A.L.E.A.
ASOCIACIÓN DE LOTERÍAS, QUINIELAS Y CASINOS ESTATALES DE ARGENTINA

IRAM
Instituto Argentino
de Normalización
y Certificación

REFERENCIAL IRAM N° 19
SEGUNDA EDICIÓN 2022-04

Organismos públicos reguladores
y administradores de juegos de azar
y organizaciones privadas autorizadas para la
explotación del juego de azar

REQUISITOS
DE GESTIÓN DE LA CALIDAD

Segunda Edición
Abril de 2022 ©

Índice

Organismos públicos reguladores y administradores de juegos de azar y organizaciones privadas autorizadas para la explotación del juego de azar

Requisitos de Gestión de la Calidad

0 ANTECEDENTES

Los Organismos que conforman la Asociación de Loterías Estatales de Argentina (ALEA) asumen el compromiso con la Responsabilidad Social. Este compromiso se manifiesta, especialmente, consolidando la transparencia, la eficacia y la idoneidad de sus procesos y la gestión en general de sus organizaciones, toda vez que los recursos obtenidos, a través de la explotación y administración de los juegos de azar, tienen como destino fortalecer los recursos del Estado para políticas sociales.

Los Organismos Reguladores miembros de ALEA tienen, en algunos casos, la experiencia de certificación de sus procesos bajo distintas normas de gestión; iniciativas que en cada una de ellas han permitido consolidar procesos de mejora organizacional continua, estableciendo así políticas públicas sólidas que fortalecen sus capacidades.

Teniendo en cuenta las diversas experiencias, en el año 2017, ALEA tomó la decisión de desarrollar, en conjunto con el Instituto Argentino de Normalización y Certificación (IRAM), un Referencial específico para la gestión de la calidad que responda a los procesos particulares de la actividad y que sea representativo del sector, consolidando así un marco de referencia para todos sus actores.

Este Referencial denominado “Organismos públicos reguladores y administradores de juegos de azar y organizaciones privadas autorizadas para la explotación del juego de azar - Requisitos de gestión de la calidad”, publicado en mayo de 2018, se constituyó como una herramienta adecuada para alcanzar los fines mencionados.

Con el pasar del tiempo y en base a la experiencia adquirida por la Unidad Coordinadora de Gestión de Calidad de ALEA, surge la necesidad de una revisión general que acompañe la evolución de los sistemas de gestión y de la tecnología.

Los cambios principales incluyen:

- Inclusión de nuevos Términos y definiciones (Capítulo 3);
- actualización en Liderazgo y compromiso (5.1);
- incorporación del rol de Responsable del SGC (5.3);
- separación de Responsabilidad social respecto de Juego responsable (5.4 y 5.5);
- incorporación de Prevención de lavado de activos y financiación del terrorismo (5.6);
- actualización de Juego ilegal o clandestino (5.7);
- traslado de Comunicación al capítulo 5 y actualización de sus requisitos (5.8);
- actualización de Objetivos de la calidad (6.3);

- revisión y actualización del capítulo de Fiscalización (8.2);
- modificaciones en Gestión de juegos de casino y salas de juegos electrónicos (8.4);
- incorporación de Gestión, control y fiscalización de juego online (8.8);
- revisión general de las Etapas de implementación (Anexo B);
- actualización de Formación de las personas (Anexo C);
- adecuación del Mapa de Procesos (Anexo D);
- incorporación de Ciberseguridad y actualización en Seguridad de la información en el Anexo F.

El IRAM, en el marco del Decreto N°1474/94 del Poder Ejecutivo Nacional, es designado como el organismo de normalización de la Argentina. Además de sus actividades a nivel nacional, representa a la Argentina en los foros sobre normalización, regionales: COPANT, Comisión Panamericana de Normas Técnicas, y AMN, Asociación MERCOSUR de Normalización; e internacionales: ISO, International Organization for Standardization y, a través del CEA, Comité Electrotécnico Argentino en la International Electrotechnical Commission (IEC).

La Asociación de Loterías Estatales de Argentina (ALEA) nuclea a todos los organismos que regulan y controlan la actividad lúdica en el ámbito del territorio nacional. Siendo una entidad sin fines de lucro, tiene la misión estratégica de posicionarse como ente asesor, de referencia y de capacitación de los entes reguladores de Argentina en materia de control, fiscalización, modernización y optimización de recursos.

La integración nacional con sentido federal, así como la consolidación de principios éticos y de responsabilidad social, caracterizan a la asociación y a sus miembros bajo un denominador común: la recaudación de fondos para la acción social.

Más de 40 años de trayectoria y coherencia avalan la permanencia de la entidad.
Seis Comisiones de Asesoramiento tratan asuntos Jurídicos, Administrativos, de Comercialización, de Capacitación, Informáticos e Internacionales. Tres Unidades Coordinadoras trabajan sobre Prevención de Lavado de activos, Responsabilidad Social y Gestión de la Calidad, y dos áreas completan la estructura actual de ALEA: Estadística y Comunicación.

OBJETIVO GENERAL

Promover la cultura de la calidad, la innovación tecnológica y la mejora organizacional continua en las organizaciones del sector de juegos de azar, impulsando la consolidación de un modelo de desarrollo responsable y sustentable a mediano y largo plazo, propiciando, asimismo, la adopción de medidas efectivas de protección de los grupos vulnerables de nuestra población y la generación de recursos destinados al bienestar de nuestra sociedad.

OBJETIVOS ESPECIFICOS

- Incorporar a la estrategia de ALEA la promoción de la implementación y la certificación de la gestión de la calidad específica para el sector.
- Posicionar a ALEA como organismo de implementación y capacitación de procesos de calidad en organismos públicos y privados de gestión de juegos de azar, integrando el conocimiento y experiencia adquiridos por los funcionarios de los Organismos miembros de la Asociación.
- Diseñar un Referencial para la gestión de la calidad aplicable para el sector de juegos de azar de nuestro país (entre ALEA y el IRAM).

¿Qué son los referenciales de calidad?

Son documentos alineados con la norma IRAM-ISO 9001, u otra norma internacional de referencia, realizados a pedido de un organismo público u Organización representativa de la sociedad civil con el objetivo de servir de instrumento de apoyo a una política pública y cuyo alcance son todos los procesos principales o sustantivos, los de dirección y los de apoyo necesarios que gestiona la Organización o una de sus áreas.

Los requisitos establecidos en los referenciales son los necesarios para mantener bajo control los procesos principales de la Organización una vez certificada según el referencial específico y para que la Organización que así lo desee, con un esfuerzo adicional certifique la norma IRAM-ISO 9001 o la norma ISO de referencia que corresponda.

Uno de los valores agregados de los referenciales es que facilitan la incorporación de la cultura de la calidad en la Organización haciendo énfasis en la mejora continua como estrategia sistemática de desarrollo y en consecuencia promueven el uso de la metodología conocida como “PHVA” Planificar-Hacer-Verificar-Actuar, el conocimiento y aplicación de los principios de la calidad. Esta metodología cíclica es de utilidad ante la detección de situaciones no deseadas relativas al desempeño de la Organización y conlleva a tomar acciones correctivas para evitar su repetición y lograr los objetivos esperados.

Los referenciales adoptan el Enfoque Basado en Procesos, en donde, el resultado deseado se alcanza más eficientemente cuando las actividades y los recursos se gestionan como un proceso. Esto es particularmente importante en las organizaciones públicas muy acostumbradas a la lógica funcional/departamental.

Los requisitos establecidos en los referenciales y en este en particular apuntan a crear la base para la articulación sistémica y la generación de un sistema de gestión de la calidad consistente con lo establecido en la norma IRAM-ISO 9001 y son aplicables a todas las organizaciones del mismo tipo independientemente de su tamaño. Permite, a su vez, desarrollar una herramienta para gestionar procesos específicos que en las distintas estructuras y niveles se repiten o son similares, y modelizar soluciones “a medida”, permitiendo el aprovechamiento general de las mejores experiencias.

Esta experiencia es replicable en cuanto aprovecha el conocimiento y lo traslada al diseño ordenando además las futuras implementaciones.

Los referenciales permiten establecer requisitos adicionales alineados con otras normas internacionales como requisitos ambientales y de seguridad de la información.

Los referenciales IRAM prevén dos niveles: uno vinculado al alcance de los definidos como procesos básicos, que constituye el propio referencial y otro, vinculado a alcanzar los requisitos de la norma IRAM-ISO 9001.

Algunos de los referenciales, como este, proponen la implementación según un esquema evolutivo de requisitos crecientes, en tres etapas. Esta metodología permite una implementación más amigable y madurativa en la Organización, especialmente en aquellas con menos experiencia en sistemas de gestión de la calidad ya que deben recorrer un camino con metas más cortas y menos requisitos en cada auditoría.

Para obtener la certificación del referencial la Organización puede elegir auditar todos los requisitos de este (los planteados en cada una de las tres etapas) en una sola auditoría de certificación y dependerá, entre otras, de la cantidad de personal involucrado en los procesos. La certificación

implica ciclos de tres años con auditorías anuales de seguimiento. Si eligen el camino evolutivo tendrán una auditoría para cada una de las etapas, entregándose para las dos primeras un informe de auditoría de estado de cumplimiento de la etapa y la certificación se otorga cuando se cumplen todos los requisitos establecidos.

Es de destacar el concepto de construcción colectiva de cada referencial entre los equipos de expertos del IRAM y de los organismos solicitantes, así como de las partes interesadas desde la identificación de todos los procesos principales, los de dirección y apoyo, los requisitos necesarios, la definición de los alcanzados en cada etapa y finalmente su validación con los destinatarios.

1 OBJETO Y CAMPO DE APLICACIÓN

Este Referencial define los requisitos que deben cumplir los Organismos públicos reguladores y administradores de juegos de azar y organizaciones privadas autorizadas para la explotación del juego de azar para establecer, implementar, mantener y mejorar un sistema de gestión de la calidad de acuerdo con los requisitos de este Referencial.

NOTA. Ver 4.3 Determinación del alcance del sistema de gestión de la calidad.

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.

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

- IRAM-ISO 9000 - Sistemas de gestión de la calidad. Fundamentos y vocabulario
- IRAM-ISO 9001 - Sistemas de gestión de la calidad. Requisitos
- IRAM-ISO-IEC 27001 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos
- IRAM-ISO 31000 - Gestión del riesgo. Principios y guías
- IRAM-ISO 10002 - Gestión de la calidad - Satisfacción del cliente. Directrices para el tratamiento de las quejas en las organizaciones
- IRAM-ISO 26000 - Guía de responsabilidad social

Existiendo legislación pertinente en cada provincia se indica a continuación de manera no taxativa la legislación nacional que alcanza a este Referencial. En el caso de existir en el futuro, aplicará toda norma modificatoria o complementaria que se sancione al respecto:

- Ley N° 20630 Gravamen de emergencia a los premios ganados en juegos de sorteo.

- Ley N°25246 y sus modificatorias. “Encubrimiento y Lavado de Activos de Origen Delictivo”
- Ley N°25326 Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.
- Resoluciones UIF (Unidad de Información Financiera) vigentes en la materia
- AFIP (Ley de impuesto a las ganancias N° 20268 y modificatorias); Resolución General de AFIP N° 3510

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 IRAM-ISO 9000.

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 organizaciones.

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

Hold: (porcentaje de retención) Indicador que señala el porcentaje de retención o ganancia del casino de juego y que resulta de dividir el *net win* por el *drop* (recaudación). Hold teórico: Porcentaje teórico de ganancia del casino y que es el complemento del porcentaje de devolución al jugador(a). Por ejemplo, si el porcentaje con que se programó la máquina para devolución al jugador es de 89,5 %, entonces el % de hold teórico es de 10,5 %

NOTA 1. *Net Win* es el beneficio final de las máquinas automáticas de apuestas, se obtiene de la formula básica de ingresos a la máquina (billetes, TITO, etc.) menos los premios pagados.

NOTA 2. *Drop* es el término utilizado para hacer referencia a los “ingresos” o “recaudación”, ya sea a las máquinas automáticas de apuestas y/o a los juegos vivos.

Cliente: persona que podría recibir o que recibe un producto o un servicio destinado a esa persona o requerido por ella

NOTA. Se recomienda ver la definición de partes interesadas.

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados

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

NOTA. En este Referencial cuando se exprese “Dirección” se entiende que corresponde a la más alta autoridad de la Organización, independientemente de su denominación en cada Organización (por ejemplo, Presidente, Gerente general, Director ejecutivo, Directorio, etc.).

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad o usuario autorizado

Dispositivos de juegos electrónicos: referencia a máquinas automáticas de apuestas (como un todo) o bien a los distintos componentes de esta que son necesarios para su funcionamiento

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

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

Integridad: Propiedad de la información relativa a su exactitud y completitud

Islas de progresivos: grupo de máquinas, con sistema de premios especiales, que pueden ser acumulativos o no

Juego bancado: aquel en donde el Organismo Administrador fija las reglas y toma la apuesta, la cual tiene determinado, con anterioridad, cuál es el premio que va a pagar, ya sea como valor absoluto o en función del importe apostado y la tasa de probabilidad de resultar ganador. El premio es totalmente independiente de la recaudación por la venta de apuestas, lo que lo coloca en riesgo de posibles quebrantos como de ganancias extras que solo se compensan en la reiterada repetición del fenómeno

Juego ilegal o clandestino: cualquier modalidad o sistema de captación de juegos de azar que no cuenta con la autorización pertinente emanada de la autoridad jurisdiccional competente

Juego poceado: aquel en que los premios se conforman en función de la recaudación que, considerada como una torta, destina una porción a premios y hace desaparecer el factor riesgo, siendo entonces la utilidad solo en función del volumen de ventas logrado

Máquinas automáticas de apuestas: aquel juego de azar automatizado de características de resultado programado, poceado o probabilístico, y a todos aquellos juegos que, mediante un equipo o máquina electromecánica y/o electrónica y/o un programa informático específico, individual y descentralizado, posibiliten cumplir las siguientes funciones genéricas: a) Captación de apuestas. b) Elección de opciones, sea para designar el tipo de juego, variante ante resultados parciales, cancelación y finalización. c) Visualización del desarrollo y resolución del juego. d) Generación autónoma de resultados. e) Acreditación de premios, débitos de apuestas perdidas y exhibición del estado de cuentas del usuario apostador. f) Conexión al sistema de control en línea. g) Mecanismo de operación y pago de premios mediante tarjetas magnéticas, créditos, billetes y/o moneda de curso legal. h) Sistema de validación de premios pagados en forma manual fuera de la máquina

Mejora: actividad para mejorar el desempeño

Mejora continua: actividad recurrente para mejorar el desempeño

No conformidad: incumplimiento de un requisito

Objetivo: resultado a lograr

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

NOTA. Partes interesadas pueden ser ciudadanos, beneficiarios, proveedores, empleados, organismos gubernamentales, sindicatos, entre otros.

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: preservación de la confidencialidad, la integridad y la disponibilidad de la información

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 (SGC): parte de un sistema de gestión relacionado con la calidad

Sistema TITO: Sistema *Ticket in* / *Ticket out*: La máquina genera un ticket como pago de premio (*Ticket out*), que se puede apostar en esa u otra máquina (*Ticket in*), o bien hacerlo efectivo en caja o un kiosco

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

4 SISTEMA DE GESTIÓN DE LA CALIDAD

4.1 Comprensión de la Organización y de su contexto

Propósito

Entender la Organización desde el punto de vista de los grupos de interés incluyendo al personal interno de la Organización con el fin de asegurar que los servicios prestados cumplen con las necesidades de las partes interesadas.

Requisitos

La Organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica, y que afectan a su capacidad para lograr los resultados previstos de su SGC.

La Organización debe definir su orientación estratégica a mediano y largo plazo y sus objetivos estratégicos relacionados. Esta orientación y objetivos deben ser documentados y comunicados a las partes interesadas pertinentes.

La Organización debe realizar el seguimiento y la revisión de esta información por lo menos una vez al año.

NOTA. Algunas herramientas posibles de utilizar para esta determinación son las conocidas como análisis FODA, CAME, PESTEL, árbol de problemas y objetivos, diagrama de Ishikawa, etc. que se pueden aplicar en conjunto o de manera individual.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

Propósito

Entender acabadamente las necesidades y expectativas de los grupos de interés para gestionarlas de manera de optimizar la eficacia del SGC.

Requisitos

Debido a su efecto o efecto potencial en la capacidad de la Organización de proporcionar regularmente productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables, la Organización debe determinar:

a) las partes interesadas que son pertinentes al SGC;

b) los requisitos pertinentes de estas partes interesadas para el SGC.

La Organización debe realizar el seguimiento y la revisión de la información sobre estas partes interesadas y sus requisitos pertinentes.

4.3 Determinación del alcance del sistema de gestión de la calidad

Propósito

Definir de manera precisa los límites del SGC adoptado y la factibilidad de cumplimiento con los requisitos, así como las necesidades de las partes interesadas.

Requisitos

La Organización debe determinar los límites y la aplicabilidad del SGC para establecer su alcance.

Cuando se determina este alcance, la Organización debe considerar:

a) todos los procesos establecidos como obligatorios en este referencial;

b) las cuestiones externas e internas indicadas en el apartado 4.1;

c) los requisitos de las partes interesadas pertinentes indicados en el apartado 4.2;

d) los productos y servicios de la Organización.

El alcance del SGC de la Organización debe estar disponible y mantenerse como información documentada. El alcance debe proporcionar la justificación para cualquier requisito de este referencial que la Organización determine que no es aplicable dentro del alcance de su SGC.

Sólo se puede declarar la conformidad con este referencial si los requisitos determinados como no aplicables no afectan a la capacidad o a la responsabilidad de la Organización para asegurarse de la conformidad de sus productos y servicios y del aumento de la satisfacción del cliente.

NOTA. Se recomienda que en la redacción del alcance se incluyan los espacios físicos donde se desarrolla el SGC.

4.4 Control de los procesos

Propósito

Mantener bajo control y mejorar los procesos con el fin de asegurar que los servicios prestados cumplen con las necesidades de los destinatarios.

Requisitos

La Organización debe establecer, mantener y mejorar continuamente un SGC que incluya como mínimo los procesos indicados en este Referencial, sin perjuicio de incorporar otros procesos que la Organización considere como conveniente mantener controlados dentro del SGC.

La Organización debe:

a) determinar las entradas requeridas y las salidas esperadas de estos procesos;

b) determinar la secuencia e interacción de los procesos de acuerdo con los requisitos de este referencial;

c) determinar y aplicar los criterios y los métodos incluyendo el seguimiento, las mediciones y los indicadores del desempeño relacionados necesarios para asegurarse de la operación eficaz y el control de estos procesos;

d) determinar los recursos necesarios para la operación y control de estos procesos y asegurar su disponibilidad;

e) asignar las responsabilidades y autoridades para estos procesos;

f) abordar los riesgos y oportunidades emergentes de los análisis respectivos;

g) evaluar estos procesos e implementar cualquier cambio necesario para asegurarse el logro de los resultados previstos;

h) mejorar los procesos y el SGC;

La Organización debe mantener la información documentada para apoyar la operación de sus procesos y conservarla como evidencia de que los procesos se llevan a cabo según lo planificado.

NOTA. En el Anexo D se presenta a modo de ejemplo un mapa de procesos para un SGC basado en este Referencial.

5 LIDERAZGO

5.1 Liderazgo y compromiso

Propósito

Asegurar que la Dirección asume el compromiso de sostener el SGC y la responsabilidad por la eficacia de aquellas actividades que son esenciales para los propósitos de la existencia de la Organización.

Requisitos

La Dirección debe demostrar liderazgo y compromiso con respecto al SGC:

a) asegurando que se establezcan la política y los objetivos de la calidad compatibles con el contexto y la dirección estratégica de la Organización;

b) designando al Oficial de cumplimiento ante la UIF;

c) designando un responsable del SGC que dependa de la Dirección;

d) asegurando la implementación de políticas y acciones tendientes a promover una Organización socialmente responsable;

e) impulsando acciones que promuevan el juego responsable;

f) asegurando la transparencia en el juego;

g) asegurando la capacidad de adaptación frente a los cambios producidos por las TIC (Tecnologías de la Información y de la Comunicación) y la consolidación del comercio electrónico (por ejemplo, cambios culturales, tecnológicos, de modelos de negocios, de comercio electrónico, de pautas de consumo, etc.);

h) determinando los riesgos y oportunidades que es necesario abordar, incluyendo los referidos a la seguridad de la información;

i) estableciendo y revisando su planificación estratégica y evaluando los resultados de la gestión;

j) asegurando la disponibilidad de recursos para el cumplimiento de la planificación estratégica y operativa y el establecimiento y mantenimiento del SGC;

k) comprometiendo el desarrollo de competencias para un desempeño eficaz de las personas;

l) asegurando la comunicación, compresión e implementación eficaz de las políticas y estrategias;

m) disponiendo y difundiendo los manuales y/o reglas de los juegos;

n) demostrando la transparencia de la administración de los fondos y de la rendición de cuentas;

o) garantizando el monitoreo, control y evaluación de la gestión;

p) promoviendo y adoptando la mejora continua.

NOTA. La rendición de cuentas contempla la información, en general y según aplique por las características de la Organización, relativa a la captura de apuestas, resultados operativos, balance administrativo–social y destino de los fondos. Se recomienda la elaboración de un Informe de Sustentabilidad.

5.2 Política

Propósito

Asegurar un marco de referencia y un lineamiento común para toda la Organización que permita la revisión de los objetivos de la calidad. Debe asegurar el enfoque en procesos, la mejora continua, adecuarse al contexto de la Organización y enfocarse en la satisfacción del cliente y las expectativas de las partes interesadas pertinentes.

Requisitos

La Organización debe establecer, implementar y mantener una política de la calidad que:

a) sea apropiada al propósito, al contexto de la Organización y a su estrategia;

b) proporcione un marco de referencia para el establecimiento y revisión de los objetivos;

c) incluya un compromiso de cumplir con los requisitos legales, reglamentarios, estatutarios y los establecidos en este Referencial;

d) incluya un compromiso de cumplir con los requisitos de seguridad de la información, juego responsable, lucha contra el juego ilegal o clandestino y prevención del lavado de activos y financiación del terrorismo; e

e) incluya un compromiso con la mejora continua del SGC.

La política debe mantenerse como información documentada, disponible y comunicada a las partes interesadas pertinentes.

NOTA. En el caso de existencia de políticas de otros sistemas de gestión, se recomienda la elaboración de una política integrada.

5.3 Roles, responsabilidades y autoridades en la Organización

Propósito

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

Requisitos

La Dirección debe asegurar que se determinan los roles, responsabilidades y autoridades para los puestos requeridos para la operación de los procesos incluidos en el SGC y para la implementación del SGC.

La Dirección debe designar un responsable del SGC quien, independientemente de otras responsabilidades:

a) asegure que se establecen, implementan y mantienen los procesos necesarios para el SGC;

b) informe a la Dirección sobre el desempeño del SGC y de cualquier necesidad de mejora; y

c) asegure que se promueva la toma de conciencia de los requisitos del cliente en todos los niveles de la Organización.

NOTA. La responsabilidad del responsable del SGC puede incluir relaciones con partes externas sobre asuntos relacionados con el SGC. El responsable del SGC, a pedido de la Dirección, puede asignar tareas o funciones a un grupo de personas.

5.4 Organizaciones comprometidas con la responsabilidad social empresaria (RSE)

Propósito

Que la Organización asuma el compromiso de:

a) considerar los impactos de sus decisiones y actividades en la sociedad, el ambiente y la economía, especialmente las consecuencias negativas significativas;

b) prevenir la repetición de impactos negativos involuntarios e imprevistos, a través de un comportamiento transparente y ético;

Requisitos

La Organización debe:

a) gestionar las expectativas pertinentes de sus partes interesadas;

b) diseñar, implementar y mantener un programa de RSE que incluya definir, planificar, ejecutar y comunicar sus acciones de RSE;

NOTA. Las acciones de RSE incluyen orientación sobre materias fundamentales de responsabilidad social como ser, la gobernanza de la Organización, los derechos humanos, las prácticas laborales, el ambiente, los asuntos de los consumidores, la participación activa y el desarrollo de la comunidad.

5.5 Juego Responsable. Prevención, administración, operatividad y apoyo a quienes tienen conductas problemáticas con el juego

Propósito

Realizar acciones que promuevan el juego responsable asesorando, capacitando y previniendo conductas problemáticas.

Requisitos

La Organización debe:

a) gestionar las expectativas pertinentes de sus partes interesadas;

b) diseñar, implementar y mantener un programa de Promoción del Juego Responsable, que contemple como mínimo lo siguiente:

   1) la existencia de un canal de información dirigido al jugador problemático, a su familia y al público en general;

   2) la adhesión al registro único de autoexclusión vigente en su jurisdicción;

   3) la articulación con los organismos especializados para la prevención y tratamiento de las personas que tienen conductas problemáticas con el juego.

5.6 Prevención de lavado de activos y financiación del terrorismo

Propósito

Que la Organización asuma el compromiso de desempeñar un papel activo en la prevención de lavado de activos y financiación del terrorismo, y de cumplir con la legislación y las regulaciones relativas a la prevención de lavado de activos y financiación del terrorismo.

Requisitos

La Organización debe:

a) Designar los roles necesarios y requeridos por la Unidad de Información Financiera para la correcta aplicación del sistema de Prevención. Dicho personal debe ser competente y acorde al volumen de las operaciones y a las tareas a realizar dentro de la Organización.

b) Diseñar e implementar los procedimientos y controles a cumplir ante situaciones que interactúen con la prevención de lavado de activos (por ejemplo: pago de premios, elaboración de reportes, etc.). Los mismos deben estar disponibles para ser consultados por todo el personal de la Organización como así también por los organismos competentes que puedan exigirlo.

c) Desarrollar un programa de capacitación dirigido a sus funcionarios y empleados en materia de prevención de Lavado de Activos y Financiación del Terrorismo. Este programa debe atender a los perfiles y funciones pertinentes. Las capacitaciones deben diversificar sus contenidos, siendo actuales a la realidad del contexto y las directrices emanadas por los organismos internacionales y nacionales competentes.

d) Implementar herramientas tecnológicas acordes con su desarrollo operacional, que le permitan establecer de una manera eficaz el sistema de control y prevención de Lavado de Activos y Financiación del Terrorismo; utilizar metodologías de gestión de riesgos (por ejemplo: una matriz de riesgo) para poder identificar los clientes/productos, zonas geográficas, actividades, etc. más riesgosas.

e) Asegurar la adecuada conservación y custodia de la información obtenida considerando la confidencialidad, disponibilidad e integridad de la misma.

f) Conjugar el trabajo con agencias, otros organismos provinciales o extraprovinciales y concesionarios a fin de realizar acciones conjuntas (ej.: capacitaciones, análisis conjunto de tipologías, etc.).

g) Establecer un plan de mejoras para el cumplimiento de objetivos y la mitigación de los riesgos inherentes a clientes, productos, y otras variables a definir por la Organización.

h) Prestar especial atención a las nuevas tipologías de Lavado de Activos y Financiación del Terrorismo a los efectos de establecer medidas tendientes a prevenirlas, detectarlas y reportar toda operación que pueda estar vinculada a las mismas, como asimismo a cualquier amenaza de Lavado de Activos o Financiación del Terrorismo.

i) Asegurar la correcta identificación del cliente cuando sea pertinente de acuerdo a los criterios legales y reglamentarios, tanto en metodologías de juego presenciales como no presenciales.

5.7 Lucha contra el juego ilegal o clandestino

Propósito

Que la Organización propicie el cumplimiento de la legislación nacional que penaliza el juego ilegal, tanto físico como online o en redes sociales.

Requisitos

La Organización debe diseñar, implementar y mantener:

a) un programa de difusión, información y concientización contra el juego ilegal;

b) un canal para la recepción y derivación de denuncias sobre el juego ilegal a los organismos competentes.

NOTA. Es recomendable que el programa propicie el trabajo en conjunto con otros actores de la sociedad civil, privados y/o estatales.

5.8 Comunicación institucional

Propósito

Gestionar las comunicaciones internas y externas al SGC, consolidando un modelo socialmente responsable de la Organización que propicie la protección de los grupos vulnerables y la comunicación responsable en el ámbito geográfico de competencia.

Requisitos

a) La Organización debe desarrollar un plan de comunicación integral (que incluya la comunicación institucional y la comercial) que promueva tanto la toma de conciencia del personal sobre los requisitos del SGC como la gestión de las comunicaciones externas, particularmente aquellas relacionadas con las expectativas y necesidades de sus partes interesadas pertinentes.

b) El plan de comunicación debe contemplar:

    1. qué comunicar;

2. a quién comunicar;

3. quién comunica;

4. cuándo comunicar;

5. cómo comunicar.

c) El plan de comunicación debe contemplar los siguientes requisitos de publicidad responsable:

1. proporcionar información clara y no engañosa sobre los operadores y servicios autorizados por cada jurisdicción provincial. Deberá, además, ser socialmente responsable y no incentivar el juego patológico;

2. no debe dañar ni explotar las susceptibilidades, aspiraciones, credulidad, inexperiencia ni falta de conocimiento de los menores de edad, tampoco debe estar orientado o específicamente diseñado para atraer a dicha franja de la población;

3. incluir en todas las piezas de comunicación, ya sean propias o de operadores privados autorizados, mensajes legibles de promoción del juego responsable y el acceso a herramientas de autoexclusión para jugadores con problemas conductuales con los juegos de azar.

d) La Organización debe comunicar y propiciar que los operadores privados de juegos de azar autorizados en su jurisdicción (tanto físicos como en formato online), cumplan con los requisitos enumerados anteriormente en el punto c).

e) La Organización debe crear y mantener actualizado y accesible, un repositorio digital de todas las piezas de comunicación externa dirigidas al cliente (cualquiera sea su formato), para que las mismas puedan ser analizadas y evaluadas con el fin de asegurar el cumplimiento de los requisitos del punto c) precedente.

f) La Organización debe diseñar e implementar actividades de capacitación para su personal, el personal tercerizado y los responsables de la comunicación de los operadores autorizados en su jurisdicción en la temática de Comunicación Responsable de Juegos de Azar.

NOTA. Se recomienda seguir los principios y requisitos incluidos en el Código de Buenas Prácticas para la Publicidad Responsable de Juegos de Azar Online en Argentina, ampliando su aplicación a la totalidad de la comunicación sobre juegos de azar de la Organización.

6 PLANIFICACIÓN

6.1 Acciones para abordar riesgos y oportunidades

Propósito

Que el SGC actúe como una herramienta preventiva.

Requisitos

Determinar los riesgos y oportunidades que sean necesarios tratar con el fin de:

a) asegurar que el SGC pueda lograr sus resultados previstos;

b) aumentar los efectos deseables;

c) prevenir, reducir y/o mitigar los efectos no deseados.

La Organización debe considerar como elementos de entrada los resultados obtenidos de la implementación de 4.1 y 4.2 y determinar cuáles son los riesgos y oportunidades que deben ser abordados.

Las acciones definidas para abordar los riesgos y oportunidades deben estar integradas e implementadas en los procesos del SGC.

NOTA. En el Anexo E se brinda información básica sobre el abordaje de los riesgos y oportunidades.

6.2 Gestión de riesgos de seguridad de la información. Ciberseguridad

Propósito

Establecer una metodología de gestión de riesgos de seguridad de la información, considerando toda información sensible, según su confidencialidad, integridad y disponibilidad.

Requisitos

La Organización 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 1. La norma ISO/IEC 27005 da criterios para la elaboración de un sistema de gestión de riesgos de seguridad de la información.

NOTA 2. El Anexo F contiene conceptos y recomendaciones para el tratamiento en la Organización de la seguridad de la información.

6.3 Objetivos de la calidad

Propósito

Asegurar que los objetivos establecidos sean adecuados para el cumplimiento de la política de la calidad.

Requisitos

6.3.1 La Organización debe establecer objetivos de la calidad y mantener la información documentada sobre ellos:

a) en las funciones y niveles pertinentes;

b) que sean coherentes con la política de la calidad;

c) que sean medibles y pertinentes para la conformidad de los productos y servicios y para aumentar la satisfacción del cliente y de otras partes interesadas pertinentes;

d) que sean objeto de seguimiento;

e) que se comuniquen en todos los niveles pertinentes;

f) que se actualicen, según corresponda.

6.3.2 Al planificar como lograr sus objetivos de la calidad, la Organización debe determinar:

a) qué se va a hacer;

b) qué recursos se requerirán;

c) quién será responsable;

d) cuándo se finalizará;

e) cómo se evaluarán los resultados.

7 PROCESOS DE APOYO

7.1 Infraestructura

Propósito

Asegurar que la Organización dispone de y mantiene una infraestructura tal, que le permite prestar sus servicios en forma adecuada y mejorar el SGC en forma continua.

Requisitos

7.1.1 Edificios y servicios asociados

La Organización debe determinar, proporcionar y mantener la infraestructura edilicia para la operación de sus procesos y lograr la conformidad de los productos y servicios y de los clientes internos y externos.

La Organización debe asegurarse de que el espacio físico y los servicios asociados consideran:

a) salones cómodos, con iluminación y climatización adecuada y accesibilidad inclusiva;

b) habilitación por autoridad competente, en caso de corresponder;

c) instalaciones sanitarias accesibles, inclusivas, limpias y con los insumos necesarios;

d) instalaciones de primeros auxilios con personal competente para la atención del personal y del público;

e) disponibilidad de conectividad para la realización de actividades en forma remota (ver 7.1.2).

La Organización debe definir:

f) las áreas seguras para el resguardo de la información confidencial;

g) la seguridad física perimetral y los controles a realizar de entrada física.

7.1.2 Sistemas informáticos

La Organización debe determinar, proporcionar y mantener la infraestructura necesaria en tecnologías de la información y la comunicación (incluyendo hardware y software) para la operación de sus procesos y lograr la conformidad de los productos y servicios.

La Organización debe asegurarse de que los recursos proporcionados consideran:

a) la asistencia a los requerimientos de índole técnica informática y de comunicaciones de los usuarios, incluyendo la atención de requerimientos de resolución inmediata del tipo mesa de ayuda, el desarrollo de software y el procesamiento de datos en caso de corresponder;

b) la planificación del mantenimiento preventivo y correctivo de los sistemas informáticos;

c) el control y resguardo de las comunicaciones utilizadas preservando la confidencialidad, disponibilidad e integridad de la información;

d) la protección de los registros;

e) el aseguramiento y la privacidad y protección de datos personales;

f) contar con un registro de los controles implementados contra el software malicioso;

g) la correcta realización de las copias de seguridad (backup);

h) el control y la disposición de las versiones de los sistemas desarrollados, tanto propios como por terceros, para el uso de la Organización;

i) la verificación de la vigencia de las licencias del software utilizados.

La Organización debe conservar la información documentada apropiada como evidencia de que los recursos de tecnologías de la información y la comunicación son idóneos para su propósito.

7.1.3 Ambiente de trabajo

La Organización debe determinar, proporcionar y mantener el ambiente de trabajo necesario para la operación de sus procesos y para lograr la conformidad de los productos y servicios, considerando el establecimiento y mantenimiento de un plan de higiene, seguridad y ambiente aprobado por profesional matriculado y conservado como información documentada.

El plan de higiene, seguridad y ambiente debe contemplar la normativa de aplicación sea nacional, provincial y/o municipal, definir la metodología e instrumentos de medición y el control a aplicar a los proveedores de las actividades que se asignen a terceros.

7.1.4 Recursos de seguimiento y medición

La Organización debe determinar y proporcionar los recursos necesarios para asegurar la validez y fiabilidad de los resultados cuando se realice el seguimiento o la medición del equipamiento para verificar la conformidad con los requisitos.

La Organización debe asegurarse de que cuando se realice el seguimiento o la medición del equipamiento se considera:

a) la definición de las especificaciones técnicas del equipamiento;

b) el control, verificación y calibración, esto último cuando corresponda, de los recursos de seguimiento y medición que se aplican al equipamiento;

c) la competencia del personal asignado al seguimiento y medición del equipamiento.

La Organización debe conservar la información documentada apropiada como evidencia de que los recursos de seguimiento y medición son idóneos para su propósito.

NOTA. El equipamiento puede ser físico o informático. El informático puede ser, por ejemplo, un software y el no informático o físico, son, entre otros, las bolillas, bolilleros y los sistemas de audio y video.

7.2 Gestión de las personas

Propósito

Asegurar que las competencias del personal de la Organización son acordes a las funciones asignadas y las mismas se mantienen y/o desarrollan en el tiempo.

Requisitos

7.2.1 Personas

La Organización debe determinar y proporcionar las personas necesarias para la implementación eficaz de su SGC y para la operación y control de sus procesos. Esas personas deben responder a las competencias requeridas por el SGC (ver 7.2.2).

7.2.2 Conocimiento de la Organización

La Organización debe determinar y gestionar el nivel de los conocimientos necesarios para la operación de sus procesos y para lograr la conformidad de los productos y servicios.

Estos conocimientos deben mantenerse y ponerse a disposición en la medida que sea necesario.

Cuando se abordan necesidades y tendencias cambiantes, la Organización debe considerar sus conocimientos actuales y determinar cómo adquirir o acceder a los conocimientos adicionales necesarios y a las actualizaciones requeridas.

7.2.3 Competencia

La Organización debe:

a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño y eficacia del SGC;

b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas;

c) incluir actividades de inducción a la Organización y al puesto de trabajo;

d) cuando sea aplicable, tomar acciones para adquirir y desarrollar las competencias necesarias y evaluar la eficacia de las acciones tomadas;

e) conservar la información documentada apropiada como evidencia de la competencia.

NOTA. Las acciones para desarrollar las competencias necesarias pueden incluir capacitaciones, formaciones en el puesto de trabajo, tutorías, entre otras. Ver en el Anexo C las directrices para las buenas prácticas en la planificación de la formación.

7.2.4 Toma de conciencia

La Organización debe asegurarse que las personas que realizan el trabajo bajo el control de la Organización tomen conciencia de:

a) la Misión, Visión y Valores de la Organización;

b) las estrategias definidas en función de la Misión, Visión y Valores de la Organización;

c) la política de la calidad;

d) los objetivos de la calidad;

e) su contribución a la eficacia del SGC incluidos los beneficios de una mejora del desempeño;

f) las implicancias del incumplimiento de los requisitos del SGC.

7.3 Control de la información documentada

Propósito

Asegurar que:

a) el personal de la Organización utiliza documentos aprobados por personal autorizado y en su versión vigente;

b) los registros son conservados en forma segura y pueden ser fácilmente localizados en el caso que se necesite consultarlos.

Requisitos

La información documentada se debe controlar para asegurar que esté:

a) disponible y sea idónea para su uso, dónde y cuándo se necesite;

b) protegida contra modificaciones no intencionadas;

c) almacenada y preservada su legibilidad;

d) identificado el control de cambios y su disposición;

e) accesible de acuerdo con los niveles de confidencialidad establecidos.

La documentación de origen externo que la Organización determine como necesaria para la operación de sus procesos se debe identificar y, según sea apropiado, controlar.

7.4 Seguridad de la información

7.4.1 Seguridad de los recursos humanos

Propósito

Asegurar que tanto el personal como las demás partes interesadas pertinentes (por ejemplo, proveedores, concesionarios, etc.) comprendan sus responsabilidades respecto a la seguridad de la información, en base a las funciones que cumplan o que desempeñen (previo, durante y finalizada la relación).

Requisitos

La Organización 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 la extinción de la relación laboral o contractual;

b) tener un registro de las actividades de sensibilización y concientización sobre los riesgos de seguridad de la información;

c) 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. Considerar estos requisitos en la definición de competencias (7.2.3). Se puede encontrar más información sobre Seguridad de los recursos humanos en el Anexo F.

7.4.2 Gestión de activos

Propósito

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

Requisitos

La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados, elaborarse y mantenerse en un inventario con la nominación del propietario de dichos activos.

7.4.3 Clasificación de la información

Propósito

Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la Organización.

Requisitos

La Dirección debe asegurar la existencia de una metodología donde se contemple la clasificación de la información en términos de la importancia de su revelación o modificación no autorizada frente a requisitos legales, valor, sensibilidad y criticidad. Esta metodología debe desarrollar e implementar criterios de uso para manipular la información, de acuerdo con el esquema de clasificación de la información adoptado por la Organización.

La Dirección debe asegurar la existencia de evidencia de la clasificación y el etiquetado de la información.

7.4.4 Control de acceso

Propósito

Limitar el acceso a los sistemas de procesamiento de información y la información documentada mantenida como evidencia de conformidad con los requisitos.

Requisitos

La Organización debe:

a) limitar el acceso a los sistemas, servicios e información únicamente a los usuarios autorizados;

b) evidenciar el control de accesos por medio de:

    1) la gestión de privilegios;

    2) el registro de usuarios;

    3) el registro de accesos permitidos y no permitidos;

    4) la política de gestión de contraseñas.

7.4.5 Planificación e información de la continuidad del negocio

Propósito

Mantener las actividades de la Organización, contrarrestando las posibles interrupciones y protegiendo sus procesos críticos de los efectos de fallas significativas de los sistemas de información o desastres y asegurar su reanudación oportuna.

Requisitos

La Organización debe:

a) elaborar, documentar e implementar planes de continuidad de sus procesos críticos a fin de mantener o restablecer sus operaciones y asegurar la disponibilidad de la información (al nivel requerido y en las escalas de tiempo requeridas) luego de la interrupción o falla;

b) los planes de continuidad deben ser controlados, probados y actualizados periódicamente para asegurar que sean válidos y eficaces durante situaciones adversas;

c) comunicar a las personas sobre el plan de continuidad y aplicar un plan de entrenamiento.

7.4.6 Incidentes de seguridad de la información

Propósito

Asegurar un enfoque coherente y eficaz para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos.

Requisitos

La Organización debe definir un procedimiento para la gestión de incidentes de seguridad de la información para:

a) mantener el registro de los eventos e incidentes de seguridad de la información;

b) revisar regularmente los registros;

c) contar con registros del tratamiento de los eventos de seguridad de información;

d) evaluar la eficacia de las medidas adoptadas.

7.5 Gestión legal y técnica

Propósito

Asegurar el cumplimiento de los requisitos legales y reglamentarios vigentes y asistir legalmente a la Organización.

Requisitos

La Organización debe establecer un proceso que:

a) asegure el cumplimiento de los requisitos legales y reglamentarios;

b) atienda los asuntos legales que surjan respecto de sus actividades, sus normas internas, y a su relación con otras entidades;

c) provea servicios de asesoría legal, de representación en litigios y en negociaciones, y en la elaboración de documentos legales para la Organización;

d) recopile, mantenga actualizada y comunique a los niveles pertinentes, la normativa vigente incluyendo la relacionada con la seguridad de la información. Esta normativa se debe mantener como información documentada.

8 PROCESOS OPERATIVOS

8.1 Captura de apuestas, sorteos y pagos de premios (juegos lotéricos)

8.1 1 Captura de apuestas

La Organización debe establecer, implementar y mantener un proceso de captura de apuestas para sus juegos que:

a) contemple todas las disposiciones establecidas en el reglamento del juego que se trate;

b) garantice el ingreso de los datos correspondientes a la o las jugadas solicitadas por el apostador;

c) entregue al apostador un comprobante en cualquier tipo de soporte con el cual pueda presentarse a efectivizar su premio en caso de obtenerlo;

d) asegure el intercambio de datos informáticos de la apuesta de modo de poder construir el universo de apuestas del concurso o juego en cuestión en el momento del sorteo.

Debe mantenerse información documentada de la metodología utilizada y asegurar la confidencialidad, integridad y disponibilidad de los datos de acuerdo con un análisis de la seguridad de información que aplique según la característica de los mismos.

8.1.2 Sorteos

La Organización debe establecer, implementar, mantener y documentar un proceso de sorteo para sus juegos que:

a) verifique la integridad del archivo de captura de apuestas;

b) se realice bajo condiciones controladas en cada uno de sus pasos, garantizando la transparencia del acto;

c) tenga siempre como objetivo principal obtener el resultado del sorteo;

d) contemple todas las contingencias posibles que resulten de un análisis cuya información documentada debe ser guardada y mantenida;

e) promocione la participación del público y la comunicación a través de más de un soporte de comunicación masiva.

8.1.3 Liquidación y pagos de premios

La Organización debe establecer, implementar, mantener y documentar un proceso de liquidación y pago de premios para sus juegos que:

a) permita la realización de los pagos de premios a los clientes/participantes en función del tipo de juego y cantidad, así como los controles establecidos (incluidos los relacionados con prevención de lavado de activos y financiación del terrorismo, ver 5.6);

b) asegure la confidencialidad de los datos del ganador según la normativa que aplique.

8.2 Fiscalización

8.2.1 Fiscalización en casinos y salas de juego

8.2.1.1 Fiscalización de máquinas automáticas de apuestas

8.2.1.1.1 Incorporación de dispositivos de juegos electrónicos

La Organización debe establecer, implementar y mantener un procedimiento para la incorporación de dispositivos de juegos electrónicos que contemple como mínimo:

a) declaración jurada de los datos de identificación del fabricante, importador, comercializador o distribuidor, que incluya procedencia, marca, modelo, Nº de serie único, fecha de fabricación de la máquina; también detallar en el caso que sea reacondicionada;

b) la existencia de numeración dado por el Organismo regulador o el Casino (numeración de máquina en sala), a través de placa, código QR, etc.;

c) la existencia del certificado de seguridad eléctrica emitido por un organismo competente acreditado por el Organismo Argentino de Acreditación;

d) los requisitos a verificar en el informe de ensayo del software y del juego (comportamiento de las máquinas, funcionamiento del generador de números aleatorios RNG, *Random Number Generator* basado en software, hardware, criptográfico, y de los juegos en todas sus características) emitido por laboratorio reconocido por el organismo regulador;

e) la disponibilidad de información sobre la tabla de pagos, la línea de apuestas y la apuesta máxima;

f) la existencia del manual de operaciones y antecedentes del juego, en español;

g) la definición de las condiciones para las altas y/o bajas de Máquinas;

h) la definición de las condiciones para la incorporación y/o modificación de dispositivos (apiladores de billetes (*stackers*), aceptadores o validadores de billetes, lectores de tarjetas, etc.). Se debe mantener información documentada de la metodología aplicada en la verificación de los requisitos del procedimiento.

8.2.1.1.2 Control de dispositivos de juegos electrónicos

La Organización debe establecer, implementar y mantener un procedimiento para el control del parque de dispositivos de juegos electrónicos que contemple:

a) la ubicación georreferenciada de cada máquina;

b) el plano de distribución (*layout*) de cada sala, con indicación, de existir, de islas de progresivos (intrajurisdiccionales o interjurisdiccionales), pozo acumulado, etc.;

c) un sistema en tiempo real (*online*) para el control del funcionamiento integral del dispositivo de juegos electrónicos, que contemple contadores y la totalidad de eventos, incluyendo las alertas por máquinas *offline*, fuera de servicio, en mantenimiento o cualquier otra contingencia que impida que la máquina esté operable;

d) la definición de las condiciones para las modificaciones (cambios de juegos, denominaciones, cambios de *hold*, etc.)

e) la definición de las condiciones para correlación de juegos en vivo (cuando el dispositivo de juego ofrezca una partida que se reconoce ser una simulación de un juego de casino en vivo, tal como el Póquer, Veintiuno (Black Jack), Ruleta, etc., las mismas probabilidades asociadas con el juego en vivo serán evidentes en el juego simulado).

f) la definición de los procedimientos de seguridad de las áreas lógicas de las máquinas (donde se alojan los componentes electrónicos que tienen potencial de afectar el resultado y la integridad del dispositivo de juego, tales como CPU, unidad central de almacenamiento, PSD, dispositivo de almacenamiento de programas, componentes que administran el cifrado y descifrado de datos críticos, controlador de comunicaciones de electrónicos, etc.);

g) la definición de las condiciones de operabilidad de los sistemas que estén integrados con los dispositivos, cuando sea aplicable, tales como sistemas de fidelización (componente integrado de identificación del jugador, lectores de tarjetas integrados, lectores de código de barras integrado, escáneres biométricos integrados, etc.) o sistemas de pago (Tickets, Impresoras, Tickets en línea, Tickets en *offline*, Sistemas Cajas, Kioscos TITO, etc.);

h) cuando sea aplicable, la definición de las condiciones de los dispositivos que contemplen la escalabilidad a nuevas tendencias, tales como juegos que incorporen una representación gráfica o una simulación de un objeto físico que es usado para determinar el resultado del juego (realidad aumentada);

i) la definición de las condiciones para los requisitos básicos relativos al hardware independiente y específico integrado a la máquina, tales como PCB (identificación alfanumérica y, cuando sea aplicable, un número de revisión);

j) el mantenimiento, las reparaciones/auditorías del equipo que aseguren su idoneidad original en el cumplimiento de los requisitos de incorporación.

Debe conservarse información documentada del cumplimiento de los requisitos establecidos en el procedimiento.

8.2.1.1.3 Padrón del parque de dispositivos de juegos electrónicos

La Organización debe establecer, implementar y mantener un procedimiento para el padrón jurisdiccional del parque de dispositivos de juegos electrónicos que contemple:

a) ingreso y egreso al sistema padrón o maestro;

b) inclusión y exclusión de una máquina al parque de máquinas de una sala;

c) modificación de características detalladas de máquinas en el padrón (*master list*).

Debe conservarse información documentada del cumplimiento de los requisitos establecidos en el procedimiento.

8.2.1.2 Fiscalización de Juegos de Paño

La Organización debe establecer, implementar y mantener un procedimiento para el funcionamiento de las mesas de paño que contemple:

a) la ubicación georreferenciada de cada mesa en la jurisdicción;

b) el plano de distribución *(layout*) de cada sala, con indicación del tipo de mesa;

c) la definición de las condiciones para la incorporación, baja y/o modificación de mesas;

d) la definición de las condiciones para la modificación de las características de juego de las mesas (tipo de bancas, cantidad de bancas autorizadas, montos de apuestas mínimas y máximas, saltos de bancas, etc.);

e) el registro de la descripción de distintas modalidades de juegos (bancados, poceados, etc.);

f) la disponibilidad de información sobre la tabla de pagos según el juego y su reglamento;

g) la definición de las condiciones para la incorporación de sistemas de fidelización, bajas y/o modificación de mesas;

h) la base de datos o padrón jurisdiccional con cada uno de los juegos (mesas) y sus características (*master list*).

Debe conservarse información documentada del cumplimiento de los requisitos establecidos en el procedimiento.

8.2.1.3 Fiscalización a través de Salas de Vigilancia

En el caso de que la Organización posea un circuito cerrado de televisión (CCTV), debe establecer, implementar y mantener un procedimiento para su funcionamiento que contemple:

a) el control a través de la sala de vigilancia del correcto desarrollo de los juegos vivos en los casinos o salas de juego, según las normas vigentes, verificando permanentemente, el adecuado funcionamiento y operación de los sistemas y equipamientos afectados a la actividad, impidiendo el uso de procedimientos que tiendan a alterar el juego limpio que determina el resultado del juego;

b) la garantía del correcto funcionamiento de un sistema de CCTV en las mesas donde se exploten juegos de Casino y máquinas de juego y conservar los registros en soportes (medios de almacenamiento sobre sistemas DVR, sistema de videograbación digital, y NVR, sistema de videograbación de red, etc.) por el tiempo que establezca la normativa vigente de la Organización, siendo responsable de su guarda, intangibilidad y debida confidencialidad;

c) la definición de la visualización de las imágenes (a través de un software, presencial, en línea, etc.);

d) la definición del sistema (centralizado, monitoreo en línea o remoto, etc.) estableciendo políticas de utilización, permitiendo crear distintos perfiles de usuario con diferentes permisos sobre las cámaras y el registro fílmico de las mismas;

e) la definición del control de las actividades complementarias del juego, tales como cajas, recuento y tesoros;

f) el control y registro del equipamiento de la sala de vigilancia, grabaciones en resguardo, libros y/o planillas de registros de eventos, el control de stock de los precintos (cuando corresponda), otros elementos de la sala de vigilancia, etc.;

g) el correcto registro de todos los eventos, y cuando sea necesario, su comunicación y elevación;

h) la conformación de equipos específicos y correcta formación y permanente capacitación del personal de la sala de vigilancia;

i) las medidas de seguridad (alarmas, biométricos, etc.);

j) la definición de la intervención a través de la sala de vigilancia, cuando correspondiera y si se tuviera reconocimiento facial, la identificación a través de los sistemas del público que ingresa a la Sala de Juego, con el objetivo de impedir el ingreso a todas aquellas personas que, por distintos motivos, se encuentren excluidas para acceder a la Sala de Juego.

Debe conservarse información documentada del cumplimiento de los requisitos establecidos en el procedimiento.

8.2.2 Fiscalización de puntos de venta oficiales

La Organización debe establecer, implementar y mantener un procedimiento para la fiscalización y control de sus puntos de venta oficiales que contemple:

a) la verificación de cumplimiento de los reglamentos de concesión;

b) la verificación de las condiciones de explotación comercial del punto de venta;

c) la verificación del correcto funcionamiento de las terminales de captura de apuestas y otros dispositivos utilizados para tal fin;

d) la aplicación de multas y/o sanciones ante el incumplimiento.

Debe conservarse información documentada del cumplimiento de los requisitos establecidos en el procedimiento.

8.2.3 Fiscalización de otros juegos

La Organización debe establecer, implementar y mantener un procedimiento para la fiscalización y control de otros juegos que realice, considerando los requisitos establecidos en este referencial, en particular los definidos en los Capítulos 7 y 8 que sean de aplicación para asegurar el control de la fiscalización.

NOTA. Los otros juegos pueden incluir hipódromos, entre otros.

8.3 Atención al cliente y partes interesadas (incluye gestión de reclamos)

La Organización debe establecer, implementar, mantener y documentar un proceso de atención al cliente y partes interesadas que debe asegurar la existencia de canales para su atención. Estos canales deben permitir la participación a través de la formulación de consultas, peticiones, quejas, reclamos y denuncias como así también felicitaciones y sugerencias, además de facilitar la asistencia en información y orientación sobre los productos y servicios que brinda la Organización.

8.3.1 Quejas, reclamos y denuncias

El proceso de quejas, reclamos y denuncias debe:

a) ser visible y accesible al cliente y otras partes interesadas;

b) determinar los criterios para cada categoría y realizar la clasificación una vez recibida;

c) contar con una identificación única por queja, reclamo o denuncia para asegurar su trazabilidad;

d) registrar todo el proceso que involucra la resolución, como así también los responsables de su tratamiento;

e) guardar la debida confidencialidad e imparcialidad;

f) generar los informes y estadísticas para la gestión.

NOTA 1. Se incluye un flujograma en Anexo G ilustrativo del tratamiento de quejas y reclamos.

NOTA 2. A modo de orientación se recomienda la lectura de la norma IRAM-ISO 10002.

8.4 Gestión de juegos de casino y salas de juegos electrónicos

La Organización debe establecer, implementar y mantener un procedimiento para sus casinos y salas de juegos electrónicos que contemple:

a) la estructura jerárquica y sus misiones y funciones pertinentes;

b) la comunicación entre las autoridades del juego y de la Organización que contemple la diferencia de horarios;

c) un sistema de contabilidad que impacte directamente en la contabilidad central de la Organización;

d) la realización de controles cruzados entre la gestión del juego y la Organización;

e) la atención al cliente y partes interesadas (ver 8.3);

f) la gestión del personal que incluya el establecimiento de turnos y horarios de trabajo.

8.5 Gestión económico-financiera

Propósito

Gestionar los recursos económico-financieros, con el fin de alcanzar los objetivos de la Organización y del SGC y brindar información en tiempo y forma.

Requisitos

La Organización debe:

a) planificar el presupuesto de recursos y gastos;

b) ejecutar, controlar y registrar los hechos económicos;

c) realizar el seguimiento presupuestario y patrimonial;

d) evaluar y analizar las desviaciones presupuestarias y la conciliación de cuentas;

e) comunicar y publicar la gestión de los hechos económicos.

8.6 Control de procesos, productos y servicios suministrados externamente

Establecer la metodología de evaluación integral de los proveedores de suministros de productos, prestación de servicios/obras y de profesionales de modo de definir su habilitación y permanencia en el listado de proveedores, a fin de asegurar el cumplimiento de los requisitos mínimos necesarios para el suministro de productos y servicios.

NOTA. Se recomienda que los softwares utilizados orientados a los procesos operativos (por ejemplo, captura de apuestas), sean certificados por una tercera parte independiente.

8.6.1 Evaluación de desempeño del proveedor

Con el fin de retroalimentar el listado de proveedores habilitados, el área responsable debe utilizar una evaluación de desempeño basada en una metodología que incluya los criterios para la calificación que conforma el resultado, conforme el tipo de bien y/o servicio contratado.

Las evaluaciones se realizarán de acuerdo con el grado de criticidad e impacto del proveedor en el proceso.

8.7 Comercialización a través de puntos de venta oficiales

La Organización debe establecer, implementar, mantener y documentar un modelo de comercialización, que contemple todas las relaciones, requisitos y normativas que apunten a:

a) establecer la relación comercial entre la Organización y su punto de venta;

b) establecer la relación entre el punto de venta y el cliente.

Este documento debe contener, además:

c) el tipo y modalidad del contrato que regirá la relación;

d) contemplar el modelo de negocios.

8.8 Gestión, control y fiscalización de juego online

La Organización debe establecer, implementar y mantener procesos y procedimientos para la gestión, control y fiscalización de juego online que contemplen:

a) el desarrollo de un marco de referencia estratégico documentado que explicite:

   1. el modelo de mercado (abierto, cerrado o mixto, con cantidad de licencias autorizadas);

   2. el modelo de gestión y negocio a utilizar, definiendo:

      a. sí es de explotación directa y única estatal (monopolio estatal en explotación y/o control de los juegos de azar online); o

      b. sí es de explotación mixta (estatal y/o privada) con control y fiscalización estatal; o

      c. sí es de explotación privada con control y fiscalización estatal;

   3. la determinación de los actores privados que pueden explotar los juegos de azar regulados y autorizados (operadores) y los requisitos generales que deben cumplir;

4. la definición sobre los juegos a ser autorizados y explotados, indicando los juegos autorizados a los que se puede apostar, personas autorizadas a apostar, las personas inhibidas a apostar y el ámbito geográfico en el que se puede apostar;

5. las políticas públicas destinadas a la protección de los grupos vulnerables, haciendo especial hincapié en las políticas de prevención del juego patológico y promoción del juego responsable, los límites a la publicidad y la protección de menores de edad, entre otros;

b) los requisitos técnicos exigibles a los operadores de las licencias autorizadas definidos por la Organización, como ser la identificación de los servidores, la integridad y resguardo de datos de apuestas y apostadores y las características de los componentes del sistema técnico, entre otros;

c) la identificación y operación de las herramientas que permitan proteger la seguridad de la cuenta de cada apostador;

d) la identificación y operación de las herramientas que posibiliten asegurar y garantizar la trazabilidad y seguimiento de todas las apuestas realizadas en las plataformas autorizadas;

e) las certificaciones y homologaciones existentes del software utilizado en las plataformas por parte de los operadores autorizados en la jurisdicción, como asimismo la existencia de registros oficiales de entes certificadores en cada jurisdicción o, en su defecto, el reconocimiento de certificaciones avaladas por otras jurisdicciones a través de acuerdos interjurisdiccionales;

f) los medios de pago permitidos para la realización de apuestas, retiros de fondos y/o cobro de premios en la jurisdicción;

g) las herramientas y técnicas utilizadas para constatar la edad y domicilio de los apostadores registrados en las plataformas utilizadas por los operadores autorizados en la jurisdicción;

h) las herramientas y técnicas utilizadas para garantizar el respeto jurisdiccional en la captación de apuestas por parte de los operadores autorizados en la jurisdicción;

i) las políticas y herramientas desarrolladas para promover y garantizar la publicidad responsable de los juegos de azar online;

NOTA. Ver más información en Código de Buenas Prácticas para la Publicidad Responsable de Juegos de Azar Online en Argentina.

j) las políticas y herramientas desarrolladas para promover y garantizar la prevención del juego patológico y la promoción del juego responsable en el marco del juego online;

k) las políticas y herramientas desarrolladas para promover y garantizar la integridad de las apuestas deportivas;

l) la gestión de los reclamos, quejas y/o sugerencias realizadas por los apostadores en cada plataforma autorizada, así como un monitoreo centralizado por parte de la Organización que garantice la gestión efectiva de los intereses y expectativas de las partes interesadas pertinentes;

m) la existencia y gestión de un registro unificado de apostadores por parte de la Organización;

n) las políticas y herramientas desarrolladas para prevenir y luchar contra el juego ilegal online;

o) las herramientas y técnicas utilizadas para evitar la transferencia de fondos entre jugadores en las plataformas de juego utilizadas por los operadores autorizados;

p) las herramientas y técnicas utilizadas para asegurar un efectivo monitoreo y control de los impuestos y cánones a pagar por parte de los operadores autorizados.

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 operativos y de la satisfacción de las partes interesadas, la Organización debe:

a) identificar los indicadores necesarios para asegurar resultados válidos;

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 SGC.

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

9.2 Satisfacción del cliente y las partes interesadas

Propósito

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

Requisitos

La Organización debe determinar métodos que le permitan obtener información relativa a la percepción de estas partes interesadas 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;

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 Organización son revisados regularmente por la Dirección para poder tomar las medidas que permitan una mejora continua.

Requisitos

La Dirección debe revisar el SGC de la Organización, al menos una vez al año, para asegurarse de su conveniencia, adecuación, eficacia y alineación continuas con la dirección estratégica de la Organización.

9.3.1 Entradas de la revisión

a) el estado de las acciones de las revisiones por la dirección previas;

b) los cambios en las cuestiones externas e internas que sean pertinentes al SGC;

c) los cambios en la orientación estratégica a mediano y largo plazo (4.1);

d) la información sobre el desempeño y la eficacia del SGC, incluyendo la información del proceso de atención al cliente y partes interesadas;

e) la adecuación de los recursos;

f) los resultados de las auditorías (internas y externas, y del sistema de prevención contra el lavado de activos y la financiación del terrorismo, etc.);

g) la eficacia del tratamiento de las acciones correctivas implementadas;

h) la eficacia de las acciones tomadas para abordar los riesgos y las oportunidades;

i) las oportunidades de mejora.

En particular respecto a la seguridad de la información, la Organización debe:

j) revisar 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;

k) definir los métodos, y responsabilidades para su verificación;

l) informar los resultados a la dirección de la Organización de manera fehaciente;

m) mejorar continuamente la pertinencia, adecuación y eficacia de los objetivos de seguridad de la información.

9.3.2 Salidas de la revisión

La Organización debe incluir decisiones y acciones relacionadas a:

a) las oportunidades de mejoras;

b) cualquier necesidad de cambio en el SGC;

c) las necesidades de recursos.

La Organización debe mantener información documentada como evidencia de los resultados de las revisiones por la dirección.

9.4 Auditoría interna

Propósito

La Organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información acerca de la conformidad del SGC.

Requisitos

Establecer, implementar y mantener un programa de auditorías para asegurar el cumplimiento de los requisitos de su SGC y que el mismo se mantiene eficazmente.

El programa debe incluir:

a) la frecuencia, los métodos, las responsabilidades, la elaboración de informes, y debe tener en consideración la importancia de los procesos involucrados, los cambios que afectan a la Organización y los resultados de las auditorías previas;

b) los criterios de las auditorías y el alcance de cada una de ellas;

c) la selección del equipo auditor, según su calificación, para asegurar la objetividad y la imparcialidad del proceso de auditoría;

d) establecer un plazo para que el auditado presente el plan de acción para realizar las correcciones y la toma de las acciones correctivas.

La Organización debe conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ellas.

10 MEJORA

10.1 No conformidades y acciones correctivas

Propósito

Asegurar que se identifican, analizan y se toman acciones ante las no conformidades para evitar que vuelvan a ocurrir.

Requisitos

Cuando ocurra una no conformidad la Organización debe:

a) reaccionar ante la no conformidad y, cuando sea aplicable:

   1. tomar acciones para controlarla y corregirla;

2. 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:

1. la revisión y el análisis de la no conformidad;
2. la determinación de las causas de la no conformidad;
3. la determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir;
4. la implementación de cualquier acción necesaria;
5. la revisión de la eficacia de cualquier acción correctiva necesaria
6. la actualización de los riesgos y oportunidades determinados durante la planificación y
7. si fuera necesario, mediante la realización de cambios al SGC.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.
La Organización 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.

NOTA. Las fuentes de las no conformidades pueden incluir las quejas, reclamos, sugerencias, las salidas no conformes, los incidentes de seguridad de la información, entre otras.

10.2 Mejora Continua

Propósito

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

Requisitos

La Organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGC.

La Organización debe considerar los resultados del análisis y la evaluación, y las salidas de la revisión por la dirección, para determinar si hay necesidades u oportunidades que deben considerarse como parte de la mejora continua.

La Organización debe determinar y seleccionar las oportunidades de mejora e implementar cualquier acción necesaria para cumplir los requisitos del cliente y aumentar su satisfacción. Estas deben incluir:

a) mejorar los productos y servicios para cumplir con los requisitos, así como considerar las necesidades y expectativas futuras;

b) corregir, prevenir o reducir efectos no deseados;

c) mejorar el desempeño y la eficacia del SGC.

Anexo A
(Informativo)

Principios de la gestión de la calidad 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.

Obtiene un beneficio medible al:

a) aumentar el número de clientes y con ello los beneficios económicos;

b) afianzar la productividad del esfuerzo, ya que, al estar bien dirigidos y enfocados a datos fiables, los esfuerzos reciben la contraprestación debida;

c) mejorar la fidelización de clientes. Los clientes confían en la empresa;

d) aumentar el liderazgo en el mercado, que es consecuencia de todo lo anterior.

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.

Las actuaciones que se exigen dentro de la normativa para que la Dirección dé prueba de compromiso con el SGC son una serie de tareas que se recomienda llevar a cabo:

a) comunicar a la Organización la importancia de satisfacer los requisitos del cliente (los legales y los reglamentarios);

b) establecer la política de la calidad y los objetivos de la calidad;

c) poner los recursos necesarios al servicio de la Organización;

d) revisar directamente si se cumplen los objetivos marcados.

La alta Dirección debe asegurarse que se cumplen los requisitos generales del sistema y que el SGC se mantenga íntegro, aunque se produzcan cambios.

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.

Anexo B
(Informativo)

Etapas de implementación

CAPÍTULO		Etapas de implementación		
		I	II	III
1 OBJETO Y CAMPO DE APLICACIÓN		No aplica		
2 DOCUMENTOS NORMATIVOS PARA CONSULTA				
3 TÉRMINOS Y DEFINICIONES				
4 SISTEMA DE GESTIÓN DE LA CALIDAD	4.1 Comprensión de la Organización y de su contexto	Completo		
	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Completo		
	4.3 Determinación del alcance del sistema de gestión de la calidad	Completo		
	4.4 Control de los procesos	Completo		
5 LIDERAZGO	5.1 Liderazgo y compromiso	Completo		
	5.2 Política	Completo		
	5.3 Roles, responsabilidades y autoridades en la Organización	Completo		
	5.4 Organizaciones comprometidas con la responsabilidad social empresaria (RSE)	Completo		
	5.5 Juego Responsable. Prevención, administración, operatividad y apoyo a quienes tienen conductas problemáticas con el juego	Completo		
	5.6 Prevención, lavado de activos y financiación del terrorismo	Completo		
	5.7 Lucha contra el juego ilegal o clandestino	Completo		
	5.8 Comunicación institucional	Completo		
6 PLANIFICACIÓN	6.1 Acciones para abordar riesgos y oportunidades	Completo		
	6.2 Gestión de riesgos de seguridad de la información. Ciberseguridad	Completo		
	6.3 Objetivos de la calidad	Completo		

CAPÍTULO		Etapas de implementación		
		I	II	III
7 PROCESOS DE APOYO	7.1 Infraestructura		Completo	
	7.2 Gestión de las personas		Completo	
	7.3 Control de la información documentada		Completo	
	7.4 Seguridad de la información		7.4.1, 7.4.2, 7.4.4, 7.4.5 a), 7.4.6	Completo
	7.5 Gestión legal y técnica		Completo	
8 PROCESOS OPERATIVOS	8.1 Captura de apuestas, sorteos y pagos de premios (juegos lotéricos)		Completo	
	8.2 Fiscalización		Completo	
	8.3 Atención al cliente y partes interesadas (incluye gestión de reclamos)		Completo	
	8.4 Gestión de juegos de casino y salas de juegos electrónicos		Completo	
	8.5 Gestión económico-financiera		Completo	
	8.6 Control de procesos, productos y servicios suministrados externamente		Completo	
	8.7 Comercialización a través de puntos de venta oficiales		Completo	
	8.8 Gestión, control y fiscalización de juego online		Completo	
9 EVALUACIÓN DEL DESEMPEÑO	9.1 Seguimiento, medición, análisis y evaluación		a)	Completo
	9.2 Satisfacción del cliente y las partes interesadas	a)	b)	Completo
	9.3 Revisión por la Dirección			Completo
	9.4 Auditoría interna			Completo
10 MEJORA	10.1 No conformidades y acciones correctivas	a)	b1) y b2)	Completo
	10.2 Mejora continua			Completo

Anexo C
(Informativo)

Formación de las personas

Debido a la incidencia de las personas en los resultados de la Organización, se recomienda contar con un plan de capacitación que permita el desarrollo de las competencias de acuerdo con las necesidades de formación detectadas. Sin perjuicio de las actividades de capacitación que surjan de la detección de necesidades, es conveniente incluir en el plan, actividades de formación alineadas a la estrategia de la Organización, sobre las temáticas siguientes:

a) juego responsable;
b) prevención de lavado de activos y financiación del terrorismo;
c) juego ilegal o clandestino;
d) juego online;
e) ciberseguridad;
f) seguridad de la información;
g) política de la calidad y los objetivos de la calidad;
h) a contribución a la eficacia del SGC, incluidos los beneficios de una mejora del desempeño y las implicaciones del incumplimiento de los requisitos del SGC y los legales y reglamentarios;
i) la preservación y mantenimiento de los conocimientos de la Organización:

Como evidencia de la gestión de la capacitación de las personas se recomienda mantener información documentada de:

a) el relevamiento de las necesidades de formación (por ejemplo, mediante evaluaciones de desempeño);
b) el plan de capacitación;
c) el programa de los cursos;
d) la planilla de asistencia;
e) las constancias de aprobación de los participantes;
f) la evaluación de la eficacia de las acciones formativas.

Es recomendable que los programas de los cursos incluyan en sus contenidos, de existir, la legislación de aplicación que es pertinente a la formación de los participantes.

NOTA 1. Se recomienda que la planificación de la capacitación incluya entrenamientos tutorados; la elaboración de material didáctico propio; entre otras actividades.

NOTA 2. Es conveniente que para la preservación de los conocimientos, la Organización elabore guías o documentos con lineamientos que incluyan conocimientos adquiridos con la experiencia; lecciones aprendidas de los fracasos y de proyectos de éxito; casos de resultados de las mejoras en los procesos, productos y servicios y disponga de una biblioteca digital que permita a las personas acceder a fuentes externas (por ejemplo, normas, material académico, conferencias, recopilación de conocimientos provenientes de clientes o proveedores externos).

NOTA 3. Se recomienda medir la eficacia e impacto de la capacitación, definiendo métodos tales como la observación, pruebas de competencia, resolución de problemas, entre otros e involucrar en esta responsabilidad a los jefes del personal evaluado.

Anexo D
(Informativo)

Mapa de procesos

(#) Incluye los procesos de seguimiento, satisfacción del cliente, revisión por la dirección, auditoría interna y mejora continua

Anexo E
(Informativo)

Consideraciones para la Gestión de Riesgos

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

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 SGC.

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

a) 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;

b) establecer una metodología de registro y mapeo de riesgos, que incluya su actualización y revisión periódica;

c) 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;

d) prever la manera de comunicación interna sobre cada riesgo detectado.

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

Las etapas del proceso de gestión de riesgos comprenden:

1. Establecimiento del contexto

Para realizar un análisis eficaz del riesgo 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:

a) 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 esta 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.

b) 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 incluyen además de los requisitos legales y reglamentarios, 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.

a) 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.

b) 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.

c) 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 prestablecidos.

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)

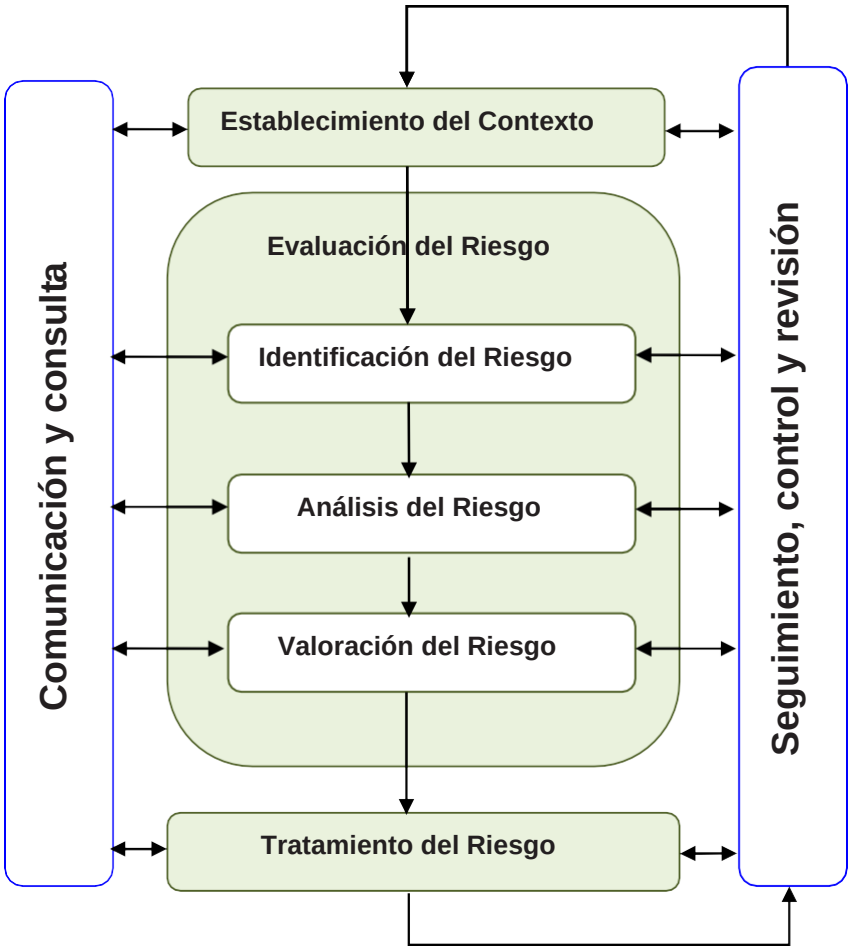
Se debe efectuar el seguimiento y control de la eficacia de las medidas de mitigación adoptadas, comunicando y consultando a los interesados internos y externos.

Recomendación:

Se debería tener en cuenta durante todas las etapas del proceso de gestión de riesgos, una continua “Comunicación y Consulta” con las partes interesadas externas e internas, de manera que ellos entiendan los fundamentos con los cuales se toman las decisiones y las razones por las cuales se requieren acciones específicas.

De este modo se trata de asegurar que los distintos puntos de vista sean considerados adecuadamente al definir los criterios de riesgo y al valorar los riesgos.

A continuación, se presenta una síntesis de las actividades a considerar en la gestión de riesgos.



5. Detección de oportunidades

El riesgo es comúnmente interpretado como negativo, por ejemplo, el riesgo de que no se cumplan las especificaciones.

Las oportunidades pueden surgir como resultado de una situación favorable para lograr un resultado previsto: un conjunto de circunstancias que permita a la Organización atraer clientes, desarrollar nuevos productos y servicios. Las oportunidades también pueden conducir a: adopción de nuevas prácticas (más eficientes y/o eficaces), lanzamiento de nuevos productos, apertura de nuevos mercados, establecimiento de asociaciones, utilización de nuevas tecnologías, y otras. Las acciones para abordar las oportunidades también pueden incluir la consideración de los riesgos asociados. El riesgo es el efecto de la incertidumbre sobre el logro de los objetivos y dicha incertidumbre puede tener efectos positivos o negativos.

Una desviación positiva que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efectos positivos del riesgo tienen como resultado oportunidades. En la búsqueda de acciones para abordar riesgos, también se pueden detectar oportunidades, lo que en general es visto como el lado positivo del riesgo. Identificar esas oportunidades es parte de la gestión del riesgo.

Anexo F
(Informativo)

Buenas prácticas de seguridad de la información

La información es un recurso que, como otros activos importantes, tiene valor para una Organización y, por consiguiente, es necesario que sea 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 ciberseguridad es un conjunto de medidas de protección de la información, a través del tratamiento de las amenazas que ponen en riesgo la información que es tratada por los sistemas de información que se encuentran interconectados. Este tratamiento se puede realizar con recursos tecnológicos y análisis de vulnerabilidad.

La ciberseguridad está comprendida dentro de la Seguridad de la Información.

A nivel empresarial, se recomienda que las organizaciones que se conectan al Ciberespacio implementen un Sistema de Gestión de la Seguridad de la Información (SGSI) para identificar y gestionar riesgos relacionados con la seguridad de la información que puedan afectar al negocio. La serie de normas ISO/IEC 27000 para los sistemas de gestión de seguridad de la información provee la orientación y buenas prácticas requeridas para implementar dicho sistema. Una consideración clave para implementar un SGSI es asegurarse de que la Organización tenga un sistema para, de manera continua, identificar, evaluar, tratar y gestionar los riesgos de seguridad de la información relacionados al negocio, incluyendo la provisión de servicios en Internet, directamente a los usuarios finales o suscriptores, a cargo de un proveedor de servicios.

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 otro de los aspectos sensibles y vulnerables de toda Organización.

1. Gestión de activos

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

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.

Se recomienda incluir en dicho inventario, 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.

2. Control de acceso

Se recomienda:

a) definir las áreas críticas de acceso a los sistemas y servicios informáticos que afectan a la información sensible, indicando los usuarios autorizados.

b) 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.

c) nominar la persona nexo con las áreas que administran los servidores de cada repartición.

3. Seguridad del equipamiento

Se recomienda:

a) 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;

b) definir un emplazamiento seguro y el tipo de protección del equipamiento y servicios de apoyo según el análisis del riesgo realizado;

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

d) cuando se requiera eliminar un activo o la reutilización de equipos, definir una metodología para resguardar información durante el proceso de reutilización o eliminación segura;

e) inculcar las prácticas de escritorio y pantalla limpia;

f) definir los resguardos para la utilización de equipos y de activos, fuera de las instalaciones.

4. 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.

5. 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:

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

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

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

d. 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.

6. 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 afecte 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.

7. Ciberseguridad

Más allá de los lineamientos de seguridad de la información a tener en cuenta en los juegos de azar, es necesario pensar en la periferia de la Organización y especialmente en las partes interesadas encargadas de la Tecnología de la Información y la Comunicación que proveen servicios esenciales para el soporte al juego en línea.

De acuerdo con normas internacionales, el ciberespacio es un ambiente en donde interactúan los seres humanos, el software y los servicios que en Internet se ofrecen.
Algunos activos que se recomienda asegurar para mejorar el estado de la ciberseguridad son:

- Información
- Aplicaciones
- Red
- Internet
- Infraestructura

A continuación, una descripción de los activos que se encuentran en el ciberespacio:

1. La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información en general.

2. La seguridad de las aplicaciones es un proceso realizado para aplicar los controles y las mediciones para las aplicaciones, con el fin de gestionar el riesgo. Los controles y las medidas pueden ser implementados sobre la propia aplicación (sus procesos, componentes, software y resultados), sus datos (datos de configuración, datos del usuario, datos de la Organización), y sobre todas las tecnologías, los procesos y los actores que participan en el ciclo de vida de la aplicación.

3. La seguridad de la red tiene que ver con el diseño, la implementación y la operación de redes, para el logro de los fines de la seguridad de la información en las redes, entre las organizaciones, y entre organizaciones y usuarios.

4. La seguridad en Internet tiene que ver con la protección de los servicios relacionados con Internet y los sistemas TIC y las redes, como una extensión de seguridad de red de las organizaciones. La seguridad en Internet se relaciona también con la disponibilidad y la fiabilidad de los servicios de Internet.

5. La seguridad de la infraestructura se ocupa de la protección de los sistemas que son proporcionados u operados por proveedores de infraestructura crítica, como la energía eléctrica, telecomunicaciones y los servicios de agua. Se busca que estos sistemas y redes estén protegidos y sean resilientes ante los riesgos de seguridad de la información, los riesgos de seguridad de red, los riesgos de seguridad en Internet, así como los riesgos de la ciberseguridad.

A continuación, se presenta cada uno de los dominios de la norma:

- Aplicación
- Servidores
- Usuario final
- Ingeniería social

La convergencia de las TIC ha propiciado diferentes tipos de ataques cada vez más sofisticados

- *Hacking*
- *Phishing*
- *Spyware*

Los principales lineamientos o buenas prácticas de ciberseguridad a seguir son:

Controles de aplicaciones
- Contar con políticas empresariales
- Manejo de sesiones web
- Evitar ataques de *scripting*
- Revisar código
- Servicios autenticados y seguros

Controles de servidor
- Usar estándares de configuración
- Actualizaciones periódicas
- Generar registros (logs)
- Uso de antivirus y *antispyware*
- Análisis de vulnerabilidades
- Revisiones periódicas de *malware*

Controles de usuario final
- Instalar actualizaciones (OS, sistema operativo por sus siglas en inglés)
- Aplicaciones actualizadas
- Uso de antivirus y *antispyware*
- Bloqueadores de scripts
- Bloquear ventanas emergentes
- Filtros de *phishing*
- Uso de *firewall* personal y Sistema de detección de intrusiones (IDS) en el host (HIDS)

Controles de Ingeniería social
- Políticas de seguridad
- Clasificación de la información
- Sensibilizaciones
- Controles técnicos aplicables
- Procedimientos

Se recomienda que se extienda la aplicación de las buenas prácticas de este anexo a los proveedores de servicios para el juego en línea o los proveedores que tengan alguna función crítica dentro del ciberespacio de la Organización.

NOTA. Ver más información en la norma ISO/IEC 27032:2012 - *Information technology - Security techniques - Guidelines for cybersecurity.*

8. Seguridad de los recursos humanos

8.1 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.

Se recomienda que el personal reciba un detalle de cuáles serán sus responsabilidades y las de la Organización con relación a la seguridad de la información, y registrar la comprensión como información documentada.

8.2 Durante el empleo

Se recomienda que la máxima autoridad garantice la concientización, educación y capacitación en seguridad de la información a través de actividades periódicas, así como las responsabilidades y la forma de cumplimiento. Asimismo, se recomienda incluir actualizaciones regulares en las políticas y procedimientos organizacionales, que sean pertinentes a su tarea.

En el caso de haber incidentes significativos, se recomienda realizar una concientización 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, mal uso de los equipos que inhabiliten los mismos, técnicas de seguridad lógica, encriptado, etc.

8.2.1 Proceso disciplinario: se recomienda que la máxima autoridad defina un 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 propia de cada Organización.

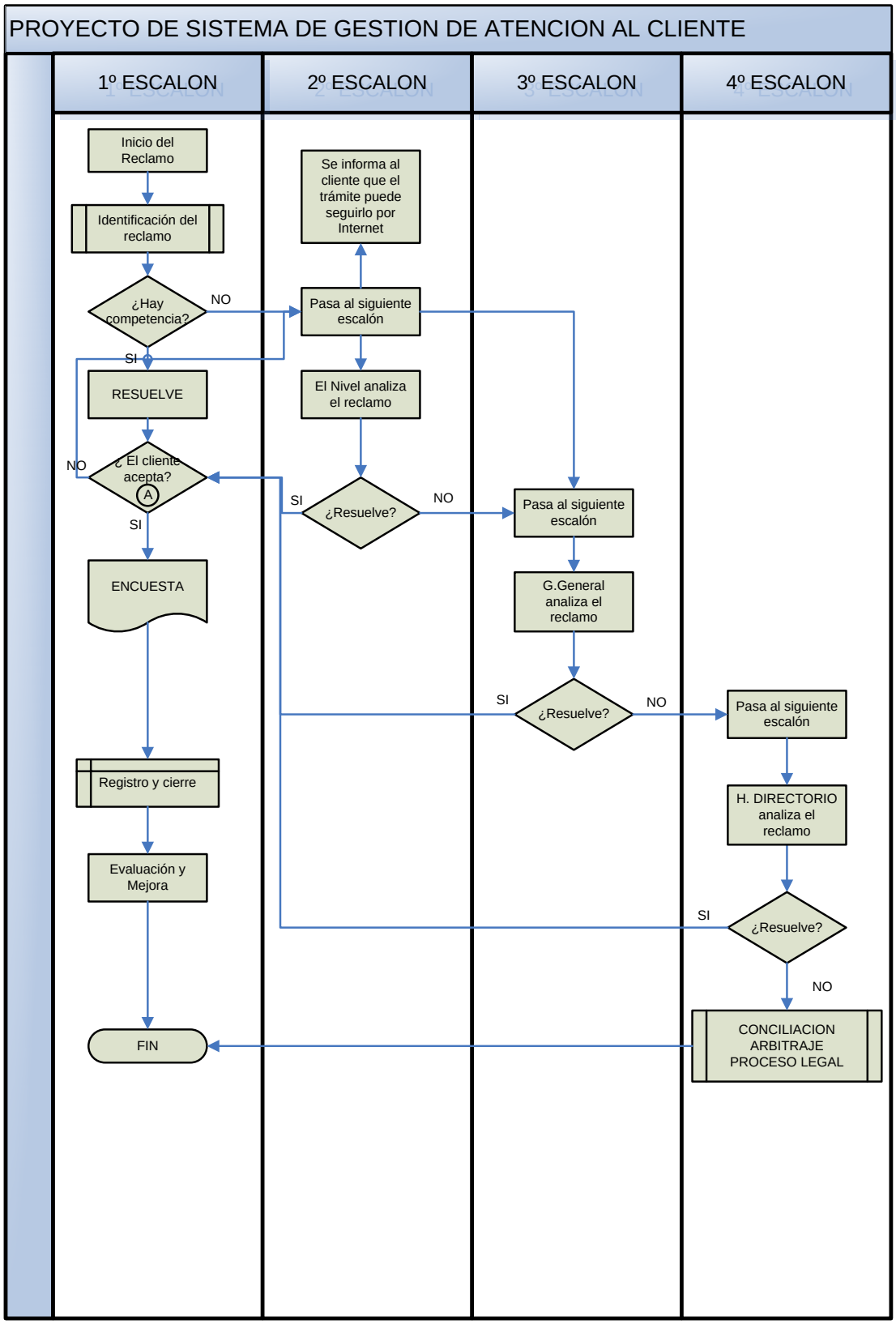
8.3 Desvinculación o cambio de puesto

En el caso de que se produzca una desvinculación del personal o un cambio de puesto, se recomienda que la máxima autoridad competente y la persona afectada, dejen constancia por medio de un acta, de las responsabilidades y las obligaciones de seguridad de la información que continúen siendo vigentes, luego de dicha desvinculación o cambio de puesto.

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

Anexo G
(Informativo)

Flujograma de un proceso tipo de Atención al cliente



Anexo H
(Informativo)

Documentación sugerida a los efectos de la incorporación de dispositivos de Juegos Electrónicos

ENTIDAD	DATOS	DOCUMENTACIÓN
NUEVOS PROVEEDORES	Antecedente del fabricante Experiencia del fabricante Manifestación de la vida útil de las máquinas	Declaración jurada del Fabricante
MÁQUINA	Marca Modelo Serie Gabinete Presentación (video – rodillo – híbridas – otras) Fecha de fabricación o re fabricación	Certificado emitido por el fabricante
	Especificaciones, características e instrucciones	Manual del gabinete
	Número de despacho de Aduana	Constancia de nacionalización (N° de despacho)
	Identificación unívoca de la máquina (marca, modelo y/o N° de serie)	
	Titularidad (propias o alquiladas) Marca, modelo, tipo, identificación	a) Factura de compra b) Copia del contrato de alquiler, leasing, etc.
JUEGO	Nombre del juego Porcentaje de retorno teórico Código de identificación (Game Prom) Firma digital y método (algoritmo)	Certificado emitido por Laboratorio Acreditado por OAA
	Tablas de Pago Línea de apuestas Apuesta máxima	Par Sheet del fabricante
	Idioma del juego	Par Sheet del fabricante y/o NOTA emitida por el fabricante
	Guía completa de instrucciones sobre uso y tabla de pagos en idioma Español	Manual del Juego

ENTIDAD	DATOS	DOCUMENTACIÓN
SISTEMAS OPERATIVOS	Fabricante Código de identificación y versión (Data Prom) Descripción y Detalles Firma digital y método (algoritmo)	Certificado emitido por Laboratorio Acreditado por OAA
	Denominación de contadores electrónicos y mecánicos Fórmula de Cálculo del NETWIN Idioma de auditoría Listado de eventos de máquina	NOTA emitida por el fabricante
POZOS PROGRESIVOS	Firma digital y método (algoritmo)	Certificado emitido por Laboratorio Acreditado por OAA
	Tipo Topes Especificaciones técnicas Porcentaje de incremento	Certificado emitido por Laboratorio Acreditado por OAA y/o Par Sheet del Fabricante
	Condiciones de explotación	
	Topes configurados (mínimo y máximo) Porcentaje de incremento	DDJJ del Concesionario o quien explota
	Controladores externos de pozos progresivos	
	Firma digital y método (algoritmo)	Certificado emitido por Laboratorio Acreditado por OAA
	Tipo Topes Especificaciones técnicas Porcentaje de incremento	Certificado emitido por Laboratorio Acreditado por OAA y/o Par Sheet del Fabricante

Certificado del fabricante: información emitida por el fabricante con carácter de declaración jurada.

Data Prom: código de identificación de un Sistema Operativo. Esta terminología puede variar en función a cada fabricante.

Firma Digital: es el algoritmo de resumen que, a partir de una entrada, que puede ser un texto o un archivo, permite crear una salida alfanumérica de longitud normalmente fija, que representa un resumen de datos de entrada y que solo puede volver a crearse con esos mismos datos. La firma digital proporciona una herramienta para detectar la alteración y/o manipulación del contenido de los datos que generaron la Firma Digital del software originalmente firmado.

Game Prom: código de identificación de un Juego. Esta terminología puede variar en función a cada fabricante.

Par Sheet: documentación con contenido técnico de propiedad exclusiva del fabricante.

Anexo I
(Informativo)

Equipo de trabajo

Integrante:	Representó a:
Sr. Román ASEF	LOTERÍA PROVINCIAL DE CÓRDOBA SOCIEDAD DEL ESTADO (LPCSE)
Téc. Fernando BOSELLI	INSTITUTO PROVINCIAL DE JUEGOS DE AZAR EN NEUQUÉN (IJAN)
Lic. Ayelén CASTELLS	LOTERÍA DE LA CIUDAD DE BUENOS AIRES (LOTBA)
Arq. Jesús GIORDANO	LOTERÍA PROVINCIAL DE CÓRDOBA SOCIEDAD DEL ESTADO (LPCSE)
Abg. Maximiliano MONTANI	INSTITUTO DE AYUDA FINANCIERA A LA ACCIÓN SOCIAL ENTRE RÍOS (IAFAS)
Ing. Rodrigo MORENO	INSTITUTO PROVINCIAL DE JUEGOS Y CASINOS DE MENDOZA (IPJyC)
Sr. Juan PETRUSSI	INSTITUTO DE AYUDA FINANCIERA A LA ACCIÓN SOCIAL ENTRE RÍOS (IAFAS)
Sr. Ricardo RODRÍGUEZ	INSTITUTO PROVINCIAL DE JUEGOS Y CASINOS DE MENDOZA (IPJyC)
Sr. Carlos VILLAR	INSTITUTO PROVINCIAL DE JUEGOS DE AZAR EN NEUQUÉN (IJAN)
Lic. Luis ZANAZZI	ASOCIACIÓN DE LOTERÍAS ESTATALES DE ARGENTINA (ALEA)
Ing. Silvina SUZUKI	IRAM

Asesoramiento técnico específico

Integrante:	Representó a:
Lic. Patricia BARBIERI	INSTITUTO PROVINCIAL DE LOTERÍA Y CASINOS SE DE MISIONES (IPLyC SE)
Abg. Carolina GALTIERI	LOTERÍA DE LA CIUDAD DE BUENOS AIRES (LOTBA)
Lic. Wanda LEITNER	INSTITUTO PROVINCIAL DE JUEGOS DE AZAR EN NEUQUÉN (IJAN)
Dr. Raúl QUIROGA	LOTERÍA PROVINCIAL DE CÓRDOBA SOCIEDAD DEL ESTADO (LPCSE)
Abg. Pablo ROUVIER	LOTERÍA DE LA CIUDAD DE BUENOS AIRES (LOTBA)
Téc. Sebastián VIVOT	LOTERÍA DE LA CIUDAD DE BUENOS AIRES (LOTBA)

ALEA

Sede Permanente Córdoba:
27 de Abril 252 - 1er Piso - Of. 42
X5000 AEF / Córdoba
Tel: +54-351 4216076 - 4216310 - 4239707

Centro de Reuniones (CABA):
Hipólito Yrigoyen 1180 - 8º Piso
C1086AAT - CABA.
Tel: +54-11 43814600 - 43813983

info@alea.org.ar
webmaster@alea.org.ar
www.alea.org.ar

IRAM

Casa Central:
Perú 556
C1068AAB / Buenos Aires
República Argentina

iram-iso@iram.org.ar
www.iram.org.ar
Tel: +54 11 4346 0600/01