tecnologías de Información
- Resolución 48/2005 SIGEN
- Ley 26.388
- Ley 25.326
- Resolución 56/2013
- Decreto N° 378/2005

1.2. Análisis de la normativa

A fin de promover el empleo eficiente y coordinado de los recursos de las Tecnologías de la Información y las Comunicaciones, el Decreto N° 378/2005 aprobó los Lineamientos Estratégicos que rigen el Plan Nacional de Gobierno Electrónico y los Planes Sectoriales de Gobierno Electrónico de los Organismos de la Administración Pública Nacional.

Por su parte la Decisión Administrativa N° 669/2004 de la Jefatura de Gabinete de Ministros estableció en su artículo 1° que los organismos del Sector Público Nacional comprendidos en el artículo 7° de la citada medida deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo.

Cabe destacar que el artículo 8° de la mencionada decisión administrativa, faculta al subsecretario de la gestión pública de la jefatura de gabinete de ministros a aprobar la Política de Seguridad Modelo y a dictar las normas aclaratorias y complementarias de la citada medida, pudiendo dicha autoridad delegar en el Director Nacional de la Oficina Nacional de Tecnologías de Información las facultades aludidas.

En diciembre de 2004 la Jefatura de Gabinete de Ministros estableció la obligatoriedad para los Organismos del Sector Público Nacional (comprendidos en los incisos a) y c) del artículo 8º de la ley Nº 24.156 y sus modificatorias) de:

- Dictar una política de Seguridad de la Información conforme la Política de Seguridad Modelo, o adecuar sus Políticas de seguridad conforme al Modelo aprobado.
- Conformar un Comité de Seguridad de la Información.
- Designar un Coordinador del Comité de Seguridad de la Información.
- Establecer las funciones del comité de Seguridad de la Información.

Un año después mediante Disposición Nº 6/2005 de la ONTI se aprueba la primera "Política de Seguridad de la Información Modelo" y en septiembre del 2011 se procedió a realizar la actualización de aquel modelo, en base a las actualizaciones sufridas por la norma ISO/IEC 27002 y su incorporación de temas como los que se mencionan a continuación:

- Compromiso y apoyo de la Dirección de la Organización.
- Definición clara de un alcance apropiado.
- Concientización y formación del personal.
- Evaluación de riesgo exhaustiva y adecuada a la organización.
- Compromiso de mejora continúa.
- Establecimiento de políticas y normas.
- Organización y comunicación.
- Inclusión de la cláusula o dominio de gestión de incidentes de seguridad.
- La concientización del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.

- La seguridad debe ser inherente a los procesos de información y de la organización.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- Etc.

La política de seguridad de la información mencionada ut supra se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente Tecnológico del Organismo.

Posteriormente se emitió Disposición Nº 3/2013 de la Oficina Nacional de Tecnologías de Información de Subsecretarias de Tecnologías de Gestión de la Secretaria de Gabinete y Coordinación Administrativa de la Jefatura de Gabinete de Ministros en su artículo 1º se aprobó la "Política de Seguridad de la Información Modelo" que reemplazó y actualizó a los mismos fines a la que fuera aprobada por Disposición ONTI Nº 6/2005 y por último la Disposición ONTI Nº 3/2013 fue reemplazada a los mismos fines por la Disposición ONTI Nº 1/2015.

En relación a la estructura Organizativa, mediante Decreto 78/2000 y sus modificatorios se aprobó la estructura organizativa de primer nivel operativo de la SLYT, por su parte, mediante Decreto 950/2012 se incorporan las Responsabilidad Primaria y Acciones correspondientes a la Dirección General de Sistemas Informáticos –DGSI- dependiente de la Subsecretaria Técnica de la Secretaria Legal y Técnica de la Presidencia de la Nación. El mencionado decreto establece entre sus responsabilidades primarias "Entender en la Administración y control de los recursos informáticos de la Secretaría" la cual es el objeto de la presente auditoría y enumera sus acciones según se transcribe a continuación:

1- Administrar y controlar los recursos informáticos de la Secretaría.
2- Determinar las necesidades en materia de equipamiento informático de la Secretaría.
3- Intervenir en la selección y capacitación de lenguajes, programas y utilitarios aplicables al equipamiento informático.
4- Efectuar el mantenimiento y explotación de los equipos informáticos.
5- Realizar y coordinar el mantenimiento preventivo y de emergencia del equipo informático.

6- Entender en la formulación de planes de desarrollo tecnológico a corto y mediano plazo para optimizar el desempeño de la Secretaría, analizando su factibilidad, beneficios, riesgos y costos.
7- Evaluar la adquisición de nuevas tecnologías de software y hardware necesarias para alcanzar los objetivos propuestos.
8- Prestar a las distintas áreas de la Secretaría el soporte y actualización de los sistemas de administración de la información.
9- Entender en la capacitación del personal de la Secretaría para el uso y aprovechamiento de los recursos informáticos en función de las modificaciones que pudieran implementarse tanto en materia de hardware como de software.
10- Administrar los equipos y sistemas de cómputo de la Secretaría.
11- Efectuar permanentemente los respaldos de información para asegurar el resguardo y recuperación de la misma.
12- Intervenir en la administración de los espacios físicos para el emplazamiento de los equipos a partir de los requerimientos técnicos específicos en cada caso.
13- Intervenir en la definición y control de las tareas desarrolladas por proveedores externos.
14- Entender en los procesos de digitalización de la documentación correspondiente.

Finalmente, mediante la Resolución SLYT N° 56/2013 se aprueba el Organigrama correspondiente quedando conformado en la actualidad como se muestra en el Anexo II.

La ley 25.326, tiene por objeto la protección integral de datos personales asentados en archivos, registros, banco de datos, u otros medios técnicos de tratamientos de datos, sean estos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43 de la Constitución Nacional.

Así mismo considerando que las Normas de control Interno para Tecnología de la Información tienen sus antecedentes en las Pautas de Control Interno para Sistemas y Tecnología de la Información emitidas oportunamente por la Sindicatura General de la Nación. El Síndico General de la Nación aprueba en el artículo 1 de la Resolución

48/05 SIGEN las Normas de control Interno para Tecnología de la Información para el sector Público Nacional.

En la Resolución mencionada ut supra se establece que la unidad de Tecnología de la Información-TI- debe desarrollar, documentar y comunicar políticas y procedimientos respecto de las actividades relacionadas con la TI. Tales políticas y procedimientos deben mantenerse actualizados, deben especificar las tareas y controles a realizar en los distintos procesos, así como los responsables y las sanciones disciplinarias asociadas con su incumplimiento.

Al propio tiempo la TI debe garantizar el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual de software, seguridad de la información así como de las demás normas aplicables. Como también establecer convenios o contratos formales con aquellos terceros con los que existan intercambios de información o prestación de servicios relacionados con la TI.

En lo que refiere a la Seguridad la misma norma establece que se debe garantizar el cumplimiento de las normas establecidas en cuanto al deber de disponer de una política de seguridad de la información.

Es dable destacar que según lo establece la Resolución SIGEN Nº 48/2005 las Unidades de Auditorías Internas definidas en la ley 24156, deben contemplar la ejecución de auditorías de sistemas, debiendo reunir los responsables de llevarla a cabo, los requisitos de competencia técnica, independencia y autoridad para efectuar revisiones objetivas de los controles informáticos y preparar informes sobre sus hallazgos y recomendaciones.

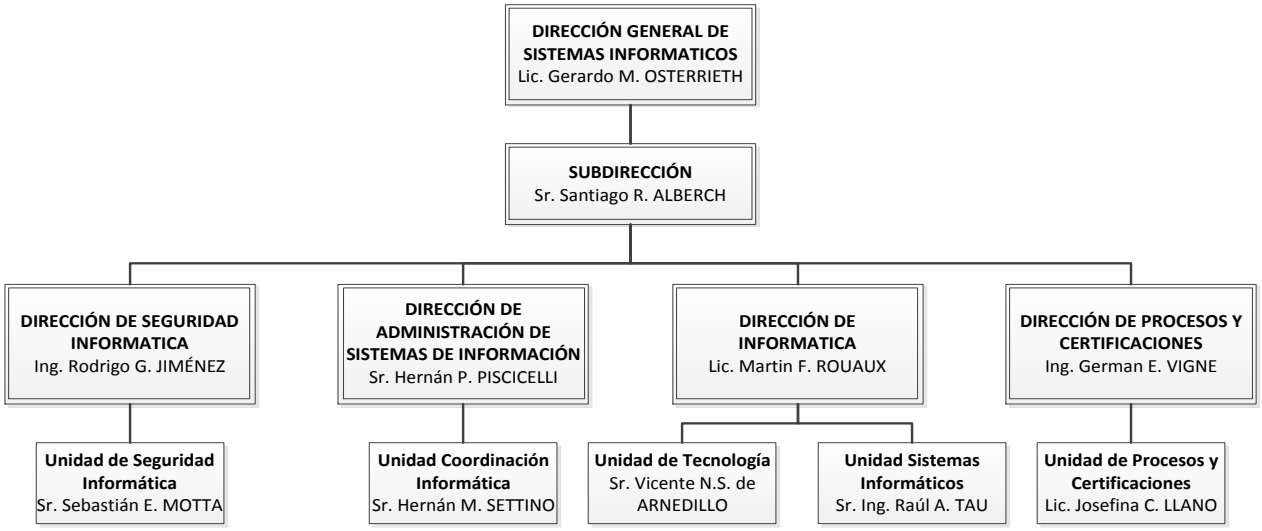
SECRETARÍA LEGAL Y TÉCNICA
DE LA PRESIDENCIA DE LA NACIÓN

UNIDAD DE AUDITORÍA INTERNA
INFORME FINAL N° 05/2017

"PROCEDIMIENTOS INHERENTES A LA ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS INFORMÁTICOS"

ANEXO II

Organigrama:



SECRETARÍA LEGAL Y TÉCNICA
DE LA PRESIDENCIA DE LA NACIÓN

UNIDAD DE AUDITORÍA INTERNA
INFORME FINAL N° 05/2017

"PROCEDIMIENTOS INHERENTES A LA ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS INFORMÁTICOS"

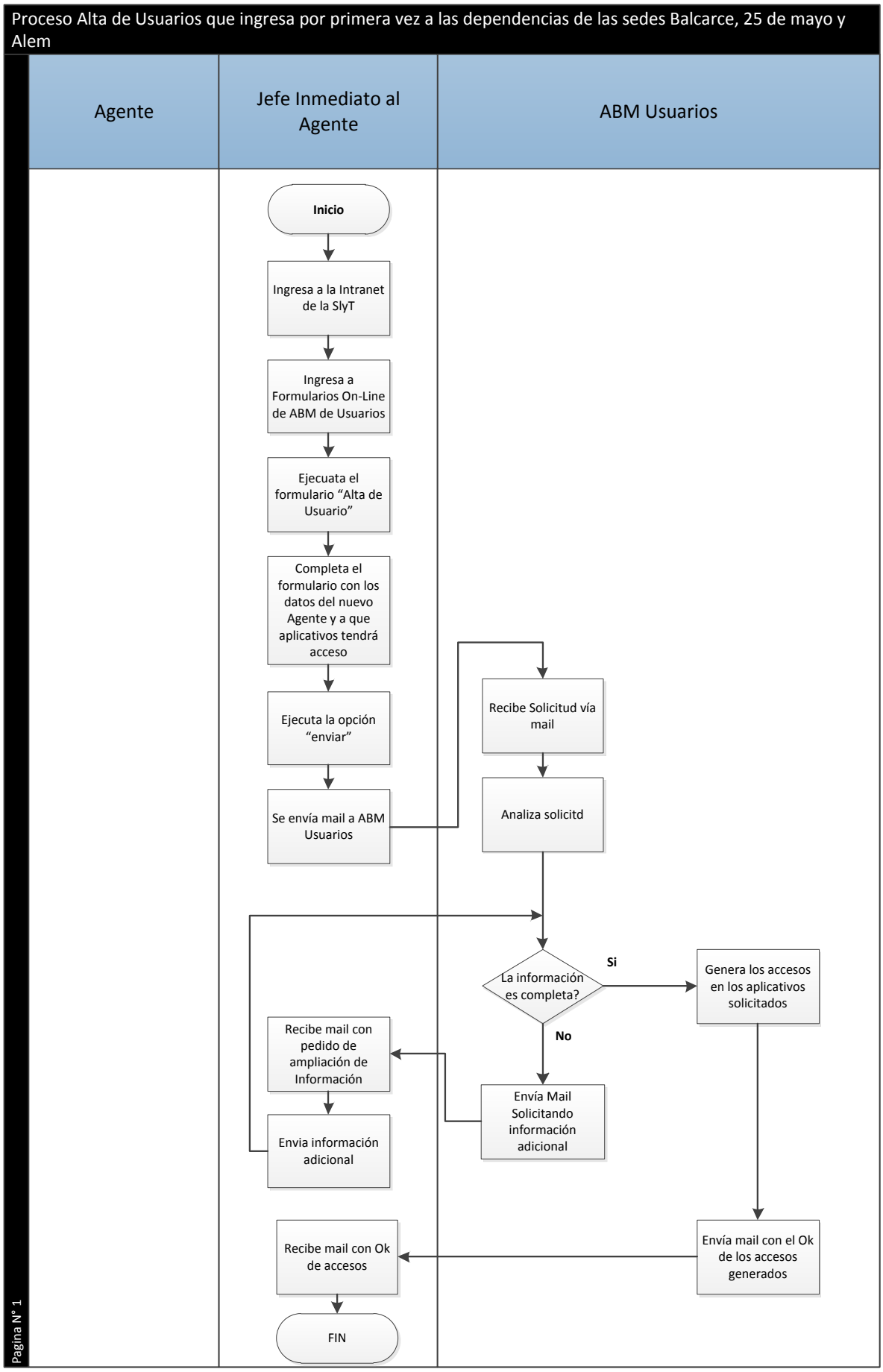
ANEXO III

1. Procedimientos:

Dentro de las tareas de campo realizadas por esta UAI se mantuvieron entrevistas con diversos agentes de la Dirección General de Sistemas Informáticos (DGSI) con el fin de relevar el procedimiento aplicado al "Alta, Baja, y Modificación de Usuarios" y al proceso de "Backup"

Como resultado de este análisis surgen los flujogramas que se adjunta a continuación:

1.1 Alta, Baja Y modificación de Usuarios:


Proceso Alta de Usuarios que ingresa por primera vez a las dependencias de las sedes Balcarce, 25 de mayo y Alem
Agente
Jefe Inmediato al Agente
ABM Usuarios
Inicio
Ingresa a la Intranet de la SlyT
Ingresa a Formularios On-Line de ABM de Usuarios
Ejecuata el formulario "Alta de Usuario"
Completa el formulario con los datos del nuevo Agente y a que aplicativos tendrá acceso
Ejecuta la opción "enviar"
Se envía mail a ABM Usuarios
Recibe Solicitud vía mail
Analiza solicitd
La información es completa?
Si
No
Genera los accesos en los aplicativos solicitados
Recibe mail con pedido de ampliación de Información
Envía Mail Solicitando información adicional
Envia información adicional
Recibe mail con Ok de accesos
Envía mail con el Ok de los accesos generados
FIN
Pagina N° 1

Proceso Alta de Usuarios que ingresa por primera vez a las dependencias de las sedes Balcarce, 25 de mayo y Alem.

Este Formulario se utiliza para dar de Alta a un Agente que ingresa por primera vez a la SLyT de las dependencias de las sedes Balcarce, 25 de mayo y Alem

Jefe Inmediato al Agente:

1. Ingresa a la Intranet de la SLyT
2. Ingresa al formulario On-line de ABM de Usuarios.
3. Ejecuta el formulario "Alta de usuario"
4. Completa el formulario con la siguiente Información:

a- Información del Nuevo Agente

- Nombre y Apellido
- DNI
- Legajo
- Interno
- Dependencia

b- Permisos y accesos, en esta parte del formulario tiene la opción de tildar las siguientes opciones:

- Correo electrónico (mail)
- Acceso a Internet
- Acceso a Carpetas de Dependencia, puede seleccionar "no", "Solo lectura" o "control total"

c- Aplicaciones, en esta parte del formulario tiene la opción de tildar los aplicativos y sus accesos dentro de este.

c 1-APO

Correos: consultas, crear, y reportes

APO actualizaciones: consultas, crear, modificar, reingresos, bifurcar, reportes, transferir, borrar transferencia y modificar transferencia

APO Proyecto: consultas, crear, modificar, reingresos, reportes, transferir, borrar transferencia y modificar transferencia

APO Leyes: consultas, crear, modificar, reingresos, reportes, transferir, borrar transferencia y modificar transferencia

APO Biblioteca: listar, crear y reportes.

c 2-PSA

PSA Carrito: solicitud y solicitud y aprobación

PSA Planeamiento: planeamiento

PSA Suministros: autorización de pedidos, entrega de pedidos, devoluciones, transferencia entre depósitos,

PSA Patrimonio: administración de pedidos y gestión para responsable patrimonial.

PSA Compras y recepción de bienes: admin. de compras, aut. por faltante de stock, ingreso de facturas, recepción de bienes (comprados), recepción de bienes de uso y administrador de proveedores

PSA Caja Chica: carga de gasto, rendición y cierre autoriz.

c 3-META 4

ABM gestión de personal: ABM personal, ABM periodo, ABM rol, consultas, listados y reportes

ABM organización: ABM externa, ABM interna, ABM legal, consultas, listados y reportes

ABM gestión de tiempo: ABM incidencias, ABM presencias, ABM vacaciones, ABM horas extras, ABM solicitud de licencias, consultas, listados y reportes

Nomina: liquidación de nómina, consultas, listados y reportes

c 4-Otros

Lex Doctor: Lex Doctor

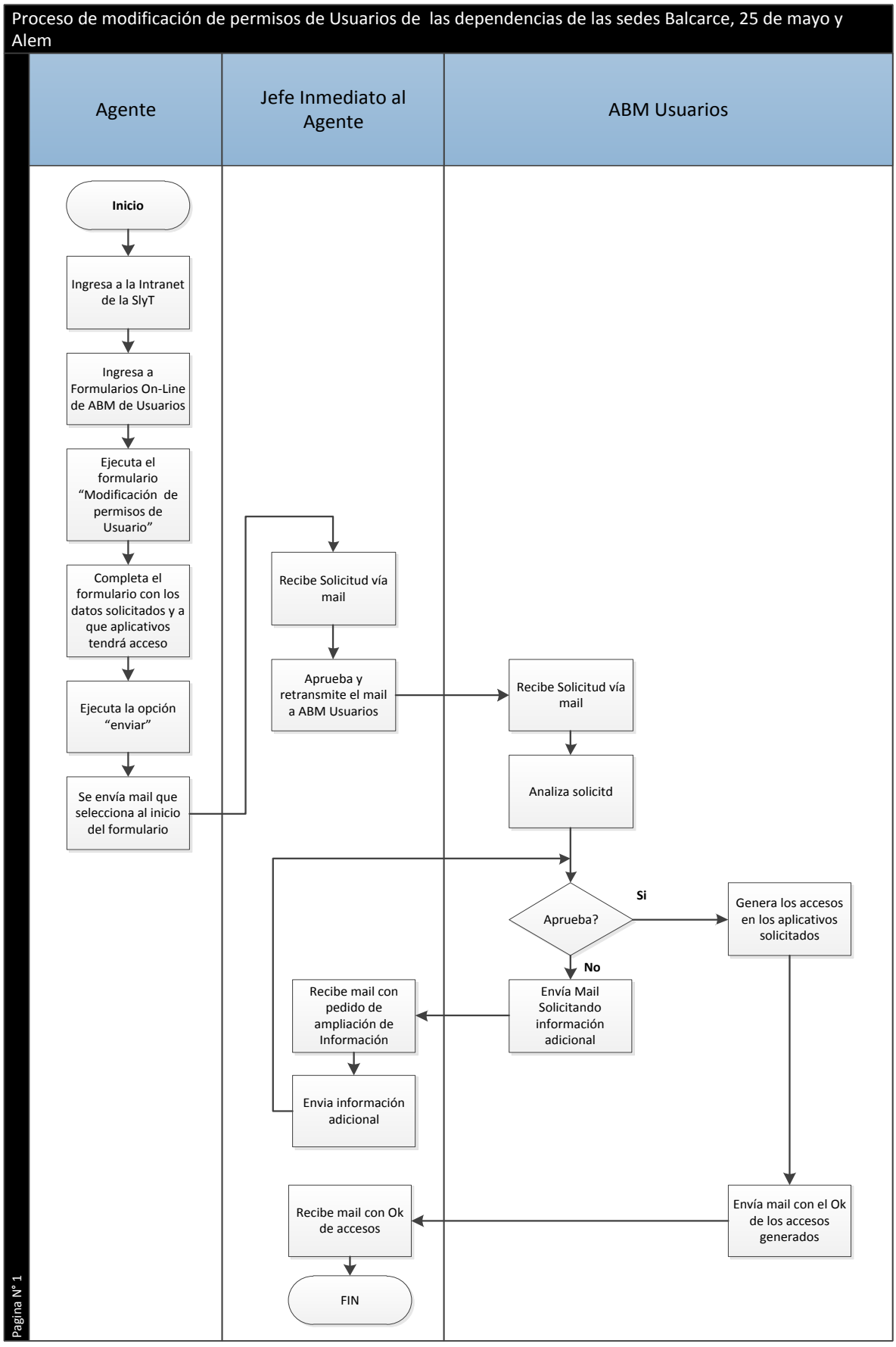
SLU / eSIDIF: SLU / eSIDIF:

c 5-Obsrvaciones**:** campo texto habilitado para tal fin

5. Ejecuta la opción enviar, y la solicitud viaja vía mail al usuario ABMUSUARIOS@SLYT.GOV.AR.

ABM USUARIOS:

6. Ingresa a la casilla de ABM Usuarios, que es visualizada por el grupo de ABM Usuarios de segundo nivel. En caso de solicitar accesos a los Aplicativos de Meta4 o PSA deriva por sistemas al Jefe de la Unidad o al Director para que realicen los accesos a estos dos aplicativos.
7. Realiza análisis de la información recibida para el alta del usuario (que el solicitante sea Jefe Inmediato o superior del Usuario a dar de alta o modificar, que el formulario este bien confeccionado)
8. Genera los accesos necesarios. En caso de un nuevo usuario da de alta según el formulario enviado por el supervisor en el Active Directory
9. Notifica vía mail de la generación del nuevo perfil


Proceso de modificación de permisos de Usuarios de las dependencias de las sedes Balcarce, 25 de mayo y Alem
Agente
Jefe Inmediato al Agente
ABM Usuarios
Inicio
Ingresa a la Intranet de la SlyT
Ingresa a Formularios On-Line de ABM de Usuarios
Ejecuta el formulario "Modificación de permisos de Usuario"
Completa el formulario con los datos solicitados y a que aplicativos tendrá acceso
Ejecuta la opción "enviar"
Se envía mail que selecciona al inicio del formulario
Recibe Solicitud vía mail
Aprueba y retransmite el mail a ABM Usuarios
Recibe Solicitud vía mail
Analiza solicitd
Aprueba?
Si
Genera los accesos en los aplicativos solicitados
No
Envía Mail Solicitando información adicional
Recibe mail con pedido de ampliación de Información
Envia información adicional
Envía mail con el Ok de los accesos generados
Recibe mail con Ok de accesos
FIN
Pagina N° 1

Proceso modificación de permisos de Usuarios de las dependencias de las sedes Balcarce, 25 de mayo y Alem.

Agente:

1. Ingresa a la Intranet de la SLyT
2. Ingresa al formulario On-line de ABM de Usuarios
3. Ejecuta el formulario "Modificación de permisos de usuarios"
4. Completa el formulario con la siguiente Información:
   - **a-** Información del autorizante.
   - **b-** Información del autorizante
   - **c-** c- Completa el campo texto de "Agregar permisos a los actuales que ya posee", con los accesos solicitados a aplicativos o carpetas.
   - **d-** Completa el campo texto de "Eliminar Permisos", con los accesos solicitados a aplicativos o carpetas.
   - **e-** Completa el campo observaciones, en caso de querer realizar alguna aclaración adicional.
5. Ejecuta la opción enviar, y la solicitud viaja vía mail al usuario descripto en el punto 4. a- (Autorizante)

Autorizante o Jefe Inmediato:

6. Recibe solicitud vía mail.
7. Aprueba y retransmite el mail a ABM Usuarios.

ABM USUARIOS:

8. Ingresa a la casilla de ABM Usuarios, que es visualizada por el grupo de ABM Usuarios de segundo nivel. En caso de solicitar accesos a los Aplicativos de Meta4 o PSA deriva por sistemas al Jefe de la Unidad o al Director para que realicen los accesos a estos dos aplicativos.
9. Realiza análisis de la información recibida para el alta del usuario (que el solicitante sea Jefe Inmediato o superior del Usuario a dar de alta o modificar, que el formulario este bien confeccionado)

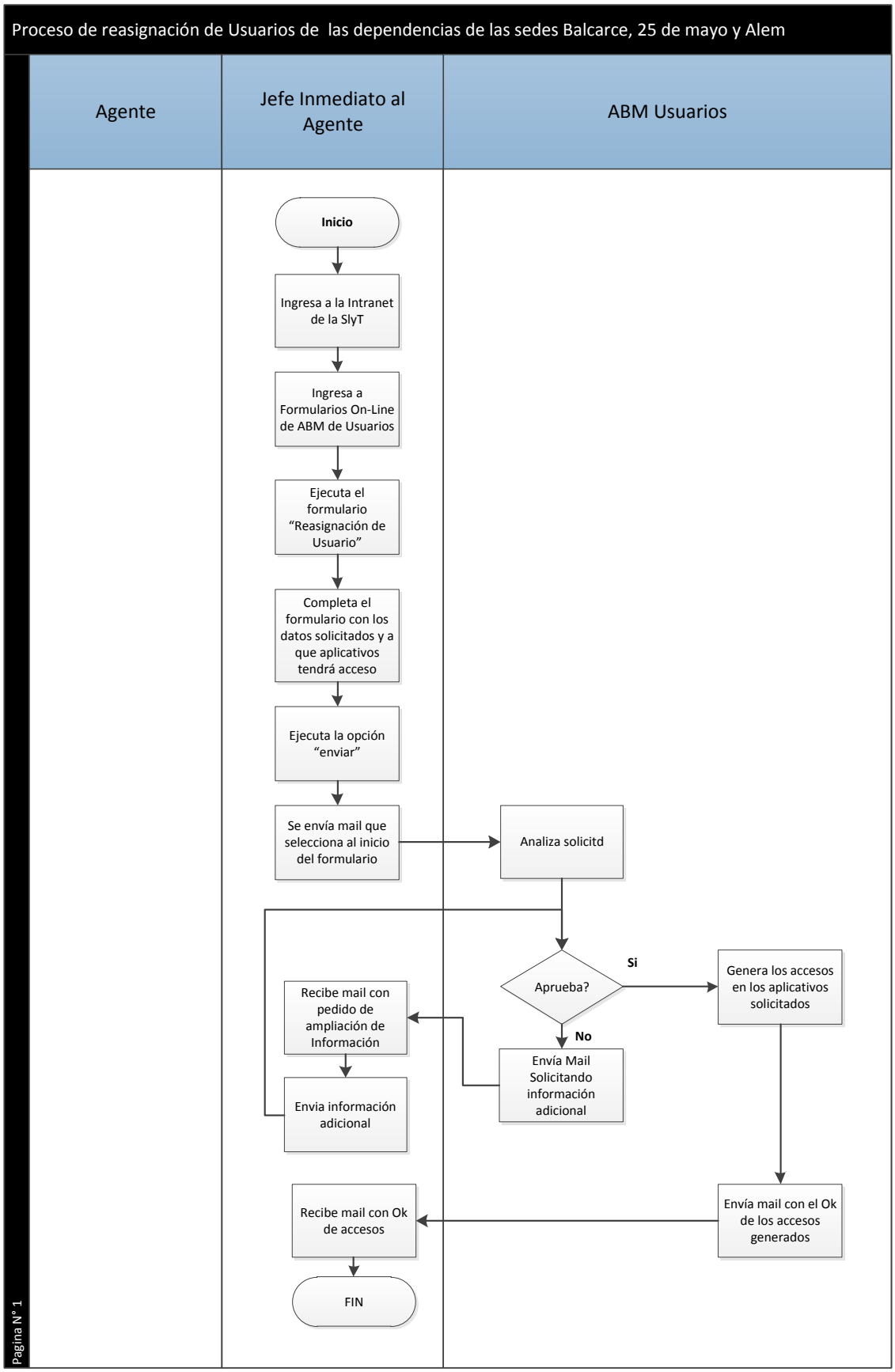
   9.1 Si no aprueba solicitud, solicita vía mail ampliación de información

   Autorizante o Jefe Inmediato:

   9.2 recibe mail y envía información adicional.

   ABM USUARIOS:

   9.3 Recibe mail y continúa en el punto 10
10. Aprueba solicitud
11. Genera los accesos necesarios
12. Notifica vía mail de la generación del nuevo perfil


Proceso de reasignación de Usuarios de las dependencias de las sedes Balcarce, 25 de mayo y Alem
Agente
Jefe Inmediato al Agente
ABM Usuarios
Inicio
Ingresa a la Intranet de la SlyT
Ingresa a Formularios On-Line de ABM de Usuarios
Ejecuta el formulario "Reasignación de Usuario"
Completa el formulario con los datos solicitados y a que aplicativos tendrá acceso
Ejecuta la opción "enviar"
Se envía mail que selecciona al inicio del formulario
Analiza solicitd
Aprueba?
Si
No
Genera los accesos en los aplicativos solicitados
Envía Mail Solicitando información adicional
Recibe mail con pedido de ampliación de Información
Envia información adicional
Envía mail con el Ok de los accesos generados
Recibe mail con Ok de accesos
FIN
Pagina N° 1

Proceso reasignación de Usuarios de las dependencias de las sedes Balcarce, 25 de mayo y Alem.

Jefe Inmediato al Agente:

1. Ingresa a la Intranet de la SLyT
2. Ingresa al formulario On-line de ABM de Usuarios.
3. Ejecuta el formulario "Alta de usuario"
4. Completa el formulario con la siguiente Información:
   - **a-** Nombre y Apellido del Usuario reasignado
   - **b-** Unidad de origen y destino
   - **c-** Permisos y accesos, en esta parte del formulario tiene la opción de tildar las siguientes opciones:
     - Correo electrónico (mail)
     - Acceso a Internet
     - Acceso a Carpetas de Dependencia, puede seleccionar "no", "Solo lectura" o "control total"
   - **d-** Aplicaciones, en esta parte del formulario tiene la opción de tildar los aplicativos y sus accesos dentro de este.

     d 1-APO

     Correos: consultas, crear, y reportes

     APO actualizaciones: consultas, crear, modificar, reingresos, bifurcar, reportes, transferir, borrar transferencia y modificar transferencia

     APO Proyecto: consultas, crear, modificar, reingresos, reportes, transferir, borrar transferencia y modificar transferencia

     APO Leyes: consultas, crear, modificar, reingresos, reportes, transferir, borrar transferencia y modificar transferencia

     APO Biblioteca: listar, crear y reportes.

     d 2-PSA

     PSA Carrito: solicitud y solicitud y aprobación

     PSA Planeamiento: planeamiento

     PSA Suministros: autorización de pedos, entrega de pedidos, devoluciones, transferencia entre depósitos,

     PSA Patrimonio: administración de pedidos y gestión para responsable patrimonial.

     PSA Compras y recepción de bienes: admin. de compras, aut. por faltante de stock, ingreso de facturas, recepción de bienes (comprados), recepción de bienes de uso y administrador de proveedores

PSA Caja Chica: carga de gasto, rendición y cierre autoriz.

d 3-META 4

ABM gestión de personal: ABM personal, ABM periodo, ABM rol, consultas, listados y reportes

ABM organización: ABM externa, ABM interna, ABM legal, consultas, listados y reportes

ABM gestión de tiempo: ABM incidencias, ABM presencias, ABM vacaciones, ABM horas extras, ABM solicitud de licencias, consultas, listados y reportes

Nomina: liquidación de nómina, consultas, listados y reportes

d 4-Otros

Lex Doctor: Lex Doctor

SLU / eSIDIF: SLU / eSIDIF:

d 5-Obsrvaciones**:** campo texto habilitado para tal fin

5. Ejecuta la opción enviar, y la solicitud viaja vía mail al usuario ABMUSUARIOS@SLYT.GOV.AR.

ABMUSUARIOS:

6. Ingresa a la casilla de ABM Usuarios, que es visualizada por. el grupo de ABM Usuarios de segundo nivel. En caso de solicitar accesos a los Aplicativos de Meta4 o PSA deriva por sistemas al Jefe de la Unidad o al Director para que realicen los accesos a estos dos aplicativos.

7. Realiza análisis de la información recibida para el alta del usuario. (que el solicitante sea Jefe Inmediato o superior del Usuario a dar de alta o modificar, que el formulario este bien confeccionado)

7.1 Si no aprueba solicitud, solicita vía mail ampliación de información

Autorizante o Jefe Inmediato:

7.2 recibe mail y envía información a adicional.

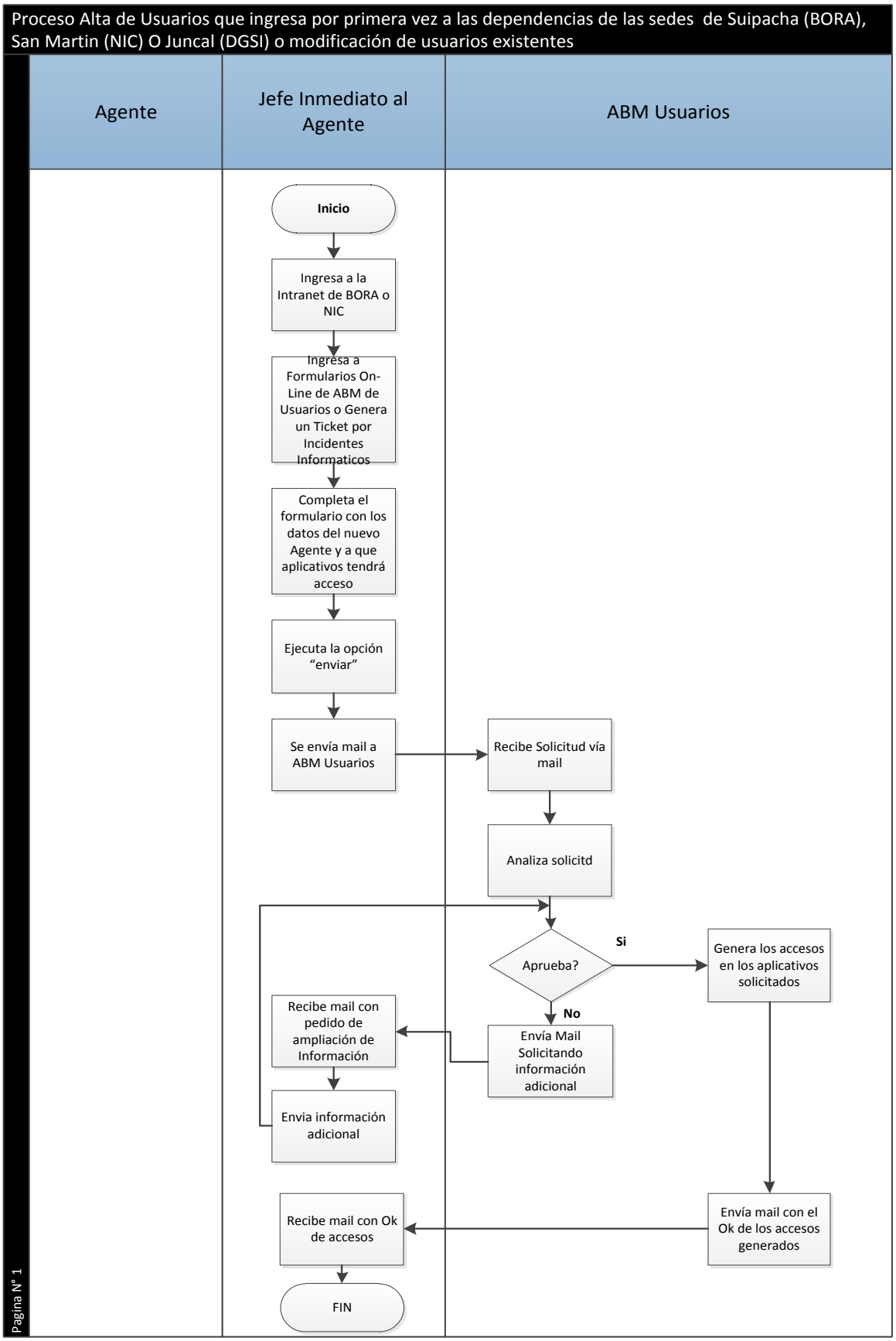
ABM USUARIOS:

7.3 Recibe mail y continúa en el punto 8

8. Aprueba solicitud. Si la reasignación es a otra dependencia de la SLyT (BORA NIC), primero realiza baja al dominio SLyT y aplicativos bajo esta orbita, y luego genera el alta al nuevo dominio y aplicativos

9. Genera los accesos necesarios

10. Notifica vía mail de la generación del nuevo perfil


Proceso Alta de Usuarios que ingresa por primera vez a las dependencias de las sedes de Suipacha (BORA), San Martin (NIC) O Juncal (DGSI) o modificación de usuarios existentes
Agente
Jefe Inmediato al Agente
ABM Usuarios
Inicio
Ingresa a la Intranet de BORA o NIC
Ingresa a Formularios On-Line de ABM de Usuarios o Genera un Ticket por Incidentes Informaticos
Completa el formulario con los datos del nuevo Agente y a que aplicativos tendrá acceso
Ejecuta la opción "enviar"
Se envía mail a ABM Usuarios
Recibe Solicitud vía mail
Analiza solicitd
Aprueba?
Si
Genera los accesos en los aplicativos solicitados
No
Envía Mail Solicitando información adicional
Recibe mail con pedido de ampliación de Información
Envia información adicional
Envía mail con el Ok de los accesos generados
Recibe mail con Ok de accesos
FIN
Pagina N° 1

Proceso Alta de Usuarios que ingresa por primera vez a las dependencias de las sedes BORA, NIC, o Juncal o modificación de usuarios existentes

Se utilizan los formularios ABM Alta de Usuarios y/o ticket (Redmini o ServiceDesk)

Jefe Inmediato al Agente:

1. Ingresa a la Intranet de BORA o NIC Según corresponda
2. En On-line de ABM Usuarios Ingresa al formulario "Altas"

   Completa el formulario con la siguiente Información:

   a- Información del Nuevo Agente o existente

   - Nombre y Apellido
   - Dependencia

   b- Permisos y accesos, en esta parte del formulario tiene la opción de tildar las siguientes opciones:

   - Correo electrónico (mail con o sin acceso desde el celular, Outlook sin conexión)
   - Acceso a buzones compartidos
   - Acceso a Internet (Permisos de Navegación)
   - Acceso a Carpetas de Dependencia, puede seleccionar "no", "Solo lectura" o "control total"

   c- Aplicaciones varias. (BORA: BAS, Publicaciones, etc.) – (NIC; Vilma,etc)

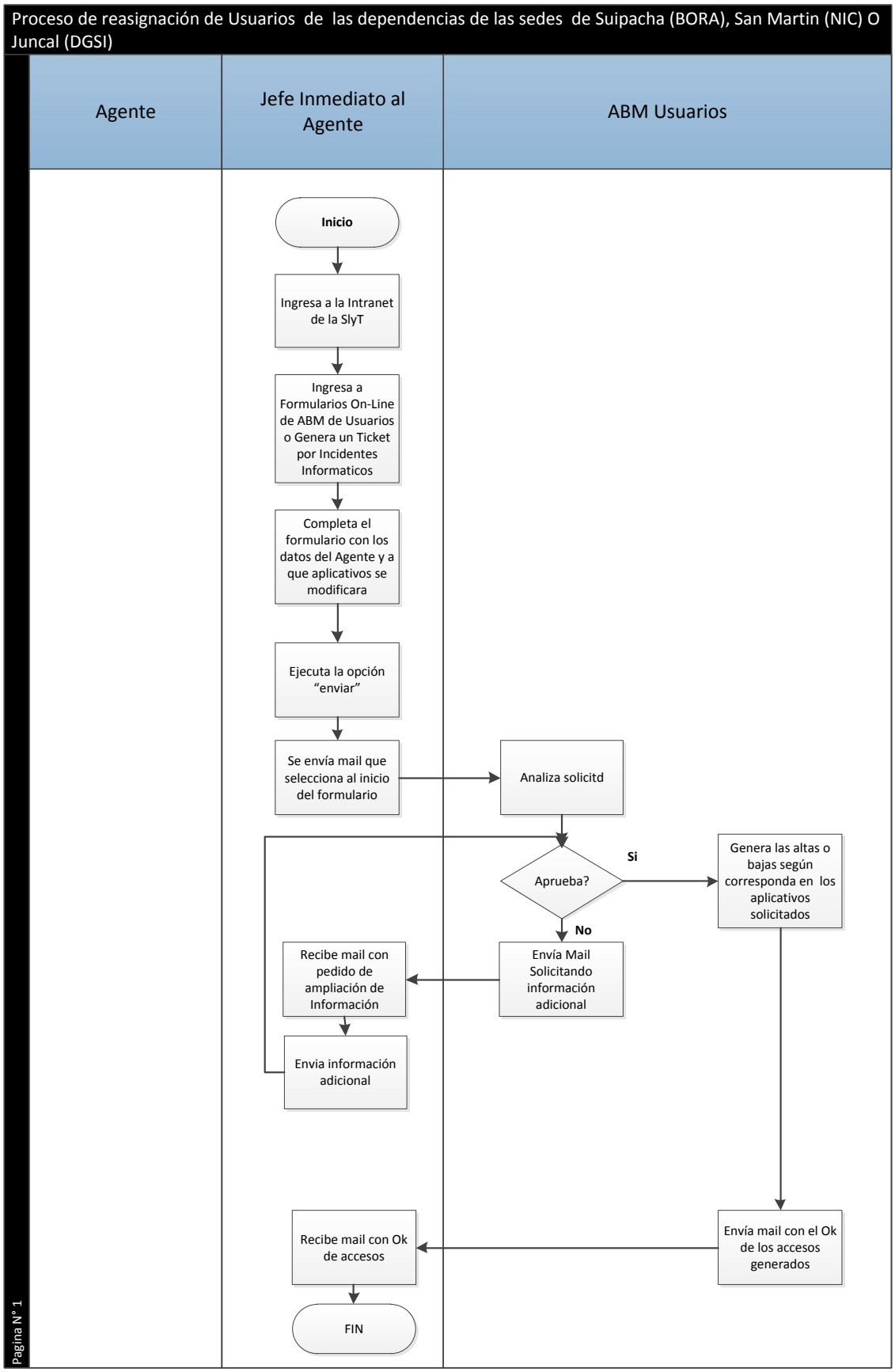
O Ingresa a Ticket de Incidentes Informáticos, e ingresa la misma información en el campo detalle

ABM USUARIOS:

3. Ingresa a la casilla de ABM Usuarios, que es visualizada por el grupo de trabajo.
4. Realiza análisis de la información recibida para el alta del usuario. Puede solicitarle al Jefe inmediato del Agente ampliación de la información enviada.
5. Genera los accesos necesarios
6. Notifica vía mail de la generación del nuevo perfil

Jefe Inmediato del Agente:

7. Recibe mail con ok de acceso generado


Proceso de reasignación de Usuarios de las dependencias de las sedes de Suipacha (BORA), San Martin (NIC) O Juncal (DGSI)
Agente
Jefe Inmediato al Agente
ABM Usuarios
Inicio
Ingresa a la Intranet de la SlyT
Ingresa a Formularios On-Line de ABM de Usuarios o Genera un Ticket por Incidentes Informaticos
Completa el formulario con los datos del Agente y a que aplicativos se modificara
Ejecuta la opción "enviar"
Se envía mail que selecciona al inicio del formulario
Analiza solicitd
Aprueba?
Si
No
Genera las altas o bajas según corresponda en los aplicativos solicitados
Envía Mail Solicitando información adicional
Recibe mail con pedido de ampliación de Información
Envia información adicional
Envía mail con el Ok de los accesos generados
Recibe mail con Ok de accesos
FIN
Pagina N° 1

Proceso reasignación de Usuarios dentro o fuera de la dependencia actual. Aplicables a las dependencias de las sedes Suipacha (BORA, San Martin (NIC), Juncal (DGSI).

Autorizante o Jefe Inmediato:

1. Ingresa a la Intranet de la SLyT
2. Ingresa al formulario On-line de ABM o Usuarios o Ticket.
3. En On-line de ABM Ejecuta el formulario "Reasignación de usuarios", Completa el formulario con la siguiente Información :

   a- Nombre y Apellido del Usuario reasignado

   b- Unidad de origen y destino

   c- Permisos y accesos, en esta parte del formulario tiene la opción de tildar las siguientes opciones:

   - Correo electrónico (mail)
   - Acceso a Internet
   - Acceso a Carpetas de Dependencia, puede seleccionar "no", "Solo lectura" o "control total"

   d- Aplicaciones, en esta parte del formulario tiene la opción de tildar los aplicativos y sus accesos dentro de este.

   O Ingresa a Ticket de Incidentes Informáticos, e ingresa la misma información en el campo detalle.

4. Ejecuta la opción enviar, y la solicitud viaja vía mail al usuario descripto en el punto

ABM USUARIOS:

5. Ingresa a la casilla de ABM Usuarios, que es visualizada por el grupo de trabajo.
6. Realiza análisis de la información recibida para el alta del usuario. Puede solicitarle al Jefe inmediato del Agente ampliación de la información enviada.
7. Aprueba solicitud
8. Genera las bajas y altas correspondientes. En caso de cambio de dominio debe dar de baja el usuario actual y generar uno nuevo al nuevo dominio
9. Notifica vía mail de la generación del nuevo perfil

Se procedió a realizar la compulsa entre los procesos relevados vs. Los procesos documentados y aprobados por el Comité de Seguridad de la Información mediante Acta Nº 4 de fecha 7 de noviembre de 2012, suministrados a esta UAISLyT por la DGSI.

De la compulsa efectuada se constató que el proceso referente a baja de usuarios no se estaría cumpliendo en su totalidad. Toda vez que la Dirección de Recursos Humanos no le estaría informando a la DGSI los agentes que fueron dados de baja, el sector de Sistemas encargado del mantenimiento de Usuarios de las sedes de Juncal, San Martin y Suipacha semanalmente corren un scrip para determinar cuáles son las estaciones de trabajo o usuarios que no tuvieron actividad en los últimos 60 días y procede a su desactivación (no borrado).

Así mismo consideramos que las altas de nuevos Agentes deberían ser informadas por RRHH al momento de realizar el alta de sus datos en el Sistema Meta4/SHARA, de esta forma la DGSI cuando recibe la solicitud de alta de un nuevo usuario por Jefe del agente podría verificar la validez del mismo.

Se solicitó a la DGSI listado de usuarios activos en los distintos sistemas de información con acceso cifrado. Luego se procedió a verificar los mismos contra el sistema Meta4 para corroborar que los usuarios mencionados continúen perteneciendo a esta Secretaría.

El análisis se realizó sobre usuarios de APO, PSA, Aplicativos del NIC y accesos de Windows, a continuación se detallan los resultados obtenidos:

Sistema APO: es un sistema de utilización en la sede de Balcarce para la administración de expedientes:

Detalle	Cantidad de Usuarios	% respecto al total de Usuarios
Usuarios Correctos	200	59,70%
Agentes que no pertenecen más a la SLyT	77	22,99%
Agentes Transferidos a la Sede Suipacha / Campichuelo	15	4,48%
Agentes Transferidos a la Sede San Martin	4	1,19%
Agentes Transferidos a la Sede 25 de Mayo	1	0,30%
Agentes que no figuran en la base META4 (Posibles locaciones de servicio)	38	11,67%
Total de Usuario activos en el sistema APO	**335**	**100%**

En el cuadro podemos observar que de los 335 usuarios activos, solo 200, que representa el 59,70% de usuarios son los que deberían estar activos toda vez que son

agentes que continúan prestando servicios en la Secretaria, los 135 usuarios restantes (40,30%), no pertenecen más a esta Secretaria o fueron transferidos a otra delegación que no utiliza este Software. Sobre los 39 agentes que no figuran en la base del Sistema META4, no se pudo constatar si aún continúan vinculados a esta Secretaria.

Con el fin de realizar la compulsa en relación a los agentes transferidos a otra dependencia se procedió a comparar los mail dados de alta en el sistema APO vs los que figuran en el Sistema META 4

Se amplió el análisis de los Agentes que figuran aun activos en el Sistema APO y que no pertenecen más a la SLyT, a continuación se detallan las cantidades de Agentes por año de Baja de la SLyT:

Año de Baja	Cantidad de Agentes que no pertenecen más a la SLyT	% respecto al total de Agentes que no pertenecen más a la SLyT
2011	2	2,60%
2012	2	2,60%
2013	12	15,58%
2014	11	14,28%
2015	16	20,78%
2016	32	41,56%
2017	2	2,60%
Total de Usuario que no Pertenecen más a la SLyT	**77**	**100,00%**

Sistema PSA: es un desarrollo que se utiliza en todas las sedes para la administración de bienes patrimoniales por partes de los responsables asignados - para la solicitud mediante el modulo “Carito” de bienes de consumo y exclusivamente en la sede de 25 de mayo para la administración y planificación del stock de bienes de consumo.

Detalle	Cantidad de Usuarios	% respecto al total de Usuarios
Usuarios Correctos	150	60,98%
Agentes que no pertenecen más a la SLyT	73	29,67%
Agentes Transferidos a la Sede Suipacha / Campichuelo	12	4,88%
Agentes Transferidos a la Sede San Martin	9	3,66%
Agentes Transferidos a la Sede 25 de Mayo	0	0

Detalle	Cantidad de Usuarios	% respecto al total de Usuarios
Agentes que no figuran en la base META4 (Posibles locaciones de servicio)	2	0,81%
Total de Usuario activos en el sistema PSA	**246**	**100,00%**

En el cuadro anterior podemos observar que de los 246 usuarios activos, solo 150 que representan el 60,98% de usuarios son los que deberían estar activos toda vez que son agentes que continúan prestando servicios en la Secretaria, los 96 usuarios restantes (39,02%), no pertenecen más a esta Secretaria o fueron transferidos a otra delegación que no utiliza este Software. Sobre los 2 agentes que no figuran en la base del Sistema META4, no se pudo constatar si aún siguen vínculos a esta Secretaria.

Con el fin de realizar la compulsa en relación a los agentes transferidos a otra dependencia se procedió a comparar los mail dados de alta en el sistema APO vs los que figuran en el Sistema META 4.

Se amplió el análisis de los Agentes que figuran aun activos en el Sistema PSA y que no pertenecen más a la SLyT, a continuación se detallan la cantidad de Agentes por año de Baja de la SLyT:

Año de Baja	Cantidad de Agentes que no pertenecen más a la SLyT	% respecto al total de Agentes que no pertenecen más a la SLyT
2011	2	2,74%
2012	3	4,11%
2013	6	8,22%
2014	4	5,48%
2015	9	12,33%
2016	45	61,64%
2017	4	5,48%
Total de Usuario que no Pertenecen más a la SLyT	**73**	**100%**

Sistemas DAPHNE, GDE, VILMA, S1, REDMINE, APPNIC, PHPLIST, DRUPAL, WORDPRESS: son software que se utilizan en la sede San Martin (NIC):

Detalle	Cantidad de Usuarios	% respecto al total de Usuarios
Usuarios Correctos	54	96,43%
Agentes que no figuran en la base META4 (Posibles locaciones de servicio)	2	3,57%
Total de Usuario activos en el sistema PSA	**56**	**100,00%**

Sobre los 2 agentes que no figuran en la base del Sistema META4, no se pudo constatar si aún continúan vinculados a esta Secretaria.

Acceso a Windows de las Sedes Balcarce, Alem y 25 de mayo:

Detalle	Cantidad de Usuarios	% respecto al total de Usuarios
Usuarios Correctos	255	89,79%
Agentes que no pertenecen más a la SLyT	1	0,35%
Agentes Transferidos a la Sede Suipacha / Campichuelo	15	5,28%
Agentes Transferidos a la Sede San Martin	12	4,23%
Agentes Transferidos a la Sede 25 de Mayo	1	0,35%
Agentes que no figuran en la base META4 (Posibles locaciones de servicio)	0	0
Total de Usuario activos en el sistema PSA	**284**	**100,00%**

Con el fin de realizar la compulsa en relación a los agentes transferidos a otra dependencia se procedió a comparar los mail que figuran en el listado enviado a esta UAI por la DGSI vs los que figuran en el Sistema META 4

1.2 Proceso de Backup

Dado que los equipos que contienen la información a resguardar mediante el proceso de backup se encuentran en distintos lugares físicos, se relevó el mismo en ambos lugares exponiéndose a continuación un narrativo del proceso de Backup Balcarce (Sedes Balcarce, 25 de Mayo y Alem) y del de Juncal (Sedes Suipacha, San Martin y Juncal).

1.2.1 Proceso Juncal:

Se realizan dos procesos de Backup, uno diario y otro semanal, a su vez este último tiene un proceso de resguardo semanal u otro de resguardo anual. Se utiliza el NetBackup que es un software de copia de seguridad que ofrece capacidad completa de copia de seguridad y recuperación.

a) Proceso Diario:

De servidores contenedores de datos y software a full, programados y de activación automática a D2D ("Disk-to-Disk). Permite almacenar un mes de Backup.

b) Proceso Semanal (retención mensual):

De servidores contenedores de datos y software a full, programados y de activación automática a LTO (Linear Tape-Open) Se almacenan las cintas de Backup por un periodo máximo de un mes. Se ejecuta todos los días miércoles al finalizar el proceso de backup diario.

c) Proceso Semanal (retención anual):

De servidores contenedores de datos y software a full, programados y de activación automática a LTO (Linear Tape-Open) Se almacenan las cintas de Backup por un periodo máximo de un año. Se ejecuta todos los días viernes al finalizar el proceso de backup diario.

En los casos de backup a LTO, las cintas son almacenadas en una caja de seguridad ubicada en la sede de Juncal.

Según se pudo relevar se realizan pruebas de restore para verificar la consistencia de dichos backup, seleccionando equipos al azar backpeados a cualquiera de los medios/juegos. Se documentan dichas recuperaciones en un archivo Excel.

1.2.2 Proceso Balcarce:

Se realizan dos procesos de Backup, uno diario y otro semanal. Se utiliza el NetBackup que es un software de copia de seguridad que ofrece capacidad completa de copia de seguridad y recuperación.

a) Proceso Diario:

Se puede dividir en backups Full y Diferencial. Los Full se realizan en general los fines de semana, y los diferenciales se realizan durante la semana. Se realizan en cintas LTO5, a excepción de los backups del Exchange, que se realiza en un D2D. La retención de estos backups es anual. Pasado el período de retención, las cintas se sobrescriben.

b) Proceso Semanal:

Se realizan backups full de las bases de datos de mayor criticidad, del Exchange, y del File Server. Se realizan en un grupo especial de cintas LTO5, que se retiran el lunes del robot y se envían a Juncal. El período

de retención de estas cintas es de una semana. Se ejecuta los fines de semana.

En los casos de backup a LTO5 tanto de Balcarce como de Juncal, las cintas son almacenadas en una caja de seguridad ubicada en la sede de Juncal.

A continuación se detallan los procesos de back up dentro del sofware "NetBackup 7.5":

Archivos, aplicaciones y base de datos:

CSWVDB1: se realiza un backup full los días domingos a las 8:00 am y un backup diferencial de lunes a viernes a las 2:30 am.

CSWVFS: se realiza un backup full los días sábados a las 9:00 am y un backup diferencial de lunes a viernes a las 11:00 pm.

CSWVIIS1: se realiza un backup full los días domingos a las 1:00 pm y un backup diferencial de martes a sábado a la 1:00 am (se realiza un backup de la carpeta C:\inetpub.)

MSWVAPP1: se realiza un backup full los días domingos a las 7:00 pm y un backup diferencial de lunes a sábado a las 12:30 am (se realiza un backup de la carpeta C:\inetpub y de la carpeta G:\MSSQL, donde se alojan los backup diarios de las bases de datos realizados por el MSSQL).

MSWVFS: se realiza un backup full los días sábados a las 6:00 am y un backup diferencial de martes a viernes a la 2:20 am (se realiza un backup de la carpeta C:\fileServer y c:\SLYT).

CSWVFSR: Se realiza un backup full mensual, el primer lunes de cada mes. (se realiza un backup de la carpeta D:\DASI\documentos\Documentación interna Estructura\config BKP – AP – Manuales).

Exchange 2010:

Se realiza un Backup full de lunes a domingo a las 13:00 am (se realiza un backup de las bases Activos, informática y Public Folder Database1.

Backups VMware:

Estos backups son realizados los fines de semana cada cuadro semanas, y son sólo full. Los mismos se realizan en los medios LTO5 según se detalla a continuación:

VM_CSWVIIS1: Se realiza un Backup full el domingo a las 0:00 am (se realiza un backup que contiene a la virtual CSWVII1).

VM_DC-DHCP-EXN: Se realiza un Backup full el sábado a las 3:00 am (se realiza un backup que contiene a la virtuales CSWVDC1, CSWVDHCP1, CSWVEXN1).

VM_EXMBX1-CSWVVCS61: Se realiza un Backup full el sábado a las 0:30 am (se realiza un backup que contiene a la virtual CSWVEXMBX1 y CSWVVCS61).

VM_TMG01-TMG06: Se realiza un Backup full el sábado a las 8:00 am (se realiza un backup que contiene a la virtuales CSWVTMG01 y CSWVTMG06).

VM_CSWVRADIUS-CSWVPS: Se realiza un Backup full el domingo a las 17:00 pm (se realiza un backup que contiene a la virtuales CSWVRADIUS y CSWVPS).

VM_CSWVSS-CSWVSSS: Se realiza un Backup full el sábado a las 0:00 am (se realiza un backup que contiene a la virtuales CSWVSS y CSWVSSS).

VM_CSWVTMG05-CSWVRPT: Se realiza un Backup full el sábado a las 12:00 am (se realiza un backup que contiene a la virtuales CSWVTMG05 y CSWVRPT).

VM_PPSDB-PPSIIS: Se realiza un Backup full el domingo a las 8:00 am (se realiza un backup que contiene a la virtuales CSWVPPSDB y CSWVPPIIS).

VM_MSWVAPP1-MSWVFS: Se realiza un Backup full el domingo a las 3:00 am (se realiza un backup que contiene a la virtuales MSWVAPP1 y MSWVFS).

VM_CSWVVCS-CSWVME: Se realiza un Backup full el sábado a las 12:00 pm (se realiza un backup que contiene a la virtuales CSWVVCS y CSWVME).

VM_CSLREDMINE02: Se realiza un Backup full el domingo a las 5:00 am (se realiza un backup que contiene a la virtual CSLREDMINE02).

Pruebas de Restore

Tanto en juncal como en Balcarce se realizan pruebas de restore para verificar la consistencia de los backups, en el caso de Juncal se pudo observar que los mismos no tienen una frecuencia establecida, en cambio en Balcarce se realizan de manera semanal.

Dichas pruebas consisten en la restauración de mails de una casilla en particular, restauración de archivos de backup de bases de datos, restauración de VM, restauración de archivos de file server. Dado que la restauración de las VM lleva bastante tiempo, esta prueba se realiza de manera más espaciada. Se documentan dichas recuperaciones en un archivo Excel

2.- Análisis de la Política de Seguridad de la Información

La política de seguridad de la Información se dictó en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo. Esta debe ser conocida y cumplida por toda la planta de personal del Organismo, tanto se trate de funcionarios políticos como técnicos, y sea cual fuera su nivel jerárquico y su situación de revista.

En este sentido se procedió analizar la última modificación de la Política de Seguridad de la SLyT aprobada el 12 de agosto de 2014. La misma fue elaborada teniendo en cuenta lo normado por Decisión Administrativa 669/04 y Disposición Nº 6/2005 de la ONTI.

De dicho análisis se pudo verificar que las normas utilizadas para la confección de dicha política de seguridad no se encuentran vigentes. Toda vez que la Decisión Administrativa 669/04 fue modificada por Decreto N° 1067/2015 y la Disposición ONTI Nº 6/2005 la fue reemplazada por la Disposición ONTI Nº 3/2013 y a su vez esta fue reemplazada por la Disposición ONTI Nº 1/2015. En este sentido esta UAISLyT entiende que la Política de Seguridad de la Información de la SLyT se encuentra desactualizada, debiendo ser adecuada y actualizada conforme normativa vigente.

Al propio tiempo se constató que la estructura definida en la Política de la Seguridad de información de esta Secretaría, no guardaría relación con la normada en la Disposición Nº 1/2015 de la ONTI, que determina Cuatro capítulos introductorios, con los términos generales y el establecimiento de la Evaluación y el Tratamiento de los riesgos, divididos en 1-Introducción, 2-Terminos y Definiciones, 3-Estructura de la Política Modelo, y 4-Evaluación y Tratamiento del Riesgo.

Y Catorce cláusulas que abarcan los diferentes aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente. Cada cláusula contiene un número de categorías o grupo de controles de seguridad principales.

Las catorce cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

- Política de Seguridad (1) - Política de Seguridad de la Información
- Organización (2) - Organización Interna - Dispositivos móviles y trabajo remoto
- Recursos Humanos (3) - Antes del Empleo - Durante el Empleo – Cese del Empleo o cambio del puesto de trabajo
- Gestión de Activos (3) - Responsabilidad sobre los activos - Clasificación de la Información - Gestión de medios
- Gestión de Accesos (5) - Requerimiento para la Gestión de Acceso - Administración de Gestión de Usuarios - responsabilidades del Usuario - Control de Acceso a Sistemas y Aplicaciones - Control de Acceso al sistema operativo
- Criptografía (1) - Cumplimiento de requisitos Legales
- Seguridad Física y Ambiental (2) - Áreas seguras - Emplazamiento y protección de equipos
- Seguridad de las Operaciones (7) - Procedimientos y responsabilidades operativas - Protección contra malware (código malicioso) - Resguardo (backup) - Registro y monitoreo - Control de software operacional - Administración de vulnerabilidad técnica - Consideraciones sobre auditoría de los sistemas de información
- Seguridad de las Comunicaciones (2) - Gestión de red - Procedimientos y controles de intercambio de la información
- Adquisición, Desarrollo y Mantenimiento de Sistemas (5) - Requerimiento de Seguridad de los Sistemas - Seguridad en los Sistemas de Aplicación - Seguridad de los archivos del Sistemas - Seguridad de los procesos de desarrollo y soporte - Vulnerabilidad técnica
- Relaciones con Proveedores (2) - Seguridad de la información en las relaciones con el proveedor - Supervisión y revisión de los servicios del proveedor
- Gestión de Incidentes de seguridad de la información (2) - Informe de eventos y debilidades de la seguridad de la información - Gestión de los incidentes y mejoras de la seguridad de la información
- Gestión de la Continuidad del Organismo (2) - Gestión de continuidad del Organismo - Redundancias
- Cumplimiento (3) - Cumplimiento de requisitos legales - Revisiones de la Política de Seguridad y la compatibilidad Técnica - Consideraciones de Auditorías de Sistemas

Por último, por cada categoría, se establece un objetivo y contiene uno o más controles a realizar.

A modo de síntesis se enuncia a continuación la estructura de cada cláusula o dominio:

1. Generalidades
2. Objetivos
3. Alcance
4. Responsabilidades
5. Política
    - Categorías
    • Objetivo
    - Controles

Del mismo modo se pudo constatar que al diseñar la Política de Seguridad de la información para la SLyT no se contemplaron todos los ítems establecidos en el Modelo de Política de Seguridad de la información para organismos de la Administración Pública Nacional aprobado por la ONTI. Puntualmente en lo que hace referencia al compromiso de confidencialidad.

Así mismo mediante acta de reunión del día 28/7/2011 el Comité de Seguridad de la Información determinó en lo que refiere al acuerdo de confidencialidad denominado "Compromiso de Confidencialidad" dejar sin efecto el acuerdo de confidencialidad aprobada por acta número 2. Toda vez que el Comité consideró que sería suficiente con el hecho que el personal de los distintos organismos que integran la SLyT, al ingresar a sus puestos de trabajo, tengan como requisito firmar documentación que certifica el vínculo laboral donde se incluyen temas de confidencialidad. Así mismo en el Acta mencionada precedentemente se aprueba un acuerdo de confidencialidad para personal externo a la SLyT

En nuestra opinión debería existir el acuerdo de confidencialidad para los agentes internos de la SLyT, ello en concordancia con lo que establece la Disposición 1/2015 de la ONTI en su apartado -7.1.3 Control: Términos y condiciones de contratación.- y el Modelo de Política de Seguridad de la información para organismos de la Administración Pública Nacional aprobado por la ONTI, ambos mencionan que: *"como parte de sus términos y condiciones iniciales de empleo, los empleados cualquiera sea su situación de revista,* ***firmará un compromiso de confidencialidad*** *o no divulgación, en los que respecta al tratamiento de la*

información del Organismo". Así mismo aclara que la copia firmada del Compromiso debe ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

Es dable destacar que la Política de Seguridad de la Información en su apartado 6 - "Organización"- establece que: "*La seguridad de la información es una responsabilidad del Organismo, 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 de la información. El* ***Comité de Seguridad de la Información es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo.*** *El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.* El último Comité de Seguridad de la Información nombrado por Resolución 74/2012 de la SLyT, dejó de cumplir con sus funciones, dado que la mayoría de sus miembros no pertenecen más a esta Secretaría.

3.- Data Center

Se procedió analizar el "Manual de Normas y Procesamientos para el Acceso Físico al Data Center" emitida el 2 de marzo de 2016. Esta UAI SLyT no pudo verificar que la misma haya sido aprobada por el Comité de Seguridad de la Información.

Cabe destacar que en el ámbito de la Secretaría Legal y Técnica existen 2 Data Center, uno ubicado en la sede de Suipacha y otro en la sede de Balcarce.

1.1.1 Data Center Sede Suipacha:

En términos generales se pudo constatar que el Manual de Normas y Procesamientos para el Acceso Físico al Data Center se estaría cumpliendo, con la salvedad de los puntos que se detallan a continuación:

Sobre el punto V.V1.3. que indica que: *"Cada Jefe o Director de informática será responsable de la administración del equipo instalado en el Centro de Datos respectivo, según corresponda, los cuales entre otras cosas, deberán definir los tiempos estimados de vida útil para programar con anticipación el cambio oportuno de los mismos"*. Se pudo constatar que el responsable del DC no poseía dicha información.

Sobre el punto V.V2.6. que determina: *"El Jefe de Informática deberá gestionar el mantenimiento preventivo y/o correctivo de las instalaciones eléctricas y demás sistemas de protección por lo menos una vez al año o la periodicidad que indique el grado de certificación del Centro de Datos"* se envió a esta UAI auditoria externa realizada por la empresa TESLA el 20 de diciembre de 2016, con el siguiente Objeto: *"Describir el estado de situación de las instalaciones eléctricas asociadas al nuevo CPD (centro de procesamiento de datos) BOLETIN OFICIAL de la calle Suipacha 767 de la Ciudad Autónoma de Buenos Aires"* Este informe tiene varias recomendaciones que a la fecha siguen pendientes de regularización.

1.1.2 Data Center Sede Balcarce:

En términos general se pudo constatar que el Manual de Normas y Procesamientos para el Acceso Físico al Data Center se estaría cumpliendo, con la salvedad de los puntos que se detallan a continuación:

Con referencia al punto V.V2.6 del Manual de Normas y Procesamientos para el Acceso Físico al Data Center, el responsable del Data Center no pudo suministrar a esta Auditoria información sobre el último control realizado sobre la *situación de las instalaciones eléctricas del DC.*

SECRETARÍA LEGAL Y TÉCNICA
DE LA PRESIDENCIA DE LA NACIÓN

UNIDAD DE AUDITORÍA INTERNA
INFORME FINAL N° xxx/2017

"PROCEDIMIENTOS INHERENTES A LA ADMINISTRACIÓN Y CONTROL DE LOS RECURSOS INFORMÁTICOS"

ANEXO IV

En relación a las principales aplicaciones utilizadas por esta Secretaría las mismas se detallan por ámbito de aplicación:

Principales Aplicativos dentro del ámbito - NIC AR

Se detallan las aplicaciones de uso interno y externo

1. Internas
   1.1. Infraestructura (Sistemas): Aplicaciones para uso y administración del sector de infraestructura.
   - GAPRS: Aplicación de monitoreo para monitoreo de publicación de zonas de DNS.
   - Fred: Core de negocios de Nic.ar
   - Mailer: Aplicación de envíos de mail de NIC.
   - Autozona: Aplicación para controlar las publicaciones de zona de DNS y evitar errores.

   1.2. Comisión Fiscalizadora
   - Gestión Financiera: Aplicación para comisión fiscalizadora que permite ver los reportes de los ingresos de NIC.

   1.3. Acceso libre NIC
   - APPNIC: Intranet para NIC
   - Vilma: Backend de NIC para uso de soporte de varios niveles.
   - Socializar: Aplicación

2. Externas
   2.1. Públicas
   - NIC: Web de publicación y administración de dominios de internet .AR
   - Punto.ar: Web de formularios de contacto para atención al público de Nic.ar

Principales Aplicativos dentro del ámbito - Boletín Oficial

Nombre de la aplicación	Tipo	Descripción	Tipo de Usuario	Tipo de Licencia	Vto. de Licencia
Web Boletín Oficial	Publica	WEB Publica del Boletín Oficial de la República Argentina, es el medio oficial en el que se publican los actos emanados del Poder Ejecutivo Nacional y las leyes sancionadas por el Congreso de la Nación. La publicación de una norma en el Boletín Oficial, es un paso necesario para que esta norma pueda entrar en vigencia. A su vez, los documentos que aparecen en el Boletín Oficial son tenidos por auténticos y obligatorios por el efecto de dicha publicación, y por comunicados y circulados dentro de todo el territorio nacional. Primera Sección: Legislación y Avisos Oficiales Segunda Sección: Sociedades Tercera Sección: Contrataciones Cuarta Sección: Dominios de Internet	Publico	Desarrollo Interno (DI)	N/A
Publicaciones	Interna	Aplicación core de BORA para la Gestión de avisos de 1a 2da y 3a sección cargados por Organismos, Sociedades, Juzgados, que se publican en el Boletín Oficial tanto en la versión Web como en la versión impresa.	Publicaciones, Atención al Público, DV, Cta Cte.	(DI)	N/A
Extranet Presidencia	Privada	Carga de Avisos de 1a Sección desde Presidencia de la Nación	Dirección General de Despacho y Decretos, Subsecretario Técnico	(DI)	N/A
Delegación Virtual (DV)	Publica	Aplicación Pública para el ingreso de avisos Comerciales para publicar en el Boletín Oficial en 2da Sección.	Publico (con restricciones)	(DI)	N/A
Extranet Oficial (EN)	Publica	Aplicación Pública para que Organismos y Juzgados Publiquen avisos en el Boletín Oficial.	Publico (con restricciones)	(DI)	N/A
Precargados (PC)	Publica	Aplicación Publica para buscar avisos (Sucesorios) ya cargados y efectuar el pago de los mismos	Publico	(DI)	N/A

Nombre de la aplicación	Tipo	Descripción	Tipo de Usuario	Tipo de Licencia	Vto. de Licencia
Suscripciones	Interna	Sistema de gestión de Suscriptores para Alertas y ediciones del Boletín Oficial	Suscripciones	(DI)	N/A
Back End Extranet Judicial / Oficial 1.5	Interna	Aplicación para ABM de Usuarios Públicos de EXTRANET Oficial, en la cual se gestiona el Alta de usuarios y se asocia la Tarjeta de Coordenadas correspondiente	Publicaciones	(DI)	N/A
Gestión Operativa – Back de DV y PC	Interna	Gestión de Avisos cargados en DV y PC, los cuales una vez gestionados pasan a la aplicación de Publicaciones.	DV	(DI)	N/A
Firmantes – Sistema de operativa – Clientes / Administración	Interna	Aplicación para Registro de Firmas - primer paso a efectuar por los interesados en realizar publicaciones a través de Delegación Virtual en el cual se da de Alta a los usuarios y se asocia la Tarjeta de coordenadas respectiva	Firmantes	(DI)	N/A
Pgplattform	Interna	Aplicación para alta de usuarios Administradores los cuales pueden administrar firmantes.	Firmantes	(DI)	N/A
BAS	Interna	Sistema de Gestión de Facturación de los Avisos publicados en el Boletín Oficial,	Atención al Público, DV, Cta Cte.	Provisto por terceros	Licencia Perpetua
Cuentas Corrientes	Interna	Aplicación para gestionar las Cuentas Corrientes de los Organismos y proceder a la facturación, por intermedio de BAS, de los Avisos ya publicados en el Boletín Oficial	Cta Cte.	(DI)	N/A
Ciclope	Interna	Herramienta documental provista por Dot SA; originalmente para el reemplazo de Bolex, pero solo fue cambiada la interfaz de carga.	Publicaciones	-	-
Convera	Interna	Herramienta de indexación y creación de bases de datos documentales. Utilizada para la indexación de los PDF del Boletín Oficial.	Actualmente fuera de uso.	(DI)	N/A

Nombre de la aplicación	Tipo	Descripción	Tipo de Usuario	Tipo de Licencia	Vto. de Licencia
Binfovir	Interna	Aplicación de auto consulta para el usuario de Biblioteca e Informes (Secciones 1ra, 2da y 3ra).	Publicaciones, Atención al Público, DV, Cta Cte.	(DI)	N/A
Apoyin	Interna	Para gestión administrativa de Apoyo Informático de la DNRO, que devino en una página de consulta sobre la recaudación de la DNRO.	Dirección Administrativa Contable	(DI)	N/A
Informes Segunda	Interna	Aplicación de Biblioteca e Informes para el enriquecimiento de información contenida en las publicaciones de segunda sección.	Atención al Publico	(DI)	N/A
Aplicación Oficios	Interna	Recepción y gestión de Oficios, pedidos de informes, contestación y notificación a usuarios sobre temas referidos a la población de avisos.	Mesa de Entradas	(DI)	N/A
Bolex	Interna	Aplicación de Biblioteca e Informes para el enriquecimiento de información contenida en las publicaciones de primera sección, y la gestión de normativa actualizada.	Publicaciones	(DI)	N/A
Atención al Cliente	Interna	Registro y Gestión de consultas de llamadas del Publico	Call Center	(DI)	N/A
Generación de tarjetas coordenadas DV	Interna	Generación de tarjetas de coordenadas para ser utilizadas por DV y Extranet Oficial	Sistemas	(DI)	N/A
Desbloqueo de Tramites - ABM Org. - Bandejas Tramites	Interna	Aplicación para Desbloqueo de trámites, ABM de Organismos y Modificación de estados de Tramites de Publicaciones	Sistemas	(DI)	N/A
Tarjetas de Accesos - Molinetes de Ingreso	Interna	Aplicación para gestión de Tarjetas de accesos de Público y de Agentes del Boletín Oficial.	Guardia, RRHH (Suipacha)	Provisto por terceros	Licencia Perpetua
TBS BioAdmin	Interna	Gestión y Administración de Biométrico - Suipacha	RRHH Suipacha	Provisto por terceros	Licencia Perpetua
SmartPSS (Cámaras NVR – Suipacha – campichuelo - NIC)	Interna	Aplicación para Gestionar y Monitorear por medio de las Cámaras de circuito cerrado.	Guardia, Dirección Nacional, Sistemas	Provisto por terceros	Licencia Perpetua

Nombre de la aplicación	Tipo	Descripción	Tipo de Usuario	Tipo de Licencia	Vto. de Licencia
Gestión de Asterisk	Interna	Gestión Y Administración de Líneas Telefónicas e Internos y estadísticas de llamadas	Sistemas	Provisto por terceros	Licencia Perpetua
Comap	Interna	Monitoreo y Alertas de Grupo Electrógeno	Sistemas	Provisto por terceros	Licencia Perpetua
Poseidon	Interna	Monitoreo y Alertas de Temperatura y Humedad de DC	Sistemas	Provisto por terceros	Licencia Perpetua
Servicedesk	Interna	Sistema de gestión de Tickets cargados por los usuarios Internos de las distintas sedes	Usuarios, Sistemas	Licencia	Sin información
Input Info Solution - Kodak	Interna	Software Input Info Solution que se usa en el proceso de Digitalización de Documentación con los escaners Kodak	Digitalización	Licencia	-
APP movile – Android + Apple	Publica	Ídem Web Boletín para Movile	Publico	(DI)	N/A
Google Analitics	Privada	Estadísticas de Acceso y utilización de la WEB del Boletín Oficial	Dirección Nacional	Provisto por terceros de licencia gratuita	N/A
Estadisticas Google Play + Apple Store	Privada	Estadísticas de descargas y usos de la APP Móviles	Dirección Nacional	Provisto por terceros de licencia gratuita	N/A

Principales Aplicativos dentro del ámbito - Balcarce

Nombre de la aplicación	Tipo	Descripción	Tipo de Usuario	Tipo de Licencia	Vto. de Licencia
Intranet	Desarrollo propio	Intranet de la Secretaria Legal y Técnica	Interno de la SLYT	(DI)	N/A
Redmine DASI	Customizacion Freeware	Ticket para reportar incidentes a DASI	Freeware	N/A	N/A
Redmine Infraestructura DGA	Customizacion Freeware	Ticket para solicitar tareas a la UCS Infraestructura	Freeware	N/A	N/A

Nombre de la aplicación	Tipo	Descripción	Tipo de Usuario	Tipo de Licencia	Vto. de Licencia
APO	Desarrollo ADC	Automatización de Procesos Operativos	Desarrollo ADC sin Licencia	(DI)	N/A
APO v2	Desarrollo ADC	Automatización de Procesos Operativos 2	Desarrollo ADC sin Licencia	(DI)	N/A
Autogestión RRHH	Desarrollo ADC	Gestión de Ausencias, Licencias y recibos de sueldo	Desarrollo ADC sin Licencia	(DI)	N/A
PSA	Desarrollo ADC	Sistema Administrativo Financiero, Patrimonio, Insumos	Desarrollo ADC sin Licencia	(DI)	N/A
Meta4	Software	Gestión de RRHH y Nomina	Licenciado	Perpetua	Sin vencimiento
SARHA	Desarrollo AFIP Decreto 888/2016 Min Modernización.	Gestión de RRHH y Nomina	Decreto 888/2016 MM	N/A	N/A
Owncloud	Freeware	Compartidor de Documentos en la Web	Freeware	N/A	N/A