ANEXO I

REGLAMENTO TÉCNICO DE JUEGO ON LINE
EN LA PROVINCIA DE BUENOS AIRES

ÍNDICE

3.6.3 Controles de la lógica del juego.

3.7 **Terminales de usuario y terminales físicas de carácter accesorio.**

3.7.1 Identificación de terminales.

3.7.2 Funcionalidad de la terminal.

3.7.3 Terminales de usuario.

3.7.3.1 Instalación de componentes en la terminal de usuario.

3.7.3.2 Desventaja por la calidad de la conexión.

3.7.3.3 Información sobre la calidad de la conexión.

3.7.3.4 Funcionalidad reducida para ciertas terminales de usuario.

3.7.3.5 Recursos mínimos de la terminal.

3.8 **Sesión de usuario.**

3.8.1 Desconexión por inactividad.

3.8.2 Registro de las sesiones de usuario.

3.9 **Interfaz gráfica**

3.9.1 Datos del juego

3.9.2 Datos del participante.

3.9.3 Premios.

3.9.4 Juegos de cartas.

3.9.5 Simulación de elementos de la vida real.

3.9.6 Interfaz gráfica de terceros.

3.10 **Juegos**

3.10.1 Integración con proveedores y en redes de juego con otros operadores.

3.10.2 Deshabilitación de un juego o de una sesión de usuario.

3.10.3 Juego incompleto.

3.10.4 Juego automático.

3.10.5 Repetición de la jugada.

3.10.6 Jugadores virtuales.

3.10.7 Juego «en vivo».

3.10.8 Pozos, pozos progresivos, y premios adicionales.

3.10.9 Juegos a través de canales de comunicación «en diferido».

4. **SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**

4.1 Requisitos de Seguridad

4.2 Componentes Críticos

4.3 Gestión de la seguridad del sistema técnico de juego

4.4 Gestión de riesgos

ANEXO I: REGLAMENTO TÉCNICO DE JUEGO ON LINE EN LA PROVINCIA DE BUENOS AIRES

Documento que desarrolla las especificaciones técnicas de juego, trazabilidad y seguridad que deben cumplir los sistemas técnicos de juego habilitados en la Provincia de Buenos Aires y sus mecanismos de control.

1. **DISPOSICIONES GENERALES**

1.1 **Objeto**

La presente tiene por objeto el desarrollo de las especificaciones técnicas que deben cumplir los sistemas técnicos de juego de los operadores habilitados en la Provincia de Buenos Aires, de regulación del juego y los mecanismos de control de los mismos.

La infraestructura técnica de los operadores garantizará la supervisión por parte del Instituto Provincial de Lotería y Casinos (en adelante, IPLYC) de las operaciones de juego realizadas, la obtención de los registros generados durante su desarrollo y la generación y puesta a disposición de cualquier otra información que sea considerada relevante.

A estos efectos se establecen las especificaciones para el almacenamiento de los registros de operaciones de juego y su trazabilidad, en el formato y de conformidad con el procedimiento establecido por el IPLYC. Asimismo, se detallan los requerimientos de seguridad de los sistemas de información utilizados para el juego, tanto física como lógica, así como los de organización y gestión de los mismos.

1.2 **Definiciones**

A los efectos de esta reglamentación, los términos técnicos que en ella se emplean tendrán el sentido que se establece en el presente apartado.

1.2.1 Sistema técnico de juego

Se entiende por sistema técnico de juego el conjunto de equipos, sistemas, terminales, instrumentos y material software empleado por el operador para la organización y desarrollo de la actividad de juego. El sistema técnico de juego soporta todas las operaciones necesarias para la organización y desarrollo de la actividad de juego, así como la detección y el registro de las transacciones correspondientes entre los jugadores y el operador.

Los elementos básicos del sistema técnico de juego son la Unidad central de juegos y el Sistema de Reportes y Control.

1.2.2 Unidad Central de Juegos

Se entiende por Unidad Central de Juegos el conjunto de elementos técnicos necesarios para procesar y gestionar las operaciones realizadas por los participantes en los juegos.

Forman parte de la Unidad Central de Juegos, la plataforma de juegos y el software de los juegos.

1.2.3 Plataforma de juego

Se entiende por plataforma de juego la infraestructura de software y hardware que constituye la interfaz principal entre el participante y el operador de juego.

La plataforma de juego ofrece al jugador las herramientas necesarias para abrir o cerrar su cuenta de juego, grabar, editar la información de su perfil, depositar o retirar fondos de su cuenta de juego o visualizar el detalle o un resumen de los movimientos de su cuenta.

La plataforma de juego incluye cualquier elemento técnico que muestre información relevante al participante sobre los juegos ofrecidos por el operador, así como cualquier software cliente que el participante tenga que descargarse e instalar en su equipo para poder interactuar con la plataforma.

La plataforma de juego permite al operador gestionar el registro de usuario y la cuenta de juego de los participantes, así como las transacciones financieras de juego, informar sobre los resultados de los juegos, habilitar o deshabilitar los registros y las cuentas y establecer todos los parámetros configurables.

Forman parte de la plataforma de juegos las bases de datos de juego y la pasarela de pagos.

1.2.4 Bases de datos de juego.

Se entiende por bases de datos de juego el conjunto de almacenes lógicos en los que se registran y conservan los datos de carácter personal de los participantes en los juegos, los relativos a la totalidad de las transacciones realizadas por éstos y la información relativa a resultados de eventos o acontecimientos deportivos, coeficientes y demás datos relevantes a los efectos del desarrollo y gestión de actividades de juego.

1.2.5 Pasarela de pagos.

Se entiende por pasarela de pagos al conjunto de sistemas e instrumentos técnicos que permiten realizar las transacciones económicas entre el participante y el operador de juego y que contiene la lógica necesaria para transferir fondos desde el medio de pago empleado por el participante al operador y desde éste al participante.

1.2.6 Software de Juego.

El software de juego consiste o está formado por los módulos que permiten gestionar cada uno de los juegos, autorizar e implementar las reglas de cada uno de ellos y a los que se accede desde la plataforma de juego.

1.2.7 Generador de números aleatorios.

El generador de números aleatorios es el componente software o hardware que, mediante procedimientos que garantizan su aleatoriedad, genera los resultados numéricos que son empleados por el operador para determinar el resultado de determinados juegos.

1.2.8 Sistema de Reportes y Control

Es el sistema de seguimiento, vigilancia y control mediante reportes y/o consultas a una réplica de la base de datos, del operador con los datos del sistema de juegos de producción.

El Sistema de Reportes y Control está compuesto por la Réplica de la Base de Datos (RBD).

1.2.9 Réplica de la Base de Datos (RBD)

La base de datos de réplica es la que contiene los datos de monitorización y control replicados desde la base de datos de producción del operador y a la que en todo momento puede acceder el IPLYC.

1.2.10 Registro de usuario

Se entiende por registro de usuario al proceso de registro único que permite al participante acceder a las actividades de juego de un determinado operador y en la que se recogen, entre otros, los datos que permiten la identificación del participante y los que posibilitan la realización de transacciones económicas entre éste y el operador de juego.

1.2.11 Cuenta de juego

Se entiende por cuenta de juego a la cuenta abierta por el participante, de forma vinculada a su registro de usuario, en la que se cargan los ingresos de las cantidades económicas destinadas por éste al pago de la participación en las actividades de juego y se abonan los importes de los premios obtenidos por la participación.

2. **REGISTRO DE USUARIO, CUENTA DE JUEGO Y MEDIOS DE PAGO**

2.1 **Registro de usuario**

Un participante debe registrarse para poder participar en el juego. La unificación de los registros de usuario de los operadores conformará el registro de jugadores.

2.1.1 Proceso

El registro de usuario queda comprendido tanto por la etapa de verificación de los datos aportados por el participante, así como por la etapa de identificación del mismo.

2.1.2 Verificación

El registro de usuario debe verificar los datos del participante garantizando que no se encuentra incluido como persona inhabilitada para jugar. Una persona está inhabilitada para jugar cuando se encuentre comprendida en las prohibiciones subjetivas del Art. 150º de la Ley Nº 15.079.

Asimismo, la verificación del usuario implicará dar cumplimiento al Art. 161º del Anexo I del Decreto Reglamentario de la Ley Nº 15.079, referido a los Participantes – Jugadores.

2.1.3 Identificación

El operador deberá garantizar la identidad del participante utilizando uno de los procedimientos que a continuación se detallan:

- Cuando el medio de pago a utilizar por el participante pueda suministrar la información necesaria para garantizar la identidad de la persona, quedará identificada de forma automática.
- Cuando el medio de pago a utilizar por el participante no permita identificar a la persona, deberán utilizarse otros métodos manuales de identificación, que deberán ser aprobados por el IPLYC.

El operador deberá contar con un servicio de identificación de los datos de los participantes suficiente para determinar la veracidad del registro. Este servicio podrá ser prestado por terceros que presten servicios profesionales de verificación de identidad.

2.1.4 Acceso a juego

Un participante podrá comenzar a jugar en la plataforma una vez superado con éxito el proceso completo de registro de usuario.

2.1.5 Acceso del operador a bases de datos con información de los participantes.

El IPLYC establecerá los mecanismos y procedimientos necesarios para el acceso a la información necesaria a los fines de realizar el registro del usuario.

Asimismo, el IPLYC proporcionará a los operadores de un servicio online de consulta del Registro de autoexclusión de la Provincia de Buenos Aires, así como de los Planes sociales que corresponda.

2.1.6 Responsabilidad

El operador es responsable del proceso de registro de usuario, así como de la verificación de la veracidad de los datos de los participantes almacenados en sus bases de datos.

2.1.7 Información del participante

El registro de usuario recogerá los datos definidos en el Art.162º de la Ley Nº 15.079 así como los que se definen a continuación y a futuro determine el IPLYC:

- Nombre y apellido
- Tipo y Número de Documento
- Dirección donde se domicilia
- CUIL/CUIT

- Fecha Nacimiento
- Sexo
- Dirección de correo electrónico
- Teléfono (Opcional)

Asimismo, deberá recoger aquellos otros datos que permitan la realización de las transacciones económicas y las que el operador de juego considere necesarias para llevar a cabo la actividad.

2.1.8 Activación del registro de usuario y limitación en la participación

El operador dispondrá de un procedimiento documentado de registro y activación de usuario que recogerá los requisitos de identificación y limitación de la participación, establecidos en la Ley Nº 15.079 y normativas complementarias.

2.1.9 Registro y resguardo de información

Los operadores deberán registrar y conservar la totalidad de las gestiones, consultas y requerimientos que hubieran realizado para la verificación e identificación de los datos aportados por los solicitantes, así como cuantos documentos hubieran recibido o empleado con este fin. Asimismo, deberán dejar constancia de la fecha, hora y minuto de estas transacciones.

Esta información se resguardará junto a los datos correspondientes al registro de usuario por un plazo no menor a 5 (cinco) años luego del cierre de la cuenta de usuario.

2.1.10 Verificaciones posteriores al registro

El operador establecerá los procedimientos y mecanismos necesarios para garantizar que un mismo participante no dispone de varias cuentas de usuario en su plataforma.

El operador es responsable de la veracidad y del contraste periódico de los datos que figuren en sus registros de usuario, en los términos establecidos por la presente.

Revisión periódica de los registros de usuario: El operador establecerá un procedimiento técnico, que permita la revisión periódica de los registros de usuario en los términos establecidos en la presente.

La periodicidad de dicho contraste deberá no ser menor de 2 veces mensuales y para la verificación de autoexclusión tanto temporal como definitiva este contraste deberá realizarse en cada inicio de sesión.

2.1.11 Suspensión y cancelación de registro de usuario

En caso de que un registro de usuario ya no sea válido, se deberá suspender la cuenta.

El operador conservará los datos de los registros de usuario cancelados. En el registro se detallará el momento de cancelación y el motivo.

2.2 **Cuenta de juego**

2.2.1 Identificación para el acceso

Una vez que se haya completado el proceso de registro se asignará al participante un identificador único de usuario. Los accesos al registro de usuario y a la cuenta de juego deben estar reservados en exclusiva al participante titular del registro.

2.2.2 Suspensión por inactividad

El operador deberá suspender la cuenta de juego de un participante cuando el tiempo de inactividad supere los 12 (doce) meses.

2.2.3 Suspensión cautelar de la cuenta de juego.

El operador podrá, previa notificación al IPLYC, suspender cautelarmente al participante que haya tenido, a su juicio, un comportamiento colusorio o fraudulento o que haya permitido la utilización de su cuenta de juego por terceros, hasta que se demuestren los hechos.

2.2.4 Cierre de cuenta de juego.

Una vez cumplidos los 12 (doce) meses de suspendida la cuenta, se procederá al cierre de la misma. Asimismo, el IPLYC podrá solicitar el cierre de cuentas de juego con anterioridad a dicho plazo. Si hubiere saldo en la cuenta será remitido al IPLYC a fin de que se destine al cumplimiento de los fines de dicho Organismo.
Cuando una cuenta de juego fuese cerrada, el participante deberá volver a registrarse para volver a ingresar a la plataforma.

2.2.5 Registro de la suspensión/cierre de la cuenta de juego.

El operador mantendrá un registro de estos usuarios. El registro incluirá la fecha y el motivo del mismo.

2.2.6 Funcionalidad de la cuenta de juego.

Cuando el operador gestione fondos depositados por los participantes deberá utilizar una cuenta de juego para mantener el registro contable de las operaciones.

Cada registro de usuario tendrá vinculada una única cuenta de juego. En la cuenta de juego se reflejarán todas las transacciones que supongan una alteración del saldo del participante, tales como los depósitos realizados por el participante, los cargos por el importe de la participación en los juegos, los abonos por los bonos ofrecidos por el operador y los premios obtenidos por el participante.

La cuenta de juego estará denominada en moneda de curso legal argentina. En caso de ser necesario, y para la obligatoriedad en el correcto desarrollo de algún juego en particular, el operador deberá informar al IPLYC, que mecanismos de conversión de moneda utilizará, para obtener la autorización correspondiente.

Las correcciones, anulaciones o ajustes se reflejarán en apuntes independientes, sin que, en ningún caso, se pueda borrar la transacción original corregida, anulada o ajustada.

Deberán registrarse las apuestas que una vez formalizadas hayan sido anuladas por parte del operador, indicándose de forma clara el motivo de su anulación.

Los apuntes contables en la cuenta de juego permitirán conocer de forma clara la naturaleza de la transacción y el momento en que se realiza.

2.2.7 Autenticación del usuario y política de contraseñas

El acceso al registro de usuario deberá contar con mecanismos de seguridad para autenticar al usuario en la plataforma.

La autenticación del usuario podrá realizarse mediante la utilización de contraseñas. La política de contraseñas deberá contemplar, los siguientes requisitos mínimos:

• Deberá establecerse, por defecto o por el participante, una contraseña inicial de usuario.

• Durante el proceso de definición de la contraseña de usuario, el participante deberá ser informado sobre buenas prácticas en la elección de contraseñas seguras.

• La longitud mínima de la contraseña será de ocho caracteres o dígitos, e incluirá elementos de tres de los siguientes grupos: números, letras minúsculas, letras mayúsculas y otros símbolos.

• La contraseña no podrá contener ninguno de los siguientes datos: el nombre de usuario, el seudónimo, el nombre o apellidos o la fecha de nacimiento del participante.

• Deberá ofrecerse al usuario un recordatorio de cambio de contraseña con una frecuencia mínima anual, aunque no es obligatorio que el usuario realice el cambio.

• El mecanismo de identificación mediante usuario y contraseña deberá bloquearse si se producen en un mismo día más de cinco intentos de acceso erróneos. El operador podrá establecer un límite inferior a este requisito.

El sistema del operador estará diseñado para requerir la autenticación del participante ante cada inicio de sesión de usuario, y en el caso de uso de contraseñas, la introducción de la contraseña. El sistema no utilizará cookies u otros mecanismos para evitar la autenticación del usuario o la introducción de la contraseña.

El operador podrá proporcionar otros métodos de autenticación del usuario siempre que ofrezcan un nivel de seguridad mayor que el de la contraseña.

El sistema conservará registro de todos los intentos de acceso, ya sean con o sin éxito, para su posterior auditoría.

El operador dispondrá de un procedimiento documentado de seguridad de acceso del usuario en el que se describirá:

• El modo en que se protege el registro de usuario de accesos no autorizados.

• La existencia o no de un medio indirecto, o asistido por personal del operador, de acceder al registro de usuario, previa superación de preguntas antes de conceder el acceso o renovarlo.

• El tratamiento de identificadores de usuario o contraseñas perdidos.

• El operador dispondrá de un procedimiento para detectar las cuentas inactivas durante un tiempo razonablemente prolongado y requerirá un nivel de autenticación superior al normal o verificaciones adicionales a través del servicio de atención al cliente, antes de permitir reanudar la actividad de juego, especialmente las extracciones de fondos. El umbral de tiempo de inactividad para solicitar un nivel de autenticación o verificación adicional definido por el operador no podrá ser superior a seis (seis) meses.

• Asimismo, el operador dispondrá de un procedimiento para detectar dentro de lo razonable accesos no autorizados a la cuenta de los participantes, intentos de suplantación de identidad o acceso a sus datos personales.

• Adicionalmente, el operador dispondrá de un procedimiento para detectar cambios bruscos en el comportamiento de un participante, y en particular del importe de los depósitos o extracciones, e iniciará alguna acción para prevenir que la cuenta de juego pueda estar siendo accedida por un tercero.

2.2.8 Registro de acceso

Cuando un usuario inicie o cierre sesión se deberá mantener información del evento. Del mismo se debe resguardar:

- Cuenta de juego
- Fecha y hora (inicio/cierre)
- IP
- Dispositivo cliente
- Localización de la terminal de usuario

2.2.9 Información al participante sobre su última conexión.

Una vez autenticado el usuario, el sistema le mostrará la fecha y hora de su último acceso.

2.2.10 Opciones para el usuario

Historial: El participante dispondrá en tiempo real del saldo de la cuenta de juego y del registro de todas las participaciones o jugadas efectuadas, al menos, en los últimos 30 (treinta) días.

El participante, podrá consultar en tiempo real un resumen, al menos por año natural, de los movimientos en su cuenta de juego que incluya: el saldo inicial, la suma de los depósitos realizados, la suma de las extracciones realizadas, la suma de los cargos por el importe de la participación en los juegos, la suma de los abonos por los eventuales bonos aceptados por el participante y por los premios obtenidos, y el saldo final.

El sistema estará diseñado para poder emitir en tiempo real y previa solicitud del participante un documento que incluya la información descrita en el párrafo anterior y en el que consten los datos de identificación del operador y del participante. El operador dispondrá de un procedimiento que permita a aquellos usuarios que no dispongan de cuenta de juego activa en el operador en el momento de la consulta, obtener dicha información a través de los canales de atención a los usuarios del operador. Ante esta solicitud del participante, una vez realizadas las comprobaciones de identidad necesarias, el operador deberá poner a disposición del usuario el documento solicitado en el plazo máximo de 10 (diez) días.

Configuración de la sesión: El usuario podrá configurar límites de tiempo de sesión y crédito para jugar de acuerdo al apartado 6 1) del presente Anexo. Está configuración deberá diferenciarse tanto para avisos, así como cierre de sesión automático. Las modificaciones a dichos límites deberán resguardarse junto al registro de usuario.

En caso de alcanzar el límite de tiempo o de crédito estando en proceso de un juego no finalizado, el usuario podrá optar por continuar el mismo o retirarse, pero no deberá poder iniciar otro proceso de juego.

El IPLYC podrá solicitar establecer límites máximos según lo requiera.

Ofertas promocionales: Si las condiciones de las ofertas promocionales establecieran una cantidad a acumular, por ejemplo, de puntos, el participante deberá poder consultar los puntos que ha acumulado o los que le restan para cumplir las condiciones.

2.2.11 Saldo del usuario

Unidades de la cuenta de juego: la unidad monetaria de la cuenta de juego es la moneda de curso legal argentina.

El operador puede emplear otras unidades como puntos de bonificación («bonus») u otros. La plataforma registrará el saldo y los movimientos expresados en cada una de las unidades. Asimismo, el operador deberá informar al IPLYC, el mecanismo de conversión de moneda autorizado.

2.2.12 Prohibición de transferencias entre participantes.

El operador establecerá los procedimientos técnicos necesarios que impidan las transferencias entre cuentas de juego asociadas a diferentes registros de usuario.

2.2.13 Procedimiento de control de los depósitos de los participantes.

Las obligaciones del operador en relación con los fondos de los participantes deben cumplimentar con la existencia de un procedimiento que permita garantizar su correcto funcionamiento.

2.2.14 Límites de depósito y tiempo de juego.

El operador mantendrá un registro con las modificaciones en los límites de depósito y tiempo de juego detallada por registro de usuario. El registro incluirá la fecha y el motivo de la modificación. Deberá quedar registrado si la modificación fue solicitada por el jugador o establecida por el operador.

2.2.15 Saldo acreedor.

Sin perjuicio de otras limitaciones a la participación, si no existe suficiente saldo disponible en la cuenta de juego en el momento en que el jugador desee realizar una participación en el juego o una apuesta, la participación en el juego deberá ser rechazada.

En consecuencia, ninguna cuenta de juego puede presentar saldo acreedor como consecuencia de haberse permitido la participación en el juego sin existir saldo suficiente.

2.3 **Medios de pago**

2.3.1 Registro de las operaciones de pago y cobro.

El operador deberá conservar o estar en disposición de obtener el apunte detallado de cada operación de depósito o retirada junto con toda la información asociada a cada operación.

2.3.2 Transferencia de fondos.

El operador establecerá un procedimiento para ordenar al medio de pago que corresponda la transferencia de fondos en un plazo máximo de 48 horas. Este procedimiento deberá prever que en caso excepcional de no cumplirse el plazo referido deberá ser previamente notificado al IPLYC.

2.3.3 Procedimiento de control de las operaciones de pago y cobro.

El operador implantará un procedimiento de contraste de las operaciones de pago y cobro respecto a los apuntes en la cuenta de juego o en el software de juego, que incluirá:

• La cuenta de juego asociada a registro de usuario en estado diferente a activo no realizan movimientos indebidos.

• La verificación de que los importes de depósitos y extracciones se corresponden con los importes de operaciones realizadas a través de los medios de pago.

• La verificación de que no existen depósitos realizados por los participantes por encima de los límites de depósito que tuviera fijados cada uno de ellos.

• La verificación de que las extracciones se ordenan en un plazo máximo de 48 horas, a excepción de las causas previstas excepcionalmente y que hubieran sido previamente notificadas al IPLYC.

El procedimiento se ejecutará con periodicidad mínima mensual.

2.4 **Protección de datos personales**

2.4.1 Protección de datos

Los operadores establecerán los procedimientos técnicos adecuados para mantener la privacidad de los datos de los participantes de conformidad con la Ley Nº 25.326.

Los operadores deberán asimismo implantar sobre los ficheros y tratamientos las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos y dar cumplimiento al deber de secreto impuesto por dicha normativa.

2.4.2 Política de privacidad

El operador publicará en la plataforma de juego su política de privacidad.

Para completar el proceso de registro de usuario, el participante deberá dar su consentimiento a la política del operador. La plataforma registrará la aceptación del participante y el contenido de la política de privacidad o un enlace al texto de la misma, cuyo contenido deberá ser autorizado por el IPLYC.

Cualquier modificación posterior de la política de privacidad requerirá su comunicación al usuario y su aceptación.

El operador dispondrá de un plan técnico y operativo para asegurar la privacidad de los datos de los usuarios.

3. **JUEGO**

3.1 **Reglamentación básica del juego**

El operador ofrecerá juegos y modalidades de conformidad con el Art. 147º del Anexo I del Decreto Reglamentario de la Ley Nº 15.079 y la Regulación Básica de Juegos y Apuestas establecida por el IPLYC.

Los operadores deberán implantar en su sistema de juego los procedimientos necesarios para cumplir los requisitos establecidos en la reglamentación básica de los juegos y, en particular, los que se detallan a continuación:

• Reglas particulares del juego.

• Reclamos de los participantes.

• Obligaciones de información a los participantes.

• Promoción de los juegos.

• Canales y medios de participación.

• Objetivo del juego.

• Participación en el juego y límites a la participación.

• Desarrollo del juego, determinación y asignación de los premios.

• Formalización de apuestas o jugadas y supuestos de anulación y aplazamiento.

• Pago de premios.

El operador implantará un procedimiento, que ejecutará con periodicidad mínima mensual, mediante el que verificará que su oferta de juego se adecua con la normativa vigente, que las modalidades y variantes dentro de cada tipo de juego son conformes a la normativa vigente en cada momento, así como que se utilizan las versiones de software homologadas.

El operador conservará un registro de los juegos activos en cada momento, en el que se indicará el juego, la modalidad o variante, en su caso, el nombre comercial y la versión homologada.

3.2 **Redirección dominio**

El operador establecerá procedimientos y mecanismos para garantizar que todas las conexiones realizadas por usuarios registrados en la plataforma, hacia un dominio que sea propiedad o esté controlado por el operador de juego, su matriz o sus filiales se dirijan a un sitio web con nombre de dominio bajo la zona especial que designe el IPLYC.

Para ello, el operador deberá implantar medidas que le permitan, en la medida de lo posible, detectar y evitar conexiones a través de tecnologías de red cuyo fin sea ocultar la dirección IP del jugador.

El operador deberá disponer de un procedimiento que permita contrastar la geolocalización de la IP del jugador, con su país de residencia y, en su caso, los medios de pago utilizados, con el fin de detectar posibles fraudes por parte del jugador.

3.3 **Porcentaje de retorno al participante**

El operador determinará para cada juego, modalidad o variante, el valor o rango de valores esperados para el porcentaje de retorno, respetando los valores de la normativa vigente.

El operador implantará un procedimiento que permita garantizar el correcto funcionamiento del retorno esperado al participante, mediante el que se verifique con periodicidad mínima mensual que el porcentaje de retorno al participante obtenido en cada uno de los juegos, modalidades o variantes, se corresponde con el valor o rangos esperados.

En los casos en que detecten desviaciones significativas, el operador deberá desactivar los juegos afectados, modalidades o variantes, hasta que determine y subsane la incidencia. De confirmarse la existencia de un funcionamiento anormal, el operador notificará al IPLYC, indicando la causa, el periodo temporal, los jugadores e importes afectados, así como las medidas adoptadas.

En aquellos juegos donde el porcentaje de retorno pueda depender de parámetros configurables en el sistema técnico, como por ejemplo las tablas de premios, el operador conservará registro de cualquier cambio en dichos parámetros.

3.4 **Tablas de premios**

Las tablas de premios, en aquellos juegos en que existan, serán públicas y accesibles para los participantes e incluirán todas las combinaciones ganadoras posibles y una descripción del premio correspondiente a cada combinación.

La información del programa de premios deberá indicar claramente si los premios están cuantificados en unidades de cuenta, unidad monetaria o en alguna otra unidad establecida.

La información del programa de premios reflejará cualquier cambio en el valor del premio que pueda producirse en el transcurso del juego. A estos efectos, será suficiente que el operador disponga y muestre un recuadro en un lugar destacado en la interfaz gráfica del juego en el que aparezcan los referidos cambios en el valor de los premios.

Cuando existan pozos o multiplicadores de los premios que se muestren en las pantallas, deberá quedar especificado si el pozo o el multiplicador afecta al programa de premios o no.

El operador conservará registro de las tablas de premios de cada juego, de manera que estos cambios podrán ser auditados.

Las tablas de premios no podrán ser cambiadas durante el juego, excepto en aquellos casos en que este hecho esté previsto en las reglas particulares y el participante sea adecuadamente informado.

3.5 **Generador de números aleatorios (GNA)**

3.5.1 Funcionamiento del GNA.

El generador de números aleatorios deberá cumplir, como mínimo, los siguientes requisitos:

• Los datos aleatorios generados deben ser estadísticamente independientes.

• Los datos aleatorios deben estar uniformemente distribuidos dentro del rango establecido.

• Los datos aleatorios deben permanecer dentro del rango establecido.

• Los datos aleatorios generados deben ser impredecibles (su predicción debe ser irrealizable por computación sin conocer el algoritmo y la semilla).

• Las series de datos generados no deben ser reproducibles.

• Instancias diferentes de un GNA no deben sincronizarse entre sí de manera que los resultados de unos permitieran predecir los de otro.

• Las técnicas de semillado/resemillado no deben permitir la realización de predicciones sobre los resultados.

• Los mecanismos de generación deben haber superado con éxito distintas pruebas estadísticas que demuestren su carácter aleatorio.

El sistema técnico puede compartir un GNA o una instancia del mismo para uno o varios juegos si esto no afecta al comportamiento aleatorio del sistema.

3.5.2 Métodos de escalado.

Los métodos de escalado deben cumplir los requerimientos exigidos a los GNAs.

Los métodos de escalado deben ser lineales y no deben introducir ningún sesgo, patrón o predictibilidad y deben poder someterse a pruebas estadísticas reconocidas.

3.5.3 GNA hardware.

En el caso de utilizarse un GNA hardware deberá cumplir los mismos requisitos, adaptados a las características técnicas del hardware y, de existir, acreditar que el personal que lo opera no puede influir en los resultados. En los supuestos de utilización de un GNA hardware operado por personal, el operador deberá disponer de un procedimiento para minimizar los hipotéticos riesgos que pudieran llegar a afectar a la generación de resultados.

3.5.4 Fallos en el GNA.

El operador deberá implementar un sistema de monitorización del GNA que le permita detectar sus fallos, así como los mecanismos que deshabiliten el juego cuando se produzca un fallo en el GNA.

3.5.5 Resemillado del GNA.

El operador deberá disponer de un procedimiento de resemillado del GNA.

3.6 **Lógica del juego**

3.6.1 Lógica independiente de la terminal de usuario.

Todas las funciones y la lógica que resulten críticas para la implementación de las reglas del juego y la determinación del resultado deben ser generadas por la unidad central de juegos, de manera independiente a la terminal de usuario.

3.6.2 Aplicación del GNA en los juegos.

El rango de valores del GNA debe ser preciso y no distorsionar el porcentaje de retorno al participante.

El método de traslación de los símbolos o resultados del juego no debe estar sometido a la influencia o controlado por otro factor que no sean los valores numéricos derivados del GNA.

Los eventos de azar deben estar regidos exclusivamente por el generador de números aleatorios y no debe existir ninguna correlación entre unas jugadas y otras. El juego no debe descartar ningún evento de azar, excepto en aquellos casos en que esa circunstancia esté contemplada en las reglas del juego.

El juego no debe manipular los eventos de azar, ni manual, ni automáticamente, ni para mantener un porcentaje de retorno mínimo al participante.

Cuando las reglas del juego requieran que se sortee una secuencia de eventos de azar (por ejemplo, las cartas de un mazo), los eventos de azar no serán resecuenciados durante el transcurso del juego, excepto en aquellos casos en que esta circunstancia esté contemplada en las reglas del juego.

3.6.3 Controles de la lógica del juego.

El juego debe estar diseñado de manera de minimizar el riesgo de manipulación. Se adoptarán las medidas técnicas, organizativas y procedimentales que impidan comportamientos que supongan desviaciones de las reglas del juego.

El operador dispondrá de un procedimiento documentado que describa las medidas que aplica en su sistema para garantizar que:

• El juego se desarrolla de acuerdo con las reglas del juego.

• Los datos de juego se graban en el sistema.

• Los resguardos o documentos identificativos de una apuesta o participación se protegen frente a su posible manipulación.

• El sistema controla el tiempo de comercialización de apuestas o la participación. El momento en que se cierre la comercialización debe ser aquel que esté establecido en

las normas que regulan el juego y en todo caso será anterior al final del evento que desencadena el resultado del juego.

• El sistema controla el fondo de premios constituido.

• El procedimiento de determinación de ganadores funciona correctamente, y no permite introducir ganadores que no cumplan las condiciones para ser premiados o dar por no ganadores a aquellos que sí las cumplen.

• El sistema concederá los premios a los participantes que figuren en la lista de ganadores de forma efectiva.

• Todos los tipos de transacciones que puedan ser creadas durante la operación del juego, incluyendo las dedicadas a la gestión de excepciones, cambios de parámetros del sistema, anulaciones, acciones en modo manual, deberán registrarse en el sistema, junto con la correspondiente pista de auditoría.

Cualquier modificación, alteración o borrado de los datos debe dejar traza de auditoría, especialmente cuando exista intervención manual.

3.7 **Terminales de usuario y terminales físicas de carácter accesorio.**

Se consideran terminales al conjunto de elementos software y hardware que interactúan directamente con el participante.

Son terminales de usuario aquellos dispositivos finales que son proporcionados por el participante y que pueden ser elementos hardware, como la computadora personal, el teléfono móvil o smartphone, o elementos software como el sistema operativo o el navegador web.

Son terminales físicas de carácter accesorio las terminales no proporcionadas por el participante y destinadas a la interacción directa con éste. Se incluyen tanto las terminales para el autoservicio del participante, como las terminales destinadas a ser atendidos por personal del operador u otros, así como las soluciones mixtas. Estas terminales físicas sólo podrán operar con autorización previa del IPLYC.

3.7.1 Identificación de terminales.

La plataforma deberá ser capaz de identificar los diferentes tipos y versiones de terminales, y se conservará registro de los mismos. Salvo razones técnicas debidamente justificadas, la plataforma deberá registrar si el participante está utilizando una solución específica proporcionada para dispositivos móviles.

3.7.2 Funcionalidad de la terminal.

La terminal únicamente se encargará de la interacción con el participante y la presentación.

La lógica del juego o cualquier elemento de aleatoriedad deben ser realizados por la unidad central de juego de forma independiente a la terminal.

Las operaciones que realice la terminal deben tener una confirmación síncrona de la unidad central de juegos para tener la consideración de formalizadas y para extender resguardos acreditativos de apuestas o depósitos realizados.

Todas las transacciones realizadas a través de la terminal serán registradas en la unidad central de juegos y asociadas a una persona que se deberá haber autenticado previamente. Los registros permitirán identificar las transacciones realizadas desde cada terminal.

3.7.3 Terminales de usuario.

A continuación, se establecen los requisitos técnicos de aplicación a las terminales de usuario.

3.7.3.1 Instalación de componentes en la terminal de usuario.

Si el uso del sistema de juego exige la instalación de cualquier componente en el equipo del participante, se deberá requerir el consentimiento expreso del participante previo a la instalación.

3.7.3.2 Desventaja por la calidad de la conexión.

El operador está obligado a introducir en sus sistemas técnicos todos los medios posibles para tratar de reducir el riesgo de que ciertos clientes estén en desventaja frente a otros por factores técnicos que pueden afectar a la velocidad de la conexión.

El participante debe ser informado en aquellos casos en que el tiempo de respuesta pueda tener un impacto significativo sobre la probabilidad de ganar.

3.7.3.3 Información sobre la calidad de la conexión.

El sistema informará al participante acerca de la no disponibilidad de comunicación con el sistema de juego tan pronto como lo detecte.

El software de juego no debe verse afectado por el mal funcionamiento de los dispositivos de los participantes finales, a excepción de la puesta en funcionamiento de los procedimientos previstos para finalizar las partidas o juegos incompletos.

3.7.3.4 Funcionalidad reducida para ciertas terminales de usuario.

Las terminales de usuario que disponen de una interfaz gráfica más reducida que otros, (como por ejemplo los dispositivos móviles frente a las computadoras personales) podrán ofrecer algunos contenidos que no puedan visualizarse completamente como en las otras terminales. La plataforma podrá ofrecer, por razones estrictamente técnicas derivadas de las características de la terminal, distinta funcionalidad en los diferentes tipos de terminales.

El participante debe ser informado de las limitaciones de información o funcionalidad de la terminal y aplicación cliente que está utilizando, y aceptarlo de modo expreso.

El operador mitigará los riesgos derivados de la falta de información o de funcionalidad en una determinada terminal ofreciendo la misma información por otros medios.

Salvo impedimentos técnicos debidamente justificados, toda la información que aparezca en la interfaz debe aparecer también en la de una terminal. Cuando no sea posible incluir todas las informaciones o enlaces en la interfaz del juego, se ofrecerán desde un enlace, desde un menú o desde otra aplicación de la misma terminal.

3.7.3.5 Recursos mínimos de la terminal.

La plataforma no procesará los juegos de la terminal si no dispone de todos los recursos mínimos para permitir jugar sin problemas técnicos y sin desventajas.

3.8 **Sesión de usuario.**

Se denomina sesión de usuario al período de tiempo que un usuario permanece conectado al sitio web del operador, y que comprende desde la autenticación válida del usuario en el sistema hasta la desconexión del mismo.

3.8.1 Desconexión por inactividad.

El tiempo de desconexión por inactividad del usuario será como máximo de veinte minutos; transcurrido este tiempo, la plataforma debe desconectar al usuario.

Cuando el operador realice comunicaciones de carácter básicamente unidireccional donde el comportamiento esperado del usuario sea pasivo, como por ejemplo en la retransmisión de un evento deportivo en directo, podrá entenderse que el usuario sigue activo, aunque no realice ninguna acción.

Si técnicamente es posible, se informará al participante que la sesión está por concluir o se dará por terminada.

3.8.2 Registro de las sesiones de usuario.

La plataforma conservará registro de las sesiones de usuario, con detalle de los tiempos de inicio y fin de sesión de usuario, del mecanismo de autenticación utilizado por el usuario, y la causa de desconexión o inactividad.

En el caso de que la terminal pertenezca al usuario, la plataforma permitirá identificar, si técnicamente es posible, el tipo de dispositivo (PC, smartphone u otros), la aplicación/versión utilizada (navegador o aplicación concreta), y en su caso la dirección IP.

En el caso de que la terminal pertenezca a un operador, permitirá identificar el tipo y versión de la terminal, así como, si técnicamente es posible, la terminal concreta.

3.9 **Interfaz gráfica**

3.9.1 Datos del juego

El nombre del juego que el participante está jugando debe ser claramente visible en todas las pantallas asociadas.

Las instrucciones del juego deben ser fácilmente accesibles. La interfaz gráfica debe incluir toda la información necesaria para el desarrollo del juego. La función de todos los botones de acción representados en la pantalla debe ser clara.

El resultado de cada jugada deberá mostrarse, si técnicamente es posible, de forma instantánea al participante y mantenerse durante un lapso de tiempo razonable.

3.9.2 Datos del participante.

La pantalla debe mostrar el saldo actual del participante en moneda de curso legal argentina y las apuestas realizadas, unitarias y totales.

3.9.3 Premios.

La interfaz deberá indicar claramente si los premios se muestran en moneda de curso legal argentina o en créditos. No deberán alternarse diferentes representaciones que puedan confundir al participante.

Si se ofrecen premios aleatorios asociados a una jugada o apuesta, el participante debe conocer el importe máximo que puede obtener a partir de la apuesta o jugada que va a realizar.

El participante debe ser informado cuando el importe del premio aleatorio se determine en función del importe de la jugada o apuesta. Cuando el texto o los elementos gráficos anuncien un premio máximo, este premio debe poder ser conseguido mediante un único juego.

3.9.4 Juegos de cartas.

Los juegos de cartas deben cumplir que:

• Las caras de las cartas deben mostrar claramente el valor de las mismas.

• Las caras de las cartas deben mostrar claramente el palo/color de las mismas.

• Los jokers o comodines deben distinguirse del resto de cartas.

• La utilización de más de una baraja en el juego debe mostrarse claramente.

• Si las cartas son barajadas durante el juego, debe informarse claramente sobre la frecuencia con que se realiza y mostrarse el momento en que se realiza.

3.9.5 Simulación de elementos de la vida real.

Los juegos que simulan elementos de la vida real (ruletas, máquinas tragamonedas u otros), deben comportarse de la forma más parecida posible al comportamiento de dichos elementos físicos. La probabilidad de que ocurra algún acontecimiento en la simulación que afecte el resultado del juego debe ser equivalente a la del dispositivo físico en la vida real.

3.9.6 Interfaz gráfica de terceros.

Se considerará que una interfaz gráfica es de terceros cuando el operador no la ofrezca como parte de su plataforma o cuando el operador incluya un enlace a su descarga y junto al enlace esté claramente especificado que el operador no es responsable del mismo.

El operador deberá informar a los participantes que decidan utilizar una interfaz de usuario de terceros en relación con que la funcionalidad y la información que reciban pueden no ser completas.

3.10 **Juegos**

3.10.1 Integración con proveedores y en redes de juego con otros operadores.

El operador será responsable de las operaciones de juego realizadas a través de terceros o proveedores. Los sistemas técnicos de terceros o proveedores se considerarán a estos efectos parte del sistema técnico del operador y deberán cumplir las especificaciones establecidas en la normativa vigente.

El operador deberá garantizar que cualquier integración con los sistemas de otro operador se realiza de tal forma que cumpla las especificaciones establecidas en esta reglamentación.

3.10.2 Deshabilitación de un juego o de una sesión de usuario.

La plataforma debe permitir que, en circunstancias excepcionales, sea posible inhabilitar un juego completo, o sesiones de usuarios concretas, dejando registro de las actuaciones y el motivo que las originó para una posterior revisión.

3.10.3 Juego incompleto.

Un juego incompleto es aquel cuyo resultado todavía no se ha producido o, si se ha producido, el participante no ha podido ser informado de este hecho.

Ante un juego incompleto, las reglas particulares del juego determinarán la actuación de la plataforma, que podrá esperar al participante, anular el juego o seguir en el mismo hasta que sea completado.

• Si el juego incompleto se debe a una pérdida de conexión de la terminal del usuario, la plataforma mostrará el juego incompleto cuando el participante vuelva a conectarse.

• El operador deberá disponer de un procedimiento documentado de gestión de las incidencias de indisponibilidad de uno, varios o todos los componentes, que incluya las medidas técnicas asociadas. Los componentes deben realizar un autodiagnóstico, un chequeo de los archivos críticos y un chequeo de las comunicaciones entre los distintos componentes.

• Tras la recuperación, el sistema técnico de juego debe proceder a tratar los juegos en curso afectados por la interrupción.

El sistema técnico guardará registro de las interrupciones de servicio, con su inicio, duración, y servicios afectados para posterior revisión.

3.10.4 Juego automático.

Si el sistema ofrece consejos sobre estrategia de juego o funcionalidades de juego automático, tales recomendaciones o funcionalidades deben ser veraces y asegurar que se alcance el porcentaje de retorno obligatorio.

Se garantizará que el participante mantiene el control del juego cuando se proporciona la funcionalidad de juego automático. El participante podrá controlar el importe máximo del juego automático o de la apuesta máxima y el número de apuestas automáticas. El participante podrá desactivar en cualquier momento la funcionalidad de juego automático.

Cuando se use la funcionalidad de juego automático, las informaciones mostradas en pantalla (duración, elementos gráficos u otras) serán las mismas y presentarán las mismas características que cuando el juego no es automático. La interfaz mostrará adicionalmente el número de jugadas automáticas transcurridas o restantes.

La funcionalidad de reproducción automática no podrá poner en desventaja a un participante, y ni la secuencia de las partidas automáticas, ni cualquier estrategia que sea aconsejada al participante deberá resultar engañosa.

En el caso de los juegos en que intervenga simultáneamente más de un participante, todos los participantes deben ser informados y aceptar un participante que ha establecido la funcionalidad de juego automático.

3.10.5 Repetición de la jugada.

La plataforma debe proporcionar al participante la opción de repetición de la jugada, mostrándolo como una reconstrucción gráfica o una descripción inteligible que deberá reproducir todos los lances del juego que puedan tener repercusión sobre su desarrollo. La opción de repetición deberá suministrar toda la información necesaria para reconstruir las últimas diez partidas de la sesión de usuario en curso.

3.10.6 Jugadores virtuales.

3.10.6.1 Jugadores virtuales proporcionados por el operador.

El operador puede utilizar inteligencia artificial mediante jugadores virtuales, también denominados robots, si así lo permitiera expresamente la regulación del juego correspondiente.

En el caso de los juegos en que intervenga simultáneamente más de un participante, todos los participantes deben ser informados y aceptar la presencia de un jugador virtual.

Los jugadores virtuales o automáticos deberán estar identificados claramente en la interfaz.

El jugador virtual no debe tener ninguna ventaja técnica sobre los participantes, y no tendrá acceso a información que no esté al alcance de éstos.

3.10.6.2 Jugadores virtuales utilizados por participantes.

El operador puede facilitar a los participantes inteligencia artificial mediante la utilización de jugadores virtuales o robots, si así lo permite la regulación del juego correspondiente.

El operador informará sobre si permite o no el uso de jugadores virtuales o robots por parte de los participantes. En los supuestos en los que los permita e intervengan simultáneamente más de un participante, el operador debe asegurarse de que el resto de participantes conozcan quién es un jugador virtual o robot. En los casos en los que no los permita e intervengan simultáneamente más de un participante, deberá tratar de evitar que los participantes hagan uso de jugadores virtuales y tan pronto detecte su uso deberá comunicar esta circunstancia a los participantes. Los participantes deberán disponer de un mecanismo para denunciar la existencia de un posible jugador virtual.

El operador dispondrá de procedimientos para detectar si un participante está utilizando técnicas de inteligencia artificial.

3.10.6.3 Juegos metamórficos.

Los juegos metamórficos o de evolución, deben:

• Informar de las reglas aplicables en cada momento o fase de juego.

• Mostrar al participante la suficiente información para indicar la cercanía de la siguiente metamorfosis. Por ejemplo, si el participante va recogiendo elementos, la interfaz debe mostrar el número de elementos que el participante ha recogido, los que son necesarios para la metamorfosis o los que le faltan para conseguirlo.

• La probabilidad de una metamorfosis no debe ser variada en función de los premios obtenidos por el participante en previas partidas. Cualquier excepción debe ser previamente autorizada por el IPLYC.

• Las informaciones y el juego no deben ser engañosos o ambiguos.

3.10.6.4 Participante en estado «ausente».

Durante un juego en que intervenga simultáneamente más de un participante, la plataforma debe permitir al usuario establecer un estado de «ausente» o «pausa» que puede ser utilizado si el participante necesita dejar de jugar durante un periodo breve que nunca será superior a veinte minutos. En estado «ausente» el participante no realiza nuevas jugadas. Si realizara alguna jugada su estado dejar de ser «ausente» automáticamente. Si las acciones no afectan al juego (p. ej., consulta de la ayuda) se mantendrá el estado de «ausente».

3.10.6.5 Juegos multiparticipante con anfitrión.

En los juegos donde un participante es el anfitrión, éste podrá decidir si acepta a cualquier participante o si sólo lo acepta a través de una invitación. El anfitrión no podrá excluir participantes de la mesa una vez han sido previamente aceptados a la misma.

3.10.7 Juego «en vivo».

A estos efectos se denominan «en vivo» a aquellos juegos que utilizan un croupier real o una mesa de juego real como dispositivo de juego, cuando dicho juego se integra con un sistema de retransmisión y de apuestas online.

Los participantes podrán visualizar una retransmisión online que permita seguir el juego y conocer el resultado.

Deberán existir procedimientos de actuación para la resolución de las incidencias que puedan suceder durante las operaciones de juego en vivo.

Los dispositivos automáticos de reconocimiento y registro utilizados deben estar equipados con una modalidad de funcionamiento manual que permita la corrección de un resultado erróneo. El participante debe ser informado de que la modalidad manual se encuentra activa. Cada vez que se active la modalidad de funcionamiento manual se debe dejar la traza que permita su posterior revisión.

Deberán existir procedimientos para tratar interrupciones en el juego provocadas por la discontinuidad en el flujo de datos, video y voz.

3.10.8 Pozos, pozos progresivos, y premios adicionales.

Siempre que la reglamentación básica de los juegos correspondientes lo permita, el operador podrá crear pozos, pozos acumulados, pozos progresivos o premios adicionales.

La plataforma informará al participante de forma clara cuando esté aportando fondos a pozos y la manera en que un participante puede optar a los mismos. Todos los participantes que contribuyen al pozo deben poder optar a ganarlo a lo largo del desarrollo del juego. La descripción de las condiciones del pozo y los requisitos para ganarlo deben ser comunicados al participante.

Las condiciones del pozo deben contemplar cualquier conclusión o interrupción, prevista o imprevista, del juego, así como interrupciones técnicas del sistema.

El sistema del operador llevará una contabilidad asociada a la gestión de los pozos que permita el control de los mismos, identificando como mínimo:

– La creación de cada pozo.

– Los periodos de tiempo en que ha estado activo cada pozo.

– Las características configurables del pozo activas en cada momento.

– Los juegos o máquinas que participan o contribuyen al pozo en cada momento.

– El saldo del pozo en todo momento, diferenciando la contribución al mismo de cada tipo de juego o máquina.

– Los premios concedidos en base al pozo, con detalle del ganador, importe y momento en que se produjo.

– El registro de las acciones manuales que afecten al saldo del pozo.

– Las operaciones de transferencia o redirección a otro pozo.

– El cierre de un pozo o el momento en que se produzca su baja.

El operador deberá disponer de un procedimiento que permita el control de los pozos, garantizando que el pozo se crea, gestiona, y concede de manera acorde con las reglas del juego.

En particular, con periodicidad mínima mensual, el operador deberá comprobar:

• El correcto funcionamiento y los saldos y movimientos de los pozos.

• Que una vez constituido y abierto el pozo, las condiciones no cambian hasta que éste haya sido ganado por uno o varios participantes y su importe hecho efectivo.

• Que el procedimiento de determinación de ganadores funciona correctamente. El procedimiento no debe permitir introducir ganadores que no cumplan las condiciones para ser premiados, ni tampoco no dar por ganadores a aquellos que sí las cumplan.

• Que el sistema concede los premios a los participantes que figuran en la lista de ganadores.

• Si existen, se prestará especial atención a los sistemas de redirección del pozo en los que parte del pozo acumulado es redirigido a otro fondo, donde puede ser ganado posteriormente. El sistema de redirección del pozo no puede utilizarse con la finalidad de posponer la concesión de un premio indefinidamente.

La inoperatividad del pozo deberá ser comunicada a los participantes mediante la visualización en su terminal de mensajes como «pozo cerrado» o similares. No será posible ganar un pozo acumulado que se encuentre previamente cerrado.

3.10.9 Juegos a través de canales de comunicación «en diferido».

A estos efectos se tendrán la consideración de juegos «en diferido» aquellos juegos cuya aleatoriedad o alguno de los elementos para llegar al resultado se hayan obtenido con anterioridad al inicio de la interacción de los participantes con el juego durante la partida.

El operador adoptará las medidas técnicas, de seguridad y organizativas necesarias para evitar que ni el propio operador, su personal, u otros participantes puedan obtener ventajas derivadas del conocimiento previo, incluso parcial, de los elementos que pueden determinar el resultado.

4. SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

4.1 **Requisitos de Seguridad**

Los requisitos de seguridad del sistema técnico de juego que a continuación se establecen tienen como objetivo proteger la información de los usuarios y sus cuentas de juego asociadas, así como también garantizar que el juego se desarrolla de manera correcta.

El operador debe garantizar las condiciones de seguridad física y lógica de todo el Sistema Técnico de Juego, de forma que se asegure la integridad y disponibilidad del juego y de la información generada y gestionada producto de la operación.

Para ello, debe tener implementado un sistema de gestión de la seguridad que utilice como guía los estándares ISO/IEC 27002:2013, 27001:2013 y 27005:2011, GLI 27 y contemple las políticas, procesos, procedimientos y controles que protejan los elementos críticos referidos en los siguientes ítems y se enfoquen hacia los siguientes aspectos de la operación del sistema técnico de juego:

- Garantizar la integridad, confidencialidad y privacidad de los datos e información transmitidos entre los dispositivos de conexión remota y el Sistema Técnico de Juego que son transportados dentro de la red pública de Internet y entre los distintos componentes del sistema en la red privada del operador.
- Garantizar la integridad, confidencialidad y privacidad de los datos e información procesada y almacenada en el Sistema Técnico de Juego.
- Conservar en las bases de datos en línea o sus respaldos históricos la información de los eventos de control, de resultados y de apuestas generados en el Sistema Técnico de Juego durante la vigencia del contrato de concesión.
- Gestionar los riesgos operacionales y tecnológicos del Sistema Técnico de Juego derivados de las posibles amenazas y vulnerabilidades sobre cada uno de los componentes del sistema.
- Otros que el operador considere necesarios para garantizar el adecuado desarrollo del juego y su operación.

Si el operador cuenta con certificaciones de sistemas de gestión de seguridad en uno de los estándares guía para los procesos y sistemas que soportan la operación del Sistema Técnico de Juego, podrán validarse con el ente certificador para efectos de dar por cumplido lo requerido en el presente apartado.

4.2 **Componentes Críticos**

Los componentes críticos son los elementos cuya seguridad debe ser gestionada ya que su impacto en el desarrollo del juego es importante.

Son elementos críticos:

- La cuenta de usuario, la cuenta de juego y el procesamiento de los medios de pago: los componentes del Sistema Técnico de Juego que almacenan,

manipulan o transmiten información sensible de los jugadores como datos personales, de autenticación, o económicos y los que almacenan el estado puntual de los juegos, apuestas y su resultado.

- En el generador de números aleatorios: los componentes del Sistema Técnico de Juego que transmiten o procesan números aleatorios que serán objeto del resultado de los juegos y la integración de los resultados del GNA en la lógica del juego.
- Las conexiones con IPLYC y las redes de comunicación que transmiten información sensible de los jugadores.
- El Sistema de Reportes y Control: Réplica de la base de datos (RBD)
- Los puntos de acceso y las comunicaciones desde y hacia los componentes críticos anteriores.

4.3 **Gestión de la seguridad del sistema técnico de juego**

El operador deberá implementar un sistema de gestión de la seguridad, que protegerá especialmente los componentes críticos referidos en el número anterior.

Los procedimientos de seguridad deberán estar dirigidos a implementar medidas concretas de seguridad, partiendo de una evaluación de los riesgos. El operador deberá planificar las revisiones periódicas y realizar las revisiones derivadas de los cambios significativos.

4.4 **Gestión de riesgos**

La gestión de riesgos deberá utilizar el estándar guía ISO/IEC 27005:2011 para implementar los procesos que permitan realizar el evaluación, análisis, tratamiento y aceptación de los riesgos a los que está sometido el Sistema Técnico de Juego. El operador deberá mantener los registros y evidencias que permitan evidenciar el cumplimiento de la adecuada gestión de riesgos en los procesos de auditoría que se realicen.

4.5 **Políticas de Seguridad**

Los operadores deberán contar con procedimientos de seguridad que serán comunicados a la totalidad de sus empleados y, en su caso, a las entidades colaboradoras externas.

4.6 **Organización de la seguridad de la información**

Los operadores deberán establecer un marco de gestión para la seguridad de la información indicando las funciones y responsabilidades de su personal.

4.7 **Seguridad en la comunicación con los participantes**

Deben adoptarse mecanismos de autenticación que permitan al sistema de juego identificar al participante, y que, a su vez, permitan al participante identificar al sistema de juego.

El operador deberá establecer los sistemas y mecanismos que garanticen la confidencialidad de las comunicaciones de los participantes con sus sistemas técnicos de juego y, en particular, con la unidad central de juegos y su réplica. Las comunicaciones serán cifradas en los casos de transmisión de datos personales (registro de usuario) o económicos (cuenta de juego).

En relación con las comunicaciones, el operador adoptará las medidas que resulten necesarias para garantizar la integridad y el no repudio en los casos de transmisión de datos personales o económicos, y en las transacciones de participación en el juego.

4.8 **Seguridad de recursos humanos y terceros**

El plan de seguridad del personal del Operador incluirá acciones formativas, y será considerado en la gestión de la contratación del personal, prestando especial atención a los permisos de acceso a la información y a los elementos críticos.

Cuando el Operador necesite de los servicios de proveedores que requieran acceso, procesamiento, comunicación o tratamiento de la información, o bien el acceso a instalaciones, productos o servicios relacionados con el juego, éstos terceros deberán cumplir la totalidad de los requisitos de seguridad exigibles al resto de usuarios técnicos.

4.9 **Seguridad física y medioambiental**

Los planes de seguridad de los Operadores deberán incluir, en relación con la seguridad física de los elementos del Sistema Técnico de Juego y de su réplica, lo siguiente:

- Seguridad perimetral para las áreas que contienen elementos críticos e información sensible: tarjetas de acceso, etc.
- Control de acceso físico a las instalaciones en las cuales se encuentren los equipos, tanto para usuarios técnicos como para personal externo, que incluya elementos físicos, procedimientos de autorización, registros de acceso y servicios de vigilancia.
- Protección de los equipos críticos frente a riesgos ambientales: agua, fuego, etc.
- Protección de los equipos críticos frente a cortes del suministro eléctrico y otras interrupciones causadas por fallos en instalaciones de soporte. El cableado de suministro eléctrico debe estar protegido.
- Control de acceso al cableado de comunicaciones si transporta información crítica sin cifrar.
- Mantenimiento de las instalaciones y equipos.

- Dispositivos que contienen información deben ser borrados de manera segura o destruidos antes de ser reutilizados o retirados.
- Equipos que contienen información no pueden ser trasladados fuera de las instalaciones seguras sin la correspondiente autorización.

4.10 **Gestión de comunicaciones y operaciones**

Se debe garantizar la segura y correcta operación del sistema técnico de juego, así como las comunicaciones:

- Los componentes críticos deberán ser monitoreados para evitar que puedan utilizarse versiones diferentes de la homologada.
- Las comunicaciones entre los componentes de los sistemas técnicos de juego garantizarán la integridad y la confidencialidad.
- Las tareas se segregarán entre las diferentes áreas de responsabilidad, para minimizar la posibilidad de acceso no autorizado y potenciales daños.
- Se separarán las tareas de desarrollo, pruebas y producción.
- Los servicios proporcionados por terceras partes deben incluir controles y métricas de seguridad en los contratos, y deben ser periódicamente auditados y monitorizados.
- Se adoptarán medidas de protección contra código malicioso.
- Deben hacerse regularmente copias de seguridad con la frecuencia adecuada y conservarse custodiadas según quede recogido en el plan de copias de seguridad.
- Se adoptarán medidas de seguridad en la red de comunicaciones.
- Se adoptarán medidas de seguridad en la manipulación de soportes portátiles, así como de borrado seguro o de destrucción de los mismos, que se plasmarán en un procedimiento documentado.
- Los relojes de todos los componentes, especialmente los críticos, deberán estar sincronizados con una fuente de tiempo fiable. La fuente de tiempo fiable puede no ser la misma para cada componente. El operador establecerá medidas y controles para evitar la manipulación de las marcas de tiempo o su alteración posterior, especialmente en los registros de auditoría.
- Deberán generarse y guardarse registro de auditoría de actividades de todos los usuarios, excepciones y eventos de seguridad de la información durante un periodo mínimo de dos años.
- Los registros de auditoría estarán protegidos frente a la alteración y el acceso indebido.
- Las actividades del administrador del sistema y del operador del Sistema deberán quedar registradas.
- Se realizará un análisis periódico de los registros de auditoría. Se tomarán acciones en función de las incidencias detectadas.

4.11**Control de acceso**

Los accesos del personal del Operador y otros usuarios técnicos deben cumplir los siguientes requisitos:

- Debe existir una política de acceso a información documentada, que será revisada periódicamente por el IPLYC
- Se debe asegurar el acceso autorizado e impedir el no autorizado mediante controles en el alta de usuarios, gestión de privilegios de acceso, revisión periódica de los privilegios de acceso y política de gestión de las contraseñas.
- Los usuarios deben seguir buenas prácticas en el uso de contraseñas y proteger adecuadamente la documentación y soportes en su puesto de trabajo.
- Los usuarios únicamente tendrán acceso a los servicios que han sido autorizados a usar.
- No existirán usuarios genéricos y todos los usuarios accederán con su usuario propio único.
- El sistema debe autenticar todos los accesos, ya sea personal propio, de mantenimiento u otros, ya sea de otros sistemas y componentes (por ejemplo la pasarela de pagos). También debe ser autenticado el personal del IPLYC u otro personal que actúe en su nombre.
- Las redes se segregarán en función del área y responsabilidad de la tarea o función.
- El acceso a los sistemas operativos requerirá un mecanismo de autenticación seguro.
- Se restringirá y se controlará el uso de programas que permitan evitar los controles de acceso y de seguridad.
- Las sesiones de usuario tendrán un tiempo máximo de duración de la conexión y un tiempo de desconexión por inactividad.
- El personal de soporte informático tendrá restringido el acceso a los datos reales de las aplicaciones. Los datos reales sensibles estarán ubicados en entornos aislados.
- Se gestionarán los riesgos asociados a dispositivos móviles.
- Si existe el teletrabajo, se comprobará que el riesgo asociado está gestionado en el marco del plan de seguridad.

4.12 **Compra, desarrollo y mantenimiento de los sistemas**

Se deberá analizar el impacto en la seguridad en la toma de decisiones de compra, desarrollo y mantenimiento de los sistemas de información.

4.13 **Gestión de incidentes de seguridad**

El operador deberá disponer de un procedimiento documentado de gestión de incidentes de seguridad.

Todos los incidentes de seguridad deberán ser registrados y se documentarán de forma clara y concisa los hechos, los impactos y las medidas adoptadas.

4.14 **Gestión de la disponibilidad del servicio**

El Operador deberá disponer de un plan de gestión de la disponibilidad del servicio. El Operador deberá considerar dentro del plan cada uno de los siguientes servicios:

- Registro del jugador, cuentas de juego, incluyendo la posibilidad de realizar depósitos y retirar fondos.
- Servicios de juego.
    - El plan indicará el tiempo máximo de indisponibilidad acumulada mensual, así como el tiempo máximo de recuperación para cada servicio.
    - El Operador adaptará su infraestructura y procesos, e implantará las medidas necesarias para cumplir los objetivos fijados en su plan de gestión de la disponibilidad.

4.15 **Plan de prevención de pérdida de información**

El operador debe disponer de un plan que garantice que no se pierdan datos o transacciones que afecten o puedan llegar a afectar al desarrollo de los juegos, a los derechos de los participantes o al interés público e indique el riesgo asumido por el operador.

El operador adaptará su infraestructura y procesos, e implantará las medidas necesarias para cumplir los objetivos fijados en su plan, estableciéndose los siguientes mínimos:

- Se conservarán copias de la información en un lugar alejado convenientemente de los datos que pretende salvaguardar.
- La copia de la información se protegerá de accesos no autorizados mediante medidas de seguridad equivalentes a las de la información a salvaguardar.

El operador deberá disponer de un procedimiento documentado de actuación en caso de pérdida de información que incluirá los mecanismos para atender las reclamaciones de usuarios, la continuación de los juegos o apuestas interrumpidas, y cualesquiera otras situaciones que pudieran derivarse.

En caso de producirse una pérdida de datos, el operador deberá informar al IPLYC, con carácter inmediato, indicando las acciones tomadas y una estimación de la repercusión de la pérdida.

4.16**Gestión de la continuidad de negocio**

El operador debe disponer de un plan de continuidad de negocio para el mantenimiento de la operativa de juego ante desastres, que incluya las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y de una réplica de la unidad central de juegos que permita el normal desarrollo de la actividad.

El plan de continuidad de negocio determinará uno o varios escenarios de recuperación indicando para cada uno de ellos los servicios recuperados y el tiempo máximo en el que estarían operativos. El operador deberá considerar dentro del plan los siguientes escenarios:

- Acceso de los participantes a sus registros de usuario y cuentas de juego, con posibilidad de consultar el saldo y los movimientos de sus cuentas de juego asociadas. El tiempo máximo para prestar de nuevo estos servicios será de una semana.
- Posibilidad de los participantes de retirar sus fondos. El tiempo máximo para prestar de nuevo estos servicios será de una semana.
- Continuación de los juegos incompletos o las apuestas pendientes, y pago de los premios válidamente conseguidos. El tiempo máximo para prestar de nuevo estos servicios será de 30 (treinta) días.
- Restablecimiento completo de todos los servicios.
- El operador adaptará su infraestructura y procesos, e implantará las medidas necesarias, para hacer realizables los objetivos fijados en su plan de continuidad de negocio.
- En caso de desastre, el operador deberá informar al IPLYC con carácter inmediato, realizando una estimación del impacto y del tiempo estimado de recuperación.

4.17 **Test de penetración y análisis de vulnerabilidades**

El ente Certificador debe realizar pruebas de técnicas de seguridad para garantizar que no existen vulnerabilidades que pongan en riesgo la seguridad y operación del Sistema Técnico de Juego. Estas pruebas llamadas de penetración, deben tener un método de evaluación de la seguridad mediante la simulación de un ataque realizado por un tercero y el análisis de vulnerabilidades consistirá en la identificación y cuantificación pasiva de los riesgos potenciales del sistema que incluyen:

Test Interno: ataque en la red interna del operador, ejemplo:

- Auditoria de red
- Auditoria de accesos a servidores.

Test Externo: ataque desde internet, ejemplo:

- Vulnerabilidades de tipo 'cross-site scripting';
- Vulnerabilidades de tipo 'spoofing';
- Vulnerabilidades de tipo inyección de SQL;
- Vulnerabilidades de tipo inyección de código;
- Vulnerabilidades derivadas de la validación de entrada / salida;
- Vulnerabilidades derivadas del análisis de tiempos;
- Vulnerabilidades de sincronización;
- Vulnerabilidades de tipo desbordamiento de memoria
- Vulnerabilidades basadas en secuestro de sesiones;
- Vulnerabilidades en los equipos de la red local;
- Vulnerabilidades basadas en 'sniffing' de la red;
- Vulnerabilidades basadas en escaladas de privilegio
- Vulnerabilidades en la gestión de contraseñas.
- Inyección de código;

- Autentificación incompleta y gestión de sesiones
- Denegación de servicio (DoS o DDoS)
- Otras vulnerabilidades que surjan luego de la aprobación del reglamento y se consideren relevantes para proteger la seguridad y operación de los juegos.

Los resultados de las pruebas y de los análisis deberán conservarse junto con las medidas correctivas aplicadas o planeadas durante la vigencia de la Concesión, para su posterior revisión o inspección dentro del proceso de auditoría.

En caso de que el resultado del análisis detecte algún fallo de seguridad muy grave, que pudiera poner en riesgo la identidad o situación patrimonial de los jugadores o permitir su suplantación, el ente certificador no emitirá la certificación correspondiente hasta tanto no se subsanen o corrijan las vulnerabilidades por parte del operador y se verifique su cumplimiento.

5. SISTEMA DE REPORTES Y CONTROL

5.1 **Sistema de Reportes y Control**

5.1.1 Descripción.

El IPLYC realizará el seguimiento, vigilancia y control mediante reportes suministrados por el operador y/o consultas a una réplica de la base de datos del operador, en adelante RBD, con los datos del sistema de juegos de producción.

Los reportes deberán ser generados en formato PDF y en alguno de los siguientes tipos estándares que permitan su fácil utilización csv, json, xml, etc. El contenido de los mismos deberá proveer la siguiente información:

- Datos registrados de los participantes y sus cuentas de juego, saldo inicial, depósitos, extracciones, dinero apostado por juego, pago o abono de premios obtenido por juego, bonos convertidos en créditos, saldo final.

- Datos contables de juego, entre los que se incluyen, como mínimo, por cada juego las participaciones o jugadas confirmadas, las jugadas anuladas o canceladas por el operador, las jugadas denegadas, dinero apostado por los participantes y las operaciones de pago o abono por premios realizadas por el operador.

- Transacciones sobre eventos de juego, entre las que se incluyen por torneo, partida o sesión, las jugadas realizadas, las jugadas anuladas y los premios obtenidos.

- Transacciones sobre los registros del participante y de juego, entre las que se incluyen, como mínimo, el registro y la apertura de cuenta, los datos aportados por los participantes, el resultado de la verificación de datos e identificación, la aceptación de los términos y condiciones, la modificación de los parámetros de

las cuentas, las transacciones económicas de la cuenta de juego y el cierre de cuentas.

- Información contable, sobre dinero apostado y jugado de los participantes y pago de premios

- Información sobre comportamiento de juego compulsivo y limitación de acceso configurada por el participante.

- Reclamos de los participantes.

La RBD deberá contener información completa sobre los ítems anteriores y en particular sobre: el proceso de registro de usuarios, datos del participante, datos de la cuenta de juego, opciones de limitación de acceso, transacciones económicas del participante, información sobre juegos y eventos relacionados, resultados, premios, bonos, reclamos así como cualquier otra información pertinente. Asimismo, deberá proveerse información sobre los juegos disponibles y versiones habilitadas. No obstante, no deberá replicarse el desarrollo de cada jugada o partida.

El operador deberá proveer el esquema de la base de datos, como así también ejemplos de consultas para ejecutar sobre la misma.

El IPLYC podrá requerir en cualquier momento durante la vigencia de la concesión, otro dato de forma general o individual en un procedimiento de control. El IPLYC podrá modificar el alcance de los datos que deban ser registrados, el período de actualización de los mismos, y los requerimientos técnicos de disponibilidad y acceso.

5.1.2 Acceso del IPLYC a la información

El operador garantizará el acceso a la información a personal autorizado por el IPLYC. Este acceso deberá utilizar protocolos seguros de comunicación, así como implementar todos los mecanismos posibles para asegurar el acceso.

5.1.3 Disponibilidad del Sistema de Reportes y Control

Durante la operación del juego, la RBD no puede presentar eventos de indisponibilidad por un periodo de tiempo que supere veinticuatro (24) horas seguidas, tiempo dentro del cual debe realizar todas las acciones para restablecer el servicio.

5.1.4 Ubicación de la Réplica de Base de Datos

El o los servidores de réplica de la base de datos de producción deberán estar alojados dentro del datacenter del IPLYC.

El IPLYC se reserva el derecho de auditar el mismo previa notificación de 24 horas al operador.

5.1.5 Canal de Comunicación de la RBD
El operador deberá disponer de una canal de comunicación con la capacidad necesaria para que desde el sistema del operador se repliquen las BBDD entre este y la RBD ubicada en el IPLYC.
Este canal de comunicación deberá utilizar protocolos seguros de comunicación, así como implementar todos los mecanismos posibles para asegurar el acceso.

5.1.6 Conservación, respaldo y recuperación de la Información de la RBD
La RBD y los registros del operador deberán conservarse durante la vigencia de la concesión y diez (10) años posteriores al cese de la misma, debiéndose establecer los sistemas de protección y respaldo que aseguren su integridad y seguridad durante ese plazo.
El operador deberá asegurar el respaldo (backup) de la totalidad de los datos de la RBD de datos dentro de un DRP (Disaster Recovery Plan).
La política de respaldo y recuperación de la RBD debe estar alineada con la política general de backup del Sistema Técnico de Juego y su plan de continuidad; así como debidamente documentada en sus procesos y responsables.
Periódicamente, con frecuencia anual, el operador debe ejecutar un conjunto de pruebas de simulación de desastre y recuperación para verificar el correcto desempeño del sistema de recuperación. Los resultados de estas pruebas deben documentarse y conservarse.

5.2 **Inspección presencial y Remota**

El IPLYC deberá tener la posibilidad de monitorear y supervisar cualquiera de los elementos de las plataformas técnicas de juego de los operadores.

Para ello, el operador deberá articular los mecanismos necesarios de comunicación segura a sus sistemas técnicos, así como permitir y facilitar en todo momento el acceso a los mismos por parte del IPLYC, independientemente de su ubicación.

IPLYC comunicará al operador su intención de realizar una conexión al sistema técnico de juego proporcionando una descripción de las funcionalidades a las que se pretende acceder y el tiempo y duración previstos para el acceso.

El operador proporcionará al IPLYC los medios para realizar un acceso seguro al sistema. El personal designado por el operador colaborará con el IPLYC para el adecuado acceso y consulta de otros sistemas y aplicaciones. El IPLYC podrá realizar grabaciones de la sesión de usuario y cuantas constataciones de hecho sean necesarios para el ejercicio de sus funciones.

Si no se requiere lo contrario, deberá entenderse que el acceso proporcionado al IPLYC es de sólo lectura y que cuenta con el nivel de autorización para acceder a todos los sistemas y aplicaciones del sistema técnico de juego sin ningún filtro en los datos a que puede acceder.

Finalizado el acceso el operador deberá cerrar el acceso seguro.

6. **JUEGO RESPONSABLE**

6.1 **Prevención del juego compulsivo y autoexclusión**

El operador deberá contar con medidas de prevención y detección de juego compulsivo. Dichas medidas deberán contemplar: a) un mecanismo por el cual cada participante pueda -tanto al momento de la registración como al inicio de cada sesión-, configurar su acceso a la plataforma de juego, estableciendo límites temporales o bandas horarias en las cuales el acceso le sea denegado, como también establecer topes o límites de depósitos -por sesión/día/mes-, los cuales deberán ser aplicados de manera inmediata por el operador, b) la emisión de alertas -visuales y sonoras- informando al usuario que ha iniciado sesión hace más de tres (3) horas, repitiendo la misma por cada nueva hora cumplida, y una notificación al final de cada sesión informando: el tiempo transcurrido de juego desde el inicio de la sesión, los tipos de juegos realizados, el estado actual de su cuenta, el monto apostado y los premios obtenidos, y c) la difusión permanente, en lugar visible, de una leyenda advirtiendo sobre los riesgos del juego, en los términos del Art. 10º de la Ley Nº 15.131, y de las vías de ayuda de dispuestas por la Provincia, incluyendo el trámite de autoexclusión.

El operador proveerá de un acceso directo y permanente, visible desde cualquier sección de la plataforma, para la solicitud de autoexclusión. Una vez solicitada la autoexclusión, el operador deberá bloquear el acceso a la persona autoexcluida de forma inmediata, por el período establecido en el Art. 8º de la Ley N º 15.131.

Asimismo, el operador deberá prever mecanismos de detección de conductas que denoten la presencia de juego patológico o compulsivo, mediante el establecimiento y seguimiento de indicadores (como por ejemplo, frecuencia de juego, montos apostados, incremento/eliminación de topes) que generen alertas. Deberá conservar y poner a disposición del IPLYC toda la información relativa a la detección de dichas conductas, incluyendo reportes históricos de la trayectoria de dichos participantes.

El IPLYC establecerá las acciones, mecanismos y procedimientos necesarios para la implementación de los requerimientos establecidos.

6.2 **Prevención del fraude y del blanqueo de capitales**

El operador dispondrá de procedimientos para la detección de fraude y el blanqueo de capitales. Los procedimientos incluirán la pronta notificación de las acciones sospechosas a los organismos públicos competentes para su investigación, conforme el Art. 154º de la Ley Nº 15.079.

En los juegos de apuestas en directo, el operador dispondrá de medidas para mitigar el riesgo de que algunos jugadores pudieran obtener ventajas sobre otros al apostar con información sobre un resultado cierto o tras un suceso que pueda alterar de manera fundamental las probabilidades de la apuesta.

6.3 **Reclamos de los participantes**

El operador deberá poner a disposición de los participantes, y de cualquier persona que pudiera verse afectada por la actuación del operador, un sistema de atención y resolución de reclamos, quejas y sugerencias.

Dicho sistema deberá contar con un acceso electrónico a través del sitio web y/o sesión de juego, el cual deberá ser fácilmente accesible para los posibles interesados, debiendo el operador dejar constancia de los datos del reclamante, de la fecha y hora de recepción de los reclamos presentados, como así también guardar registro de los movimientos y juegos donde se hubiera producido el incidente.

El operador deberá proveer al usuario información de manera cierta, clara y detallada acerca de dicho sistema de atención, el que deberá contener: dirección postal y electrónica alternativas a las que puedan dirigirse los reclamos y, en su caso, modelos normalizados; plazos para la presentación y plazos del operador de comunicación de la decisión/resolución.

La atención al participante deberá realizarse de forma gratuita y en castellano.

Plazos de los reclamos:

1. Presentación: el operador no podrá establecer un plazo límite para la presentación de los reclamos inferior a 30 (treinta) días, contados desde el momento que se produjera el hecho objeto del reclamo.

El operador emitirá una comunicación dirigida al reclamante, en la que acusará recibo de su reclamo y el plazo en que se le informará la decisión tomada al respecto.

2. Resolución: El operador resolverá el reclamo y lo comunicará al reclamante en un plazo no superior a un 30 (treinta) días, contados desde la fecha en la que el reclamo hubiera sido recibido.

Resuelto el reclamo por el operador o, en su caso, transcurridos 30 (treinta) días desde la presentación del reclamo sin que aquél hubiera comunicado su decisión, el participante podrá reclamar ante el IPLYC.

El operador deberá cumplir en enviar un reporte semanal al IPLYC detallando los reclamos recibidos y el estado de resolución al momento del envío.

El IPLYC se reserva el derecho de solicitar ampliar la información yo establecer nuevos mecanismos de comunicación.

7. **CERTIFICACION**

7.1 **Condiciones generales**

El operador deberá presentar ante el IPLYC la certificación del cumplimiento del conjunto de requerimientos impuestos en la presente.

La homologación de los sistemas técnicos de juego y el establecimiento de las especificaciones necesarias para su funcionamiento deberán cumplir con lo dispuesto en el Art. 155º de la Ley Nº 15.079, de regulación del juego, y normativa complementaria.

7.2 **Entidades designadas para emitir el informe de certificación de los sistemas técnicos de juego**

El informe de certificación de los sistemas técnicos de juego deberá ser realizado por las entidades autorizadas a estos efectos por el IPLYC, en base a las condiciones establecidas en la Resolución N° RESOL-2019-220-GDEBA-IPLYCMJGM, que rige el Registro de Laboratorios Certificadores de la Provincia de Buenos Aires.

El IPLYC publicará en su página web las entidades autorizadas para emitir el informe de certificación de los sistemas técnicos de juego.

7.3 **Elementos factibles de homologación**

La certificación debe abarcar los elementos y servicios del sistema técnico que puedan condicionar el desarrollo del juego, el acceso de los participantes y/o el sistema de reportes y control.

Son elementos factibles de homologación, según corresponda, los siguientes:

- El registro de usuario y la comprobación de las prohibiciones subjetivas.

- La integración con servicios de verificación de la identidad.

- La cuenta de juego y la gestión de los fondos de los participantes.

- La integración de la plataforma de juego con la pasarela de pagos.

- El software de juego y el generador de números aleatorios.

- La integración de la plataforma de juego con el software de juego.

- La integración con servicios de información sobre eventos, probabilidades, riesgos, precios o resultados de los mismos.

- Las aplicaciones de back-office que puedan alterar la configuración, el desarrollo y el resultado de los juegos. Por ejemplo, la aplicación de back-office que permita rectificar el ganador de una apuesta.

- El registro y la trazabilidad de los datos.

- El Sistema de Reportes y Control: Réplica de la base de datos (RBD).

- La interfaz de usuario:

o Páginas web, scripts, objetos flash, etc.

o Las aplicaciones descargables o las apps para terminales móviles.

- Las terminales físicas de carácter accesorio.

- Los elementos de juego físicos utilizados en el juego, como por ejemplo las mesas de ruleta para la versión «en vivo».

- cualquier otro elemento que pueda condicionar el desarrollo del juego, el acceso de los participantes y/o el sistema de reportes y control.

En tanto, no requieren homologación:

- La terminal de usuario personal del participante.

- Las redes públicas de telecomunicaciones.

- Los proveedores de medios de pago, las redes de medios de pago o las pasarelas de pago.

- Los proveedores de servicios de verificación de la identidad.

- Los proveedores de servicios de información sobre eventos, probabilidades, riesgos, precios o resultados de los mismos.

- Los sistemas de información del operador que no puedan alterar la configuración, el resultado o el desarrollo de los juegos, o participen en el registro y la trazabilidad de los datos. Por ejemplo:

- Las aplicaciones de back-office que únicamente consulten datos.
- El sistema de contabilidad general del operador,
- El datawarehouse del operador, si no forma parte del registro y trazabilidad del juego.

- El «call center» cuando no se utilice para realizar juego, sino para dar soporte a consultas, quejas y reclamaciones.

7.4 **Plazos y procedimiento de validación y certificación**

a) El operador deberá presentar el proyecto técnico al IPLYC al momento de la presentación de su propuesta en la convocatoria. En este se detallan los aspectos fundamentales del sistema técnico para el desarrollo de actividades de juego y, en particular, los componentes de la unidad central de juegos y del sistema de reportes y control.

b) Asimismo, el operador deberá acompañar el proyecto técnico del Informe preliminar de certificación al momento de la presentación de su propuesta en la convocatoria.
El informe preliminar deberá ser emitido por un laboratorio reconocido que certifica en base al proyecto técnico presentado que éste incluye los requisitos exigidos respecto del software, elementos de seguridad, conexiones necesarias, así como cualquier otro estándar técnico vigente para la obtención de una licencia de Juego On line en la Provincia de Buenos Aires de acuerdo a las obligaciones de la Ley N° 15.079 “Regulación del Juego on line” y sus normativas complementarias.

c) El operador deberá desarrollar el proyecto técnico que fuera acompañado del informe preliminar de certificación oportunamente remitidos. Sin perjuicio de ello podrá ampliar el proyecto a partir de requerimientos realizados por el IPYC.
El IPLYC podrá requerir al interesado cuanta información resulte necesaria acerca del proyecto técnico.

d) El operador deberá presentar el informe definitivo de certificación emitido por un laboratorio acreditado de acuerdo al apartado 7.2 del presente Anexo, en un plazo de 90 (noventa) días, contado desde que le hubiera sido notificada la resolución de otorgamiento de la licencia.

Los informes de certificación deberán pronunciarse sobre el cumplimiento de los requisitos técnicos correspondientes y tendrán como mínimo el contenido siguiente:

- En relación con la plataforma de juego, se incluirá una descripción funcional detallada de procesos soportados por la plataforma, entre otros, el registro de usuario, datos de las sesiones, cuenta de juego, información al participante de las jugadas, sistemas de cobro y pago, mecanismos de limitación a la participación, así como cualquier otro que implemente el sistema.
  El informe evaluará asimismo el comportamiento de la plataforma ante caídas del sistema, procedimientos de recuperación, gestión de sesiones, medidas contra el fraude y el blanqueo de capitales, medidas de juego responsable y obligaciones de información a los participantes.
- Para cada juego, el informe certificará la adecuación de las normas implementadas por el software con las establecidas por la reglamentación básica del juego, incluyendo, en su caso, todas las opciones posibles, política de bonos, detalle de los premios y de las probabilidades del juego, así como el porcentaje de retorno al jugador.
- En relación con el generador de números aleatorios, el informe indicará el nivel de calidad intrínseca del generador, tras superar cuantas pruebas estadísticas sean necesarias para demostrar que los datos generados son de carácter aleatorio, imprevisibles, no reproducibles, y que los métodos de escalamiento y translación son lineales e independientes de cualquier otro factor que no sea el propio generador.

- En relación con el sistema de reportes y control, el informe incluirá una descripción funcional detallada de los procesos implementados y el registro de la réplica de la base de datos de las operaciones de juego, en relación a los requisitos establecidos en el apartado 5 del presente Anexo I.

Los informes definitivos de certificación irán acompañados de una copia de los archivos críticos del software objeto de homologación firmada digitalmente por las entidades designadas al efecto, que será empleada para comprobar la integridad del software en los procedimientos de auditoria de los sistemas técnicos de juego.

Los informes de certificación incluirán un detalle de la relación de los componentes, software o hardware, calificados como críticos, con información detallada de la ubicación de cada componente en el sistema técnico de juego, denominación de los componentes y niveles de revisión. A estos efectos, se consideran como críticos los elementos que se refieran al generador de números aleatorios, al registro de usuario y la cuenta de juego, el sistema de reportes y control, las conexiones con el IPLYC, y el procesamiento de pagos.

El IPLYC podrá calificar como críticos componentes del sistema técnico de juego del operador que inicialmente no hubieran sido calificados de este modo y que motivadamente considere que afectan o puedan llegar a afectar al desarrollo de los juegos, a los derechos de los participantes, o al interés público.

Deberá contemplase como contenido mínimo del informe de certificación, la siguiente información:

- El informe incluirá en todas sus páginas, excluido el anexo, un código único de informe y en su caso versión del mismo, la fecha de emisión, la razón social de la entidad designada, el número de página y número de páginas totales.

- Apartado 1. Datos generales:

  El título o encabezado incluirá el texto «Informe preliminar/definitivo de certificación».
  Datos identificativos del informe de certificación, incluyendo un código único de informe.
  Datos identificativos del operador o del proveedor cuyo proyecto técnico se certifica.
  Datos identificativos del software y versión utilizados, así como el fabricante.
  Datos identificativos de la entidad designada para la certificación.
  Datos identificativos del tipo de certificación: Funcionalidad, seguridad o funcionalidad y seguridad.
  Datos identificativos y firma del responsable por parte de la entidad designada para la certificación.
  Fechas de emisión del informe.

- Apartado 2. Valoración y conclusiones: Se emitirá una valoración global «conforme» o «no conforme» indicando claramente si se refiere a la funcionalidad, la seguridad, o ambas.
- Observaciones de la entidad designada.
- Anexo 1. Documento evaluado e información de respaldo.

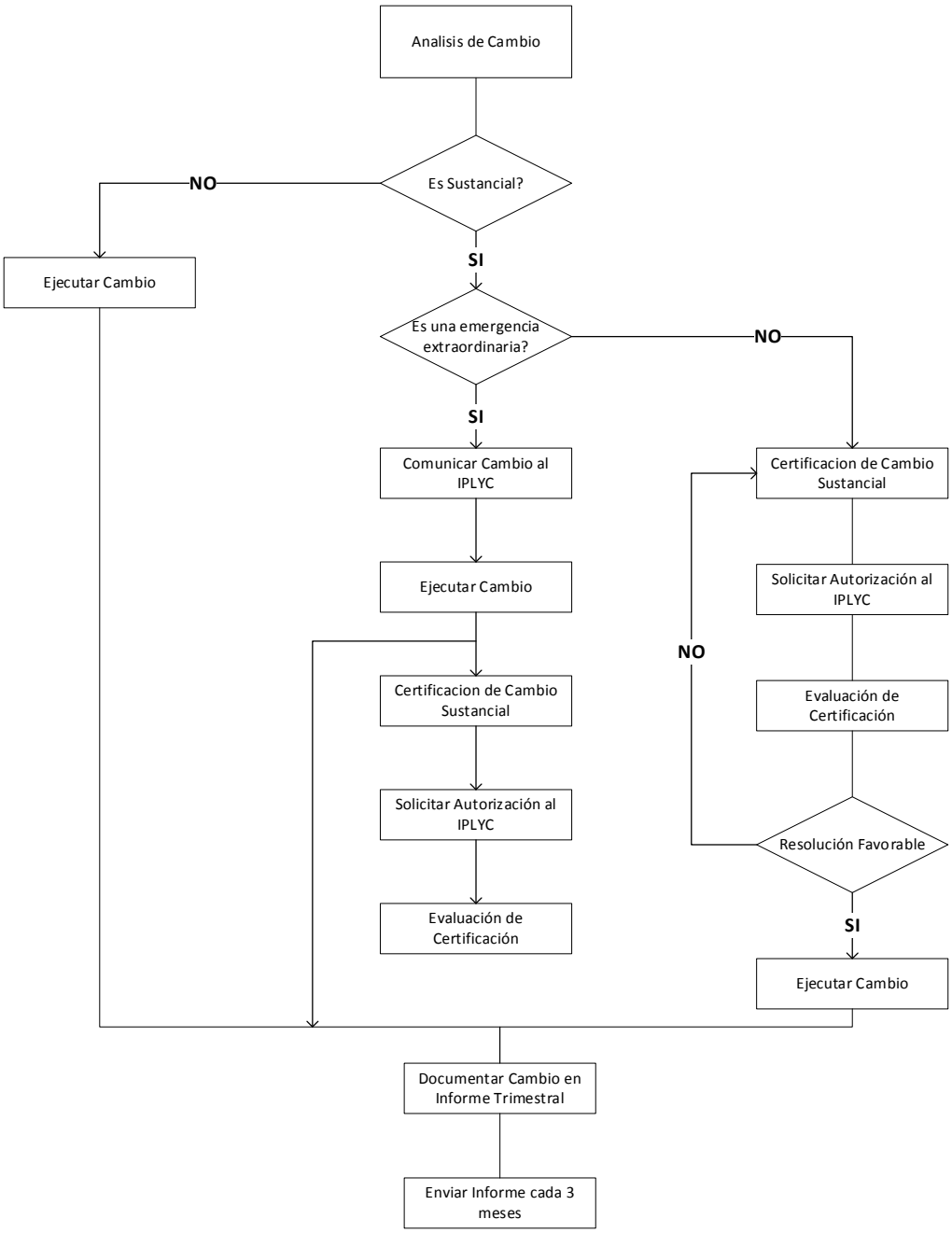
8. GESTION DE CAMBIOS

8.1 **Gestión de cambios en el sistema técnico de juego**

El operador debe disponer de un proceso formal de aprobación interna de todos los cambios, que abarca desde la petición de cambio hasta su aprobación por los responsables correspondientes. Las obligaciones de cumplimiento en materia de gestión de cambios forman parte de este proceso formal.

El objetivo del siguiente diagrama es resumir de una forma gráfica aquellas fases del procedimiento de gestión de cambio, en el que deben considerarse las obligaciones establecidas por el IPLYC.

Diagrama de gestión de cambio:



Análisis del cambio

En la fase de análisis el operador ha de evaluar si el cambio es de carácter "sustancial" o no, teniendo en cuenta los criterios de valoración establecidos en el punto 8.4 del presente documento. Sin perjuicio de ello, la evaluación de si un cambio es "sustancial" es responsabilidad del operador, que es quien mayor conocimiento posee sobre su propio sistema.

Realizada esta evaluación pueden darse dos casos:

a) En caso de que bajo el criterio del operador y de manera justificada se concluya que el cambio no es sustancial, el operador puede proceder a realizar el

cambio, sin que sea necesario realizar ninguna comunicación al IPLYC ni someter el cambio a su autorización previa.

b) En caso de que bajo el criterio del operador y de manera justificada se concluya que el cambio es sustancial, el operador deberá certificar el cambio.

En todo caso, las peticiones de cambio y las decisiones tomadas se registrarán y podrán ser objeto de posterior auditoría. Si el IPLYC estimara sustancial alguno de los cambios realizados previamente en componentes críticos, requerirá al operador para que proceda a la certificación de los cambios, sin perjuicio de la posibilidad de requerir la retirada del cambio hasta que obtenga la certificación pertinente.

Certificación de los cambios sustanciales

La puesta en producción de un cambio sustancial exige la certificación previa del sistema objeto del cambio.

Solicitar autorización al IPLYC

La solicitud de autorización de cambio sustancial se realizará a través los canales formales de comunicación con el IPLYC.

Evaluar certificación

El IPLYC evaluará la solicitud e informará la resolución de la misma.

Ejecutar cambio sustancial

El operador no debe poner en producción el cambio sustancial hasta obtener la autorización del IPLYC expresa.

Ejecutar cambio no sustancial

En caso de que, tras la evaluación del cambio por parte del operador, se determine que el cambio es no sustancial, se puede ejecutar el cambio, sin necesidad de comunicación al IPLYC.

Deberán conservarse copias de los binarios de los elementos software de todas las versiones software que se hayan utilizado en el sistema técnico efectivamente empleado en los últimos cuatro años. Estas copias podrán ser objeto de posteriores auditorías.

Documentar cambio en el informe trimestral

Cualquier cambio que se ejecute sobre un elemento crítico deberá quedar documentado en un informe que se enviará trimestralmente al IPLYC. La información relativa a la elaboración y envío del informe trimestral de cambios se detalla en el apartado 8.3 de la presente.

Envío del informe trimestral

El envío del informe trimestral se realizará a través de los canales de comunicación formales dispuestos por el IPLYC. A tal efecto, en el apartado 8.3 de la presente, se explica toda la información relativa al envío del informe trimestral de cambios.

8.2 **Cambio por emergencia extraordinaria**

Comunicar cambio al IPLYC

Las comunicaciones de cambio por emergencia extraordinaria se realizarán a través los canales de comunicación formales dispuestos por el IPLYC.

La comunicación deberá realizarse con anterioridad al cambio o en las siguientes 24 horas a su realización.

Certificación del cambio sustancial

El operador dispone de un 30 (treinta) días para presentar la documentación de certificación de los cambios desde la comunicación, o en su defecto desde que se realizó la primera de las acciones correctivas de emergencia. Se deberá presentar un informe que acredite las circunstancias excepcionales y el riesgo para la seguridad del sistema técnico de juego.

8.3 **Informe trimestral de cambios**

Cualquier cambio que se ejecute sobre un elemento crítico deberá quedar documentado en un informe que se enviará trimestralmente al IPLYC.

El informe trimestral consiste en la relación de los cambios realizados sobre componentes críticos. Para cada cambio se deberá incluir:

- Un identificador del cambio, la fecha de ejecución.

- Una descripción conceptual y cualitativa del cambio. Deberá explicar el motivo del cambio, los componentes críticos sobre los que tiene impacto y el fin que se persigue con su implementación.

- Calificación motivada del cambio como sustancial o no sustancial.

- No debe incluir binarios y no se requiere incluir huella o hash de las versiones desplegadas.

- Se podrán abstraer o agrupar aquellos cambios que respondan a la misma naturaleza o que se rijan por el mismo motivo.

Se podrá elaborar un único informe por operador o varios. En este último caso se describirán los criterios de la división.

Un ejemplo de formato de informe podría ser el siguiente:

ÍNDICE DEL INFORME

1. Cambios sustanciales realizados por emergencia extraordinaria.
2. Cambios sustanciales realizados con autorización previa del IPLYC.
3. Cambios no sustanciales en los que el criterio del operador se desvía del criterio del IPLYC para la calificación del cambio como no sustancial (de acuerdo con del apartado 8.4 del presente Anexo).
4. Cambios no sustanciales en los que el criterio del operador coincide con el criterio del IPLYC para la calificación del cambio como no sustancial (de acuerdo con el apartado 8.4 del presente Anexo).

Para cada uno de los apartados indicados anteriormente, indicar:

Identificador del Cambio	Fecha de Ejecución	Descripción Conceptual(1)	Justificación para cambios no sustanciales(2)

(1) En los casos en los que se produzca un cambio de versión del software de uno de los elementos críticos, indicar el identificador de la versión a la que se migra, en la descripción conceptual.

(2) La justificación es especialmente necesaria en aquellos casos en los que el criterio del operador se desvíe de los criterios generales del IPLYC del apartado 8.4 del presente Anexo.

El envío del informe trimestral se realiza a través los canales de comunicación formales dispuestos por el IPLYC.

8.4 **Criterios para la valoración de gestión de cambios sustanciales y no sustanciales**

Dado que la decisión sobre el carácter sustancial de un cambio requiere un exhaustivo conocimiento del sistema y un previo análisis de riesgos, la respuesta del IPLYC podrá consistir en directrices y recomendaciones generales de carácter conceptual, que ayuden al operador a tomar la decisión final. El operador deberá proporcionar suficiente información en la consulta para permitir valorar el alcance de los cambios sobre cada componente crítico.

La calificación de un cambio como “sustancial” debe partir de un criterio de proporcionalidad entre la evaluación de los riesgos asociados al cambio, la necesaria flexibilidad de un mercado en constante evolución y el coste que cada proceso de certificación representa. También ha de valorarse que también existen riesgos asociados a no realizar un cambio.

Los riesgos regulatorios deben ser evaluados tomando como referencia los objetivos de la Ley Nº 15.079, de regulación de juego, valorando entre otros:

- el impacto sobre el control de las prohibiciones subjetivas

- el juego responsable

- la compatibilidad de la oferta de juego con los juegos regulados

- el juego justo y su correcto funcionamiento

- la autenticidad y el cómputo correcto de las apuestas

- la trazabilidad de las operaciones realizadas

- la monitorización por el IPLYC a través del Sistema de Reportes y Control

- la seguridad de los juegos y especialmente en el acceso del participante

- la recuperación de datos ante cualquier incidencia

Los sistemas técnicos de juego revisten una gran complejidad. Las dependencias entre los elementos hardware, software y de red que constituyen la unidad central de juegos y el acoplamiento que puede existir entre sus diferentes componentes software complican la definición de cambio sustancial sobre los elementos clasificados como críticos. Esto hace muy difícil enumerar todos los tipos de cambio que pueden presentarse y valorar el impacto y alcance de los mismos en cada sistema técnico concreto.

Por todo ello la primera valoración respecto a si un cambio debe ser calificado como "sustancial" corresponde al propio operador que es el principal conocedor de su sistema técnico.

Es importante tener en cuenta que la complejidad técnica de un cambio no está directamente relacionada con el riesgo asociado al cambio desde el punto de vista de cumplimiento normativo. Por ejemplo, un cambio en los parámetros de los juegos no será considerado un cambio sustancial pero su puesta en producción podría suponer un incumplimiento de los requisitos y limitaciones de los juegos; un cambio en la interfaz gráfica normalmente no será considerado un cambio sustancial pero su puesta en producción podría suponer un incumplimiento de las obligaciones de información al jugador.

Aunque la decisión en la valoración de si un cambio es sustancial o no es del operador, el IPLYC vela por que todos los operadores sigan criterios de valoración similares que atiendan a los objetivos de la normativa y que sean proporcionados. En este contexto, a continuación, se desarrolla el criterio del IPLYC en la calificación de un cambio como "sustancial" en determinados supuestos, sin perjuicio de que justificadamente el criterio del operador pueda desviarse de esta recomendación, en cuyo caso se deberá informar de forma motivada en el informe trimestral de cambios.

El criterio del IPLYC se va actualizando conforme se van planteando situaciones o ejemplos de interés para varios operadores y para adaptarse a la rápida evolución tecnológica del sector. Se han identificado los principales riesgos en la incorporación de nuevos juegos en tres áreas: la integración entre los diferentes componentes software, el correcto funcionamiento de la sesión destinada al juego de máquinas de azar y el correcto funcionamiento de los juegos. En este escenario es posible definir en qué casos la incorporación de un nuevo juego o de una nueva tecnología de acceso constituye un cambio sustancial y por tanto debe ser previamente homologado. Con ello se reducen de forma significativa las cargas para los operadores y para el IPLYC y se agiliza la puesta en producción de nuevos juegos y de nuevas tecnologías de acceso, dando respuesta a una demanda del sector sin reducción de las garantías seguridad de la homologación.

En el marco de gestión de cambios en los supuestos de incorporación de nuevos juegos o nuevas tecnologías de acceso es el siguiente:

- Será necesario certificar la integración de cada operador B2C con las diferentes plataformas de cada uno de sus proveedores (móvil, PC, etc.). La certificación específica de cada uno de los juegos y de cada una de las tecnologías de acceso disponibles podrá ser realizará tanto por operador como por el proveedor.

- Desde un punto de vista operativo, los operadores B2C que deseen incorporar nuevos juegos a su oferta de juego no necesitan solicitar ante el IPLYC cambio sustancial si ha homologado previamente los juegos, siempre que la integración del operador B2C con el proveedor ya está homologada.

Los supuestos de cambio analizados se clasifican en los siguientes grupos:

- Cambios sustanciales de seguridad

- Cambios sustanciales relativos al registro de usuario

- Cambios sustanciales relativos a la cuenta de juego

- Cambios sustanciales relativos al software de juego

- Cambios que podrían NO ser sustanciales

Cambios sustanciales de seguridad

1. Es cambio sustancial la incorporación de un nuevo CPD o su traslado a una ubicación diferente a los ya existentes.

2. Es cambio sustancial la modificación del esquema de autenticación de los participantes en el sistema técnico de juego o la implementación de un nuevo método de autenticación en la comunicación con los participantes.

Cambios sustanciales relativos al registro de usuario

3. Es sustancial el cambio en los procedimientos de verificación de identidad de los usuarios, del tratamiento de las respuestas, de la lógica de comprobaciones o de la activación de usuarios.

Ejemplos:

- Cambios en las consultas al Registro de Autoexclusión
- Cambios en las consultas al Servicio Web de Verificación de Jugadores.

Cambios sustanciales relativos a la cuenta de juego

4. Cambios en el modo de integración con los proveedores de juego.

5. Cambio íntegro de la pasarela de pagos.

Cambios sustanciales relativos al software de juego

6. Un cambio mayor de la versión del software de juego previamente homologado.

7. La incorporación de un nuevo proveedor de software de juego.

8. Cambio en el modelo de integración del operador con el proveedor de software de juego. En caso de que existan varios tipos de integración, deberán certificarse todas ellas. Por ejemplo, si existe una integración con la plataforma para PC y otra integración con la plataforma para móvil, será necesario certificar la correcta integración del operador con su proveedor para todos los supuestos.

9. La incorporación de un nuevo juego en los siguientes casos:

- Si se trata de un desarrollo propio.
- Si el juego es proporcionado por un proveedor que carece de licencia.
- Si el juego es proporcionado por un proveedor con licencia, pero dicho juego no ha sido homologado previamente por el proveedor.

10. Cambio en juegos o variantes de juegos homologados, cuando supongan el despliegue de nuevos componentes software críticos para el correcto desarrollo del juego. No será necesario certificar variantes de juego cuando los cambios se limiten a la parametrización del cambio ya certificado.

11. La puesta en producción de nuevas tecnologías de acceso a juegos.

12. En el caso de las apuestas deportivas, la inclusión de apuestas en directo.

13. Cambios que modifiquen la generación de los números aleatorios y el tratamiento de esta información.

Cambios que podrían NO ser sustanciales

Cambios relativos a la funcionalidad que podrían no ser sustanciales:

14. Sistemas de propósito general que ya han sido homologados previamente, o cambios sobre los mismos que no supongan una alteración de la lógica de componentes críticos:

- Software de propósito general: sistemas operativos, librerías de desarrollo, base de datos, servidor web, servidor de aplicaciones, etc.
- Elementos de red o de cableado.
- Equipos hardware.

15. Cambios realizados sobre el software del componente crítico:

- Mantenimiento correctivo, corrección de errores o bugs.
- Cambios que afecten únicamente al rendimiento.
- Cambios que implementen políticas promocionales o de fidelización, siempre que no supongan grandes cambios en la cuenta de juego y que garanticen la trazabilidad de las operaciones.

16. Cambios en las fuentes de información documentales utilizadas para la acreditación de la veracidad de los datos asociados al registro de usuario.

17. Inclusión de nuevos medios de pago sobre la pasarela de pagos previamente homologada.

18. Cambios en la interfaz web.

19. Para un operador B2C no se considera sustancial la inclusión de nuevos juegos siempre y cuando se den las siguientes circunstancias:

- Los juegos están previamente homologados por un proveedor que es titular de una licencia de juego.
- La integración del operador con el proveedor de juego ya ha sido homologada previamente.

20. La parametrización de juegos previamente homologados siempre que no suponga el despliegue de nuevos componentes software críticos para el funcionamiento del juego.

Cambios relativos a la seguridad que podrían no ser sustanciales:

La seguridad debe ser entendida como un proceso iterativo e incremental. La incorporación de nuevos elementos o cambios sobre el sistema técnico de juego deben llevarse a cabo en el marco de la gestión de la seguridad de la información del operador, pero no necesariamente será objeto de una nueva certificación.

21. Los cambios en políticas, procesos, procedimientos o medidas técnicas u organizativas, siempre que no supongan un menoscabo o una pérdida de garantías sobre las previamente homologadas.

22. La seguridad relativa a nuevas tecnologías o aplicaciones de acceso del participante (por ejemplo, aplicaciones para smartphones) deberá someterse a los controles definidos por el operador y serán objeto de las “pruebas de penetración y análisis de vulnerabilidades” establecidos en la normativa. La correcta gestión de la seguridad deberá acreditarse a través de los informes de auditoría bianuales.

G O B I E R N O DE LA P R O V I N C I A DE B U E N O S A I R E S
2019 - Año del centenario del nacimiento de Eva María Duarte de Perón

Hoja Adicional de Firmas
Anexo

Número: IF-2019-09345168-GDEBA-IPLYCMJGM

LA PLATA, BUENOS AIRES
Viernes 12 de Abril de 2019

Referencia: Anexo I - Reglamento Tecnico

El documento fue importado por el sistema GEDO con un total de 54 pagina/s.

Digitally signed by GDE BUENOS AIRES
DN: cn=GDE BUENOS AIRES, c=AR, o=MINISTERIO DE JEFATURA DE GABINETE DE MINISTROS BS AS, ou=SUBSECRETARIA para la MODERNIZACION DEL ESTADO, serialNumber=CUIT 30715471511
Date: 2019.04.12 18:39:52 -03'00'

Matias Lanusse
Presidente
Instituto Provincial de Lotería y Casinos

Digitally signed by GDE BUENOS AIRES
DN: cn=GDE BUENOS AIRES, c=AR, o=MINISTERIO DE JEFATURA DE GABINETE DE MINISTROS BS AS, ou=SUBSECRETARIA para la MODERNIZACION DEL ESTADO, serialNumber=CUIT 30715471511
Date: 2019.04.12 18:39:52 -03'00'