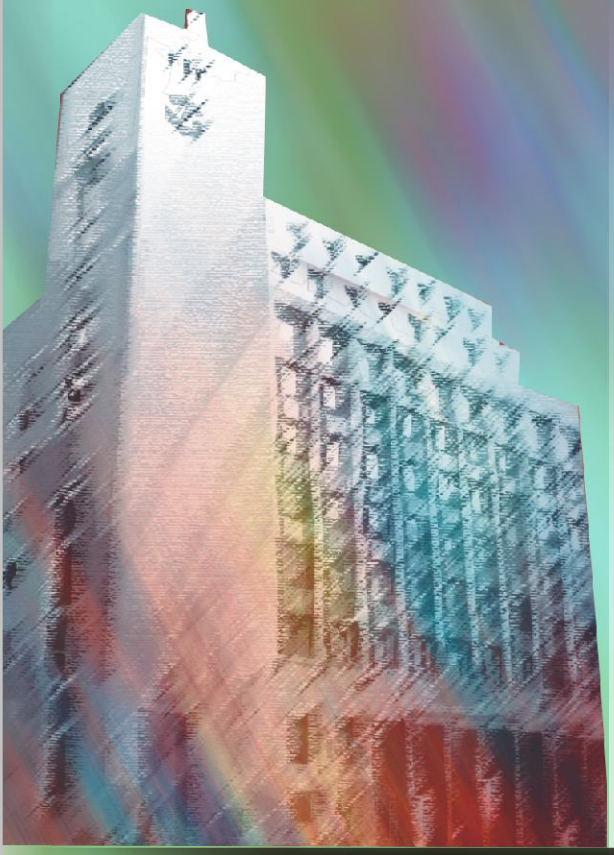
SIGEN
Sindicatura General de la Nación
Presidencia de la Nación

Referencial
IRAM
Nº 13



UAI
Unidades de Auditoría Interna del Sector Público Nacional

Requisitos
de Gestión de la Calidad

Segunda edición 2017

IRAM
Referencial Nº 13

Segunda edición
2017

Unidades de Auditoría Interna del Sector Público Nacional

Requisitos de gestión de la calidad

2017

Segunda Edición

Índice

Unidades de Auditoría Interna del Sector Público Nacional

Requisitos de gestión de la calidad

0 ANTECEDENTES

La SINDICATURA GENERAL DE LA NACIÓN (SIGEN), órgano rector del Sistema de Control Interno del Poder Ejecutivo Nacional, coordina actividades de control orientadas a lograr que la gestión del Sector Público Nacional alcance los objetivos de gobierno mediante un empleo adecuado de los recursos en el marco legal vigente.

El modelo de control actual, establecido por la Ley N° 24.156, dispone que el Sistema de Control Interno está conformado por la Sindicatura General de la Nación, órgano normativo, de supervisión y coordinación, y por las Unidades de Auditoría Interna del Sector Público Nacional creadas en cada jurisdicción y/o entidad del Poder Ejecutivo Nacional, las que dependen jerárquicamente de la autoridad superior de cada organismo y actúan coordinadas técnicamente por la SIGEN.

Como órgano rector, la SIGEN fomenta las buenas prácticas y la optimización de recursos en pos del fortalecimiento del control interno. Para ello se propuso, una vez más, construir una herramienta que promueva la estandarización de procesos, la formación y crecimiento del personal y la mejora continua de los sistemas de gestión.

Entendiendo que el desarrollo de un marco normativo y técnico para promover la calidad y mejora continua de la gestión de las Unidades de Auditoría Interna del Sector Público Nacional, contribuye significativamente al logro de los objetivos estratégicos, se ha suscripto un Convenio Marco de Cooperación con el Instituto Argentino de Normalización y Certificación (IRAM) para promover de manera permanente la calidad en las áreas de su competencia.

Según el Decreto N° 1474/94 del Poder Ejecutivo Nacional, por el cual se crea el Sistema Nacional de Normas, Calidad y Certificación, el IRAM es designado como el organismo de normalización de la Argentina. Además de sus actividades a nivel nacional, representa a la República Argentina ante las organizaciones regionales sobre normalización como la Comisión Panamericana de Normas Técnicas (COPANT) y la Asociación MERCOSUR de Normalización (AMN), y ante las organizaciones internacionales: International Organization for Standardization (ISO) e International Electrotechnical Comission (IEC) en conjunto con la Asociación Electrotécnica Argentina (AEA).

En el contexto del Convenio Marco de Cooperación Institucional SIGEN-IRAM, se ha conformado un equipo de trabajo técnico integrado por profesionales de la SIGEN y de las Unidades de Auditoría Interna del Sector Público Nacional, y el IRAM, para revisar y validar en forma conjunta el presente “Referencial Normativo de Gestión de la Calidad”.

Esta revisión se encuentra fundamentada en la publicación en el mes de septiembre del año 2015 de la nueva versión de la norma ISO 9001 que incorpora cambios importantes para los sistemas de gestión de la calidad, agregando requisitos que la acercan a los modelos de excelencia y que recopilan las necesidades de la gestión organizacional tales como, considerar el contexto, ampliar la visión de “clientes” para establecer una vinculación con las “partes interesadas” e implementar acciones dentro de los procesos para abordar los riesgos y oportunidades.

La primera edición del Referencial N° 13 se basó en la versión 2008 de la norma ISO 9001. Ante la utilidad de los cambios introducidos en la revisión 2015 de la norma ISO 9001 y con el propósito de facilitar el camino de las Unidades de Auditoría Interna del Sector Público Nacional hacia la mejora,

haciendo compatible el Referencial N° 13 con la norma ISO 9001:2015, se consideró oportuno efectuar la revisión y publicar esta segunda edición del Referencial N° 13.

1 OBJETO Y CAMPO DE APLICACIÓN

Este Referencial presenta los requisitos de un sistema de gestión de la calidad para las Unidades de Auditoría Interna del Sector Público Nacional. Su objeto es contribuir al adecuado funcionamiento de las mismas.

Se especifican los requisitos para un sistema de gestión de la calidad, cuando una Unidad de Auditoría Interna del Sector Público Nacional:

a) desea demostrar su capacidad para proporcionar regularmente productos que satisfagan los requisitos de las partes interesadas pertinentes y los legales y reglamentarios aplicables, y

b) aspira a consolidar la aplicación eficaz de sus procesos, promoviendo la mejora continua del sistema de gestión de la calidad.

La implementación de este Referencial propone un esquema evolutivo, de requisitos crecientes, en tres (3) etapas. Esta metodología permite una implementación más amigable y una maduración progresiva de la organización. En el anexo C se indica la tabla con los requisitos establecidos para cada etapa.

ALCANCE

Este Referencial define los requisitos aplicables del sistema de gestión de la calidad para la planificación, el desarrollo de auditorías, el seguimiento de las observaciones y la ejecución de otras actividades por parte de la Unidad de Auditoría Interna (UAI).

Todos los requisitos de este Referencial se consideran aplicables al sistema de gestión de la calidad de una UAI, por lo tanto no es posible exceptuar el cumplimiento de ninguno de ellos.

ARTICULACIÓN CON LA NORMA ISO 9001:2015 Y ADOPCIÓN DE NUEVOS ENFOQUES

Habiendo la UAI cumplido todos los requisitos de este Referencial, se encontraría orientada hacia la certificación de la norma ISO 9001:2015, ya que esta segunda edición del Referencial se ha alineado a la nueva estructura de alto nivel establecida por la misma. En este sentido, los nuevos enfoques incorporados a los requisitos tales como: comprensión de la organización y su contexto, compresión de las necesidades y expectativas de las partes interesadas y las acciones para abordar riesgos y oportunidades, son contemplados en el presente Referencial.

En consecuencia, con la incorporación de algunos requisitos adicionales, la UAI podría estar en condiciones de certificar la ISO 9001:2015.

La relación entre los requisitos del Referencial y la ISO 9001:2015 puede apreciarse en el anexo A.

Los requisitos para la gestión de la calidad de este Referencial se basan en los siete principios expresados en la nueva versión de la ISO 9001.

Los principios se encuentran disponibles en el anexo B.

Para facilitar la adopción del pensamiento basado en riesgos, además de los requisitos adaptados a la gestión de las mismas, se han incluido dos anexos informativos: el anexo D desarrolla las principales consideraciones para la gestión de riesgos y el anexo E presenta buenas prácticas para la Seguridad de la Información.

Mejora continua y procesos

Al igual que en la primera edición y fortaleciendo la alineación con la norma ISO 9001:2015, este Referencial propicia el enfoque basado en procesos, promoviendo la operación eficaz y la mejora continua de las Unidades de Auditoría Interna. A continuación se presentan dos gráficos incluidos en la ISO 9001:2015, que son ilustrativos en relación a la identificación de los procesos y la gestión integrada para la mejora continua.

La figura 1 proporciona una representación esquemática de cualquier proceso y muestra la interacción entre sus elementos. Los puntos de control del seguimiento y la medición, que son necesarios para el control, son específicos para cada proceso y variarán dependiendo de los riesgos relacionados.

Figura 1 - Representación esquemática de los elementos de un proceso.

El ciclo Planificar-Hacer-Verificar-Actuar (PHVA) puede aplicarse a todos los procesos y al sistema de gestión de la calidad como un todo.

La figura 2 ilustra cómo los capítulos 4 a 10 pueden agruparse en relación con el ciclo PHVA.

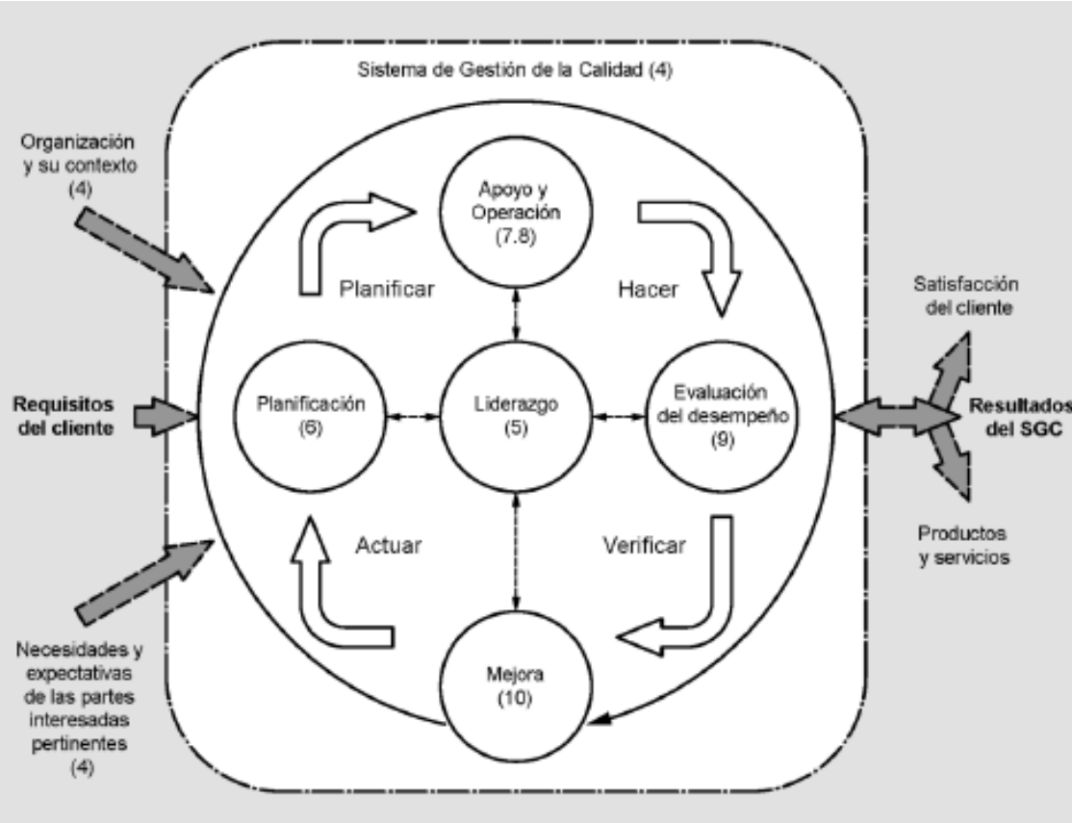


Figura 2 - Representación de la estructura de la norma IRAM-ISO 9001:2015 con el ciclo PHVA, que se puede analizar en equivalencia con los capítulos de este Referencial.

El ciclo PHVA puede describirse brevemente como sigue:

- Planificar: establecer los objetivos del sistema y de sus procesos, y los recursos necesarios para generar y proporcionar resultados de acuerdo con los requisitos del cliente y las políticas de la organización;

- Hacer: implementar lo planificado;

- Verificar: realizar el seguimiento y, cuando sea aplicable, la medición de los procesos y los productos y servicios resultantes respecto a las políticas, los objetivos y los requisitos, e informar sobre los resultados;

- Actuar: tomar acciones para mejorar el desempeño, cuando sea necesario.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta de utilidad para la aplicación de este documento.

IRAM-ISO 9000:2015 - *Sistemas de gestión de la calidad. Fundamentos y vocabulario.*

IRAM-ISO 9001:2015 - *Sistemas de gestión de la calidad. Requisitos.*

IRAM-ISO 31000:2015 - *Gestión de riesgos. Principios y guías.*

IRAM 17551:2009 - *Sistema de gestión de riesgos. Requisitos.*

IRAM-ISO/IEC 27001:2015 - *Sistemas de gestión de la seguridad de la información. Requisitos.*

Referencial IRAM 16:2016 - *Gestión de la identificación e involucramiento con las partes interesadas*.

Normativa de aplicación para la gestión de las Unidades de Auditoría Interna del Sector Público Nacional, publicada en la Intranet de la SIGEN, en el link “Normativa”.

3 TÉRMINOS Y DEFINICIONES

En lo que respecta a los términos referidos a la gestión de la calidad, se aplican los términos y definiciones incluidos en la norma ISO 9000:2015.

No obstante, a continuación se presentan las definiciones de los principales términos de los sistemas de gestión de la calidad y los particulares de las actividades para la gestión de las Unidades de Auditoría Interna.

Acción correctiva: acción para eliminar la causa de una no conformidad y evitar que vuelva a ocurrir.

Calidad: grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos.

Cliente: persona u organización que podría recibir o que recibe un producto o un servicio destinado a esa persona u organización o requerido por ella. Para este Referencial, se consideran clientes a:

- SIGEN;
- Máxima autoridad del organismo;
- Auditados.

Además de los identificados precedentemente, la UAI, de acuerdo a sus actividades y/o las características del organismo, podrá determinar otros clientes para su sistema de gestión de la calidad.

Contexto de la organización: combinación de cuestiones internas y externas que pueden tener un efecto en el enfoque de la organización para el desarrollo y logro de sus objetivos.

Corrección: acción para eliminar una no conformidad detectada.

Dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel.

En este Referencial cuando se exprese “Dirección” se entiende que corresponde a la más alta autoridad de la UAI, independientemente de su denominación en cada organización (por ejemplo, Auditor Interno Titular, Gerente, Director, etc.).

Eficacia: grado en el que se realizan las actividades planificadas y se logran los resultados planificados.

Eficiencia: relación entre el resultado alcanzado y los recursos utilizados.

Gestión: actividades coordinadas para dirigir y controlar una organización.

Gestión de la calidad: actividades coordinadas para dirigir y controlar una organización con respecto a la calidad.

Información documentada: información que una organización tiene que controlar y mantener, y el medio que la contiene.

NOTA. La información documentada puede hacer referencia a:

- la información generada para que la organización opere (por ejemplo, procedimientos, instructivos, modelos, etc.);
- la evidencia de los resultados alcanzados (registros);
- el soporte o medio que la contiene, por ejemplo, papel, digital, sistema informático.

Infraestructura: sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de la organización.

Mejora: actividad para mejorar el desempeño.

Mejora continua: actividad recurrente para mejorar el desempeño.

No conformidad: incumplimiento de un requisito.

NOTA. En la gestión de las Unidades de Auditoría Interna, las no conformidades pueden ser, entre otras:

- una queja de un usuario o parte interesada;
- no alcanzar un resultado esperado;
- omitir actividades definidas en un procedimiento.

Organización: persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

Parte interesada: persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

Procedimiento: forma especificada de llevar a cabo una actividad o un proceso.

Proceso: conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto.

Producto: salida de una organización que puede producirse sin que se lleve a cabo ninguna transacción entre la organización y el cliente.

Registro: documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas.

Requisito: necesidad o expectativa establecida, generalmente implícita u obligatoria.

Riesgo: efecto de la incertidumbre sobre el logro de los objetivos.

Salida: resultado de un proceso.

Seguridad de la información: es la protección de la información “sensible” de una amplia variedad de amenazas, con el objeto de asegurar la continuidad del cumplimiento de sus misiones y funciones, mi-

nimizar los riesgos y maximizar el retorno de lo invertido y las oportunidades de sus operaciones. Se logra con el conjunto de actividades y controles para preservar la información sensible respecto de la confidencialidad, integridad y disponibilidad.

Servicio: salida de una organización con al menos una actividad, necesariamente llevada a cabo entre la organización y el cliente.

Sistema de gestión: conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.

Sistema de gestión de la calidad: parte de un sistema de gestión relacionado con la calidad.

Trazabilidad: capacidad para seguir el histórico, la aplicación o la localización de un objeto.

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y de su contexto

Propósito

Conocer el contexto en el que la UAI desarrolla sus actividades, para fortalecer su capacidad de gestión y planificar acciones ante situaciones externas y/o internas que pueden afectarla.

Requisitos

Con referencia al contexto, la UAI debe determinar las situaciones externas e internas que son pertinentes para su propósito y dirección estratégica y que afectan o podrían afectar su capacidad para lograr los resultados previstos de su sistema de gestión de la calidad.

La UAI debe realizar periódicamente el seguimiento y la revisión de la información sobre estas situaciones externas e internas, analizar su impacto y probabilidad de ocurrencia en los procesos, así como en los productos y servicios brindados.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

Propósito

Comprender las necesidades y expectativas de las partes interesadas, incluyendo al propio personal de la UAI, a fin de determinar los requisitos a los que deben dar respuesta las actividades del sistema de gestión de la calidad.

Requisitos

La UAI debe contar con información documentada sobre:

a) la identificación de las partes interesadas que son pertinentes al sistema de gestión de la calidad, y;

b) los requisitos pertinentes de estas partes interesadas para el sistema de gestión de la calidad.

La UAI debe realizar en forma periódica el seguimiento y la revisión de la información sobre estas partes interesadas y de sus requisitos pertinentes para el sistema de gestión de la calidad.

La UAI debe planificar el vínculo con las partes interesadas identificadas como pertinentes para el sistema de gestión de la calidad y conservar la información documentada de esa planificación.

La planificación debe considerar:

a) la información a solicitar y/o suministrar para la gestión eficaz de los procesos;

b) los canales para la comunicación eficaz con cada una de ellas;

c) los recursos necesarios para la vinculación, incluyendo las personas competentes para su gestión;

d) la asignación de las responsabilidades para la ejecución de las tareas planificadas.

4.3 Control de los procesos

Propósito

Controlar y mejorar los procesos con el fin de asegurar que los servicios prestados cumplan con los requisitos de las partes interesadas.

Requisitos

La UAI debe determinar la secuencia e interacción entre los procesos de su sistema de gestión de la calidad.

En particular para cada uno de los procesos del apartado 8, la UAI debe:

a) determinar las entradas requeridas y las salidas esperadas de estos procesos, considerando los requisitos pertinentes de las partes interesadas;

b) asignar los roles y las responsabilidades;

c) determinar los criterios y métodos (incluyendo el seguimiento, las mediciones y los indicadores de desempeño), para asegurar la operación eficaz de los procesos;

d) determinar los recursos necesarios;

e) evaluar los resultados e implementar cualquier cambio necesario para asegurar que se logren los resultados previstos.

5 LIDERAZGO

5.1 Liderazgo y compromiso

Propósito

Asegurar que la Dirección asume el compromiso de implementar, coordinar y mantener el sistema de gestión de la calidad y la responsabilidad por la eficacia de aquellas actividades que son esenciales para los propósitos de la existencia de la UAI.

Requisitos

La Dirección debe:

a) tomar conocimiento periódico de la eficacia del sistema de gestión de la calidad, sus procesos y niveles de servicios;

b) asegurar que la política de la calidad y los objetivos de la calidad estén alineados con el contexto de la UAI;

c) promover la toma de conciencia del enfoque basado en procesos;

d) gestionar los recursos necesarios para el sistema de gestión de la calidad;

e) promover que el sistema de gestión de la calidad logre los resultados previstos;

f) promover el involucramiento del personal, dirigiendo y apoyando a las personas para contribuir a la eficacia del sistema de gestión;

g) gestionar la confidencialidad, integridad y disponibilidad de la información sensible, por medio de un análisis de riesgo de la seguridad de la información;

h) promover la mejora continua.

NOTA. En el anexo E se describen “Buenas Prácticas de Seguridad de la Información”.

5.2 Política

Propósito

Asegurar un marco de referencia y lineamiento común para la UAI, que permita la revisión de los objetivos de la calidad. Debe propiciar no solo el enfoque en los procesos y la mejora continua, sino también ser adecuada al contexto de la organización, con foco en la satisfacción de los requisitos de las partes interesadas.

Requisitos

La política de la calidad debe:

a) ser aprobada y revisada periódicamente por la Dirección;

b) establecer el compromiso de cumplir con los requisitos del sistema de gestión de la calidad, incluyendo los legales y reglamentarios, de seguridad de la información y de la mejora continua;

c) estar disponible como información documentada para las partes interesadas;

d) comunicarse, entenderse y aplicarse dentro de la organización.

5.3 Roles, responsabilidades y autoridades

Propósito

Asegurar que las responsabilidades y autoridades para los roles pertinentes se asignen, se comuniquen y se entiendan dentro de la UAI.

Requisitos

La Dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse que los procesos están dando los resultados previstos;

b) informar a la Dirección sobre el desempeño del sistema de gestión de la calidad incluyendo la seguridad de la información, las oportunidades de mejora y sobre la necesidad de cambio o innovación;

c) asegurarse que se promueva en todo el personal de la UAI el enfoque en el cumplimiento de los requisitos de las partes interesadas;

d) asegurarse que la integridad del sistema de gestión de la calidad se mantiene cuando se planifiquen e implementen cambios en dicho sistema.

6 PLANIFICACIÓN

6.1 Acciones para abordar riesgos y oportunidades

Propósito

Determinar los riesgos y oportunidades generales del sistema, incluyendo explícitamente los referidos a la seguridad de la información, que sean necesarios tratar con el fin de:

a) asegurar que el sistema de gestión de la calidad pueda lograr los resultados previstos;

b) prevenir o reducir efectos indeseados;

c) lograr la mejora continua.

Requisitos

La UAI debe identificar y analizar los riesgos y oportunidades respecto del cumplimiento de sus objetivos y planificar las acciones para su tratamiento.

Debe planificar la manera de:

a) integrar e implementar en los procesos del sistema de gestión de la calidad, las acciones de tratamiento y/o mitigación de riesgos definidas;

b) evaluar la eficacia de estas acciones.

NOTA. Las opciones para tratar los riesgos y oportunidades pueden incluir: evitar riesgos, asumir riesgos para perseguir una oportunidad, eliminar la fuente de riesgo, cambiar la probabilidad o las consecuencias, compartir el riesgo o mantener riesgos mediante decisiones informadas.

En anexo D se indica una orientación sobre las actividades para un análisis de riesgos.

6.1.1 Gestión de riesgos de seguridad de la información

Propósito

Establecer una metodología de gestión de riesgos de seguridad de la información sensible, que considere su confidencialidad, integridad y disponibilidad.

Requisitos

La Dirección debe:

a) definir un proceso para el análisis, valoración, evaluación y tratamiento adecuado de los riesgos significativos de seguridad de la información, que permita obtener resultados coherentes, válidos y comparables;

b) establecer y mantener criterios sobre los riesgos de seguridad de la información, incluidos aquellos que fundamentan su aceptación.

NOTA 1. La ISO/IEC 27005 informa sobre criterios para la elaboración de un sistema de gestión de riesgos de seguridad de la información.

NOTA 2. El tratamiento “adecuado” se entenderá como el que está relacionado a la complejidad del proceso.

6.2 Objetivos de la calidad y planificación para lograrlos

Propósito

Asegurar que los objetivos de la calidad establecidos sean pertinentes a la gestión de la UAI y su contexto.

Requisitos

Los objetivos de la calidad deben ser:

a) coherentes con la política de la calidad y tener en cuenta los requisitos generales del sistema y de la seguridad de la información;

b) medibles;

c) pertinentes para la conformidad de los productos y servicios y para el aumento de la satisfacción de las partes interesadas;

d) objeto de seguimiento;

e) comunicados;

f) revisados periódicamente para evaluar su pertinencia.

La UAI debe conservar información documentada sobre los objetivos de la calidad.

Durante la planificación para lograr sus objetivos de la calidad, la UAI debe determinar:

a) lo que se va a hacer;

b) qué recursos se requerirán;

c) quién será responsable;

d) cuándo se finalizará;

e) cómo se evaluarán los resultados.

6.2.1 Planificación de los cambios

Propósito

Garantizar que los cambios en el sistema de gestión de la calidad se lleven a cabo de manera planificada y sistemática.

Requisitos

La UAI debe considerar:

a) el propósito del cambio y cualquiera de sus potenciales consecuencias;

b) la integridad del sistema de gestión de la calidad;

c) la disponibilidad de recursos;

d) la asignación o reasignación de roles y responsabilidades.

7 PROCESOS DE APOYO

7.1 Infraestructura

Propósito

Asegurar que la UAI dispone y mantiene una infraestructura tal que le permite cumplir con sus funciones de manera eficaz.

Requisitos

La UAI debe asegurar que dispone de:

a) infraestructura física y los servicios asociados que permitan la prestación del servicio, de acuerdo con la planificación realizada;

b) registros de los bienes asignados a la UAI;

c) sistemas informáticos (hardware y software) apropiados para realizar la gestión del servicio de acuerdo a la normativa vigente y la planificación realizada; y acordes para garantizar la adecuada confidencialidad, integridad y disponibilidad de la información gestionada por la UAI.

d) espacios adecuados para el personal contemplando iluminación, climatización y circulación.

NOTA. En el anexo E se describen “Buenas Prácticas de Seguridad de la Información”.

7.2 Gestión ambiental

Propósito

Generar conciencia ambiental en el personal de la UAI promoviendo el uso racional de los recursos.

Requisitos

La UAI debe:

a) propiciar la disminución de producción de residuos y la despapelización, contribuyendo así a la protección y conservación del medio ambiente, siguiendo el concepto de “3R”, basado en reducir, reutilizar y reciclar;

b) adoptar acciones tendientes a desarrollar en el personal hábitos de consumo responsable y sostenible.

NOTA. Por “despapelización” se consideran las acciones que adopta la UAI tendientes a disminuir el uso del papel. Por ejemplo, evitar las impresiones, imprimir en doble faz, promover la digitalización de trámites y comunicaciones, entre otras.

7.3 Capacitación de los recursos humanos

Propósito

Asegurar la competencia y formación del personal de la UAI.

Requisitos

La UAI debe:

a) determinar la competencia de las personas basándose en la educación, formación o experiencia apropiadas;

b) gestionar, de acuerdo a los roles y responsabilidades, la necesidad de incorporar, actualizar o mejorar las competencias del personal de la UAI;

c) gestionar e implementar la realización de las actividades de formación necesarias para que el personal pueda obtener y actualizar las competencias requeridas;

d) conservar la información documentada de la determinación de las competencias, la evaluación de las competencias de las personas y de las acciones de formación.

NOTA. En relación a las competencias del personal, se deben considerar todas las necesarias para que las personas puedan desempeñarse cumpliendo los requisitos del sistema de gestión, incluyendo los conocimientos requeridos para las prácticas de seguridad de la información implementadas; los conceptos básicos de la gestión de la calidad y los requisitos de este Referencial; la comprensión de la normativa de aplicación a los procesos, entre otras.

7.4 Control de la información documentada

Propósito

Asegurar que:

a) el personal de la UAI utiliza documentos aprobados y en su versión vigente;

b) la información documentada es conservada en forma segura y puede ser fácilmente localizada en el caso que se necesite consultarla.

Requisitos

La UAI debe mantener información documentada que describa la metodología para:

a) revisar y aprobar la información documentada antes de su puesta en vigencia;

b) actualizarla cuando sea necesario, identificando y controlando sus cambios;

c) asegurar su disponibilidad para su uso cuándo y dónde se necesite;

d) asegurar su almacenamiento, preservación, conservación y disposición (según corresponda al tipo de documentación y a la normativa);

e) definir los requisitos para el ingreso y egreso de la documentación en la UAI;

f) definir los activos de información a preservar y la protección de su confidencialidad, integridad y disponibilidad.

La información documentada conservada como evidencia de la conformidad debe protegerse, en todos los casos, contra modificaciones no intencionadas.

La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación de los procesos, se debe identificar y controlar.

NOTA 1. En la definición de requisitos para el ingreso y egreso de la documentación en la UAI, deberá considerarse cuando sea aplicable, la interacción con las áreas responsables del organismo (por ejemplo, Mesa de Entradas y Salidas, Secretaría y Despacho, entre otras).

NOTA 2. Los activos de la información incluyen la información propiamente dicha y los recursos que le dan soporte a la información, por ejemplo, notebook, sistema operativo en red, pen drive, software, etc.

7.5 Gestión de bienes y/o servicios

Propósito

Gestionar la provisión de todos los bienes y servicios que requiere la UAI para su correcto funcionamiento.

Requisitos

La UAI debe:

a) relevar las necesidades de bienes y/o servicios para el funcionamiento eficaz de la UAI;

b) solicitar la provisión de bienes y/o servicios detallando sus especificaciones técnicas;

c) identificar y evaluar a los proveedores de bienes y servicios específicos, manteniendo la evidencia documentada;

d) verificar que los productos cumplen con las especificaciones de la solicitud y registrar los resultados de su evaluación.

NOTA 1. Se consideran proveedores específicos (internos y/o externos) aquellos relacionados directamente con la eficacia en el cumplimiento de los resultados de la UAI.

NOTA 2. Dentro de los servicios, se incluyen aquellos relacionados con los servicios informáticos que pueden ser suministrados por otras áreas de soporte ajenas a la UAI y/o al propio organismo al que pertenece la UAI.

8 PROCESOS PRINCIPALES

8.1 Planeamiento

Propósito

Establecer la metodología a implementar para la formulación, seguimiento, control y análisis de desvíos del plan anual de auditoría.

Contemplar en el plan de auditoría, la evaluación de los factores de riesgo de las operaciones, procesos y/o áreas auditables, a los efectos de contribuir con la eficacia y eficiencia de la gestión del organismo.

Requisitos

La UAI debe mantener información documentada para:

a) identificar los procesos de la organización a auditar;

b) elaborar y conservar una evaluación de riesgos que incluya la clasificación de los riesgos, la ponderación del impacto y su probabilidad de ocurrencia;

c) determinar el universo de proyectos de auditoría a realizar de acuerdo a los resultados de la evaluación de riesgos y los requisitos de las partes interesadas;

d) realizar y evidenciar la revisión y actualización de los planes plurianuales como mínimo una vez al año;

e) verificar que lo indicado en los informes de la SIGEN, el resultado de planes anteriores, las recomendaciones del Comité de Control o de Auditoría, sean tomados en cuenta en la realización del nuevo plan;

f) determinar las capacidades y disponibilidades para la planificación de los proyectos de auditoría;

g) definir los proyectos de auditoría a incluir en la planificación anual y establecer los cronogramas de emisión de informes y lineamientos de trabajo;

h) asegurar el cumplimiento de los plazos de presentación requeridos por la normativa para la aprobación del plan;

i) realizar el seguimiento de la ejecución del plan anual, registrando los desvíos y analizando sus causas.

8.2 Desarrollo de Auditorías

Propósitos

Ejecutar los proyectos previstos en el plan anual de auditoría, con el debido análisis de cronogramas y recursos requeridos, y la explicitación clara del alcance y programas de trabajo a ejecutar; actualizándolos en función de los cambios que ocurrieren.

Obtener evidencias y, cuando corresponda, formular observaciones con sus respectivas recomendaciones sobre las áreas y los procesos auditados.

Confeccionar los papeles de trabajo, que constituyen los elementos de prueba de la realización del trabajo de auditoría y de las decisiones tomadas en consecuencia, y son la base para la preparación del informe de auditoría.

Requisitos

La UAI debe mantener información documentada para:

a) planificar el proyecto de auditoría indicando: objeto, alcance, programas de trabajo, cronograma de tiempos y recursos requeridos;

b) determinar las actividades de campo a realizar;

c) registrar los avances del desarrollo de la auditoría;

d) identificar las observaciones y su relevancia, las causas que las originan y la incidencia, así como también la ponderación y/o cuantificación de los desvíos;

e) asegurar la trazabilidad de cada una de las observaciones a incorporar en el informe de auditoría;

f) elaborar, supervisar y controlar el informe de auditoría, exponiendo las observaciones, recomendaciones y conclusiones que surjan de las evidencias obtenidas, como así también las consideraciones y sugerencias que propendan a la mejora del desempeño del proceso auditado.

g) emitir el informe de auditoría y comunicar a los destinatarios que corresponda, controlando su carga en el Sistema de Seguimiento de Informes y Observaciones (SISIO) Web vigente.

8.3 Seguimiento de las observaciones

Propósito

Realizar el seguimiento del estado de las observaciones vigentes que surgen de los informes de auditoría (internos y externos) y del cumplimiento de las acciones correctivas propuestas tendientes a subsanar los desvíos, contribuyendo a la mejora del Sistema de Control Interno del organismo.

Requisitos

La UAI debe mantener información documentada para:

a) verificar el uso de los criterios de clasificación de los estados de las observaciones;

b) constatar que las observaciones clasificadas como No Regularizables, Regularizadas y En Trámite tengan su respaldo en evidencias válidas y suficientes;

c) verificar que las medidas correctivas implementadas por los auditados, sean conducentes a la regularización de la observación y estén evidenciadas mediante documentación válida y suficiente;

d) constatar que los nuevos estados de las observaciones hayan sido debidamente actualizados en el SISIO Web vigente, o el que en el futuro lo reemplace;

e) consolidar toda la documentación y su recopilación para la elaboración del informe de auditoría de seguimiento de recomendaciones.

8.4 Otras actividades

Propósito

Ejecutar otras actividades definidas en el plan anual de auditoría para dar cumplimiento a requerimientos especiales (por ej. denuncias, bonos de consolidación, pedidos del Poder Judicial, AGN, otros) solicitados por normas especiales o por autoridades con competencias para ello.

Requisitos

La UAI debe:

a) establecer y clasificar los diferentes tipos de actividades a realizar;

b) definir el objeto del trabajo, su alcance y la normativa aplicable;

c) planificar, desarrollar, supervisar y controlar las tareas;

d) describir las tareas realizadas y su resultado;

e) verificar la existencia de documentación que respalde el resultado de las actividades;

f) definir los requisitos mínimos para la comunicación de los resultados de cada una de las actividades.

NOTA. Cuando no se pueda verificar la existencia de una normativa especial o procedimiento para la realización de las actividades, la UAI deberá consultar o informar tal circunstancia a SIGEN.

9 EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

Propósito

Asegurar que los procesos son eficaces, planificando sus actividades y utilizando indicadores que permitan medir el grado de cumplimiento de las metas.

Requisitos

Para los procesos del apartado 8 y los relativos a la satisfacción de las partes interesadas, la UAI debe:

a) definir los indicadores que utiliza;

b) definir la metodología, incluyendo las responsabilidades y la periodicidad de la medición, el seguimiento y la evaluación de los resultados.

La evaluación debe considerar el desempeño de los procesos y su eficacia en el sistema de gestión de la calidad.

La UAI debe conservar la información documentada de los resultados y su análisis.

9.2 Satisfacción de las partes interesadas

Propósito

Conocer la opinión de las partes interesadas pertinentes respecto de las actividades desarrolladas por la UAI para identificar oportunidades de mejora en la prestación del servicio.

Requisitos

La UAI debe determinar métodos que le permitan obtener información relativa a la percepción de las partes interesadas pertinentes respecto al cumplimiento de sus requisitos. Estos métodos deben incluir:

a) la planificación de los elementos de entrada;

b) la obtención de la información;

c) su utilización en la identificación de acciones para la mejora y

d) la comunicación de los resultados y las acciones a implementar.

NOTA. Los métodos determinados para obtener información de la percepción de las partes interesadas pueden incluir elementos de entrada de fuentes como encuestas, entrevistas, notas recibidas, evaluaciones del servicio, entre otras.

9.3 Revisión por la Dirección

Propósito

Asegurar que todas las actividades y resultados relacionados con la calidad de los servicios que presta la UAI son revisados regularmente por la Dirección para poder tomar las medidas que permitan una mejora continua.

Requisitos

La Dirección de la UAI debe revisar al menos cada 12 meses:

a) sus procesos y la conformidad de sus resultados;

b) los resultados de las auditorías del sistema de gestión de la calidad y/o de las autoevaluaciones;

c) la retroalimentación y nivel de satisfacción de las partes interesadas;

d) el resultado de la resolución de las no conformidades y las acciones correctivas implementadas;

e) las quejas y reclamos que se hayan recibido y el tratamiento dado;

f) los resultados de las evaluaciones de riesgo del sistema de gestión de la calidad;

h) la retroalimentación de incidentes de seguridad de la información y la eficacia de la implementación de las actividades de seguridad de la información para lograr los objetivos determinados;

i) los cambios en la legislación y normativa aplicable y en el contexto donde opera;

j) el estado de las acciones tomadas en las revisiones anteriores.

Con el fin de determinar las acciones que le permitan continuar prestando sus servicios en forma confiable según las necesidades de las partes interesadas pertinentes, la Dirección debe definir acciones relacionadas con:

- oportunidades de mejora;
- necesidades de cambios en el sistema de gestión;
- necesidades de recursos.

La UAI debe conservar la información documentada analizada, así como también la información que surge como resultado de las revisiones.

9.4 Autoevaluación y auditorías internas

Propósito

Realizar una revisión sistemática de las actividades de la UAI y de su desempeño, verificando el cumplimiento de los requisitos, la implementación y el mantenimiento eficaz del sistema y el enfoque en la mejora continua.

Requisitos

La UAI debe realizar una autoevaluación o una auditoría interna de su sistema de gestión de la calidad. La Dirección de la UAI podrá optar por implementar lo establecido en los apartados 9.4.1 o 9.4.2.

9.4.1 Autoevaluación

La UAI debe establecer un programa de autoevaluación que incluya:

a) la frecuencia, que como mínimo será de una vez al año;

b) la metodología a aplicar y las responsabilidades para su ejecución;

c) la definición de las metas de desempeño esperadas;

d) la presentación y comunicación de los resultados obtenidos.

9.4.2 Auditorías internas del sistema de gestión de la calidad

La UAI debe

a) planificar, establecer, implementar y mantener un programa de auditoría que incluya la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, que debe tener en consideración la importancia de los procesos involucrados, los cambios que afecten a la organización y los resultados de las auditorías previas.

b) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría impidiendo que los auditores auditen su propio trabajo y/o exista un conflicto de intereses.

c) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.

NOTA. Para el desarrollo de auditorías internas del sistema de gestión de la calidad ver la ISO 19011 a modo de orientación.

10 MEJORA

10.1 No conformidades y acciones correctivas

Propósito

Asegurar que las no conformidades se registran, se analizan las causas que la produjeron y se implementan las acciones correctivas necesarias para evitar su reiteración y/o disminuir el riesgo asociado.

Requisitos

La UAI debe mantener información documentada que describa la metodología para la detección y el tratamiento de las no conformidades, incluyendo los reclamos y quejas, los incidentes de seguridad de la información, y la implementación -cuando corresponda- de acciones correctivas.

Debe contemplar como mínimo:

a) identificar y registrar la no conformidad, queja o reclamo e incidentes de seguridad de la información y la/s acción/es tomada/s;

b) el análisis de las causas y -de corresponder- la definición de las acciones correctivas para evitar la recurrencia;

c) la revisión de la eficacia de las acciones correctivas tomadas;

d) cuando se reciba una queja o reclamo de una parte interesada, se asegurará que en todos los casos se remite una respuesta luego del tratamiento realizado;

e) conservar información documentada como evidencia del tratamiento de las no conformidades, quejas y reclamos y de la aplicación de acciones correctivas.

NOTA. Las acciones para la gestión de los incidentes de seguridad de la información deben ser acordes con la importancia del activo de información y el riesgo asociado.

10.2 Mejora continua

Propósito

Alinear la gestión de la UAI al enfoque en la mejora continua.

Requisitos

La UAI debe considerar los resultados del análisis y de la evaluación (satisfacción de las partes interesadas, seguimiento de indicadores, revisiones por la Dirección, informes de auditorías, resultados de la formación, acciones correctivas implementadas), para determinar si hay necesidades u oportunidades que deben considerarse como parte de la mejora. Debe conservarse información documentada del análisis, de la evaluación y de la decisión de la adopción o no de oportunidades de mejora.

Anexo A
(Informativo)

Relación con los requisitos de la norma ISO 9001:2015

Capítulo del Referencial IRAM N° 13	Capítulo de la ISO 9001:2015 relacionado
1 OBJETO Y CAMPO DE APLICACIÓN	**1 OBJETO Y CAMPO DE APLICACIÓN**
2 REFERENCIAS NORMATIVAS	**2 REFERENCIAS NORMATIVAS**
3 TÉRMINOS Y DEFINICIONES	**3 TÉRMINOS Y DEFINICIONES**
4 SISTEMA DE GESTIÓN DE LA CALIDAD	**4 CONTEXTO DE LA ORGANIZACIÓN**
4.1 Comprensión de la organización y de su contexto	4.1 Comprensión de la organización y de su contexto
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	4.2 Comprensión de las necesidades y expectativas de las partes interesadas
4.3 Control de los procesos	4.4 Sistema de gestión de la calidad y sus procesos
5 LIDERAZGO	**5 LIDERAZGO**
5.1 Liderazgo y compromiso	5.1 Liderazgo y compromiso
5.2 Política	5.2 Política
5.3 Roles, responsabilidades y autoridades	5.3 Roles, responsabilidades y autoridades en la organización
6 PLANIFICACIÓN	**6 PLANIFICACIÓN**
6.1 Acciones para abordar riesgos y oportunidades	6.1 Acciones para abordar riesgos y oportunidades
6.1.1 Gestión de riesgos de seguridad de la información	7.5.3 Control de la información documentada
6.2 Objetivos de la calidad y planificación para lograrlos	6.2 Objetivos de la calidad y planificación para lograrlos
6.2.1 Planificación de los cambios	6.3 Planificación de los cambios
7 PROCESOS DE APOYO	**7 APOYO**
7.1 Infraestructura	7.1 Recursos / 7.1.3 Infraestructura
7.2 Gestión Ambiental	N/A
7.3 Capacitación de los recursos humanos	7.2 Competencia
7.4 Control de la información documentada	7.5 Información documentada
7.5 Gestión de bienes y/o servicios	8.4 Control de los procesos, productos y servicios suministrados externamente
8 PROCESOS PRINCIPALES	**8 OPERACIÓN**
8.1 Planeamiento	8.1 Planificación y control operacional
8.2 Desarrollo de auditorías	8.2 Requisitos para los productos y servicios

Capítulo del Referencial IRAM N° 13	Capítulo de la ISO 9001:2015 relacionado
8.3 Seguimiento de las observaciones	8.5 Producción y prestación del servicio 8.6 Liberación de los productos y servicios NOTA. Estos requisitos aplican parcialmente dentro de los procesos principales que ya se encuentran definidos en el Referencial.
8.4 Otras actividades	
No aplica	8.3 Diseño y desarrollo de los productos y servicios
9 EVALUACIÓN DEL DESEMPEÑO	**9 EVALUACIÓN DEL DESEMPEÑO**
9.1 Seguimiento, medición, análisis y evaluación	9.1 Seguimiento, medición, análisis y evaluación
9.2 Satisfacción de las partes interesadas	9.1.2 Satisfacción del cliente
9.3 Revisión por la Dirección	9.3 Revisión por la Dirección
9.4 Autoevaluación y Auditorías internas	9.2 Auditoría interna. NOTA. Aplica sólo a la auditoría interna. Autoevaluación no aplica.
10 MEJORA	**10 MEJORA**
10.1 No conformidades y acciones correctivas	8.7 Control de las salidas no conformes / 10.2 No conformidad y acciones correctivas
10.2 Mejora continua	10.3 Mejora

Anexo B
(Informativo)

Principios de gestión de la calidad conforme a la norma IRAM-ISO 9000:2015

Enfoque al cliente
El enfoque principal de la gestión de la calidad es cumplir los requisitos del cliente y tratar de exceder sus expectativas.

Liderazgo
Los líderes en todos los niveles establecen la unidad de propósito y la dirección, y crean condiciones en las que las personas se implican en el logro de los objetivos de la calidad de la organización.

Compromiso de las personas
Las personas competentes, empoderadas y comprometidas en toda la organización son esenciales para aumentar la capacidad de la organización para generar y proporcionar valor.

Enfoque a procesos
Se alcanzan resultados coherentes y previsibles de manera más eficaz y eficiente cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente.

Mejora
Las organizaciones con éxito tienen un enfoque continuo hacia la mejora.

Toma de decisiones basada en la evidencia
Las decisiones basadas en el análisis y la evaluación de datos e información tienen mayor probabilidad de producir los resultados deseados.

Gestión de las relaciones
Para el éxito sostenido, las organizaciones gestionan sus relaciones con las partes interesadas pertinentes, tales como los proveedores.

Sobre estos principios se recomienda prestar especial atención por parte de la máxima autoridad de la UAI al "Liderazgo"
La creación de la unidad de propósito y la dirección y gestión de las personas permiten a una organización alinear sus estrategias, políticas, procesos y recursos para lograr sus objetivos. Esto es una responsabilidad del líder.

El liderazgo debe ser presente y activo, no solo declarando el compromiso con el sistema de gestión sino demostrarlo con hechos, involucrándose en la implementación, seguimiento, análisis y revisión de los resultados y alentando al personal a comprometerse en el cumplimiento de los requisitos.

Algunos beneficios de un buen liderazgo son:

- aumento de la eficacia y eficiencia al cumplir los objetivos de la calidad de la organización;

- mejora en la coordinación de los procesos de la organización;

- mejora en la comunicación entre los niveles y funciones de la organización;

- desarrollo y mejora de la capacidad de la organización y de sus personas para entregar los resultados deseados.

El líder debe:

- comunicar en toda la organización la misión, la visión, la estrategia, las políticas y los procesos de la organización;

- crear y mantener los valores compartidos, la imparcialidad y los modelos éticos para el comportamiento en todos los niveles de la organización;

- establecer una cultura de confianza e integridad;

- fomentar el compromiso con la calidad en toda la organización;

- asegurarse de que los líderes en todos los niveles son ejemplos positivos para las personas de la organización;

- proporcionar a las personas los recursos, la formación y la autoridad requerida para actuar con responsabilidad y obligación de rendir cuentas;

- inspirar, fomentar y reconocer la contribución de las personas.

NOTA. Se presenta solo la enunciación de los principios y se destaca el concepto de Liderazgo. Se recomienda conocer el desarrollo completo de los otros principios consultando el apartado 2.3 de la norma ISO 9000:2015.

Anexo C
(Informativo)

Etapas de implementación

CAPÍTULO		Etapas de implementación		
		A	B	C
1 OBJETO Y CAMPO DE APLICACIÓN		No aplica		
2 REFERENCIAS NORMATIVAS				
3 TÉRMINOS Y DEFINICIONES				
4 SISTEMA DE GESTIÓN DE LA CALIDAD	4.1 Comprensión de la organización y de su contexto	Todo	--	--
	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Todo	--	--
	4.3 Control de los procesos	Todo	--	--
5 LIDERAZGO	5.1 Liderazgo y compromiso	a, b, c y d	e, f, g y h	--
	5.2 Política	Todo	--	--
	5.3 Roles, responsabilidades y autoridades en la organización	Todo	--	--
6 PLANIFICACIÓN	6.1 Acciones para abordar riesgos y oportunidades	--	a	b
	6.1.1 Gestión de riesgos de seguridad de la información	--	a	b
	6.2 Objetivos de la calidad y planificación para lograrlos	Determinación todo	Planificación todo	--
	6.2.1 Planificación de los cambios	--	--	Todo
7 PROCESOS DE APOYO	7.1 Infraestructura	Todo		
	7.2 Gestión Ambiental	--	Todo	--
	7.3 Capacitación de los recursos humanos	a	b, c y d	--
	7.4 Control de la información documentada	a, b y c	d, e y f	--
	7.5 Gestión de bienes y/o servicios	a y b	c y d	--

CAPÍTULO		Etapas de implementación		
		A	**B**	**C**
8 PROCESOS PRINCIPALES	8.1 Planeamiento	a, b, c, d, e, f y g	h - i	--
	8.2 Desarrollo de auditorías	a, b, c, d y e	f y g	
	8.3 Seguimiento de observaciones	a,b y c	d y e	--
	8.4 Otras actividades	a	b,c,d, e y f	--
9 EVALUACIÓN DEL DESEMPEÑO	9.1 Seguimiento, medición, análisis y evaluación	--	a y b	c y d
	9.2 Satisfacción de las partes interesadas	--	--	Todo
	9.3 Revisión por la Dirección	--	--	Todo
	9.4 Autoevaluación y auditorías internas	--	--	Todo
10 MEJORA	10.1 No conformidades y acciones correctivas	--	Todo	--
	10.2 Mejora continua	--	--	Todo

Anexo D
(Informativo)

Consideraciones para la gestión de riesgos

Referencias: IRAM 17551:2009 e IRAM-ISO 31000:2013

El análisis del riesgo proporciona la base para su valoración y orienta las decisiones con respecto a su tratamiento.

El Referencial IRAM Nº 13 en el apartado 6.1 “Acciones para abordar riesgos y oportunidades”, indica que la UAI debe determinar los riesgos y oportunidades generales del sistema, incluyendo explícitamente los referidos a la seguridad de la información, que sean necesarios tratar con el fin de:

a) asegurar que el sistema de gestión de la calidad pueda lograr los resultados previstos;

b) prevenir o reducir efectos indeseados;

c) lograr la mejora continua.

Se recomienda que la evaluación del riesgo sea considerada como todo un proceso, cuyo objetivo es comprender la “naturaleza del riesgo” y determinar el “nivel de riesgo” para el sistema de gestión de la calidad.

Para la implementación del proceso de evaluación de riesgo, se debería configurar previamente el marco organizativo para su administración. Esta configuración incluiría:

- definir una política de gestión de riesgos y establecer claramente los objetivos de la organización respecto de la gestión del riesgo, así como el umbral de aceptación. Esto debería ser comunicado a toda la organización;

- establecer una metodología de registro y mapeo de riesgos;

- definir el propietario (responsable) del riesgo, es decir la persona o entidad que posee la autoridad y responsabilidad (y, por ende, debe hacerse cargo) de gestionar el riesgo;

- prever la manera de comunicación interna sobre cada riesgo detectado;

Posteriormente se debería implementar el proceso de gestión de riesgos propiamente dicho.

Las etapas del proceso de gestión de riesgos serían:

1. Establecimiento del contexto

Para realizar un análisis de riesgos eficaz se requiere de una adecuada comprensión de la organización y los contextos estratégico, organizacional y de gestión de riesgos en los cuales tendrá lugar el resto de los procesos. A su vez se recomienda analizar tanto el contexto interno como externo.

- El "contexto interno” es entendido como todo aquello que se encuentra dentro de la organización y que puede influir en la forma en la que ésta gestiona el riesgo para alcanzar sus objetivos.

  Para la evaluación del “contexto interno”, se recomienda que el mismo esté alineado con la cultura, los procesos, la estructura y la estrategia de la organización.

Dentro del contexto interno se puede incluir la estructura de la organización, los roles, las políticas, los objetivos, las estrategias y los sistemas de información.

- El "contexto externo" se refiere al entorno o circunstancias en el que la organización busca alcanzar sus objetivos. El contexto externo puede incluir: lo cultural, social, político, jurídico, reglamentario, financiero, tecnológico, económico, natural o competitivo, ya sea internacional, nacional, regional o local.

  Para la evaluación del "contexto externo", es conveniente asegurar que se tienen en cuenta las expectativas de las partes interesadas externas.

  Dentro de contexto externo se incluye además de los requisitos legales y regulatorios, las percepciones de las partes interesadas y otros aspectos externos referidos a los riesgos específicos de la actividad.

2. Evaluación del riesgo

La evaluación del riesgo incluye las actividades sistemáticas de: identificar, analizar y valorar los riesgos.

- Identificación del riesgo: qué, por qué, dónde, cuándo y cómo los eventos podrían afectar el logro de los objetivos estratégicos y operativos de la organización.
- Analizar los riesgos: se identifican los controles existentes y se analizan los riesgos en términos de consecuencia y probabilidad en el contexto de tales controles. La combinación del impacto o consecuencia y probabilidad, permite estimar el nivel de riesgo.
- Valorar los riesgos: generalmente se lo calcula como el producto del valor del "impacto" que provoca el evento potencial y la "probabilidad de ocurrencia" de dicho evento. Los resultados se comparan respecto a los criterios preestablecidos.

Se recomienda elaborar un mapeo con los resultados de los riesgos evaluados.

3. Tratamiento de los riesgos

Se desarrollan e implementan estrategias y planes de acción específicos que permitan mitigar los riesgos y guarden una adecuada relación costo-beneficio del tratamiento elegido.
El tratamiento de los riesgos es responsabilidad de cada propietario (responsable) del riesgo y es quien debe tomar las decisiones (pueden ser: evitar; aceptar; eliminar la fuente de riesgo; modificar la probabilidad; modificar las consecuencias; compartir el riesgo con otra parte o partes; retener el riesgo).

4. Supervisar y revisar (monitorear)

Se debe efectuar el seguimiento y control de la eficacia de las medidas de mitigación adoptadas, comunicando y consultando a los interesados internos y externos.

Recomendación:

Se debería tener presente durante todas las etapas del proceso de gestión de riesgos, que se mantenga una continua "comunicación y consulta" con las partes interesadas externas e internas, de manera que se entiendan los fundamentos y las razones por los cuales se toman las decisiones y se plantean acciones específicas.
De este modo se trata de asegurar que al momento de definir los criterios de riesgo y su valoración, se han tenido en cuenta de manera adecuada los distintos puntos de vista de las partes interesadas.

En la figura 3 se presenta una síntesis de las actividades a considerar en la gestión de riesgos.

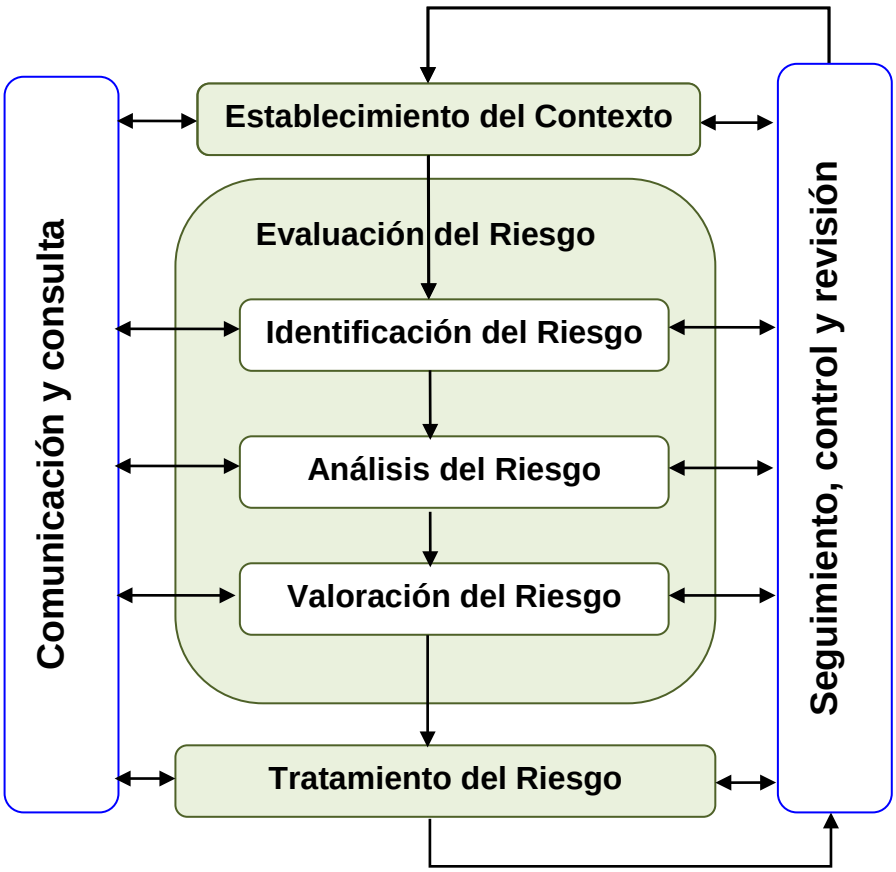


Figura 3 - Representación esquemática del proceso de Gestión de Riesgos

Anexo E
(Informativo)

Buenas prácticas de seguridad de la información

Referencia IRAM-ISO/IEC 27002:2008 - Tecnología de la información. Técnicas de seguridad. Código de práctica para la Gestión de la Seguridad de la Información.

La información es un recurso que, como otros activos importantes, tiene valor para una organización y, por consiguiente, debe ser debidamente protegida.

La seguridad de la información es la protección de la información de una amplia variedad de amenazas, con el objeto de asegurar la continuidad del cumplimiento de las misiones y funciones del organismo, minimizar los riesgos y maximizar el retorno del esfuerzo y la inversión aplicada en seguridad.

La siguiente enumeración es una breve lista de actividades, al solo efecto de tener una ilustración de algunas prácticas referidas a la seguridad de la información y que pueden orientar al personal sobre qué tratan las mismas, pero no pretende ser un desarrollo de la actividad.

Al final, se ha hecho una apertura mayor del capítulo referido a la seguridad de los recursos humanos, por considerar que es el aspecto más sensible y vulnerable de toda organización.

Gestión de activos

Se recomienda elaborar un inventario de los “activos de información sensible” actualizado y la identificación del responsable del mismo.

NOTA. Los activos de la información incluyen la información propiamente dicha y los recursos que dan soporte a la información. Por ejemplo, notebook, sistema operativo en red, etc.

En dicho inventario se debería incluir una clasificación de la información según su importancia respecto de la confidencialidad, integridad y disponibilidad. (Por ejemplo, Confidencialidad: *Pública / *Privada / *Reservada; Integridad: *Trivial / Crítica; Disponibilidad: *Alta / *Baja).

Por ejemplo:
Confidencialidad: *Pública; *Privada; *Reservada;
Integridad: *Trivial; *Crítica;
Disponibilidad: *Alta; *Baja.

Control de acceso

Se recomienda:

- Definir las áreas críticas de acceso a los sistemas y servicios informáticos que afecta a la información sensible, indicando los usuarios autorizados.

- Dejar evidencias (información documentada) del control de accesos por medio de política de contraseñas; la gestión de privilegios; el registro de usuarios; el registro de personal inhabilitado.

- Nominación de la persona nexo con las áreas que administran los servidores de cada repartición.

Seguridad del equipamiento

Se recomienda:

- Realizar un análisis de riesgo sobre las amenazas que pudieran provocar la pérdida, robo o compromiso del equipamiento afectado a los activos de la información.

- Definir un emplazamiento seguro y el tipo de protección del equipamiento y servicios de apoyo según el análisis de riesgo realizado.

- Garantizar que los medios de comunicación extraíbles (pen drive, etc.) con información sensible estén protegidos contra el acceso no autorizado (por ejemplo: encriptación).

- Cuando se requiera eliminar un activo o la reutilización de equipos, definir una metodología para resguardar información durante el proceso de reutilización o la eliminación segura.

- Inculcar las prácticas de escritorio y pantalla limpia.

- Definir los resguardos para la utilización de equipos y de activos, fuera de las instalaciones.

Seguridad de los sistemas y aplicaciones informáticas

Se recomienda que se identifiquen los requisitos de seguridad de sistemas de información y las aplicaciones informáticas. Esto incluye sistemas operativos, infraestructura, aplicaciones, productos enlatados.

Seguridad de las operaciones

Se recomienda garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información a través del establecimiento de responsabilidades y procedimientos para la gestión y funcionamiento de todas las instalaciones de procesamiento de información.

Esto incluye:

- Copias de seguridad y control de la realización correcta de las copias de seguridad (backup).

- Instrucciones para el manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución de tareas.

- Contactos de soporte en caso de dificultades operativas o técnicas imprevistas.

- Instrucciones especiales para el manejo de salidas y medios, como la gestión de salida de resultados confidenciales, incluyendo procedimientos para la eliminación segura de las salidas de resultados de tareas fallidas.

- Procedimientos de recuperación para utilizar en caso de producirse fallas en el sistema.

- Control de los cambios.

- Registro de los controles implementados contra el software malicioso.

- Criterios de mantenimiento de equipos que permitan la normal operación del área.

Gestión de la continuidad

Se recomienda que se implemente un proceso de gestión de la continuidad para asegurar la reanudación oportuna de las operaciones esenciales y minimizar el impacto en la organización cuando ocurriere un incidente o evento que afecta la seguridad de la información, a fin de recuperar las pérdidas de los activos de información (por ejemplo: desastres naturales, accidentes, fallas en el equipamiento o acciones deliberadas) a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

Es conveniente que se identifiquen los procesos críticos e integren los requerimientos de la gestión de seguridad de la información para la continuidad de las actividades, con otros requerimientos de continuidad relacionados con aspectos tales como operaciones, recursos humanos, materiales, transporte e instalaciones.

Se recomienda que las consecuencias de desastres, fallas de seguridad, pérdidas de servicio y de disponibilidad de servicio, se encuentren sujetas a un análisis de impacto en las misiones y funciones.

Seguridad de los recursos humanos

Objetivo

Asegurar que el personal entienda sus responsabilidades respecto de la seguridad de la información y sean idóneos para los roles para los cuales son considerados.

Actividades

1-Antes del ingreso

Se recomienda definir acuerdos de confidencialidad o de no divulgación y el registro de cada uno de los acuerdos suscriptos, tanto con personal interno como externo que afecten a la operación.

El personal de la UAI debería recibir un detalle de cuáles serán sus responsabilidades y las de la organización en relación a la seguridad de la información, y registrar la comprensión como información documentada.

2-Durante el empleo

La máxima autoridad de la UAI debería garantizar la concienciación y capacitación en seguridad de la información a través de actividades periódicas, así como las responsabilidades y la forma de cumplimiento. Asimismo, se deben incluir actualizaciones regulares en las políticas y procedimientos organizacionales, que sean pertinentes a su tarea.

Cuando hubiere incidentes significativos, se debería realizar una concienciación apropiada a dicho evento.

Como ejemplos de temas a tratar se pueden mencionar: protección de activos de información sensible, cambio de datos de papeles de trabajo, el mal uso de los equipos que inhabiliten los mismos; técnicas de seguridad lógica; encriptado, etc.

2.1 Proceso disciplinario: la máxima autoridad de la UAI debe aplicar el proceso disciplinario formal para sancionar y comunicar al personal que haya ocasionado una violación a la seguridad de la información, incluyendo las actuaciones que dicta la normativa.

3-Desvinculación o cambio de puesto

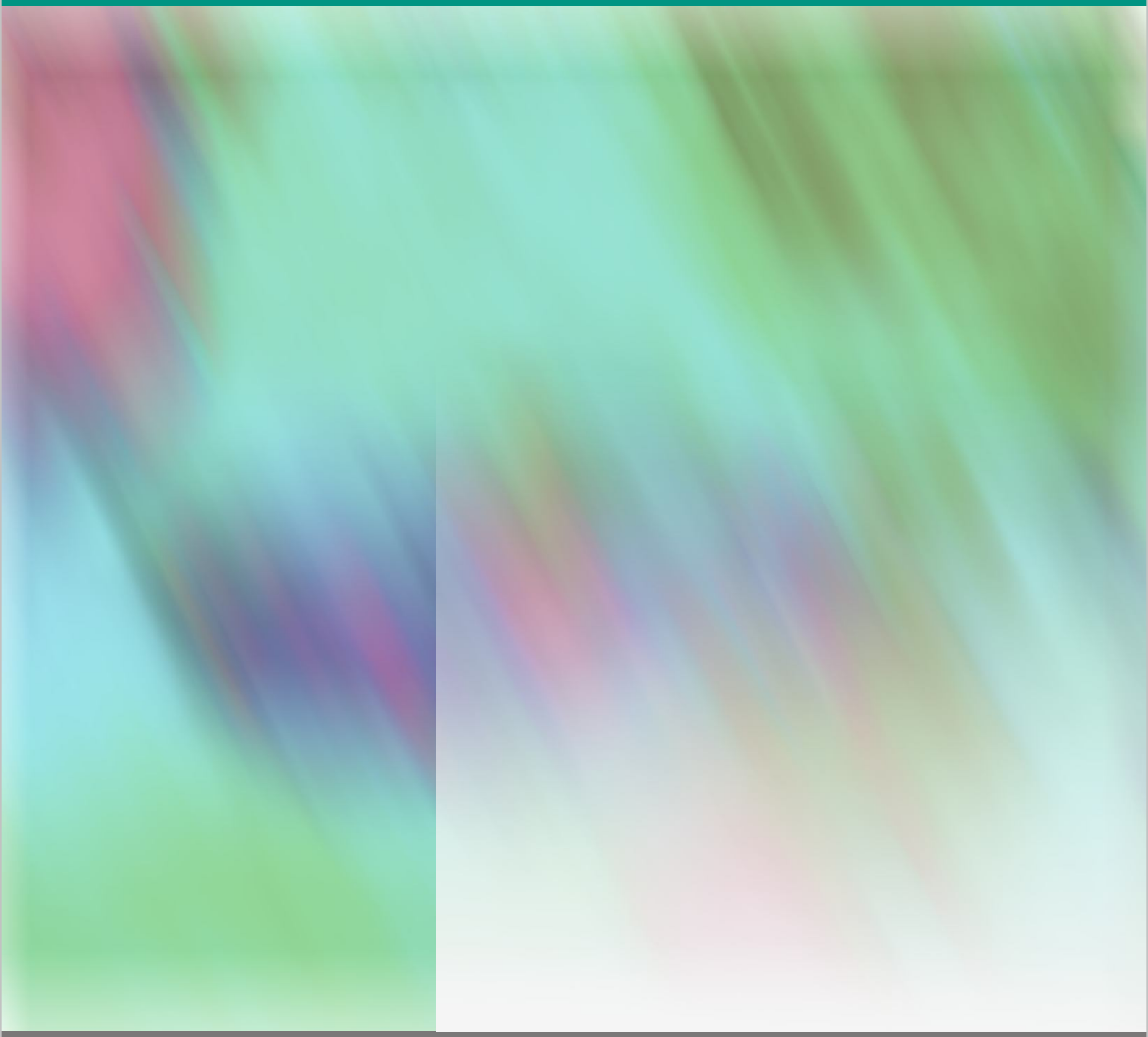
En caso que se produzca una desvinculación del personal de la UAI o un cambio de puesto, la máxima autoridad de la UAI y la persona afectada, deben dejar constancia por medio de un acta, de las responsabilidades y las obligaciones de seguridad de la información que continúan siendo vigentes, luego de la desvinculación o cambio de puesto.

Se debe garantizar ante el área correspondiente que se gestione la baja de los permisos, anulación de accesos a la información y se la desvincule de los privilegios de conectividad.

Anexo F
(Informativo)

Equipo de trabajo

ALVAREZ, Alejandro	Banco de la Nación Argentina
ANGELOMÉ, Susana Teresa	Sindicatura General de la Nación
AZPELICUETA, Sandra Fabiana	Sindicatura General de la Nación
BARNECH, Alfredo	Ministerio de Justicia y Derechos Humanos
BILICK, Guillermo	Nucleoeléctrica Argentina S.A.
CALAVIA, Marcelo	Instituto Argentino de Normalización y Certificación
CEBALLOS, Jorge Luis	Consultor independiente
CUSANO, Silvana	Ministerio de Agroindustria
DELGADO, José María	Sindicatura General de la Nación
DUJMOVIC, Gonzalo	Agua y Saneamientos Argentinos S.A.
ERTOLA, Donina María	Jefatura de Gabinete de Ministros
FILGUEIRA. Manuela	Ministerio de Modernización
FONT GUIDO, Mario	Instituto Argentino de Normalización y Certificación
FORTTI, María Valeria	Sindicatura General de la Nación
GALVAGNI PARDO, Nicolás	Ministerio de Agroindustria
GUERRERO, Natalia	Agua y Saneamientos Argentinos S.A.
KERNER, Ernesto	Instituto Argentino de Normalización y Certificación
MARTINO, Ricardo Alberto	Sindicatura General de la Nación
MINATTA, Eugenia	Nucleoeléctrica Argentina S.A.
MUSUMECI, Noelia Elisa	Jefatura de Gabinete de Ministros
PALAVECINO, Juan	Ministerio de Ambiente y Desarrollo Sustentable
PAZ RIVAROLA, Carolina	Sindicatura General de la Nación
PINOTTI, Joaquín	Ministerio de Agroindustria
PITUELLO, María de las Mercedes	Ministerio de Modernización
RUCCI, Ayelén	Sindicatura General de la Nación
SANTARELLI, Giselle	Ministerio de Ambiente y Desarrollo Sustentable
SCHMIDT, Samanta	Sindicatura General de la Nación
VOGELIUS, Mercedes	Sindicatura General de la Nación
YOAN, Yamila	Ministerio de Justicia y Derechos Humanos
ZEGA, Mariano	Banco Hipotecario S.A.
ZUCAL, Guillermo	Instituto Argentino de Normalización y Certificación



IRAM
Instituto Argentino
de Normalización
y Certificación

Perú 552/6
C1068AAB Buenos Aires, Argentina
Tel +54 11 4346-0600
Fax +54 11 4346-0601
Email iram-iso@iram.org.ar
www.iram.org.ar

SIGEN
Sindicatura General de la Nación
Presidencia de la Nación

Av. Corrientes 381
C1043AAD / Ciudad Autónoma de Buenos Aires
Capital Federal / República Argentina
Tel.: (54+11) 4312 8111/18
Fax: (54+11) 4317 2828
www.sigen.gob.ar