



Segunda edición
Diciembre 2019

REFERENCIAL IRAM N° 15

Sindicatura General de la Ciudad de Buenos Aires

UNIDADES DE AUDITORÍA INTERNA

Requisitos de Gestión de la Calidad,
Seguridad de la Información y Ambientales

AUTORIDADES DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

Lic. Horacio Rodríguez Larreta
Jefe de Gobierno

Lic. Diego Santilli
Vice Jefe de Gobierno

Dr. Felipe Miguel
Jefe de Gabinete de Ministros

Cdora. Mónica Freda
Síndica General de la Ciudad

IRAM

Referencial N° 15

Segunda edición
2019-12

Sindicatura General de la Ciudad de Buenos Aires

Unidades de Auditoría Interna

Requisitos de gestión de la calidad,
seguridad de la información y ambientales

Diciembre 2019

Segunda Edición

Diciembre de 2019 ©

No está permitida la reproducción de ninguna de las partes de esta publicación por cualquier medio, incluyendo fotocopiado y microfilmación, sin el permiso escrito del IRAM.

Índice

Página

0 ANTECEDENTES.....	5
1 OBJETO, CAMPO DE APLICACIÓN Y ALCANCE	6
2 DOCUMENTOS NORMATIVOS PARA CONSULTA.....	7
3 DEFINICIONES	8
4 SISTEMA DE GESTIÓN DE LA CALIDAD.....	10
4.1 REQUISITOS GENERALES	10
4.1.1 ORGANIZACIÓN, RESPONSABILIDADES Y AUTORIDADES	10
4.1.2 CONTROL Y SEGUIMIENTO DE LOS PROCESOS	11
4.2 GESTIÓN DE LA DOCUMENTACIÓN.....	11
5 RESPONSABILIDAD DE LA DIRECCIÓN	12
5.1 COMPROMISO DE LA DIRECCIÓN	12
5.1.1 POLÍTICA DE LA CALIDAD.....	13
5.1.2 OBJETIVOS DE LA CALIDAD Y PLANIFICACIÓN PARA LOGRARLOS	13
5.1.3 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	14
5.2 REVISIONES POR LA DIRECCIÓN	14
5.3 COMUNICACIÓN EXTERNA.....	15
6 GESTIÓN DE LOS RECURSOS.....	16
6.1 INFRAESTRUCTURA.....	16
6.2 RECURSOS HUMANOS	17
6.3 GESTIÓN DE INSUMOS	17
7 REALIZACIÓN DEL PRODUCTO Y PROVISIÓN DEL SERVICIO	18
7.1 PLANIFICACIÓN ANUAL	18
7.2 AUDITORÍA	18
7.2.1 PLANIFICACIÓN OPERATIVA DE LA AUDITORÍA.....	19
7.2.2 EJECUCIÓN DE LA AUDITORÍA	19
7.2.3 ELABORACIÓN Y EMISIÓN DE INFORMES	20
7.2.4 CONFECCIÓN DE PAPELES DE TRABAJO	20
7.2.5 SEGUIMIENTO DE LAS OBSERVACIONES	21
7.3 RÚBRICA	21
7.4 ACCESO A LA INFORMACIÓN PÚBLICA (LEY N°104).....	21
8 MEDICIÓN, ANÁLISIS Y MEJORA.....	22
8.1 SEGUIMIENTO Y MEDICIÓN DE LOS PROCESOS, PRODUCTOS Y SERVICIOS.....	22
8.1.1 PROCESOS	22
8.1.2 PRODUCTOS Y SERVICIOS	22
8.2 PERCEPCIÓN DE LOS ALCANZADOS	23
8.3 ANÁLISIS Y EVALUACIÓN	23
8.4 NO CONFORMIDADES Y ACCIONES CORRECTIVAS	23
9 SEGURIDAD DE LA INFORMACIÓN	24
9.1 ESTABLECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN.....	24
9.1.1 FLUJO DE LA INFORMACIÓN.....	25
9.2 IMPLEMENTACIÓN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	25

9.2.1	SEGURIDAD DE LOS RECURSOS HUMANOS.....	25
9.2.2	GESTIÓN DE ACTIVOS	25
9.2.3	CLASIFICACIÓN DE LA INFORMACIÓN	26
9.2.4	CONTROL DE ACCESO.....	26
9.2.5	SEGURIDAD FÍSICA Y AMBIENTAL	27
9.2.6	EQUIPAMIENTO.....	27
9.2.7	SEGURIDAD DE LAS OPERACIONES	27
9.2.8	GESTIÓN DE MEDIOS EXTRAÍBLES	28
9.3	OPERACIÓN Y SEGUIMIENTO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	28
9.3.1	REGISTRO Y SUPERVISIÓN.....	28
9.3.2	INFORMACIÓN DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	28
9.4	REVISIÓN, MANTENIMIENTO Y MEJORA DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	29
9.4.1	REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	29
10	GESTIÓN AMBIENTAL	29
10.1	CUIDADO DEL AMBIENTE.....	29
10.2	USO DE LOS RECURSOS	30
	Anexo A Etapas de implementación.....	31
	Anexo B (Informativo) Equipo de trabajo	32

Sindicatura General de la Ciudad de Buenos Aires

Unidades de Auditoría Interna

Requisitos de gestión de la calidad, seguridad de la información y ambientales

0 ANTECEDENTES

La Constitución de la Ciudad de Buenos Aires, en su artículo 133° establece que: *“La Sindicatura General de la Ciudad Autónoma de Buenos Aires, dependiente del Poder Ejecutivo, tiene personería jurídica propia y autarquía administrativa y financiera. Una ley establece su organización y funcionamiento. Su titular es el Síndico o Síndica General de la Ciudad Autónoma de Buenos Aires designado y removido por el Poder Ejecutivo, con jerarquía equivalente a la de ministro. La misión principal de la Sindicatura General es ser el órgano rector del Sistema de Control Interno del Gobierno de la Ciudad de Buenos Aires, en los aspectos presupuestarios, económicos, financieros, patrimoniales, normativos y de gestión, y ejerce la fiscalización del cumplimiento y aplicación de las mismas”*.

A través del precepto *“el que administra el patrimonio público debe rendir cuentas de sus actos”* la Constitución de la Ciudad de Buenos Aires estableció el modelo de control integral e integrado con que actualmente cuenta el Gobierno de la Ciudad conforme a los principios de Economía, Eficacia y Eficiencia. Este modelo comprende el control del sector público tanto interno como externo y está conformado por cinco (5) organismos, cada uno con competencias y funciones específicas: Sindicatura General, Procuración General, Auditoría General, Defensoría del Pueblo y el Ente Único Regulador de los Servicios Públicos.

La Sindicatura General, que abarca la faz interna del sistema de control anteriormente mencionado, en cumplimiento de la manda constitucional es creada mediante Decreto N° 245/GCBA/02 -que reafirma las disposiciones de la Constitución de la Ciudad- y la Ley N° 70, refiriendo ambos a la autarquía que le corresponde a este órgano de control.

La Ley N° 70 de la Ciudad de Buenos Aires, denominada “Ley de Gestión, Administración Financiera, y control de Sector Público” es la principal norma en materia de control público. La misma fija los sistemas de gestión, administración financiera y control del sector público de la Ciudad y establece la organización y funcionamiento de sus órganos.

A fin de completar el sistema de control interno que establece la Ley, se crean, a través del Decreto N° 757/GCBA/09, las Unidades de Auditoría Interna en unidades de ejecución presupuestaria del Gobierno de la Ciudad, recayendo en la Sindicatura General la tarea de ser el órgano normativo, de supervisión y coordinación técnica de éstas.

De esta manera, el sistema de control interno conformado por la Sindicatura General y las distintas Unidades de Auditoría Interna, comprende el plan de organización y todos los métodos y procedimientos que, en forma coordinada, adopta el Gobierno de la Ciudad en todas las jurisdicciones que componen la administración central y descentralizada cualquiera fuera su modalidad.

En el marco de la modernización de la gestión pública, uno de los pilares de la Sindicatura General de la Ciudad es la continua optimización de sus procesos promoviendo la excelencia en la administración. En dicho contexto desde el año 2007 se comenzó a trabajar en la implementación de su sistema de gestión de calidad, alcanzando en el año 2009 la certificación de sus procesos, conforme la norma IRAM-ISO 9001:2008. Conforme fue evolucionando el sistema de gestión de calidad de la Sindicatura General, el organismo logró adecuarse a los requisitos de la nueva norma IRAM-ISO 9001:2015. Por tal motivo en el año 2017 logró la Certificación demostrando el compromiso con el mantenimiento del sistema conforme a las auditorías externas realizadas por el IRAM; siendo el primer organismo público de la Ciudad de Buenos Aires que logró certificar todos sus procesos en forma conjunta.

Con todo ello, se asegura la incorporación y el cumplimiento de requisitos de calidad al trabajo diario los cuales optimizan la organización interna y los productos y servicios brindados. De esta manera, se genera mayor confiabilidad y transparencia en los alcanzados ya que internamente se efectúan controles y seguimiento en el cumplimiento de las misiones y funciones.

1 OBJETO, CAMPO DE APLICACIÓN Y ALCANCE

El objeto del presente referencial es propiciar la implementación de sistemas de gestión de calidad en las diferentes Unidades de Auditoría Interna de la Ciudad de Buenos Aires (UAIs), incorporando requisitos de las normas IRAM-ISO 9001:2015, IRAM-ISO 14001:2015 e IRAM-ISO/IEC 27001:2015, relativos a la Calidad, al Ambiente y a la Seguridad de la Información en cada organismo.

Tanto la Sindicatura General como las UAIs trabajan regidas por los requisitos legales y reglamentarios, los propios de cada organización y los establecidos por los alcanzados. Este desafío incorpora nuevos requisitos basados en las normas internacionales mencionadas, procurando optimizar los procesos y satisfacer las expectativas de los receptores de los productos y servicios. Esto significa un valor agregado tanto para la organización, como para el sistema de control interno y para los auditados.

Todo ello se basa en los nueve principios fundamentales siguientes:

- enfoque a los alcanzados;
- liderazgo;
- compromiso de las personas;
- enfoque a procesos;
- mejora;
- toma de decisiones basada en la evidencia;
- gestión de las relaciones;
- uso racional de los recursos y
- prácticas de seguridad de la información.

Este referencial propone tres niveles madurativos, brindando a las UAIs la posibilidad de emprender un camino escalonado hacia el establecimiento de sus sistemas de gestión de calidad basados en las Normas Internacionales, con lenguaje propio y contemplando las particularidades de las mismas.

El campo de aplicación del presente referencial son todas las UAIs de la Ciudad de Buenos Aires en el marco de la modernización de la administración pública, proponiendo como alcance sus procesos principales, de conducción y de apoyo.

Se pretende que todos los requisitos de este referencial que sean aplicables a todas UAIs sin importar su tipo y tamaño.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

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

Constitución de la Ciudad Autónoma de Buenos Aires.

Ley N° 70 Gestión, Administración Financiera y Control del Sector Público del Gobierno de la Ciudad de Buenos Aires.

Ley N° 104 de Acceso a la Información Pública (texto consolidado por Ley N° 6.017).

Decretos de creación de las Unidades de Auditoría Interna.

Leyes, decretos, resoluciones y circulares que regulen aspectos relativos a los procesos principales, de conducción y de apoyo de los organismos.

Resolución N° 177 - ASINF - 2003 Marco normativo de tecnología de información.

Resolución N° 41 - SGCBA - 18 Aprobación Manual SIGECI SGCBA-UAI.

Manual de Control Interno y Auditoría Gubernamental de la Ciudad de Buenos Aires.

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 14001:2015 - Sistemas de gestión ambiental. Requisitos con orientación para su uso.

IRAM-ISO 19011:2018 - Directrices para la auditoría de los sistemas de gestión.

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

IRAM-ISO 31000:2018 - Gestión del riesgo - Directrices.

ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary*

* Hasta tanto se estudie la norma IRAM correspondiente se toma la norma internacional mencionada como documento para consulta.

3 DEFINICIONES

Para el propósito de este documento, en lo referido a los sistemas de gestión de la calidad y de gestión de la seguridad de la información, son aplicables los términos y definiciones dados en la norma IRAM-ISO 9000:2015 e ISO/IEC 27000:2018. No obstante, se mencionan los principales términos utilizados, en su aplicación en la actividad específica de las UAI.

Alcanzado: son los destinatarios del servicio o producto. En este referencial se denomina así al “Cliente” definido en la norma IRAM-ISO 9000:2015 como “persona u organización (En el Poder Ejecutivo, la persona es un funcionario) *que podría recibir o que recibe un producto o un servicio destinado a esa persona u organización o requerido por ella*”.

Para los sistemas de gestión de la calidad implementados con los requisitos de este referencial, se consideran alcanzados a:

- La Sindicatura General de la Ciudad de Buenos Aires (SGCBA);
- La máxima autoridad del organismo;
- Los auditados.
- La ciudadanía

Auditor interno: persona que dirige y controla al más alto nivel la UAI. En este referencial cuando se exprese “alta dirección” se entiende que corresponde a la más alta autoridad de la UAI, responsable del sistema de gestión de la calidad según los requisitos establecidos.

Información: datos que poseen significado.

NOTA. La información puede ser generada por la propia UAI o provenir de los clientes y/o partes interesadas.

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

NOTA 1. La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

NOTA 2. La información documentada puede hacer referencia a:

- el sistema de gestión incluidos los procesos relacionados;
- la información generada para que la UAI opere (documentación);
- la evidencia de los resultados alcanzados (registros).

Documentos: información y el medio en que está contenida. Los documentos incluyen: los “internos” (desarrollados por la propia UAI), los “externos” (realizados por los clientes y/o derivados de normativa vigente) y los “registros” (propios y externos).

NOTA 1. El medio de soporte puede ser digital o físico, o una combinación de éstos.

NOTA 2. Con frecuencia, un conjunto de documentos, por ejemplo, procedimientos y registros, se denominan *documentación*.

Registro: documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas. Los registros pueden ser generados por la UAI o proporcionados por los clientes y/o partes interesadas.

NOTA. Los registros pueden utilizarse, por ejemplo, para formalizar/documentar la trazabilidad y para proporcionar evidencia de verificaciones, no conformidades, acciones correctivas, etc.

Especificación: documento que establece requisitos.

NOTA. Una especificación puede estar relacionada con actividades (por ejemplo, un documento de procedimiento y una especificación de proceso) o con productos (por ejemplo, requisitos para la elaboración del Informe de auditoría).

Mejora continua: actividad recurrente para mejorar el desempeño.

NOTA. El proceso de establecer objetivos y de encontrar oportunidades para la mejora es un proceso continuo mediante el uso de hallazgos de la auditoría y de conclusiones de la auditoría, del análisis de los datos, de las revisiones por la dirección u otros medios, y generalmente conduce a una acción correctiva.

No conformidad: incumplimiento de un requisito.

NOTA. El incumplimiento puede producirse respecto de un requisito normativo o del sistema de gestión de la calidad definido por la UAI. Por ejemplo, omisión de una tarea establecida en un procedimiento; incumplimiento de un plazo acordado; aplicación de una norma no vigente; etc.

Plan ciclo: período de tiempo pautado durante el cual las Unidades de Auditoría Interna efectúan sus actividades de control a las áreas del organismo o jurisdicción bajo su competencia.

NOTA. El plan ciclo no debería ser superior a un periodo de cuatro años.

Proceso: conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto o que interactúan, las cuales transforman elementos de entrada en resultados.

Los elementos de entrada de un proceso pueden ser diversos, por ejemplo: el resultado de otro proceso del sistema de gestión; la información suministrada por los clientes; los insumos entregados por proveedores; entre otros.

Que el “resultado previsto” de un proceso se denomine salida, producto o servicio depende del contexto de la referencia. Un proceso puede estar o no descrito en un procedimiento y generalmente se lo planifica y controla para que agregue valor con su operación.

NOTA. Cuando se menciona “proceso principal” se hace referencia a un proceso que realiza el producto que se entrega al alcanzado. En la UAI, los procesos principales son Planeamiento, Desarrollo de auditorías, Seguimiento de las observaciones y Otras actividades (capítulo 7 de este referencial).

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

NOTA 1. Los procedimientos pueden estar documentados o no.

NOTA 2. Cuando aparece el término “procedimiento documentado” dentro de este referencial, significa que el procedimiento sea establecido, documentado, implementado y mantenido. Un solo documento puede incluir los requisitos para uno o más procedimientos. Un requisito relativo a un procedimiento documentado puede cubrirse con más de un documento.

Papel de trabajo: todo elemento respaldatorio de las enunciaciones de la auditoría.

Requisito: necesidad o expectativa establecida, generalmente implícita u obligatoria. Los requisitos se definen, por ejemplo, a partir de lo expresado directamente por los clientes, lo determinado por la normativa o lo identificado como necesario en el sistema de gestión para cumplir con el objetivo de cada proceso.

NOTA 1. Generalmente implícita significa que es habitual o una práctica común para la organización, y las partes interesadas en que la necesidad o expectativa bajo consideración está implícita.

NOTA 2. Un requisito especificado es aquel que está establecido, por ejemplo, en información documentada.

NOTA 3. Los requisitos pueden ser generados por las diferentes partes interesadas o por la propia UAI.

Seguridad de la información: es la protección de la información de una amplia variedad de amenazas, con el objeto de asegurar la continuidad de las actividades ligadas a los procesos, minimizar los riesgos y detectar las oportunidades de mejora. Se logra con el conjunto de actividades y controles para preservar la información sensible respecto de la confidencialidad, integridad, disponibilidad y no repudio. Incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones del software y del hardware. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para garantizar que se alcancen los objetivos específicos de seguridad.

NOTA 1. Se recomienda que el análisis haga hincapié en los procesos críticos de la UAI.

NOTA 2. No repudio: grado en el que se puede probar que las acciones o eventos tuvieron lugar, de manera que las acciones o eventos no puedan ser repudiados después.

Sistema de gestión: conjuntos 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 relacionada con la calidad.

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

4 SISTEMA DE GESTIÓN DE LA CALIDAD

4.1 Requisitos generales

4.1.1 Organización, responsabilidades y autoridades

Propósito

Asegurar la descripción de las funciones y responsabilidades y su conocimiento por parte de todo el personal.

Requisitos

La UAI debe tener definido:

- a) la estructura operativa involucrada en los procesos del sistema de gestión de la calidad;
- b) las responsabilidades y cargos o funciones del personal;
- c) un responsable que, independientemente de las actividades inherentes a la auditoría, atienda las cuestiones relacionadas al cumplimiento de los requisitos del sistema de gestión de la calidad, incluyendo la seguridad de la información, para la conformidad con los requisitos de este referencial.

NOTA. Además de lo establecido en la normativa legal vigente, se debe asegurar que se encuentran definidas la totalidad de las responsabilidades y autoridades necesarias para las actividades descritas en los procesos.

4.1.2 Control y seguimiento de los procesos

Propósito

Realizar el control y seguimiento de los procesos con el fin de asegurar que la calidad de los servicios prestados y la gestión de la seguridad de la información que realiza, satisfagan las necesidades de los alcanzados.

Requisitos

La UAI debe:

- a) determinar los procesos necesarios para el sistema de gestión de la calidad y la secuencia e interacción de estos procesos;
- b) identificar los requisitos de los alcanzados;
- c) establecer los registros que sean necesarios para asegurar el control y seguimiento de cada proceso;
- d) Identificar los requerimientos de seguridad de la información asociados a los procesos de realización, su alcance y aplicabilidad;
- e) Evaluar los procesos e implementar cualquier cambio necesario para asegurar que estos procesos logren los resultados previstos;
- f) Mejorar los procesos y el sistema de gestión de calidad, ambiental y de seguridad de la información

NOTA 1. En relación con el punto a, se recomienda definir un mapa de procesos que contenga procesos de conducción, principales y de apoyo.

NOTA 2. En relación con el punto b), se recomienda definir en un documento, los requisitos de los alcanzados de acuerdo a la normativa vigente.

4.2 Gestión de la documentación

Propósito

Asegurar que:

- a) el personal de la UAI utilice documentos aprobados y en su versión vigente.
- b) los registros que respaldan las actividades del sistema se identifiquen, se conserven y archiven en forma segura, puedan ser fácilmente localizados y se encuentren disponibles para ser consultados.
- c) el personal identifique y conozca la normativa vigente que rige la actividad.

Requisitos

La UAI debe establecer e implementar un procedimiento documentado que defina los controles necesarios para:

- a) aprobar los documentos antes de su puesta en vigencia;
- b) revisar los documentos, realizando su actualización de ser necesario;
- c) asegurar que se utilicen solamente los documentos vigentes identificando su versión, registrando sus cambios y previniendo el uso indebido de documentos obsoletos;
- d) asegurar la distribución de las versiones actualizadas para que todo el personal tenga conocimiento y acceso a la documentación vigente que necesite para desarrollar sus actividades;
- e) asegurar que los documentos de origen externo determinados por la UAI como necesarios para la planificación del sistema de gestión de la calidad, se identifiquen y se controle su distribución;
- f) llevar un registro que identifique todos los documentos vigentes, incluyendo los de origen externo como, por ejemplo, la normativa vigente;
- g) llevar un registro que identifique todos los formularios vigentes;
- h) asegurar que los registros se identifiquen, se conserven y se archiven por plazos preestablecidos de manera segura y se facilite el acceso a ellos

NOTA. Además de los procedimientos documentados requeridos en este referencial, la UAI puede establecer otros procedimientos documentados.

5 RESPONSABILIDAD DE LA DIRECCIÓN

5.1 Compromiso de la dirección

Propósito

Asegurar que la dirección evidencie su compromiso con el desarrollo e implementación del sistema de gestión de la calidad.

Requisitos

La dirección debe:

- a) establecer una política de la calidad, que contempla la seguridad de la información y los aspectos ambientales;
- b) establecer los objetivos de la calidad, de la seguridad de la información y de los aspectos ambientales;
- c) establecer los procedimientos documentados y los registros requeridos por este referencial, y los documentos, incluidos los registros, que la UAI determine que son necesarios para asegurarse la eficaz planificación, operación y control de sus procesos;
- d) comunicar a todo el personal la importancia de satisfacer los requisitos de los alcanzados, así como los legales y reglamentarios;

- e) planificar y asegurar la disponibilidad de los recursos necesarios para el sistema de gestión;
- f) revisar el sistema de gestión de la calidad, incluyendo el seguimiento de los distintos proyectos;
- g) asegurar que se implementen las recomendaciones para la mejora continua;
- h) impulsar y propender el manejo adecuado de la confidencialidad, integridad y disponibilidad de la información;
- i) asegurar que se establezcan los procesos de comunicación interna apropiados dentro de la UAI considerando la eficacia del sistema de gestión de la calidad.

NOTA 1. Las recomendaciones para la mejora incluyen aquellas detectadas en la gestión de la UAI, su autoevaluación y las sugeridas por los alcanzados.

NOTA 2. Los requisitos para la seguridad de la información se presentan en el capítulo 9 de este referencial.

NOTA 3. Los procesos de comunicación pueden incluir notas, reuniones de trabajo, talleres de análisis y evaluación, entre otros.

5.1.1 Política de la calidad

Propósito

Establecer una política de la calidad relevante y pertinente para el contexto estratégico de la UAI y para el logro de sus metas y objetivos.

Requisitos

La dirección debe asegurarse que la política de la calidad:

- a) es adecuada al propósito de la UAI;
- b) incluye el compromiso de cumplir con los requisitos y la mejora continua del sistema de gestión de la calidad; de la seguridad de la información y de los aspectos ambientales;
- c) es comunicada y comprendida por todo el personal de la UAI;
- d) es revisada periódicamente para su adecuación;
- e) está disponible para las partes interesadas.

5.1.2 Objetivos de la calidad y planificación para lograrlos

Propósito

Establecer objetivos que contribuyan a la mejora continua de los procesos de la UAI y sus resultados.

Requisitos

La alta dirección debe asegurarse que los objetivos de la calidad:

- a) se establezcan en las funciones y los niveles pertinentes dentro de la UAI;

- b) incluyan objetivos específicos para la seguridad de la información y los aspectos ambientales;
- c) sean coherentes con la política de la calidad;
- d) sean medibles, específicos, alcanzables y con plazos temporales definidos;
- e) cuenten con una planificación de acciones asociadas para su cumplimiento;
- f) sean comunicados;
- g) sean actualizados.

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

5.1.3 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) establecer y mantener criterios sobre los riesgos de seguridad de la información, incluidos los criterios de aceptación de dichos riesgos;
- b) definir un proceso para el análisis, valoración, evaluación y tratamiento de los riesgos significativos de seguridad de la información, que permita obtener resultados coherentes, válidos y comparables.

NOTA. La norma ISO/IEC 27005 da criterios para la elaboración de un sistema de gestión de riesgos de seguridad de la información.

5.2 Revisiones por la dirección

Propósito

Asegurar que todas las actividades y resultados relacionados con la calidad de los servicios que presta la UAI son revisados periódicamente para poder tomar las medidas que permitan mejorarlos continuamente.

Requisitos

La dirección debe:

- a) revisar al menos una vez al año, lo siguiente:
 - el desempeño de los procesos del sistema de gestión de la calidad;
 - los resultados de la gestión de la calidad, incluyendo su relación con las políticas y objetivos, las metas y los plazos;

- las no conformidades y quejas, y la eficacia de las acciones aplicadas;
 - los cambios en la legislación y en la normativa aplicable;
 - los cambios en el entorno;
 - los resultados de los informes de percepción de los alcanzados;
 - los resultados de auditorías internas y externas;
 - el estado de avance de las medidas tomadas en las revisiones anteriores con el fin de determinar las acciones que le permitan continuar prestando sus servicios en forma confiable y según las necesidades o requerimientos de sus alcanzados;
- b) revisar en períodos de intervalo definidos según el análisis de riesgos de seguridad de la información:
- los resultados de las evaluaciones de riesgo para la seguridad de la información;
 - la retroalimentación de incidentes de seguridad de la información;
 - la eficacia de la implementación de los planes de seguridad de la información para lograr los objetivos determinados;
 - los resultados de auditorías internas y externas sobre seguridad de la información;
 - el cumplimiento de los objetivos de seguridad de la información;
 - el estado de las acciones derivadas de revisiones anteriores;
 - los cambios que sean relevantes para la gestión de la seguridad de la información;
- c) conservar registros de la información analizada y del resultado de las revisiones, donde deben quedar plasmadas las decisiones tomadas para la mejora del sistema de gestión de la calidad; la seguridad de la información y los aspectos ambientales;

Las decisiones mencionadas en c) deben contener las medidas necesarias para lograr la eficacia del producto y asegurar la cantidad de recursos necesaria para mantener el sistema de gestión de la calidad.

NOTA 1. La dirección podrá realizar más de una revisión al año, cuando por circunstancias internas o externas se considere la existencia de situaciones que impactan en el sistema de gestión de la calidad.

NOTA 2. Se recomienda solicitar y/o realizar auditorías internas periódicas al sistema de gestión definido en el referencial.

5.3 Comunicación externa

Propósito

Establecer una adecuada comunicación externa y mantener los registros necesarios para la gestión.

Requisitos

La dirección debe:

- a) determinar y establecer con acuerdo de las partes involucradas, una metodología eficaz para la comunicación;
- b) en la vinculación con la Sindicatura General:
 - mantener los registros de esa vinculación que se relacionan con los procesos de realización del producto.
- c) en la relación con la máxima autoridad del organismo y los auditados:
 - requerir la información necesaria para el armado de la planificación;
 - implementar las actividades de capacitación de acuerdo a las necesidades de la UAI;
 - asesorar sobre aspectos técnicos derivados de consultas de los alcanzados.
- d) en la relación con el ciudadano
 - detallar los medios de entrega de información y recepción de pedidos de información pública a través del enlace titular y/o suplente según normativa vigente.

NOTA. Se recomienda definir y documentar los distintos medios de comunicación externa.

6 GESTIÓN DE LOS RECURSOS

6.1 Infraestructura

Propósito

Disponer de un ambiente físico laboral acorde a los recursos humanos y materiales; y contar con los sistemas informáticos que permitan dar cumplimiento a los requerimientos de los alcanzados.

Requisitos

La UAI debe disponer de:

- a) la infraestructura física y los servicios asociados que permitan la prestación del servicio, de acuerdo con la planificación realizada;
- b) los registros de los bienes asignados a la UAI y su control de inventario correspondiente, como mínimo una vez al año.
- c) sistemas informáticos (hardware y software) apropiados para realizar la gestión del servicio de acuerdo a la normativa vigente y a la planificación realizada; y acuerdos para garantizar la adecuada confidencialidad, integridad y disponibilidad de la información gestionada por la UAI.

6.2 Recursos humanos

Propósito

Asegurar que todo el personal de la UAI sea competente para realizar las actividades previstas en los procesos y planificar la capacitación para actualizar o desarrollar esas competencias.

Propender a la toma de conciencia del personal de la UAI sobre las amenazas y vulnerabilidades que se enfrentan para salvaguardar la información sensible, respecto de su confidencialidad, integridad y disponibilidad.

Requisitos

La UAI debe:

- a) asegurar la competencia del personal que interviene en los procesos de realización del producto de acuerdo a sus funciones;
- b) determinar, evaluar y registrar las competencias del personal en base a la educación, formación, habilidades y experiencias;
- c) identificar las necesidades para la formación;
- d) planificar las actividades de formación necesarias para que el personal pueda desarrollar y actualizar las competencias requeridas para el puesto;
- e) implementar las acciones de formación planificadas y mantener registros de las actividades realizadas;
- f) desarrollar actividades que permitan sensibilizar y capacitar al personal de la UAI sobre las implicancias de los requisitos de gestión de calidad, seguridad de la información y ambiental;
- g) evaluar la eficacia de las capacitaciones y actividades de formación;
- h) conservar la información documentada apropiada como evidencia de la competencia del personal.

6.3 Gestión de Insumos

Propósito

Gestionar la disponibilidad de los bienes y servicios necesarios para el desarrollo de las actividades de la UAI, asegurando que los mismos cumplen con los requisitos de compra especificados.

Requisitos

La UAI debe:

- a) relevar las necesidades de compras para su funcionamiento eficaz;
- b) solicitar la adquisición detallando las especificaciones técnicas de los bienes y servicios específicos a adquirir;
- c) verificar que los productos cumplen con las especificaciones de la solicitud y registrar los resultados de la compra.

7 REALIZACIÓN DEL PRODUCTO Y PROVISIÓN DEL SERVICIO

7.1 Planificación anual

Propósito

Establecer la metodología para la confección del Plan Anual de cada UAI, que prevea considerar técnicas de identificación de riesgos y el plan ciclo para su realización, de acuerdo a la relevancia de las actividades, la misión y objetivos estratégicos de la UAI.

Requisitos

La UAI debe establecer e implementar un procedimiento documentado para:

- a) identificar los procesos a auditar de acuerdo a las definiciones de la SGCBA y las necesidades de control del organismo (objetivos de las autoridades / gestores de la Jurisdicción);
- b) relevar las actividades de control desarrolladas previamente (auditorías realizadas en los últimos 5 años del plan ciclo);
- c) elaborar una evaluación de riesgos documentada (riesgos de auditoría de no detección, inherentes y de control);
- d) seleccionar los proyectos de auditoría teniendo en cuenta los requisitos de la SGCBA, de la Jurisdicción y de los riesgos evaluados;
- e) elaborar una planificación que incluya:
 - 1. las áreas /programas /procesos a auditar para así establecer la importancia de cada auditoría;
 - 2. el objeto, alcance y principales procedimientos a aplicar en cada auditoría;
 - 3. el producto final - Nota o Informe - de cada auditoría;
 - 4. los recursos humanos necesarios;
- f) asegurar el cumplimiento de los plazos de presentación requeridos por la normativa para la aprobación de la planificación.

NOTA 1. La carga de la planificación se debe realizar mediante la plataforma SIGECI, de acuerdo a la normativa vigente.

NOTA 2. Se recomienda tomar como considerar el "Manual de Análisis de riesgos" establecido en el Manual de Control Interno y Auditoría Gubernamental de la Ciudad de Buenos Aires.

7.2 Auditoría

Propósito

Establecer los procedimientos para la ejecución de las auditorías, como un servicio a toda la UAI, para determinar si la misma emplea sus recursos y realiza sus actividades en busca del aumento de los niveles de eficacia, de eficiencia y de economía de los servicios prestados.

Requisitos

7.2.1 Planificación operativa de la auditoría

La UAI debe:

- a) clasificar las auditorías, a fin de seleccionar la metodología de trabajo;
- b) asignar a los responsables del proyecto de auditoría;
- c) elaborar la planificación operativa, con un plazo de antelación definido.

NOTA 1. La planificación operativa debería incluir como mínimo:

- Objeto, objetivo y alcance (vinculado a la planificación anual);
- Determinación del equipo de auditoría;
- Determinación de los procedimientos por fases; (de relevamiento, de ejecución y de elaboración de Informe);
- Plazos temporales por fase.

NOTA 2. La aplicación de la normativa que corresponde a la auditoría, puede evidenciar el cumplimiento de alguno de los requisitos de este apartado.

NOTA 3. Frecuentemente las auditorías se clasifican en imprevistas y planificadas y a su vez cada una de ellas en sustantivas y requeridas.

7.2.2 Ejecución de la auditoría

7.2.2.1 Auditoría planificada sustantiva

La UAI debe establecer e implementar un procedimiento documentado para:

- a) realizar la presentación de la auditoría;
- b) relevar la información referida a:
 1. la evaluación del Sistema de Control Interno (metodología COSO), incluyendo:
 - ambiente de control;
 - actividades de control;
 - riesgos;
 - información y comunicación;
 - supervisión y monitoreo;
 2. el análisis de riesgos
 - inherentes;
 - de control;
 - de no detección;
 3. la identificación de áreas críticas;
 4. la identificación de los puntos de control.

Deben conservarse los registros del relevamiento realizado;

- c) describir la metodología de obtención de la evidencia;
- d) realizar el análisis de la evidencia obtenida (pertinente, suficiente y competente);
- e) elaborar la matriz de hallazgos;
- f) elaborar los papeles de trabajo.

7.2.2.2 Auditoría imprevista sustantiva

Los requisitos son los mismos que los indicados en el apartado 7.2.2.1, con excepción de lo indicado en 7.2.2.1.a), porque esta auditoría se hace a requerimiento del auditado, de la máxima autoridad del organismo o de la Sindicatura General. Se debe informar el inicio de la misma a la SGCBA conforme a la normativa vigente.

7.2.2.3 Auditoría planificada requerida

La UAI debe:

- a) notificar al auditado y relevar la información;
- b) obtener la evidencia, analizar la misma y elaborar la matriz de hallazgos, en caso de corresponder, de acuerdo a la normativa vigente;
- c) elaborar el proyecto de Reporte de Resultados (Informe o Nota en caso de corresponder);
- d) identificar los riesgos.

7.2.2.4 Auditoría imprevista requerida

Estas auditorías se rigen por la normativa vigente sin adicionar otros requisitos.

NOTA. Cuando se menciona "auditoría requerida", se hace referencia al proceso que realiza la UAI para emitir un producto de frecuencia periódica emitido en cumplimiento de una normativa vigente.

7.2.3 Elaboración y emisión de Informes

La UAI debe:

- a) elaborar el proyecto de Informe para opinión del auditado, en caso de existir observaciones;
- b) realizar el análisis del descargo de la opinión del auditado, en caso de existir;
- c) confeccionar el Informe final;
- d) emitir el Informe final;

7.2.4 Confección de papeles de trabajo

La UAI debe:

- a) determinar los papeles de trabajo en cada etapa;

- b) mantener los registros de cada etapa del proceso de auditoría.

7.2.5 Seguimiento de las observaciones

La UAI debe:

- a) verificar y clasificar las observaciones para su seguimiento;
- b) constatar que las observaciones regularizadas tengan su respaldo en un nuevo informe o en nuevas evidencias válidas y suficientes;
- c) verificar que las medidas correctivas implementadas por los auditados estén evidenciadas mediante documentación válida y suficiente;
- d) constatar que los nuevos estados de las observaciones hayan sido debidamente actualizados;
- e) verificar que se hayan ejecutado las actividades que permiten medir la eficacia y el grado de implementación de las acciones encaradas en la corrección de las observaciones;
- f) mantener los registros de cada etapa del proceso.

7.3 Rúbrica

Propósito

Establecer la metodología para la rúbrica de libros y controlar las acciones desarrolladas.

Requisitos

La UAI debe establecer e implementar un procedimiento documentado para:

- a) recibir las solicitudes formales por la máxima autoridad de la dependencia;
- b) analizar la procedencia y pertinencia del libro y registrar la recepción;
- c) establecer las acciones para la rúbrica;
- d) asegurar el seguimiento del plazo para realizar la rúbrica;
- e) comunicar formalmente que el libro está listo para ser retirado;
- f) registrar la entrega del libro.

7.4 Acceso a la información pública (Ley N°104)

Propósito

Establecer la metodología para los requerimientos referidos a las solicitudes de información pública y controlar las acciones desarrolladas.

Requisitos

La UAI debe establecer e implementar un procedimiento documentado para:

- a) recibir las solicitudes de información pública por la máxima autoridad de la dependencia;
- b) analizar la procedencia y pertinencia de la misma y registrar dicha acción;
- c) asegurar el seguimiento de dicha solicitud durante el proceso;
- d) comunicar y registrar la respuesta a través de los canales formales;
- e) mantener los registros de cada etapa del proceso.

8 MEDICIÓN, ANÁLISIS Y MEJORA

8.1 Seguimiento y medición de los procesos, productos y servicios.

Propósito

Realizar un seguimiento de los procesos, productos y servicios por intermedio de indicadores que permitan medir su eficacia.

Requisitos

8.1.1 Procesos

Para cada proceso de realización del producto y prestación de servicio (capítulo 7) la UAI debe:

- a) definir los indicadores que utiliza;
- b) definir la metodología de medición, seguimiento de los indicadores, análisis y evaluación de los resultados;
- c) conservar la información documentada apropiada como evidencia de los resultados.

8.1.2 Productos y servicios

Para cada producto y servicio, la UAI debe:

- a) realizar el seguimiento y medir las características del producto y servicio para verificar que se cumplen sus requisitos;
- b) mantener los registros de la conformidad de la aceptación.

NOTA 1. Producto incluye los resultados de los procesos / subprocesos del capítulo 7.

NOTA 2. La conformidad de la aceptación del producto y servicio debe evidenciarse, entre otros registros, por ejemplo, con una firma, o con un listado de verificación de cumplimiento de requisitos.

8.2 Percepción de los alcanzados

Propósito

Conocer la opinión de los alcanzados respecto de las actividades desarrolladas por la UAI, para encontrar oportunidades de mejora en la prestación del servicio.

Requisitos

La UAI debe realizar el seguimiento de las percepciones de los alcanzados para medir el grado en que se cumplen sus necesidades y expectativas. La UAI debe determinar los métodos para obtener, realizar el seguimiento y revisar esta información. Estos métodos deben incluir la planificación de los elementos de entrada, la obtención de la información y su utilización en la identificación de acciones para la mejora continua.

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

8.3 Análisis y evaluación

Propósito

Evaluar la eficacia del sistema de gestión y obtener información del seguimiento y la medición.

Requisitos

La UAI debe analizar y evaluar los datos y la información apropiados que surgen por el seguimiento y la medición.

Los resultados del análisis deben utilizarse para evaluar:

- a) la conformidad de los productos y servicios;
- b) el grado de satisfacción de los alcanzados;
- c) el desempeño y la eficacia del sistema de gestión de la calidad;
- d) si lo planificado se ha implementado de forma eficaz;
- e) la eficacia de las acciones tomadas para abordar los riesgos y oportunidades;
- f) la necesidad de mejoras en el sistema de gestión de la calidad.

NOTA. Evidenciar los riesgos y oportunidades como mínimo de los procesos del capítulo 7.

8.4 No conformidades y acciones correctivas

Propósito

Registrar las no conformidades, corregirlas, analizar las causas que las produjeron e implementar las acciones para evitar su reiteración.

Requisitos

La UAI debe establecer e implementar un procedimiento documentado para:

- a) reaccionar ante una no conformidad y cuando sea aplicable;
 - tomar acciones para controlarla y corregirla;
 - hacer frente a las consecuencias;
- b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:
 - la revisión y el análisis de la no conformidad;
 - la determinación de las causas de la no conformidad;
 - la determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir;
- c) implementar cualquier acción necesaria;
- d) revisar la eficacia de cualquier acción correctiva tomada;
- e) si fuera necesario, actualizar los riesgos y oportunidades determinados durante la planificación; y
- f) si fuera necesario, hacer cambios al sistema de gestión de la calidad.

La UAI debe conservar información documentada como evidencia de la naturaleza de las no conformidades y cualquier acción tomada posteriormente y de los resultados de cualquier acción correctiva.

9 SEGURIDAD DE LA INFORMACIÓN

9.1 Establecimiento de la seguridad de la información

Propósito

Determinar los procesos necesarios, los roles y las responsabilidades para alcanzar una adecuada seguridad de la información frente a las amenazas a la confidencialidad, la integridad y la disponibilidad de la información sensible.

Requisitos

A partir del análisis de riesgos, la UAI debe:

- a) contar con los registros actualizados sobre la planificación de los objetivos de control de seguridad de la información en concordancia con la política de la calidad;
- b) asegurar que se han considerado las obligaciones legales, reglamentarias o contractuales relacionadas con la seguridad de la información;
- c) asegurar la protección de los registros;

- d) asegurar que se respeta la privacidad y protección de datos personales;
- e) definir un responsable de seguridad de la información;
- f) verificar las obligaciones contractuales de los proveedores de seguridad de la información, si los hubiera.

NOTA. Se recomienda formalizar la prestación del servicio mediante un acuerdo de prestación de servicio.

9.1.1 Flujo de la información

Propósito

Gestionar la seguridad de la información dentro de la organización.

Requisitos

La UAI debe definir los criterios para la elaboración de los acuerdos de confidencialidad o de no divulgación y el registro individual de cada uno de los acuerdos suscriptos, tanto con personal interno como externo que afecten a la operación.

NOTA. Se considera personal externo a proveedores, contratados, prestadores de servicio, etc.

9.2 Implementación de la gestión de seguridad de la información

9.2.1 Seguridad de los recursos humanos

Propósito

Asegurar que el personal comprenda sus responsabilidades, para reducir el riesgo de hurto, fraude o el mal uso de las instalaciones.

Requisitos

La UAI debe:

- a) establecer e implementar un procedimiento documentado para definir la gestión de la seguridad de los recursos humanos. Este documento debe contemplar las situaciones antes, durante y cuando se efectúe un cambio en los recursos humanos o una cancelación de sus actividades;
- b) tener un registro de las actividades de sensibilización, capacitación y concientización sobre los riesgos de seguridad de la información relacionada con los recursos humanos.

NOTA 1. Considerar estos requisitos en la definición de competencias (6.2).

NOTA 2. En relación a la seguridad de recursos humanos en situaciones anteriores a la relación laboral, podemos citar como ejemplo el pedido de antecedentes penales.

9.2.2 Gestión de activos

Propósito

Identificar los activos (información y su soporte) de la organización y definir las responsabilidades para su protección.

Requisito

La UAI debe tener un registro del inventario de activos de la información sensible con la nominación del propietario de dichos activos actualizado anualmente.

NOTA. Se considera propietario al responsable de la existencia del activo de información, más allá de su utilización.

9.2.3 Clasificación de la información

Propósito

Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

Requisitos

La dirección de la UAI debe:

- a) definir un criterio de clasificación de la información según su importancia respecto de la confidencialidad, la integridad y la disponibilidad;
- b) tener evidencia de la clasificación de la información;
- c) definir, implementar y registrar las responsabilidades de la funcionalidad correcta de los activos de información al momento de clasificarla;
- d) en base al análisis de riesgo de los activos (tanto la información como su soporte) elaborar e implementar planes y medidas que garanticen la continuidad de los procesos críticos, a fin de asegurar la disponibilidad, confidencialidad e integridad de la información frente a la materialización de una amenaza.

NOTA. Coordinar dichos planes y medidas con las actividades de control que realizan los proveedores de seguridad de la información.

9.2.4 Control de acceso

Propósito

Limitar el acceso a la información y a las instalaciones de procesamiento de información.

Requisitos

La UAI debe:

- a) limitar el acceso a los sistemas y servicios únicamente a los usuarios autorizados;
- b) evidenciar el control de accesos por medio de:
 - gestión de privilegios;
 - registro de usuarios;
 - registro de inhabilitación;
 - política de gestión de contraseñas.

NOTA. De ser necesario la UAI, deberá contar con una persona que conozca sobre estas medidas y resulte de nexo con las áreas que administran los servidores de cada repartición.

9.2.5 Seguridad física y ambiental

Propósito

Evitar el acceso físico no autorizado, daños e interferencia a la información y a las instalaciones de procesamiento de información de la UAI.

Requisitos

La UAI debe definir las áreas seguras para el resguardo de la información confidencial.

NOTA. La UAI debería tener definida la seguridad física perimetral y los controles a realizar de entrada física.

9.2.6 Equipamiento

Propósito

Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la UAI.

Requisitos

La UAI debe:

- a) definir el emplazamiento y protección del equipamiento y servicios de apoyo que afecten a la información sensible, según el análisis de riesgo correspondiente;
- b) establecer criterios para implementar prácticas de escritorio y pantalla limpia;
- c) definir la metodología para resguardar la información o eliminación segura, durante el proceso de eliminación de los activos o la reutilización de los equipos;
- d) definir e implementar las medidas de seguridad sobre la utilización de equipos y de activos, fuera de las instalaciones;
- e) establecer los criterios de mantenimiento de equipos que permitan la normal operación de la unidad.

9.2.7 Seguridad de las operaciones

Propósito

Tener conocimiento del funcionamiento correcto y seguro de las instalaciones donde se procese cualquier tipo de información, así como de la protección necesaria contra el software malicioso y evitar la pérdida de datos.

Requisitos

La UAI debe:

- a) contar con un registro de los controles implementados contra el software malicioso;
- b) asegurar la correcta realización de las copias de seguridad ("Backup").

9.2.8 Gestión de medios extraíbles

Propósito

Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación portátiles.

Requisitos

Los medios de comunicación extraíbles que contengan información sensible deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte;

Cuando ya no sea necesaria su utilización deben disponerse de manera segura.

9.3 Operación y seguimiento de la gestión de seguridad de la información

9.3.1 Registro y Supervisión

Propósito

Registrar incidentes y hallazgos de seguridad de la información y generar evidencia.

Requisitos

La UAI debe

- a) mantener el registro de los incidentes y hallazgos de seguridad de la información;
- b) revisar regularmente los registros;
- c) tener en cuenta el análisis de riesgo previamente realizado al momento de la identificación de incidentes y hallazgos de seguridad de la información.

9.3.2 Información de gestión de incidentes de seguridad de la información

Propósito

Garantizar y comunicar un enfoque coherente y eficaz para la gestión de hallazgos de seguridad de la información.

Requisitos

La UAI debe:

- a) definir un procedimiento para la gestión de incidentes y hallazgos de la seguridad de la información;
- b) contar con registros del tratamiento de los hallazgos de seguridad de la información;
- c) evaluar la eficacia de las medidas adoptadas.

9.4 Revisión, mantenimiento y mejora de la gestión de seguridad de la información

9.4.1 Revisión de la seguridad de la información

Propósito

Garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y los procedimientos de la organización.

Requisitos

La UAI debe:

- a) revisar en forma independiente, el cumplimiento de: los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información, al menos una vez al año (o cuando ocurran cambios significativos);
- b) definir los métodos y responsabilidades para su verificación;
- c) informar los resultados a la dirección de la UAI de manera fehaciente;
- d) mejorar continuamente la pertinencia, adecuación y eficacia de los objetivos de seguridad de la información.

10 GESTIÓN AMBIENTAL

10.1 Cuidado del ambiente

Propósito

Adoptar el compromiso, por parte de la alta dirección de la UAI, con respecto a la implementación de los requisitos de cuidado del ambiente.

Requisitos

La UAI debe:

- a) asegurar que se establezca en la política de calidad y en los objetivos, el compromiso con el cuidado del ambiente;
- b) comunicar la importancia de la gestión ambiental eficaz;
- c) asegurar que se implementen gestiones y mejoren los compromisos ambientales asumidos;
- d) asegurar que las personas que trabajan dentro de la UAI tomen conciencia del compromiso con el cuidado del ambiente en la política ambiental establecida;

- e) asegurar que las personas que trabajan dentro de la UAI tomen conocimiento sobre los Objetivos de Desarrollo Sostenible 2030 de la Naciones Unidas y el impacto de la gestión de la UAI en los mismos.

NOTA. Para asegurar el conocimiento sobre la Agenda de desarrollo sostenible 2030 de Naciones Unidas, se recomienda seguir el link <https://www.un.org/sustainabledevelopment/es/takeaction/>

10.2 Uso de los recursos

Propósito

Adoptar acciones tendientes al uso racional de recursos, propiciando en todo el personal la minimización del consumo al máximo posible.

Requisitos

La UAI debe:

- a) propiciar el uso racional del agua, la energía eléctrica, el gas y demás recursos públicos;
- b) propiciar uso racional del papel priorizando la no impresión;
- c) no superar el tiempo de guarda de archivos en papel establecido por la normativa vigente;
- d) configurar los equipos de impresión en la opción “económica”;
- e) gestionar las bajas de los bienes en desuso de acuerdo a los procedimientos determinados por la normativa vigente;
- f) priorizar la adquisición y/o compra consiente de productos, por ejemplo: mínima cantidad, reutilizables, son plásticos, a proveedores locales, productos biodegradables, etc.;
- g) disponer de recipientes para la separación de los residuos en origen;
- h) reducir la generación de residuos.

NOTA. La gestión del uso racional de la energía eléctrica puede incluir actividades como: mantener equipos de aire acondicionado a 24 °C; definir que el personal de cada oficina debe apagar los equipos cuando no se utilizan, utilizar lámparas de bajo consumo, entre otras.

Anexo A

Etapas de implementación

Las Unidades de Auditoría Interna (UAIs) que así lo deseen, podrán implementar los requisitos en tres etapas evolutivas, de acuerdo a la distribución de requisitos que se presenta a continuación:

Capítulo	Requisitos	Requisitos de implementación para cada Etapa		
		I	II	III
4 SISTEMA DE GESTIÓN DE LA CALIDAD	4.1 Requisitos generales	X		
	4.2 Gestión de la documentación	X		
5 RESPONSABILIDAD DE LA DIRECCIÓN	5.1 Compromiso de la dirección	X		
	5.2 Revisiones por la dirección			X
	5.3 Comunicación externa	X		
6 GESTIÓN DE LOS RECURSOS	6.1 Infraestructura	X		
	6.2 Recursos humanos		X	
	6.3 Gestión de insumos	X		
7 REALIZACIÓN DEL PRODUCTO Y PROVISIÓN DEL SERVICIO	7.1 Planificación anual	X		
	7.2 Auditoría		X	
	7.3 Rúbrica	X		
	7.4 Acceso a la información pública (Ley N°104)		X	
8 MEDICIÓN, ANÁLISIS Y MEJORA	8.1 Seguimiento y medición de los procesos, productos y servicios		X	
	8.2 Percepción de los alcanzados			X
	8.3 Análisis y evaluación			X
	8.4 No conformidades y acciones correctivas		X	
9 SEGURIDAD DE LA INFORMACIÓN	9.1 Establecimiento de la seguridad de la información		X	
	9.2 Implementación de la gestión de seguridad de la información		X	
	9.3 Operación y seguimiento de la gestión de la seguridad de la información			X
	9.4 Revisión, mantenimiento y mejora de la gestión de seguridad de la información			X
10 GESTIÓN AMBIENTAL	10.1 Cuidado del ambiente		X	
	10.2 Uso de los recursos		X	

Anexo B

(Informativo)

Equipo de trabajo

En el desarrollo de este referencial participaron las personas siguientes:

LAPORTE	Juan Pablo	SINDICATURA GENERAL DE LA CIUDAD DE BUENOS AIRES (SGCBA)
YAUNACE	Claudia	SINDICATURA GENERAL DE LA CIUDAD DE BUENOS AIRES (SGCBA)
LOCOCO	Luciano	SINDICATURA GENERAL DE LA CIUDAD DE BUENOS AIRES (SGCBA)
ROMERO	María Virginia	SINDICATURA GENERAL DE LA CIUDAD DE BUENOS AIRES (SGCBA)
GARCIA	Gabriela	SINDICATURA GENERAL DE LA CIUDAD DE BUENOS AIRES (SGCBA)
SUZUKI	Silvina	IRAM



**Instituto Argentino
de Normalización
y Certificación**



**Buenos
Aires
Ciudad**



**Sindicatura General
de la Ciudad de Buenos Aires**

Perú 552/6
C1068AAB / Buenos Aires
República Argentina
Tel/Fax +54 11 4346 0600
www.iram.org.ar

Av. Martín García 346, 6to piso
C1165ABP / Buenos Aires
República Argentina
Tel/Fax +54 11 5030-9100
www.buenosaires.gob.ar/sindicatura