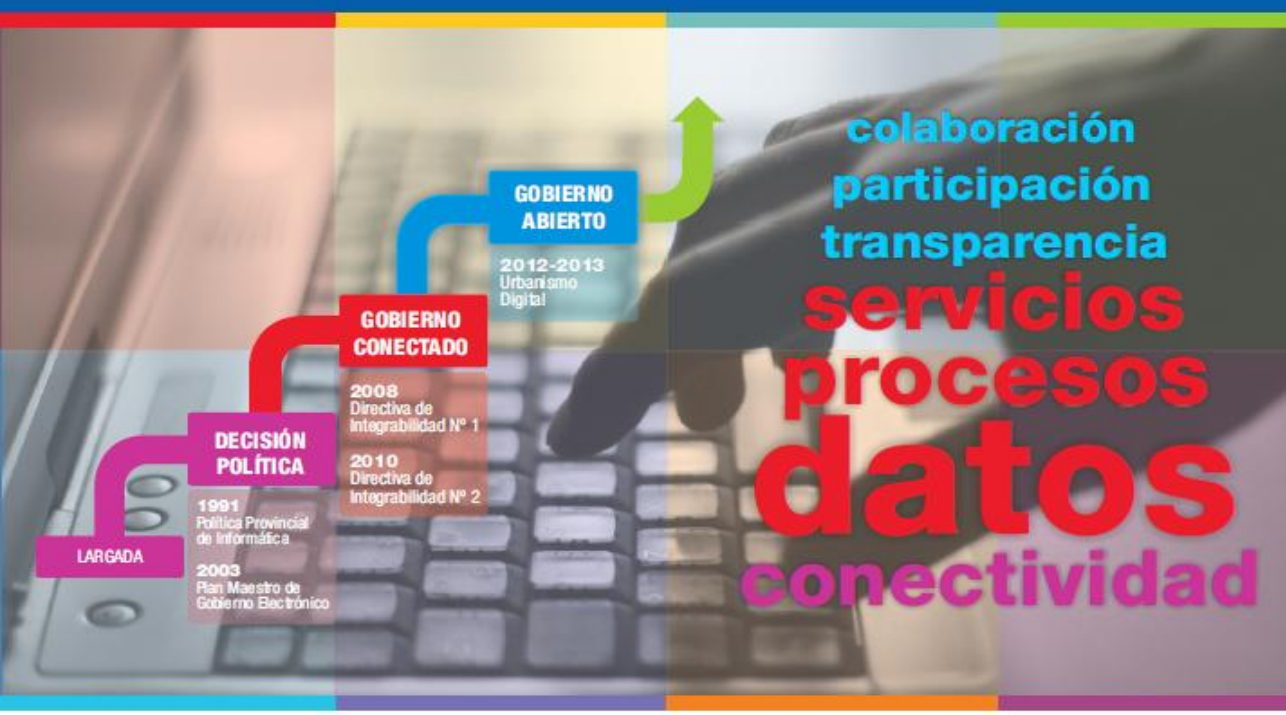
PRIMERA EDICIÓN - MARZO 2014

Referencial
IRAM
Nº 14-1

REQUISITOS DE CALIDAD DE LAS APLICACIONES INFORMÁTICAS

Integrabilidad



IRAM
Instituto Argentino de Normalización y Certificación

SECRETARÍA DE GESTIÓN PÚBLICA
GOBIERNO DE LA PROVINCIA DEL NEUQUÉN
Ministerio de Coordinación de Gabinete, Seguridad y Trabajo

neuquén
Es compromiso. Es dignidad. Es progreso. Es valor ganado.

IRAM

Referencial Nº 14-1

Primera edición
Marzo 2014

Requisitos de calidad de las aplicaciones informáticas

Integrabilidad

Parte 1 – Descripción general. Proceso de evaluación

Marzo 2014

Primera Edición
Marzo de 2014 ©

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante en la Argentina de la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

La Secretaría de la Gestión Pública del Gobierno de la Provincia de Neuquén en el marco del Plan Maestro de Gobierno Electrónico y el modelo de Urbanismo Digital, es el órgano impulsor de las iniciativas de Integrabilidad de las aplicaciones informáticas para el intercambio de datos y la convivencia digital.

Este referencial IRAM Nº 14 bajo el título general *"Requisitos de calidad de las aplicaciones informáticas- INTEGRABILIDAD"*, es el resultado del trabajo conjunto de los profesionales de ambas instituciones, la colaboración de profesionales de ThinkNet S.A. y del Laboratorio LTSL (Laboratorio de Testing San Luis).

El mismo consta de las partes siguientes:

Parte 1 - *Descripción general – Proceso de evaluación,*

Parte 2 - *Secuencia de comunicación; Atributos de las capas y Métricas de Testing.*

Está previsto para que ambos deban ser usados en forma conjunta en la versión vigente.

Índice

Página

Integrabilidad

Parte 1 – Descripción general. Proceso de evaluación

0 INTRODUCCION

Uno de los mayores desafíos que presenta la utilización de diversas aplicaciones o sistemas informáticos dentro de la función pública, es salvar la dificultad de los productos de software para integrarse con otros sistemas.

Para atender esta situación, es de gran importancia contar con criterios que permitan evaluar previamente a su incorporación, la capacidad de integración (INTEGRABILIDAD) de una aplicación informática, es decir: la capacidad que tendrá el producto de software de interoperar en distintos escenarios con otras aplicaciones y formar parte de un sistema de nivel superior. Este macro sistema genera un **entorno informático** en el cual conviven las diversas aplicaciones.

El modelo promulgado por las Directivas de Integrabilidad define las reglas de integración que buscan, por diseño, alcanzar un grado de convivencia digital que permita realizar las siguientes acciones:

- Resguardar la **seguridad** de la información identificando a todos los actores, tanto sean personas como sistemas, cubriendo el extenso espectro que va desde el Habeas Data al Open Data.

- Compartir los **datos** desde sus propias Fuentes Auténticas.

- Crear participativamente (Co-crear) los **procesos** que atraviesan tanto las organizaciones como los diversos sistemas involucrados.

- Liberar **servicios** en forma abierta para que puedan ser extendidos por otros actores y desarrolladores. (Liberando la última milla).

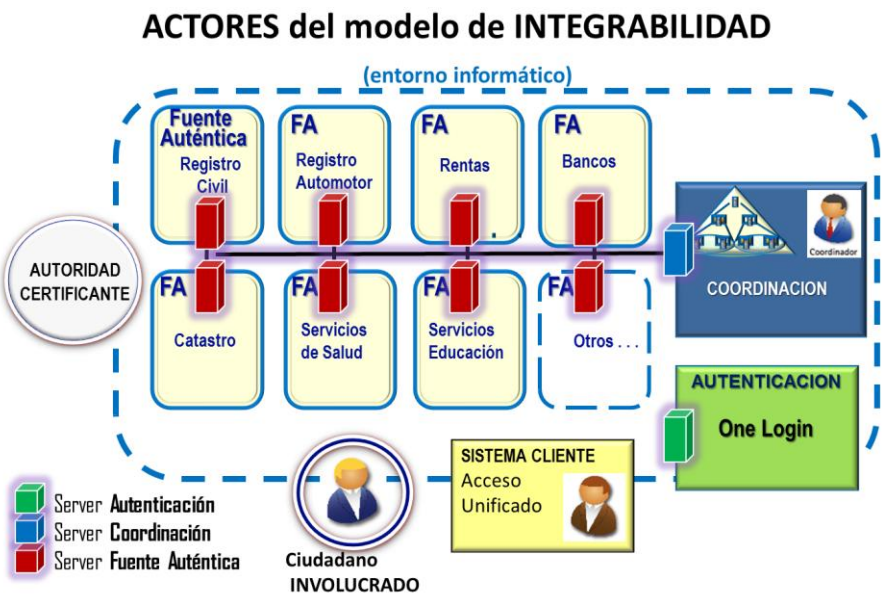
Esta jerarquía de necesidades fundamentales se esquematiza en una pirámide de cuatro capas, a saber; **SEGURIDAD, DATOS, PROCESOS** y **SERVICIOS.**

Pirámide de Necesidades

Dentro de este esquema, se entiende que un sistema o aplicación se puede ubicar en una o más capas del entorno informático, adoptando un "**Comportamiento Cliente**" cuando requiere servicios de otras aplicaciones, o un "**Comportamiento Proveedor**" cuando los ofrece.

Para satisfacer estas necesidades, en la provincia del Neuquén se ha desarrollado la PLATAFORMA de INTEGRABILIDAD.

Esta Plataforma de Integrabilidad provee los Actores estructurales necesarios para una convivencia digital equilibrada, conformando un macro sistema donde: la Autenticación está centralizada, la Autorización distribuida en función de las estructuras de poder (provincial, municipal y/o sectorial) y la Auditoría atomizada entre todos los actores involucrados, logrando total transparencia.



En las siguientes tablas se muestran:

- Los Actores provistos por la Plataforma de Integrabilidad

Actores cubiertos por la Plataforma de INTEGRABILIDAD
Servidor **LDAP**
Servidor **Autenticador**
Servidor **One Login**
Servidor **Coordinador**
Servidor **Fuente Auténtica**

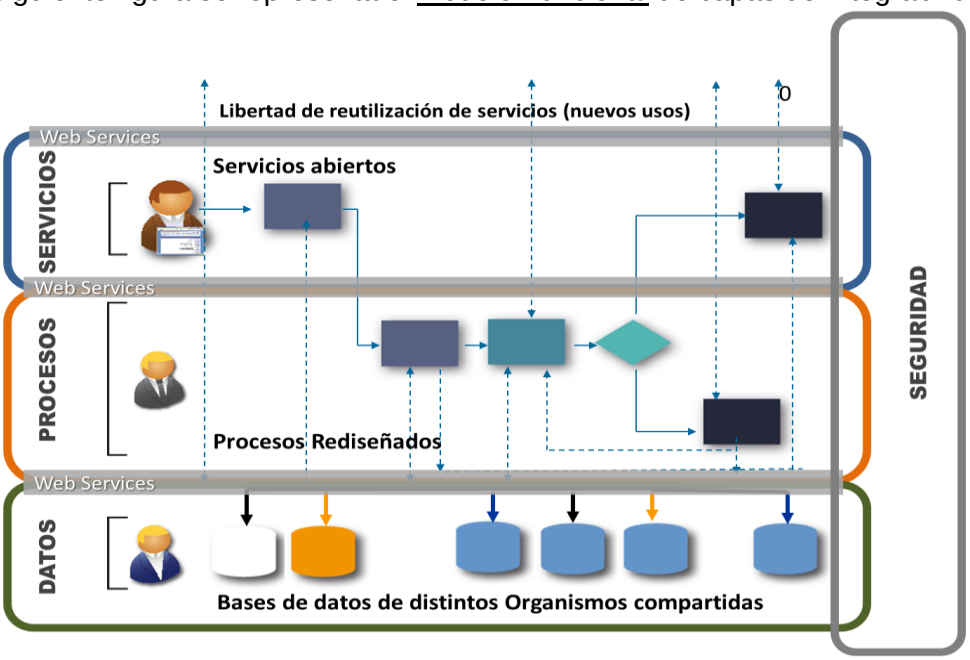
- Los roles que asumen las aplicaciones en función de los comportamientos que se requieran dentro del entorno informático.

Comportamiento	Roles de las Aplicaciones o sistemas a Certificar
Cliente de DATOS	App Cliente
Proveedor de DATOS	App Proveedora
Proveedor de PROCESOS	Motor de WorkFlow
Cliente de PROCESOS	App cliente WorkFlow
Proveedor de SERVICIOS	App Última Milla

Estos Actores interactúan mediante **protocolos** que fueron especificados en función de cubrir las necesidades planteadas por cada una de las cuatro capas: Seguridad, Datos, Procesos y Servicios y sus interrelaciones.

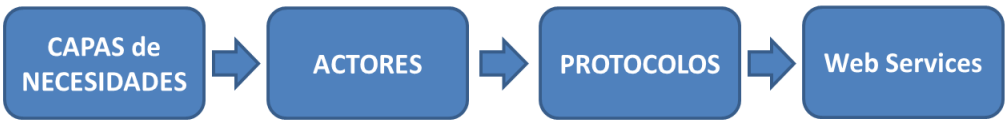
Cada capa tiene definidos protocolos de comunicación tanto para el **comportamiento cliente** como para el **comportamiento proveedor**.

En la siguiente figura se representa el modelo Funcional de capas de Integrabilidad.



El cumplimiento de los protocolos demuestra la capacidad de una aplicación de proveer servicios de información en la/s capa/s que le corresponda (comportamiento proveedor) y recibir los que requiere de otros por una vía similar (comportamiento cliente).

La línea de razonamiento contenida en este Referencial de Integrabilidad es:



1 OBJETO, CAMPO DE APLICACIÓN Y ALCANCE

El objeto de este Referencial es asegurar una descripción clara y consistente para realizar la evaluación y certificación de conformidad por parte del IRAM de cualquier producto de software o aplicación informática para la que se requiera un certificado de Integrabilidad, así como todas aquellas aplicaciones utilizadas o a ser incorporadas por los Organismos Centralizados y Descentralizados del Poder Ejecutivo Provincial.

Es responsabilidad de la **SGP**, mantener actualizadas las especificaciones de los protocolos de comunicación a medida que el entorno informático y las posibilidades tecnológicas vayan evolucionando. Estas actualizaciones se encuentran disponibles on-line y deberán ser consultadas conjuntamente y complementariamente con este referencial.

Este Referencial junto a la Política Informática, el Plan Maestro de Gobierno Electrónico, el modelo de Urbanismo Digital y las Directivas de Integrabilidad de la Secretaría de Gestión Pública del Gobierno de la Provincia del Neuquén **(SGP)**, contribuyen con las directrices que propende la Provincia del Neuquén, estando en concordancia con las corrientes internacionales sobre el uso confiable y compartido de datos.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Todo documento normativo que se menciona a continuación es indispensable para la aplicación de este documento.

Cuando en el listado se mencionan documentos normativos en los que se indica el año de publicación, significa que se debe aplicar dicha edición. En caso contrario, se debe aplicar la edición vigente, incluyendo todas sus modificaciones.

IRAM-NM-ISO/IEC 9126-1:2009 Tecnología de la información. Ingeniería de software. Calidad del producto. Parte 1 - Modelo de calidad. (ISO/IEC 9126-1:2001, IDT).

ISO/IEC TR 9126-2:2003 Software engineering – Product quality - Part 2: External metrics.

Decreto N° 0405/1991 Política provincial de informática.

Plan Maestro de Gobierno Electrónico Provincia del Neuquén (2003).

Directiva 001 GE – 2008 SEGPyCE Integrabilidad.

Directiva 002 GE – 2010 SEGPyC Integrabilidad de la Resolución 220/10.

Wiki de INTEGRABILIDAD http://wikiintegra.neuquen.gov.ar/doku.php.

3 DEFINICIONES

App-Cliente: Es un sistema o aplicación que requiere datos de fuente auténtica para realizar sus operaciones.

App-Proveedora: Es un sistema o aplicación que administra datos de una Fuente Auténtica y que son requeridos por otros organismos.

App-Cliente-Workflow: es una aplicación que está subordinada al motor de workflow.

App-Última-Milla: es una aplicación que utilizando servicios de una o varias aplicaciones, los combina y unifica de una nueva manera.

Certificación de Integrabilidad: Es la acción llevada a cabo por una entidad reconocida e independiente de las partes interesadas (por ejemplo el IRAM), mediante la cual se determina que una aplicación o un sistema Informático cumple con todas las características respectivas a los comportamientos requeridos en cada capa, así como también con las disposiciones o especificaciones técnicas aplicables.

Fuente Auténtica (FA): Cada organismo del Estado, según sus competencias, es responsable del proceso de creación mantenimiento y seguridad de algún tipo de registración y es, por lo tanto, la fuente auténtica de dichos registros. El mantenimiento de los Datos significa que ellos sean Correctos, Completos y Vigentes. Estos datos serán soportados por aplicaciones proveedoras de datos y ofrecidos mediante un Servidor de Fuente Auténtica.

Integrabilidad: Es la capacidad que tiene un producto de software de integrarse con otros para intercambiar datos y servicios de manera segura y formar parte de un sistema de nivel superior.

MABAC: del inglés “Multi Level Attribute Based Access Control” es un modelo de autorización diseñado para ambientes abiertos y multi-organizacionales, pudiendo autorizar por usuario nominado, puestos, áreas jerárquicas, grupos internos y grupos de usuarios externos (definidos por otra Fuente Auténtica).

Protocolos de Integrabilidad: son secuencias especificadas de mensajes entre los actores de Integrabilidad para poder realizar las operaciones en cada capa del modelo. Este protocolo se basa en la desconfianza entre los actores en ambientes abiertos como internet y fue desarrollado conjuntamente con la Universidad Nacional del Comahue.

Servidor-Autenticador: es un servidor que brinda servicios de autenticación centralizada tanto para sistemas como para usuarios, entregando “pases” de validez temporal (tickets) para operar en el entorno informático.

Servidor-Coordinador: es un servidor que brinda servicios de autorización tanto para sistemas como para usuarios mediante el modelo MABAC. Existen servidores coordinadores distribuidos según la estructura de poder: provincial, municipal, sectorial etc.

Servidor de Fuente Auténtica: es un servidor que brinda servicios de seguridad y acceso a datos mediante los protocolos definidos para facilitar la rápida entrada en operación de sistemas heredados que utilizan los organismos responsables de una Fuentes Auténtica.

Servidor LDAP: del inglés “Lightweight Directory Access Protocol “es un servidor que cumple con dicho protocolo de acceso a directorios. En este servidor se registran todos los actores (sistemas y usuarios) que forman parte del entorno informático.

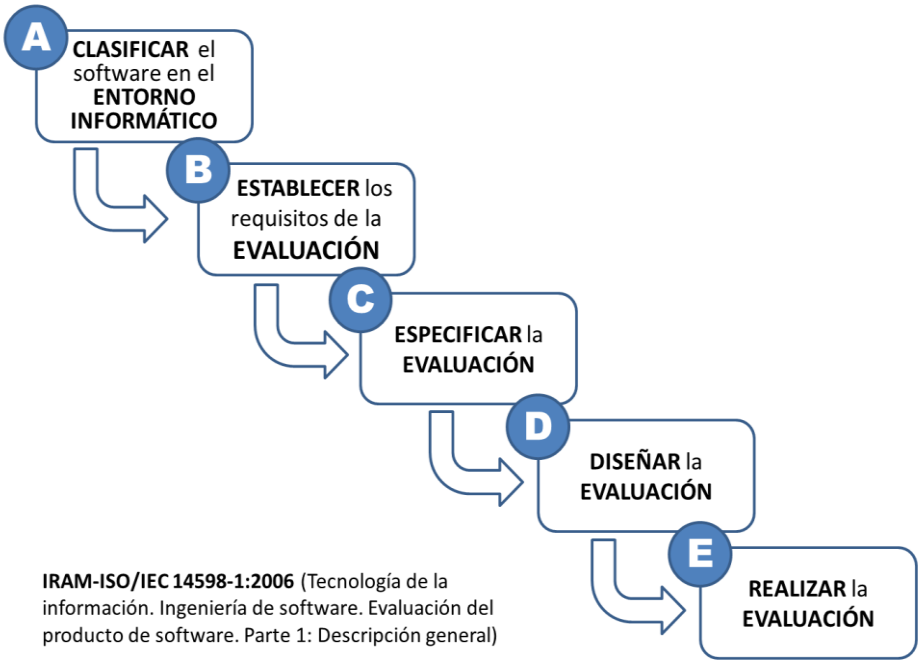
Servidor One-Login: es un servidor que permite a los usuarios acceder a varias aplicaciones o sistemas con una sola instancia de identificación o autenticación.

Servidor-Workflow: Es una aplicación que ejecuta los flujos de trabajo de uno o varios procesos.

4 PROCESO DE CERTIFICACIÓN DE INTEGRABILIDAD

4.1 Proceso de certificación

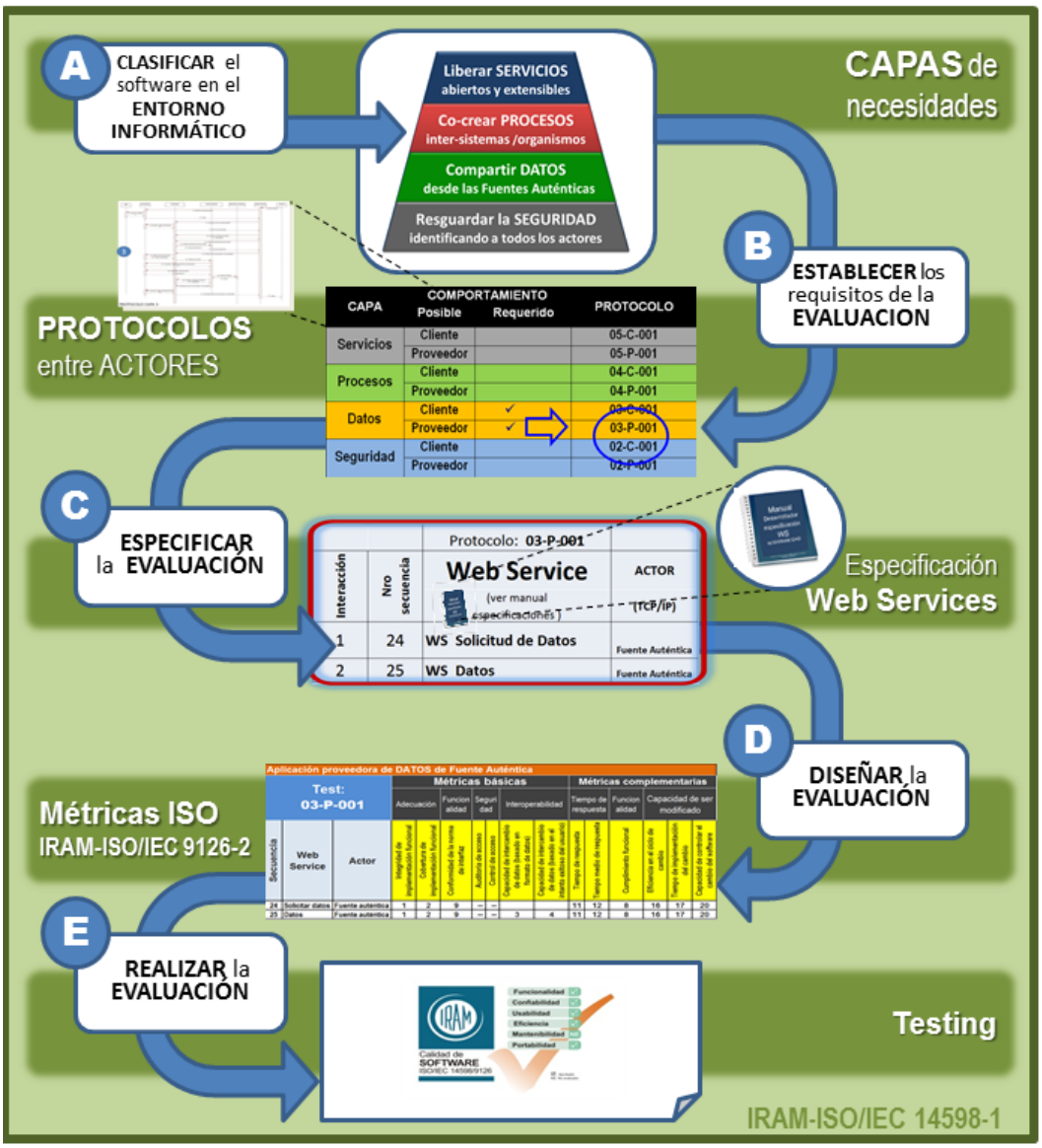
El proceso de certificación de la característica de Integrabilidad puede esquematizarse en el siguiente diagrama:



En concordancia con la norma IRAM-ISO/IEC 14598-1: la evaluación de conformidad se realiza a partir de la definición de los atributos cuantificables a medir, el método de medición, sus escalas y niveles de puntuación.

4.2 Esquematización del proceso de Certificación

El proceso completo de evaluación se resume en la siguiente infografía:



El proceso concluye con la emisión de una certificación de cumplimiento y/o recomendaciones de ajustes a la aplicación para operar según los lineamientos de la Directiva de Integrabilidad.

4.3 Actividades para la certificación

A continuación se indican las actividades para cumplir con el proceso de certificación, así como los criterios para la selección de los atributos, y el método de medición de los mismos a través de la selección de métricas.

Por lo tanto, para toda aplicación o producto software que requiera certificar la calidad de sus características de INTEGRABILIDAD se debe:

4.3.1 Clasificar el software en el entorno informático

Clasificar el software implica analizar sus roles dentro del entorno informático y determinar los comportamientos requeridos en función de los servicios que va a "suministrar y/o consumir". Es decir como cliente o como proveedor.

La determinación de estos comportamientos requeridos para la aplicación se realiza conjuntamente por la **SGP** (Organismo rector de este referencial) y el o los organismos que estén desarrollando o incorporando la nueva aplicación. El resultado de este análisis se registra en la siguiente planilla:

APLICACION:										
Servicios a "suministrar / consumir"	Comportamiento Requerido	Actor involucrado	SEGURIDAD		DATOS		PROCESOS		SERVICIOS	
			C	P	C	P	C	P	C	P

Esto permite determinar la/s capa/s del modelo en las que debe ubicarse la aplicación para poder operar correctamente.

4.3.2 Establecer los requisitos de la evaluación

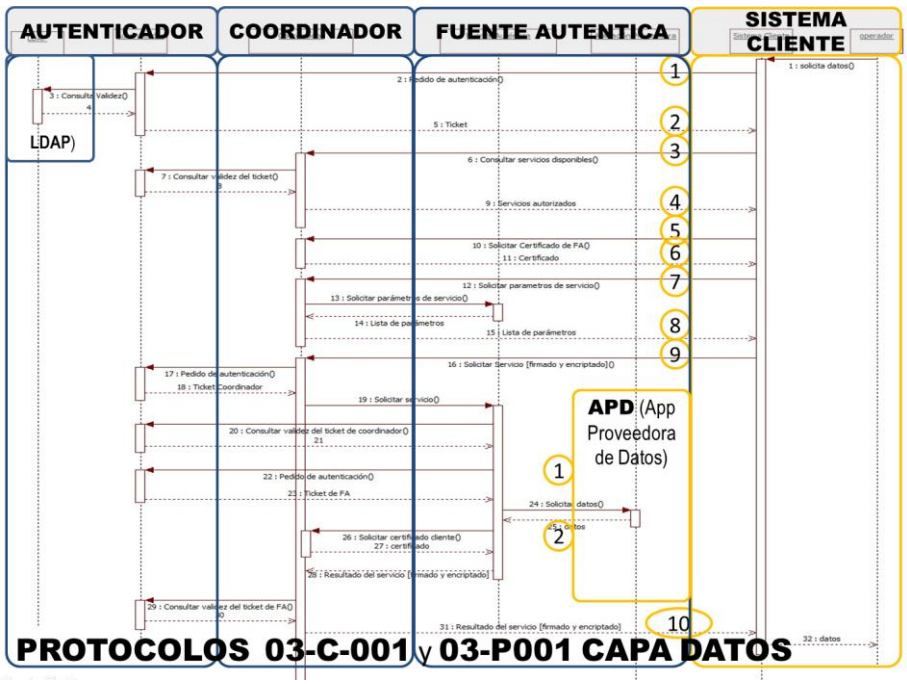
Con la clasificación realizada sobre el comportamiento de la aplicación en cada capa, se identifican los protocolos que ella debe cumplimentar, a saber:

CAPA	COMPORTAMIENTO Posible	Requerido	PROTOCOLO
Servicios	Cliente		05-C-001
	Proveedor		05-P-001
Procesos	Cliente		04-C-001
	Proveedor		04-P-001
Datos	Cliente	✓	03-C-001
	Proveedor	✓	03-P-001
Seguridad	Cliente		02-C-001
	Proveedor		02-P-001

El detalle de la tabla de protocolos se encuentra documentado en el Referencial IRAM N° 14-2 “Requisitos de calidad de las aplicaciones informáticas - Integrabilidad” *PARTE 2: Secuencia de comunicación; Atributos de las capas y Métricas de Testing;* TABLA DE PROTOCOLOS DE COMUNICACIÓN.

Como ejemplo se presenta a continuación el protocolo **003-C-001** y **03-P-001** de la capa de DATOS:

.



4.3.3 Especificar la evaluación

Identificados los protocolos requeridos, se determina la secuencia de "web services" correspondiente, para lo cual se consulta la tabla de secuencia.

Como ejemplo, se presenta el caso para Sistema PROVEEDOR de Servicios de DATOS de Fuente Auténtica "Protocolo 03-P-001".

	Nro de Secuencia
El **Protocolo 03-P-001,**presenta dos interacciones necesarias, las secuencias 24 y25	24. Solicitar datos
	25. datos

En el Manual del Desarrollador de Integrabilidad (disponible y actualizado permanentemente en la Wiki de Integrabilidad) se obtiene la especificación de los web services a soportar. Los web-services operan utilizando el formato XML bajo el protocolo estándar y abierto SOAP, pudiendo implementarse con cualquier soporte tecnológico.

Por otra parte, debe solicitarse a la **SGP** o quien ésta designe, los números de IP de los servidores de la plataforma de Integrabilidad que estén disponibles para realizar las pruebas.

Protocolo 03-P-001		
Nro. de Secuencia	**Web Service**	**Actor** (TCP/IP)
24	**WS Solicitar datos**	Fuente Auténtica
25	**WS datos**	Fuente Auténtica

4.3.4 Diseñar la evaluación

El diseño de la evaluación parte del Modelo de Calidad **ISO/IEC TR 9126-2:2003** *Software engineering – Productquality - Part 2: Externalmetrics,* de donde se extraen las características y sub-características para realizar la evaluación.

La siguiente tabla muestra las características y sub-características aplicables al modelo de Integrabilidad:

8.1 FUNCIONALIDAD	8.1.1 adecuación
	8.1.3 interoperabilidad
	8.1.4 seguridad
	8.1.5conformidad de la funcionalidad
8.2 CONFIABILIDAD	8.2.4 cumplimiento de confiabilidad
8.4 EFICIENCIA	8.4.1 comportamiento en relación al tiempo
	8.4.2 utilización de recursos
8.5 FACILIDAD DE MANTENIMIENTO	8.5.2 capacidad de ser modificado
	8.5.5 conformidad de la facilidad de mantenimiento
8.6 PORTABILIDAD	8.6.4 coexistencia

Estas Métricas aplicadas a los respectivos protocolos, determinan el Test a realizar. Como ejemplo se indican las métricas básicas y complementarias para las secuencias 24 y 25.

Aplicación proveedora de DATOS de Fuente Auténtica																
Test: 03-P-001			Métricas básicas							Métricas complementarias						
			Adecuación		Funcionalidad	Seguridad		Interoperabilidad		Tiempo de respuesta		Funcionalidad	Capacidad de ser modificado			
Secuencia	Web Service	Actor	Integridad de implementación funcional	Cobertura de implementación funcional	Conformidad de la norma de interfaz	Auditoria de acceso	Control de acceso	Capacidad de intercambio de datos (basado en formato de datos)	Capacidad de intercambio de datos (basado en el intento exitoso del usuario)	Tiempo de respuesta	Tiempo medio de respuesta	Cumplimiento funcional	Eficiencia en el ciclo de cambio	Tiempo de implementación del cambio	Capacidad de controlar el cambio del software	
24	Solicitar datos	Fuente auténtica	1	2	9	--	--			11	12	8	16	17	20	
25	Datos	Fuente auténtica	1	2	9	--	--	3	4	11	12	8	16	17	20	

Cada una de las Métricas de Testeo tiene un código, el cual se utiliza para identificar en el referencial IRAM N° 14-2 *PARTE 2: Secuencia de comunicación; Atributos de las capas y Métricas de Testing,* la prueba (testing específico) a realizar que dicta la norma ISO/IEC TR 9126-2:2003. En el ejemplo, el código 16 corresponde a la métrica de “Eficiencia en el ciclo de cambio”.

Este registro permite:

- Elaborar el Plan de Evaluación con el detalle de cada métrica indicado por la norma ISO/IEC TR 9126-2:2003.

- Diseñar los casos de prueba para cada Métrica

El diseño de la evaluación incluye la determinación de los umbrales de aceptación, validados por la **SGP**.

4.3.5 Realización de la evaluación

Con las métricas definidas y el testing especificado, el IRAM procede a realizar la evaluación de conformidad, de los atributos de cada comportamiento requerido en cada capa y, de corresponder, emite la respectiva certificación de conformidad a los requisitos de Integrabilidad definidos por la **SGP**.
Para ello procede a efectuar el Testing de cada métrica según los casos de prueba, emitir dictamen y/o recomendaciones y en caso positivo emite la certificación de conformidad.

5 VALIDEZ DE LA CERTIFICACIÓN

La certificación de conformidad de Integrabilidad de las aplicaciones o sistemas informáticos tiene validez mientras no se modifiquen: la estructura de conectividad del sistema o los requisitos de la **SGP** en su vínculo con la plataforma de Integrabilidad.

Anexo A

Conceptos complementarios

Antecedentes

La Plataforma de Integrabilidad fue concebida buscando satisfacer la pirámide de necesidades planteadas para la convivencia digital, esto es: a) Resguardar la Seguridad de la información; b) Compartir Datos desde sus Fuentes Auténticas; c) Cocrear los Procesos y d) Liberar los Servicios en forma abierta y extensible.

La arquitectura de la solución para satisfacer las capas a y b se basaron en el exitoso modelo Xroad de Estonia, que plantea un esquema equilibrado de actores en los cuales se distribuye el poder tecnológico y crea las bases del macro sistema buscado. Aquí la Autenticación está centralizada, la Autorización distribuida en función de las estructuras del poder de gestión, en nuestro caso: nacional, provincial, municipal y/o sectorial y la Auditoría completamente atomizada entre todos los actores involucrados, para lograr una total transparencia.

Para las capas c y d se utilizaron y extendieron soluciones ya desarrolladas en la provincia del Neuquén tanto para el Diseño y/o Rediseño Participativo de Procesos, como para la utilización e integración de datos, basadas en los trabajos del Ken-Orr-Institute de los Estados Unidos, aplicando los estándares abiertos disponibles.

Al igual que el modelo Xroad, la Plataforma de Integrabilidad descansa sobre la infraestructura de clave pública (PKI).

Actualmente la Plataforma de Integrabilidad está contenida dentro del Modelo de URBANISMO DIGITAL que lleva adelante el gobierno de la provincia del Neuquén, estableciendo las bases de los nuevos Servicios Públicos Digitales imprescindibles para un desarrollo enfocado en la comunidad y en el ciudadano.

Los principales Servicios Públicos Digitales en uso son:

- Servicios de conectividad.
- Servicios de autenticación y Firma Digital del ciudadano.
- Servicios de coordinación o autorización jurisdiccional en cada nivel de gobierno: provincial, municipal y sectorial.
- Servicios de registros de Fuente Auténtica.
- Servicios para el reúso legal de los datos (transparencia).

INTEGRABILIDAD VS INTEROPERABILIDAD

Una característica distintiva del modelo de Integrabilidad respecto de los esquemas de interoperabilidad más conocidos, donde se exige la comunicación entre sistemas como “pares”, a la que denominaremos interoperabilidad horizontal, es que el modelo Integrabilidad exige mecanismos de interoperabilidad vertical entre las capas definidas por el modelo dentro de los mismos sistemas y aplicaciones. Hablamos, entonces, de Interoperabilidad de Fuente Auténtica, Interoperabilidad de Procesos e Interoperabilidad de Interface Unificada.

El modelo de Integrabilidad de la SGP busca como resultado final, lograr por diseño, la intercambiabilidad de componentes o módulos de cada capa por productos de distintos proveedores y/o tecnologías, sin afectar los restantes desarrollos o aplicaciones. Esto maximiza la flexibilidad funcional necesaria para evolucionar como gran sistema, completamente alineada con la pirámide de necesidades para la convivencia digital.

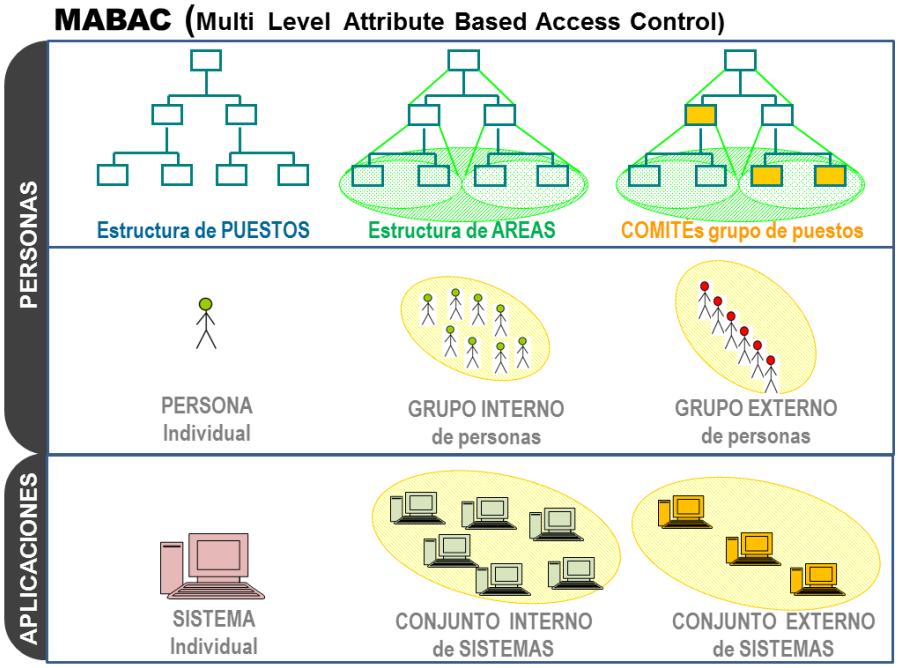
Toda esta interoperabilidad vertical debe realizarse utilizando web-services XML bajo el protocolo estándar y abierto SOAP.

Modelo MABAC de Autorización:

Desde los sistemas con pocos usuarios internos de una organización a los sistemas abiertos basados en Internet donde la cantidad de usuarios crece exponencialmente, las autorizaciones se complejizan y los modelos de autorización de usuarios han evolucionado, buscando facilitar las actividades de autorización.

El modelo MABAC (Multi Level Attribute Based Access Control) fue diseñado conjuntamente con la Universidad Nacional del Comahue buscando superar las limitaciones estáticas encontradas en los modelos actualmente en uso como Role Based Access Control (RBAC).

MABAC está diseñado para administrar Autorizaciones tanto de usuarios como de aplicaciones en el mundo de Internet donde confluyen usuarios internos y externos a la organización, en grandes cantidades y donde la autorización de los mismos puede estar delegada en distintos actores y subordinada a los registros de diferentes fuentes auténticas. Por ejemplo, autorizar a los médicos matriculados, en forma on-line en función de los datos de su propio Colegio Profesional, Fuente Auténtica de su matriculación.



El *Servidor-Coordinador* brinda servicios de autorización utilizado el modelo MABAC.

Confidencialidad desde el Habeas Data al Open Data

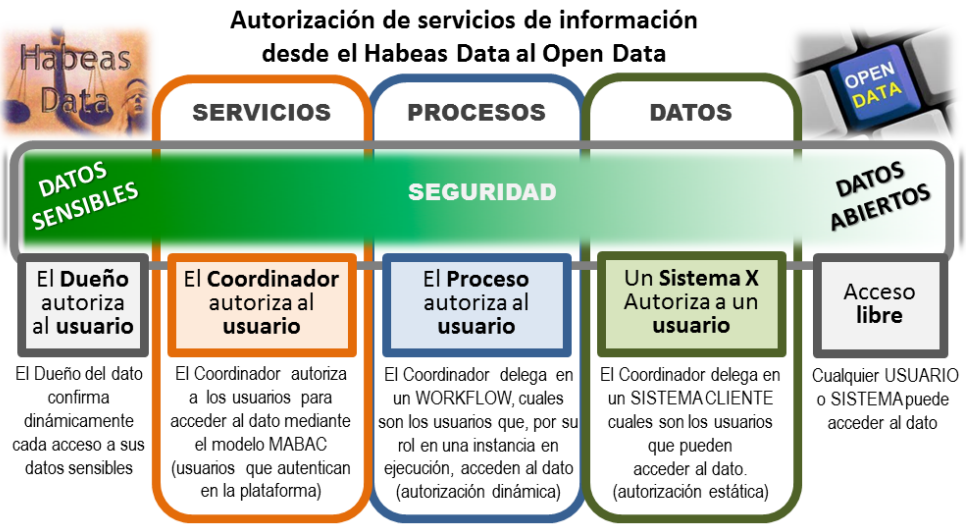
Para poder cubrir el amplio abanico de casos presentes entre el Habeas Data y el Open Data en un entorno abierto como internet, se recurre a los protocolos entre los distintos actores que combinan servicios de autenticación, autorización y confirmación.

Autenticación: Mediante el *Servidor Autenticador* se realizan dos niveles de autenticación: uno para todos los sistemas que participan del entorno informático y otro, para los usuarios.

Autorización: Mediante el *Servidor Coordinador*, los *Servidores de Workflow* y los *Sistemas Cliente* se generan distintos niveles y modelos de autorización.

Confirmación: Cualquier servicio que transfiera datos sensibles puede requerir una confirmación (autorización) previa por parte del involucrado (ciudadano), por ejemplo, mediante un SMS. Esta acción es soportada directamente por el *Servidor Coordinador*.

La extensión de los protocolos de seguridad, entre los actores del modelo Xroad sobre las capas de *procesos* y *servicios,* sumado a la flexibilidad dinámica del modelo MABAC genera la capacidad necesaria para poder administrar el abanico de casos que se presentan entre el Open Data y el Habeas Data.



Es importante destacar que en función de los roles que se le exijan a una aplicación, la misma puede llegar a tener que utilizar algunos o todos los siguientes modelos de autorización de acceso a los servicios de información.

Se presentan los casos más relevantes para mostrar las principales combinaciones partiendo de los Datos Abiertos hasta el Habeas Data.

Acceso ABIERTO: Los servicios de datos abiertos no requieren de ningún tipo de autenticación y autorización. Se encuentran así catalogados en el Servidor Coordinador y pueden ser publicados directamente sobre catálogos de datos abiertos como por ejemplo CKAN.

Acceso DELEGADO enApp-Cliente: Cada organización es responsable de sus sistemas y por ende de la autenticación y autorización a sus propios usuarios. El *Servidor-Coordinador* delega en el sistema o *App-Cliente* el manejo de sus propios usuarios. Solo es necesario autorizar los servicios de Fuente Auténtica a la App-Cliente. (Autorización Estática).

Como se ejemplifica en Estonia, este caso es similar a la situación donde las fábricas de alcohol no son responsables de los resultados del mal uso que se haga de esa bebida en los bares.

Este mecanismo en capsula los detalles de autenticación y autorización de usuarios usados internamente por las organizaciones, minimizando el impacto sobre los sistemas existentes.

Acceso DELEGADO en Servidor-Workflow: Cuando trabajamos con procesos que sobrepasan los bordes de las organizaciones, se requiere de mayor grado de control de acceso. En estos casos tendremos un motor de workflow o *Servidor-WF* y aplicaciones cliente de servicios de WF o *App-cliente-WF*, que generalmente serán de distintos organismos y también actuarán como *App-Clientes* de servicios de datos de Fuente Auténtica.

Todos los usuarios y aplicaciones involucrados deben Autenticarse en el *Servidor-Autenticador.* A su vez cada *Servidor-WF* autorizará a determinados usuarios en-cada una de las tareas de una instancia del proceso, asociando usuarios con roles de forma directa, indirecta, dinámica y/o estática.

Aquí el *Servidor-Coordinador* delega en el *Servidor de WF* la autorización dinámica de servicios de Fuente Auténtica a las *Apps-cliente-WF* consultando en línea al *Servidor-WF* sobre los derechos del usuario que esté operando esa instancia del proceso. Es así que una *App-cliente-WF* sólo podrá consumir servicios de datos de FA cuando el usuario (operador de la instancia de proceso) esté autorizado en el *Servidor- WF*.

Este control de derechos de acceso es utilizado para defenderse de ataques internos. Por ejemplo, evita que un operador malintencionado visualice datos sensibles de un ciudadano que no está realizando un trámite que los requeriría en ese momento. (Autorización Dinámica)

Acceso CONTROLADO: A una *App-Ultima-Milla* puede exigírsele utilizar los servicios de autenticación y autorización centralizada del *Servidor-Coordinador* siguiendo el modelo MABAC para autorizar las distintas funcionalidades que publique la aplicación.

Acceso Habeas Data: Mediante los servicios de confirmación del *Servidor-Coordinador*, la persona dueña del dato autoriza dinámicamente el acceso a sus datos sensibles.

Interoperabilidad de FUENTES AUTÉNTICAS (Mensajes “doble sobre”)
Los servicios de datos de los servidores de Fuente Auténtica operan con paquetes de doble sobre. Sobre externo para el ruteo entre los actores y generación de información de auditoría, firmado digitalmente por la Fuente Auténtica y sobre interno con los datos confidenciales encriptados para el cliente solicitante.

El formato del sobre interno (contenido) puede ser cualquiera que esté acordado entre el cliente y el proveedor. De todas maneras se promueve el uso de formatos estándares según el tipo de información transportada. Para el caso de GIS se adoptan, por ejemplo, los formatos abiertos de WMS, WFS, WPS etc. La aplicación cliente, luego de desencriptar el resultado y verificar la firma, debe ser capaz de interpretar el resultado obtenido.

Es un modelo que prioriza la protección de los paquetes de datos por sobre la protección de los canales de comunicación.

El objetivo de la Interoperabilidad de Fuentes Auténticas es compartir datos con seguridad, de máxima calidad, que sólo se obtienen con el reuso de los mismos desde todos los puntos de vista posibles.

Interoperabilidad de PROCESOS

Los procesos reales atraviesan múltiples organizaciones y relacionan sus diversos sistemas informáticos. Esto obliga a separar la ejecución del proceso en sí de las actividades o tareas transaccionales que los componen. Esta separación permite extender la vida útil de muchas aplicaciones que al no tener "hardcodeados" los procesos, no son afectadas por los cambios en los mismos.

El objetivo de la interoperabilidad de Procesos es soportar productos de diferentes proveedores y tecnologías, tanto del lado de los *Servidores-WF* como de las *Apps-clientes-WF.* Aquí se exige la utilización de estándares abiertos ya disponibles en el mercado, como por ejemplo BPMN2, XPDL etc.

Interoperabilidad de INTERFACE UNIFICADA (Última Milla)

Soportar Interoperabilidad de Interface Unificada: significa que una aplicación ofrece WS o APIs transaccionales para poder Integrarse con otras aplicaciones en otro "Front End" (última milla) que los integre y unifique. Estos servicios deberán estar liberados a cualquier tercero, quien los podrá utilizar y extender, desarrollándolos en cualquier plataforma y tecnología.

La necesidad de certificar esta capacidad estará dada por el análisis particular de las funcionalidades que deberán ser liberadas por la aplicación. También deben considerarse las tendencias en formatos abiertos, según la tipología de la información administrada por la aplicación. Esto implica identificar los formatos abiertos vigentes en el mercado. Por ejemplo: para intercambio de reclamos, hoy encontramos OPEN311 o para catalogación y acceso de datos abiertos, las APIs de CKAN que están estableciéndose como estándares abiertos de facto.

Como puede observarse no es posible establecer un "pasa no pasa", pero sí identificar claramente la predisposición de la aplicación a ser extensible, liberando la última milla.

El objetivo de la interoperabilidad de Última Milla es liberar a los usuarios de las limitaciones que presentan las interfaces de los sistemas para atender sus necesidades particulares, dando así la posibilidad de desarrollar interfaces unificadas que le permitan, por ejemplo, cargar simultáneamente un mismo dato en distintas aplicaciones que lo requieran o combinar funcionalidades ya desarrolladas de distintos sistemas en su propia interface, entre muchas otras.

Anexo B

Bibliografía

Para el estudio de este referencial se han tenido en cuenta los antecedentes siguientes:

IRAM Directiva 1:2004 Redacción y presentación de las normas IRAM.

IRAM-ISO/IEC 14598-1:2006 (Tecnología de la información. Ingeniería de software. Evaluación del producto de software. Parte 1 - Descripción general).

IRAM-ISO/IEC 14598-2:2007 (Tecnología de la información. Ingeniería de software. Evaluación del producto de software. Parte 2 - Planificación y gestión.

Estonian IT Interoperability Framework Abridgement of version 2.0 Ministry of Economic Affairs and Communications Department of State Information Systems (2005)

Paper Integrabilidad Ken Orr y Gustavo Giorgetti (diciembre 2007).

Anexo C

Grupo de trabajo

En el desarrollo de este Referencial Normativo participaron las personas siguientes:

Integrante	**Representa a:**
AMUNDSON Maggie	IRAM filial Comahue
AYARRA Diego	IRAM filial Comahue
CEBALLOS Jorge Luis	IRAM - Área de certificaciones TI
CUELLO Alfredo	ThinkNet– consultor
DONADELLO Domingo	IRAM - Certificación de Sistema de Gestión de Seguridad de Información y Servicios TI
GIORGETTI Gustavo	ThinkNet - Consultor
MENAL Marcelo	LTSL - Laboratorio de Testing San Luis
MUSOTTO Julio	OPTIC - Coordinador Integrabilidad
POLLINA Guillermo	Secretaría de Gestión Pública de la Provincia del Neuquén
SÁNCHEZ Alberto	LTSL - Laboratorio de Testing San Luis
VAI Claudio	OPTIC - Director de Servicios TICs

IRAM
Perú 556
C1068AAB Buenos Aires, Argentina
Tel +54 11 4346-0600
Email iram-iso@iram.org.ar
www.iram.org.ar

Secretaría de Gestión Pública
Belgrano 398, 8° Piso
CP 8300 Ciudad de Neuquén, Argentina
Tel +54 299 449-5700 / 5040
Email gestionpublica@neuquen.gov.ar
www.sgpneuquen.gob.ar

Instituto Argentino de Normalización y Certificación

Secretaría de Gestión Pública
Gobierno de la Provincia del Neuquén
Ministerio de Coordinación de Gabinete, Seguridad y Trabajo