Lotería Nacional
para la Asistencia Pública

Manual del Sistema de Gestión de Seguridad de la Información

6100

OCTUBRE 2018

DIRECCIÓN GENERAL
SUBDIRECCIÓN GENERAL DE FINANZAS Y SISTEMAS

COMERI
Comité de Mejora Regulatoria Interna
30 OCT 2018
APROBADO

LOTERÍA NACIONAL PARA LA ASISTENCIA PÚBLICA
SUBDIRECCIÓN GENERAL DE FINANZAS Y SISTEMAS

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
CONTENIDO	**REV. 00**	**LN-6100-MOP-HC-01**
	30-Oct-18	**Página 1 de 2**

CÓDIGO	DESCRIPCIÓN	REV	FECHA	ESTATUS
LN-6100-MOP-GE-01	GENERALIDADES	00	30-Oct-18	
LN-5122-MOP-01	ALCANCE (FORMATO ASI. F4, ANÁLISIS DE RIESGOS)	03	30-Oct-18	CANCELADO
LN-5122-MOP -02	METODOLOGÍA DE LA ADMINISTRACIÓN DE RIESGOS (FORMATO ASI. F3 – 1, FORMATO DE OPERACIÓN DEL EQUIPO "OBJETIVOS").	03	30-Oct-18	CANCELADO
LN-5122-MOP-03	INVENTARIO DE ACTIVOS	03	30-Oct-18	CANCELADO
LN-5122-MOP-04	ANÁLISIS DE RIESGOS (FORMATO ASI. F3 – 1, FORMA DE OPERACIÓN DEL EQUIPO "OBJETIVOS").	03	30-Oct-18	CANCELADO
LN-5122-MOP-05	TRATAMIENTO DE RIESGOS (FORMATO ASI. F3 – 1, FORMA DE OPERACIÓN DEL EQUIPO "OBJETIVOS").	03	30-Oct-18	CANCELADO
LN-5122-MOP-06	ACUERDO DE APLICABILIDAD DE LOS CONTROLES ISO/IEC 27001:2013 Y WLA	03	30-Oct-18	CANCELADO
LN-5122-MOP-07	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	03	30-Oct-18	CANCELADO
LN-5122-MOP-08	DEFINICIONES	03	30-Oct-18	CANCELADO
LN-5122-MOP-09	INFRAESTRUCTURAS CRÍTICAS RESTRINGIDAS	00	30-Oct-18	CANCELADO
LN-5122-MOP-10	INFRAESTRUCTURAS RESTRINGIDAS	00	30-Oct-18	CANCELADO
LN-5122-MOP-11	OBJETIVOS DEL SGSI	00	30-Oct-18	CANCELADO
LN-5122-MOP-12	PROCESOS CRÍTICOS (SUSTANTIVOS)	00	30-Oct-18	CANCELADO
LN-6100-MOP-PO-13	PROCEDIMIENTO DE AUDITORÍAS INTERNAS	00	30-Oct-18	

Lotería Nacional
30 OCT 2018
POR ... DE ORGANIZACIÓN Y DESARROLLO DE PERSONAL

	ELABORÓ	REVISÓ	AUTORIZÓ	REGISTRÓ
NOMBRE	LIC. JESSICA ORTÍZ BARBOSA	LIC. RAQUEL ORDOÑEZ RUÍZ	MTRO. JOSÉ LUIS RAFAEL IBARRA MANZUR	LIC. FRANCISCO J. CARRILLO BRITO
PUESTO	SECRETARIA DEL GESI	VICEPRESIDENTA DEL GESI	RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN EN LA LOTENAL Y PRESIDENTE DEL GESI	SUBGERENTE DE EMPLEO
FIRMA				

Subgerente de Empleo, encargado del Despacho de la Gerencia de Organización y Desarrollo de Personal, de conformidad con el oficio DA/1165/2018, del 14 de septiembre de 2018.

COMERI
Comité de Mejora Regulatoria Interna
30 OCT 2018
APROBADO

Anexos

CÓDIGO	DESCRIPCIÓN	REV	FECHA	ESTATUS
LN-5122-MOP-AN-01	1. INFRAESTRUCTURAS CRÍTICAS. a. CRÍTICAS RESTRINGIDAS. b. RESTRINGIDAS. 2. OBJETIVOS DEL SGSI. 3. PROCESOS CRÍTICOS (SUSTANTIVOS			CANCELADO
LN-5122-MOP-AN-02	DOCUMENTO DE INTEGRACIÓN Y OPERACIÓN DEL. GRUPO ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (GESI). FORMATO ASI F1.			CANCELADO
LN-5122-MOP-AN-03	CATÁLOGO DE INFRAESTRUCTURAS CRÍTICAS ASI F2			CANCELADO
LN-5122-MOP-AN-04	ANÁLISIS DE RIESGOS. FORMATO ASI F3 – 1, INTEGRACIÓN DEL EQUIPO DE TRABAJO DE ANÁLISIS DE RIESGOS.			CANCELADO
LN-5122-MOP-AN-05	DOCUMENTO DE RESULTADOS DEL ANÁLISIS DE RIESGOS. FORMATO ASI F3.			CANCELADO
LN-5122-MOP-AN-06	DOCUMENTO DE DEFINICIÓN DEL SGSI. FORMATO ASI F4.			CANCELADO
LN-5122-MOP-AN-07	ANÁLISIS DE RIESGOS FORMATO ASI F5-1, INTEGRACIÓN DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD.			CANCELADO
LN-5122-MOP-AN-08	DIRECTRIZ RECTORA DE RESPUESTA A INCIDENTES. FORMATO ASI F5.			CANCELADO
LN-6100-MOP-AN-09	METODOLOGÍA	00	30-Oct-18	
LN-6100-MOP-AN-10	CATÁLOGO DE VULNERABILIDADES	00	30-Oct-18	
LN-6100-MOP-AN-11	CATÁLOGO DE AMENAZAS	00	30-Oct-18	

MANUAL REGISTRADO EN
30 OCT 2018
POR LA ... DE ORGANIZACIÓN Y DESARROLLO DE PERSONAL

	ELABORÓ	REVISÓ	AUTORIZÓ	REGISTRÓ
NOMBRE	LIC. JESSICA ORTÍZ BARBOSA	LIC. RAQUEL ORDOÑEZ RUÍZ	MTRO. JOSÉ LUIS RAFAEL IBARRA MANZUR	LIC. FRANCISCO J. CARRILLO BRITO
PUESTO	SECRETARIA DEL GESI	VICEPRESIDENTA DEL GESI	RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN EN LA LOTENAL Y PRESIDENTE DEL GESI	SUBGERENTE DE EMPLEO
FIRMA				

Subgerente de Empleo, encargado del Despacho de la Gerencia de Organización y Desarrollo de Personal, de conformidad con el oficio DA/1165/2018, del 14 de septiembre de 2018.

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
GENERALIDADES	REV. 00	LN-6100-MOP-GE-01
	30-Oct-18	Página 1 de 7

OBJETIVO

Describir los elementos de la norma ISO/IEC 27001, del Sistema de Gestión de Seguridad de la Información (SGSI) y del estándar de la Asociación Mundial de Loterías, WLA-SCS, que sirva de guía para lograr las certificaciones Internacionales del SGSI y WLA, con el propósito de que la LOTENAL, cuente con una ventaja competitiva nacional e internacional, además de lograr la confianza de nuestros clientes y otras partes interesadas.

ALCANCE

Gerencia de Organización y Desarrollo de Personal, Gerencia de Administración de Personal, Gerencia de Recursos Materiales, Gerencia de Servicios Generales, Dirección de Programación y Presupuesto, Dirección de Informática, Dirección de Comercialización, Dirección de Mercadotecnia y Publicidad, Dirección Técnica Jurídica y Dirección de Evaluación de Recursos para la Asistencia Pública.

DIRECTORIO

6010000 Dirección de Administración.

6011 000 Gerencia de Organización y Desarrollo de Personal.

6012 000 Gerencia de Administración de Personal.

6015 000 Gerencia de Servicios Generales.

6110 000 Dirección de Programación y Presupuesto.

6112 000 Gerencia de Tesorería.

6113 000 Gerencia de Crédito y Cobranza.

6120 000 Dirección de Informática.

6121 000 Gerencia de Sistemas Sustantivos.

6122 000 Gerencia de Centro de Cómputo.

6123 000 Gerencia de Telecomunicaciones.

6210 000 Dirección de Comercialización.

6211 000 Gerencia de Ventas Foráneas.

6212 000 Gerencia de Ventas Área Metropolitana.

6213 000 Gerencia de Sorteos.

6214 000 Gerencia de Producción.

6215 000 Gerencia de Relación con Expendedores Ambulantes de Billetes.

6220 000 Dirección de Mercadotecnia y Publicidad.

6221 000 Gerencia de Nuevos Productos.

6222 000 Gerencia de Mercadotecnia.

POLÍTICAS

1.- Es responsabilidad del enlace designado por la unidad administrativa de la Lotería Nacional para la Asistencia Pública (LOTENAL), salvaguardar la documentación generada de la aplicación del Manual del Sistema de Gestión de Seguridad de la Información.

GLOSARIO

- **Activo**: Cualquier cosa que tenga valor para la LOTENAL.
- **Acción Correctiva**: Acción tomada para eliminar la causa de una no conformidad existente u otra situación indeseable.
- **Acción Preventiva**: Acción tomada para eliminar la causa de una potencial no conformidad, u otra situación indeseable.

- **Aceptación de riesgo**: Decisión de aceptar el riesgo.

- **Amenazas:** Son las posibles acciones que pueden explotar una vulnerabilidad.

- **Análisis de riesgo**: Uso sistemático de la información para identificar fuentes de riesgo y para estimarlas.

- **Aplicación del control:** Es la acción general que conlleva el seguimiento adecuado del o los controles que se seleccionaron durante el análisis de riesgo, mismos que se encuentran en el Anexo A de ISO/IEC 27001:2013.

- **Autenticación:** La autenticación es el proceso de detectar y comprobar la identidad de una entidad de seguridad mediante el examen de las credenciales del usuario y la validación de las mismas consultando a una autoridad determinada.

- **Autenticidad, Autenticación de billetes:** Calidad y carácter de verdadero o autorizado, es el acto de establecimiento o confirmación de un billete de lotería como auténtico, es decir que es examinado y verificado mediante un proceso preestablecido, basado en la verificación y lectura de las medidas de seguridad impresas en el mismo, así como la propia estructura del billete.

- **BSI:** Institución de Estándares Británicos (en inglés. British Standards Institution).

- **CIBELAE:** Corporación Iberoamericana de Loterías y Apuestas de Estado.

- **Clasificación:** Es el tipo de activo al que pertenece, se clasifican en:
  - **Información (I).** Archivos electrónicos y documentos impresos que contengan datos referentes a la LOTENAL, que permiten la continuación del proceso de negocio.
  - **Hardware (H).** Dispositivos relacionados a equipo de cómputo, periféricos y dispositivos electrónicos que interactúan con equipo de cómputo.
  - **Software (S).** Programas de cómputo ya sean propios o comerciales.
  - **Personal (P).** Recurso humano, que realiza la operación dentro del proceso.
  - **General (G).** Son las funciones prestadas por proveedores (energía eléctrica, internet, agua potable, etc.), además de aquellos dispositivos mecánicos y herramientas requeridos para el flujo de información.

- **Confidencialidad**: La información de la LOTENAL, no debe ser divulgada a individuos y/o entidades no autorizados.

- **Control:** La acción de control es tomada del Anexo A de ISO/IEC 27001:2013 que ayuda a mitigar la vulnerabilidad.

- **Controles Implementados:** Es el número de controles que están efectivamente en función.

- **Costo original:** Es el costo original con el que fue adquirido el activo, en este caso se le asigna un valor estándar de "10".

- **Descripción:** Características del activo como puede ser marca, número de serie modelo, función, entre otras.

- **Disponibilidad**: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

- **Dispositivo Móvil:** Dispositivo o aparato, con algunas capacidades de procesamiento de datos, que puede tener una conexión permanente o intermitente a una red, con una memoria muy limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones para distintos usos.

- **Dueño:** Gerencia, Subgerencia y/o Jefatura de la LOTENAL responsable del producto, servicio e información generada en la ejecución del proceso.

- **Enunciado de aplicabilidad**: Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

- **Evaluación del riesgo**: Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del mismo.

- **Evento de seguridad de la información**: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Fecha Cumplimiento:** Es la fecha de compromiso en la que los controles serán implementados junto con su verificación.

- **GESI:** Grupo Estratégico de Seguridad de la Información.

- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

- **Grado de aseguramiento:** Es el nivel de seguridad que el activo obtendría con respecto a la aplicación del control para mitigar la vulnerabilidad.

- **IEC:** Comisión Electrotécnica Internacional.
- **IFAI:** Instituto Federal de Acceso a la Información Pública.
- **Impacto:** Es el daño provocado por la interrupción del proceso que puede sufrir el negocio, debido a la explotación de una vulnerabilidad.
- **Implementación:** Es el plan de trabajo con fechas de cumplimiento de las acciones a realizar.
- **Implicación del riesgo residual:** Describe que es lo que puede ocurrir con el riesgo residual que se acepta.
- **Incidente de seguridad de la información**: Uno solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.
- **Infraestructuras críticas:** Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.
- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.
- **IT:** Tecnologías de Información (en inglés Information Technology).
- **Localización:** Donde se encuentra físicamente el activo.
- **LOTENAL**: Lotería Nacional para la Asistencia Pública.
- **MAAGTICSI:** Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información.
- **Nombre del Activo:** Nombre genérico del activo de información
- **Oportunidad de éxito:** Consiste en la mejora que se obtendría si se implementan los controles del Anexo "A" de ISO/IEC 27001:2013 para mitigar la explotación de la vulnerabilidad.

- **Partes Interesadas**: Son aquellos individuos o grupos que influyen en el proceso o son influenciados por él.

- **Plan Residual:** Son las acciones a realizar en caso de que se concrete un daño a través del riesgo residual asumido.

- **Probabilidad:** Es la posibilidad de que ocurra la vulnerabilidad.

- **Proceso:** Conjunto de recursos y actividades interrelacionados que transforman elementos de entrada en elementos de salida; conjunto de procedimientos.

- **Riesgo residual:** Es el riesgo que no se puede mitigar en la aplicación del control y es aceptado por la organización, es inversamente proporcional al grado de aseguramiento.

- **RNG:** Generador de números aleatorios (en inglés. Random Number Generator).

- **SAR:** Sistema de Análisis de Riesgos.

- **SIGEC:** Sistema de Gestión de Calidad

- **SCS:** Estándar de Control de la Seguridad.

- **Seguridad de información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

- **SoA**: (Statement of Applicability), Declaración de Aplicabilidad

- **Tratamiento del riesgo**: Proceso de tratamiento de la selección e implementación de medidas para mitigar el riesgo.

- **TI:** Tecnologías de la Información.

- **TIC:** Tecnologías de la Información y la Comunicación.

- **Valor del negocio:** Consiste en un parámetro para tomar decisiones sobre el activo en el caso de que un activo de información sea vulnerado o dañado, este valor se asigna en base a cuatro factores: Confidencialidad, integridad, disponibilidad y un

valor de 10 que se le da al activo, a este resultado se aplican los valores de alto, medio y bajo; ver Metodología apartado ("**VALOR DE NEGOCIO DE ACTIVOS**").

- **Valor de riesgo:** Permite tener un parámetro para tomar decisiones sobre el activo en caso que un activo de información tenga un impacto alto y una probabilidad alta.

- **Valuación del riesgo**: Proceso general de análisis y evaluación del riesgo.
- **VLT:** Terminal de Video de Lotería (en inglés. Video Lottery Terminal).
- **Vulnerabilidades.** Son los posibles riesgos que puede sufrir un activo.
- **WLA:** Asociación Mundial de Loterías.

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
PROCEDIMIENTO DE AUDITORÍAS INTERNAS	REV. 00	LN-6100-MOP-PO-13
	30-Oct-18	Página 1 de 5

OBJETIVO:

Planear, documentar y ejecutar las auditorías internas que permitan verificar la implantación, mantenimiento y su conformidad de las normas ISO que cuente la Institución y del estándar WLA así mismo seleccionar a los Auditores Internos y líderes para poder llevar a cabo las auditorías internas.

ALCANCE:

- Gerencia de Producción, Gerencia de Relación con Expendedores Ambulantes de Billetes, Gerencia de Sorteos, Gerencia de Ventas Área Metropolitana, Gerencia de Ventas Foráneas, Gerencia de Mercadotecnia, Gerencia de Nuevos Productos, Gerencia de Centro de Cómputo, Gerencia de Sistemas Sustantivos, Gerencia de Telecomunicaciones, Gerencia de Crédito y Cobranza, Gerencia de Tesorería, Gerencia de Administración de Personal, Gerencia de Organización y Desarrollo de Personal, Gerencia de Servicios Generales.

- Áreas que soliciten alguna auditoría de las normas ISO que cuente la Entidad y del estándar WLA.

POLÍTICAS:

1. Es responsabilidad de la Subdirección General de Finanzas y Sistemas, elaborar el programa anual de auditorías internas y/o extraordinarias.

2. Es responsabilidad de la Gerencia de Organización y Desarrollo de Personal / Subgerencia de Capacitación y Desarrollo realizar y gestionar los cursos de capacitación, enfocados al equipo de auditores internos del Sistema de Gestión ISO, con el que cuente la institución y al estándar WLA.

3. Es responsabilidad de la Subdirección General de Finanzas y Sistemas, hacer la selección de auditores.

4. Es responsabilidad de la Subdirección General de Finanzas y Sistemas, elaborar la agenda de auditoría.

5. Es responsabilidad de la Subdirección General de Finanzas y Sistemas, invitar a los

Gerentes a la reunión de apertura y cierre de la auditoría Interna.

6. Los auditores no deben de auditar sus propias aéreas.

7. Se debe de respetar la independencia e integridad del equipo auditor por los responsables del área.
8. Los auditores internos deben ejecutar la auditoría con base en los lineamientos establecidos en el presente documento y en la norma ISO con que cuente la LOTENAL y el estándar de la WLA.

9. Las áreas auditadas deben estar en la mejor disposición y brindar la evidencia documental, declaraciones de hechos u otra información que sea relevante para que se lleve a cabo la auditoría en los mejores términos.

10. Es responsabilidad de cada Gerencia solicitar por escrito a la Subdirección General de Finanzas y Sistemas, una auditoría extraordinaria en caso de que se considere pertinente.

11. El auditor líder puede modificar el plan de auditoría interna previa autorización de la Subdirección General de Finanzas y Sistemas.

12. Es responsabilidad del Grupo Auditor llenar, la lista de verificación.

13. Es responsabilidad del auditor líder, informar al auditado los hallazgos encontrados al final de la auditoría.

14. Es responsabilidad del auditor líder, llenar el reporte final de auditoría interna.

15. Por cada hallazgo encontrado en la auditoría interna, se debe generar una acción de no conformidad de acuerdo al procedimiento para las no conformidades y acciones de mejora.

16. Es responsabilidad de la Subdirección General de Finanzas y Sistemas informar el reporte final de auditoría.

RESPONSABLE	No. de Op.	DESCRIPCIÓN
		INICIO
Subdirección General de Finanzas y Sistemas.	1	Elabora el programa de Auditoría Interna y lo presenta en la Primera Sesión del GESI.
Subdirección General de Finanzas y Sistemas y Subgerencia de Capacitación y Desarrollo.	2	Dan a conocer programa de capacitación para auditores internos.
Subdirección General de Finanzas y Sistemas.	3	Envía oficio a las Gerencias al alcance de las certificaciones, solicitando a los enlaces y personal adicional, para capacitación de auditores internos y generar el grupo de auditores internos.
Personal de las Gerencias.	4	Reciben capacitación en el tema de auditores internos.
Subdirección General de Finanzas y Sistemas.	5	Genera el grupo de auditores internos.
	6	Genera la agenda de la Auditoría Interna
	7	Asigna el código de auditoría considerando dos campos separados por una línea diagonal: ✓ Campo 1: indica el número de la auditoría con una AI (que indica auditoría interna) seguida de un consecutivo (este consecutivo se utilizara por el número de la auditoría) AI01, AI02, AI03,…….AIXX ✓ Campo 2: indica el año en que se realiza la auditoría considerando dos dígitos: 13, 14, 15, etc…. Por ejemplo. ✓ La primera auditoría para el año 2013 será AI01/13 ✓ La segunda auditoría para el año 2013 será AI02/13 ✓ La primera auditoría para el año 2014 será: AI01/14
	8	Notifica vía oficio la reunión de apertura de la Auditoría Interna y adjunta la agenda de Auditoría Interna, a los miembros del GESI.

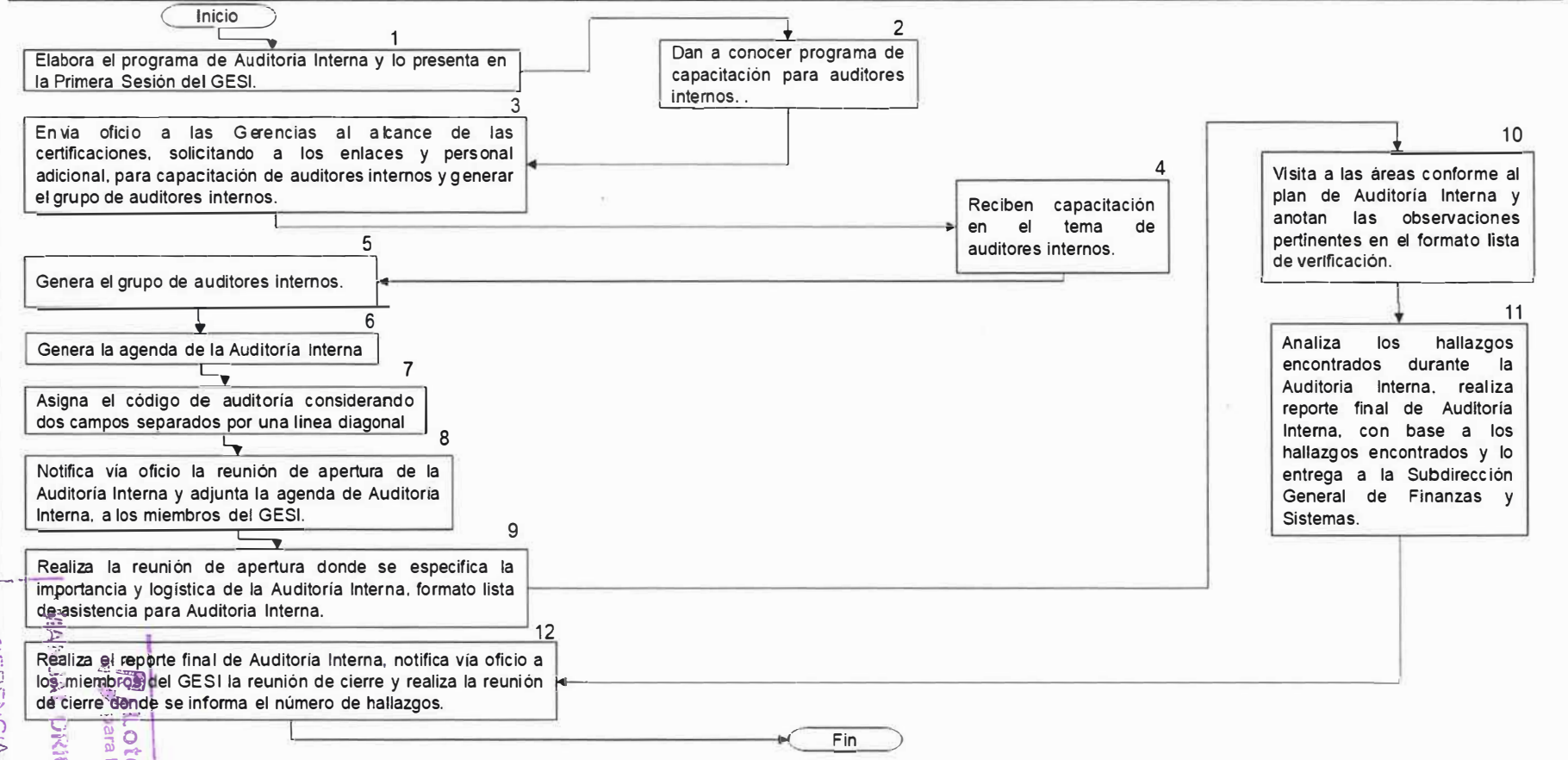
Lotería Nacional para la Asistencia Pública
COPIA FIEL DEL ORIGINAL EN PROCESO
POR LA
GERENCIA DE ORGANIZACION Y DESARROLLO DE PERSONAL

	9	Realiza la reunión de apertura donde se especifica la importancia y logística de la Auditoría Interna, formato lista de asistencia para Auditoría Interna.
Equipo auditor.	10	Visita a las áreas conforme al plan de Auditoría Interna y anotan las observaciones pertinentes en el formato lista de verificación.
	11	Analiza los hallazgos encontrados durante la Auditoría Interna, realiza reporte final de Auditoría Interna, con base a los hallazgos encontrados y lo entrega a la Subdirección General de Finanzas y Sistemas.
Subdirección General de Finanzas y Sistemas.	12	Realiza el reporte final de Auditoría Interna, notifica vía oficio a los miembros del GESI la reunión de cierre y realiza la reunión de cierre donde se informa el número de hallazgos. FIN.

Lotería Nacional

COMERI
Comité de Mejora Regulatoria Interna
30 OCT 2018
APROBADO

DIAGRAMA DE FLUJO



ANTECEDENTES

ORIGEN DE LA NORMA ISO/IEC/27001

Desde 1901, y como primera entidad de normalización a nivel mundial, British Standards Institution (BSI) es responsable de la publicación de importantes normas como:

- 1979 BS 5750 - ahora ISO 9001
- 1992 BS 7750 - ahora ISO 14001
- 1996 BS 8800 - ahora ISO 18001

La norma BS 17799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa – británica o no – un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 17799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 17799-2), publicada por primera vez en 1998, la que establece los requisitos de un SGSI para ser certificable por una entidad independiente.

Las dos partes de la norma BS 17799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 17799-2 para adecuarse a la filosofía de normas ISO de Sistemas de Gestión.

En 2005, con esquema más de 1700 empresas certificadas en BS17799-2, esté se publicó por ISO como estándar ISO/IEC 27001:2005, al tiempo que se revisó y actualizó la ISO17799. Esta última norma se renombra como ISO/IEC 27002:2005 el 1 de julio de 2007, manteniendo el contenido, así como el año de publicación formal de la revisión.

En marzo de 2006, posteriormente a la publicación de la ISO/IEC 27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

En el año de 2013, se actualiza la norma ISO 27001 versión 2005 por la versión 2013 por lo que la ISO/IEC 27001:2013 reemplaza a la ISO/IEC 27001: 2005.

RAZONES DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA WLA

Proteger la información de las partes interesadas, así como, garantizar que los objetivos y operaciones sustantivas de la LOTENAL, se realicen de acuerdo al SGSI y WLA, logrando un valor añadido para la LOTENAL protegiendo la información a través de:

Conservar la confidencialidad, la integridad y la disponibilidad de la información al aplicar un proceso de gestión de riesgos, de una forma documentada, sistemática, estructurada, repetible y eficiente.

Verificar que las operaciones sustantivas de los sorteos se realicen y gestionen de acuerdo a los controles del estándar internacional de la WLA.

Contar con herramientas para el cumplimiento, de los lineamientos estratégicos de la Entidad, que permita satisfacer las expectativas y necesidades de los clientes y ciudadanos, en cuanto a los productos y servicios.

Establecer una metodología gracias a la cual se puede gestionar la seguridad de la información de forma clara y concisa.

Que la operación continúe operando con normalidad en caso de producirse alguna contingencia.

Verificar el cumplimiento de la legislación vigente en materia de información personal y propiedad intelectual.

Identificar las incidencias que pudiera haber en el proceso del alcance del SGSI y WLA, fomentando la mejora continua, toda vez se realizan auditorías internas y externas.

A la alta Dirección le permite obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, además de poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder con todos estos elementos tomar mejores decisiones estratégicas.

Proporcionando confianza a las partes interesadas de que los riesgos se encuentran gestionados adecuadamente.

Reducir los costos y a mejorar el funcionamiento de los procesos.

Aumentar la imagen a nivel nacional e internacional.

ESTRATEGIA DE SEGURIDAD

La LOTENAL reconoce que los recursos humanos, la información y los activos de Tecnologías de la Información y Comunicaciones (TIC) son esenciales para la continuidad de las operaciones de la LOTENAL, que la información y los activos de TIC, soportan una parte importante de la operación diaria de la LOTENAL, por lo cual, toda la información y documentación que es creada por la operación y funcionamiento de la Entidad, así como, la generada con los activos de las TIC de forma manual o verbal, es propiedad exclusiva de la LOTENAL.

Por lo que es importante que la Seguridad de la Información debe ser un requisito inherente a las actividades y/o procesos del negocio y nunca debe ser una función adicional o no prioritaria en la LOTENAL, con el único fin de apoyar al cumplimiento de la misión y objetivos de la LOTENAL, incrementando y manteniendo el nivel de confianza que la sociedad mexicana tiene en nuestra LOTENAL, por lo que todos los que formamos parte de la misma somos responsables de la seguridad de la información y de los activos de TIC.

Para tal efecto, se establece que los Gerentes y todo el personal de las Gerencias al alcance de las certificaciones, son responsables de establecer, implementar y vigilar los lineamientos del SGSI y WLA y cada enlace del SGSI, debe realizar las minutas del SGSI y WLA apoyándose en la metodología de riesgos.

DESCRIPCIÓN DEL ALCANCE DEL SGSI

El establecimiento y definición del alcance del SGSI está basado en la norma internacional *ISO/IEC 27001:2013,* por lo cual el alcance del SGSI, de la LOTENAL, se refiere a los procesos sustantivos de la lotería tradicional, lotería electrónica y de apoyo en la organización, en cuanto a:

"El Sistema de Gestión de Seguridad de la Información de LOTENAL; incluye las actividades relacionadas con la preparación y operación de sorteos tradicionales y/o electrónicos; iniciando desde el diseño del sorteo, hasta el pago de premios; todo conforme a la última versión de la declaración de aplicabilidad."

1Nota: Declaración de Aplicabilidad: Se refiere al documento de Acuerdo de Aplicabilidad SoA (*Statement of Applicability*), que son los controles ISO/IEC 27001:2013 definidos por la Entidad, con fecha de revisión de agosto 2018.

CONTEXTO EXTERNO

La LOTENAL busca la mejora continua, que le permita permanecer vigente en el gusto de sus clientes cautivos y captar otros nichos de mercado mediante la venta de sus productos a través de diferentes canales, para así estar en competitividad con otras empresas u organizaciones nacionales e internacionales, modernizando sus procesos con el uso de tecnología de punta, apegándose a los lineamientos regulatorios y legales que son de su competencia, apoyándose en una Administración de Riesgos efectiva, de acuerdo con el Sistema de Gestión de Seguridad de la Información, basado en la Norma ISO/IEC27001:2013.

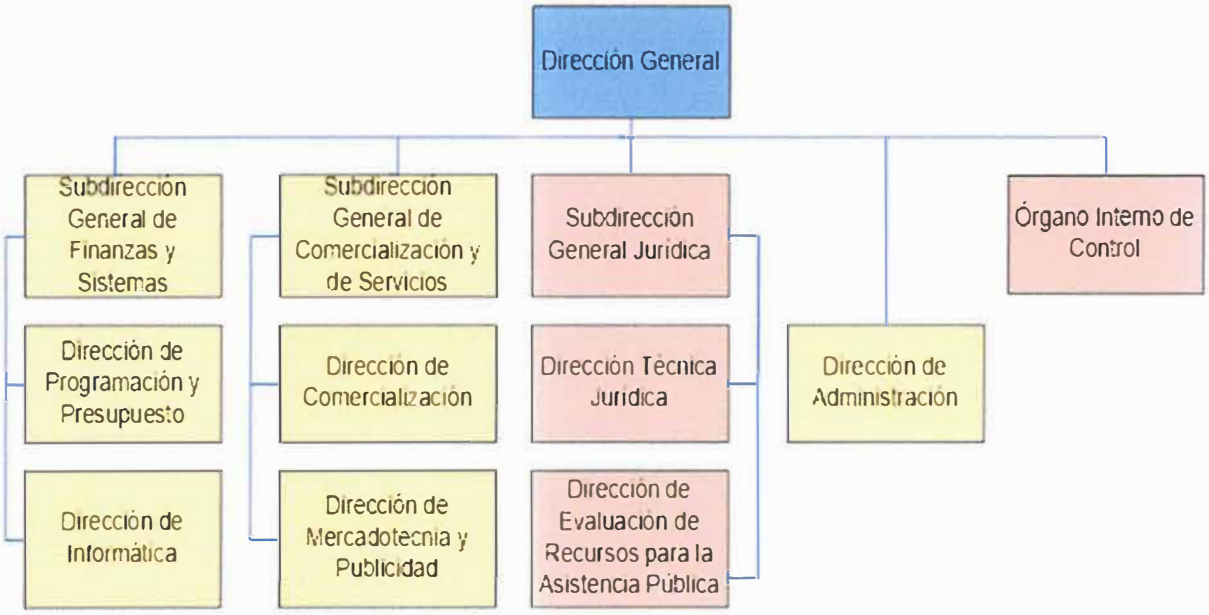
CONTEXTO INTERNO

FUNDAMENTO LEGAL

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.
- Ley Orgánica de la Administración Pública Federal.
- Ley Federal de las Entidades Paraestatales.
- Ley Federal de Archivos.
- Ley Orgánica de la Lotería Nacional para la Asistencia Pública.
- Ley Federal de los Trabajadores al Servicio del Estado, Reglamentaria del Apartado B) del artículo 123 Constitucional.
- Ley General de Responsabilidades Administrativas de los Servidores Públicos.
- Ley General de Transparencia y Acceso a la Información Pública Gubernamental.
- Ley Federal de Presupuesto y Responsabilidad Hacendaria.
- Ley del Servicio de Tesorería de la Federación.
- Ley de Planeación.
- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- Ley de Obras Públicas y Servicios Relacionados con las Mismas.

- Ley de Ingresos de la Federación.
- Ley del Impuesto Especial Sobre Producción y Servicios.
- Ley del Impuesto Sobre la Renta.
- Ley Federal de Juegos y Sorteos.
- Ley General de Bienes Nacionales.
- Ley de Impuesto al Valor Agregado.
- Ley Federal del Derecho de Autor.
- Código Fiscal de la Federación.
- Código de Comercio.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Reglamento de la Ley Orgánica de la Lotería Nacional para la Asistencia Pública.
- Reglamento Interior de la Lotería Nacional para la Asistencia Pública.
- Reglamento Interno de la Lotería Nacional para la Asistencia Pública y del Funcionamiento Interior de su Consejo de Administración.
- Reglamento de la Ley Federal de las Entidades Paraestatales.
- Reglamento de la Ley de Adquisiciones, Arrendamiento y Servicios del Sector Público.
- Reglamento de la Ley de Obras Públicas y Servicios relacionados con las mismas.
- Reglamento del Código Fiscal de la Federación.
- Reglamento de la Ley Federal de Juegos y Sorteos.
- Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.
- Reglamento de la Ley General de Transparencia y Acceso a la Información Pública.
- Reglamento de la Ley del Servicio de Tesorería de la Federación.
- Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.
- Reglamento de la Ley Federal del Derecho de Autor.
- Decreto por el que se creó la Lotería Nacional para la Beneficencia Pública.
- Decreto por el que se aprueba el Plan Nacional de Desarrollo 2013-2018.
- Presupuesto de Egresos de la Federación.
- Manual de Organización de la Lotería Nacional para la Asistencia Pública.
- Bases Generales de Sorteos de la Lotería Nacional para la Asistencia Pública.
- Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).
- ISO/IEC 27001:2013.
- WLA-SCS:2016.

ESTRUCTURA ORGÁNICA



Áreas Certificadas en ISO/IEC 27001:2013 y

Áreas de apoyo, no Certificadas en ISO/IEC 27001:2013

La LOTENAL, cuenta con una Normateca Interna, en la que todo documento publicado en la Normateca, tiene el carácter de documento normativo de observancia general y aplicación obligatoria, para todo el personal de la Entidad; en la Normateca se encuentra registrada la siguiente documentación: Ley Orgánica de la Lotería Nacional para la Asistencia Pública, Reglamentos, Manuales (General de Organización, Organización, Procedimientos, Operación y Administrativos), Lineamientos Generales, Lineamientos, Metodologías, Políticas, Bases Generales, Bases, Reglas Generales, Criterios e Incentivos, así mismo, cada Manual de Organización incluye el Marco Jurídico – Administrativo, en el que se identifica la(s) leyes internas y externas que les aplica a las Gerencias, **(Para mayor referencia consultar el "Manual Administrativo de Procedimientos de Organización y Estructuras, de la Gerencia de Organización y Desarrollo de Personal")**.

También se tiene un Sistema de Análisis de Riesgos (SAR) y un Sistema de Gestión de Calidad (SIGEC).

En el SAR, está sistematizada la metodología de riesgos, en la cual se identifica el procedimiento de cada Gerencia al alcance de la Certificación del SGSI y WLA, de cada procedimiento se identifican los activos y por cada activo se hace su análisis de riesgos.

En el SIGEC, se le puede dar seguimiento a las acciones correctivas, se pueden visualizar las minutas de seguimiento del SGSI y WLA, se pueden consultar las Minutas de las sesiones del GESI, se pueden consultar los reportes de la Revisión por la Dirección y las Auditorías Internas y Externas, así como algunos cursos del SGSI y WLA.

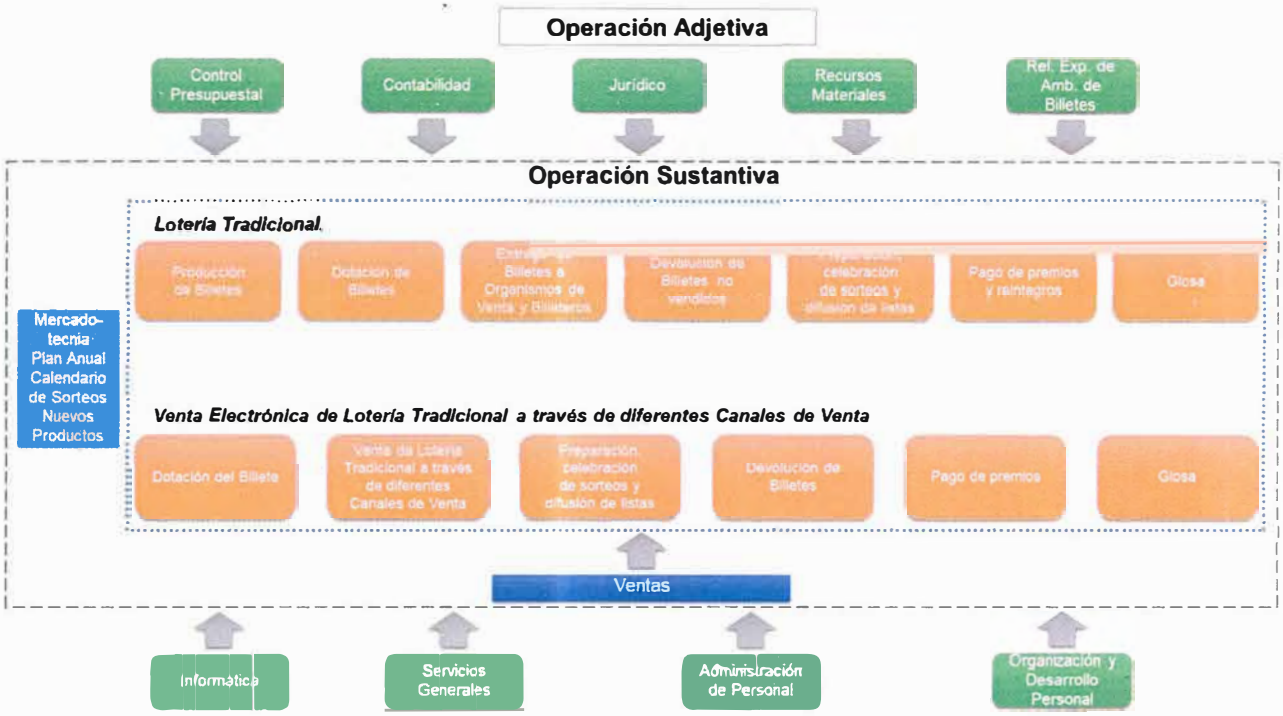
Las operaciones que se encuentran en el contexto interno son:

Operación	Gerencia (s)
Elaboración de propuestas de motivos de billete y Generación de Calendario de Sorteos, así como los estudios de mercado necesarios para impulsar las ventas en la LOTENAL, creando y/o renovando el portafolio de productos, con el propósito de buscar nuevos canales comerciales y reforzando la marca a través de distintos medios (radio, tv, spots, etc.).	• Mercadotecnia. • Nuevos Productos. • Publicidad.
Impresión, Comercialización y Devolución del billete a los organismos de ventas foráneos, locales y billeteros.	• Producción. • Ventas Área. Metropolitana. • Ventas Foráneas. • Crédito y Cobranza. • Control Presupuestal y Contabilidad.
Otorgamiento de los incentivo, ayudas asistenciales y apoyos; así como mantener actualizado el padrón de vendedores ambulantes de billetes.	• Gerencia de Relación con Expendedores. Ambulantes de Billetes.
Preparación y Celebración de Sorteo.	• Sorteos.
Administrar y Ejercer los Ingresos así como el pago de premios locales y foráneos.	• Tesorería.
Administrar las relaciones laborales en la LOTENAL, sus efectos y repercusiones en materia de remuneraciones, prestaciones, impuestos y aportaciones de seguridad social, de conformidad	• Gerencia de Administración de Personal.

con el marco jurídico aplicable.	
Reclutamiento y Selección de Personal así como, la administración y difusión de la Documentación Normativa.	• Gerencia de Organización y Desarrollo de Personal.
Seguridad Física y del Entorno.	• Gerencia de Servicios Generales.
Apoyo.	• Jurídico. • Recursos Materiales. • Informática.

Áreas involucradas en el alcance de certificación ISO/IEC 27001:2013

Esquema General del Alcance



Las operaciones incluidas en el alcance del Sistema de Gestión de Seguridad de la Información de la LOTENAL, se realizan en las instalaciones localizadas en:

Edificio	Dirección
"Moro".	Plaza de la Reforma No. 1 Col. Tabacalera C.P. 06037.
"Edison".	Edison No. 15 Col. Tabacalera CP 06037.
"Jalisco".	Av. de las Repúblicas No. 117, Col. Tabacalera, C.P. 06037.
"Rosales".	Rosales No. 15, Colonia Tabacalera, Delegación Cuauhtémoc, C.P. 06037.

PARTES INTERESADAS

Las partes interesadas para el Sistema de Gestión de Seguridad de la Información son las siguientes:

ID	Partes Interesadas
1	Secretaría de Hacienda y Crédito Público.
2	Dirección General.
3	Organismos de Venta y Billeteros.
4	Empleados y Trabajadores.
5	Proveedores y Contratistas.
6	Medios de Comunicación.
7	Entorno Social.
8	Competencia.

Las necesidades y expectativas de las partes interesadas para el Sistema de Gestión de Seguridad de la Información son las siguientes:

ID	Partes Interesadas	Necesidad	Expectativa
1	Secretaría de Hacienda y Crédito Público.	Pago de impuestos.	Buena gestión de los ingresos.
2	Dirección General.	Objetivos y Metas.	Cumplimiento de objetivos, metas y posicionamiento en el mercado.

3	Organismos de Venta y Billeteros.	Entrega de billete en tiempo.	Igualdad y Crecimiento, así como, la seguridad de las operaciones.
4	Empleados y Trabajadores.	Pago de salarios.	Estabilidad, motivación y ambiente laboral.
5	Proveedores y Contratistas.	Pago del servicio.	Entregar el servicio en tiempo y forma.
6	Medios de Comunicación.	Comunicar a la sociedad información sustantiva, positiva o negativa de la LOTENAL.	Noticia que impacte a la sociedad.
7	Entorno Social.	Productos al alcance de sus posibilidades.	Que los sorteos de la LOTENAL sean seguros y confiables, así como, mejorar la calidad de vida a través de los premios de los sorteos de la LOTENAL.
8	Competencia.	Igualdad en los precios del mercado, transparencia, mejores productos, reconocimiento en el mercado.	Mejor posicionamiento en el mercado a través de nuevos y novedosos productos.

OBJETIVOS DEL SGSI:

1. Realizar la actualización de procedimientos.
2. Gestionar e implementar la continuidad del negocio.
3. Trabajar con un Estándar reconocido a nivel mundial que permita reforzar la imagen, confianza y credibilidad de la LOTENAL.
4. Hacer transparente la Gestión de la LOTENAL.
5. Mantener actualizada y ejecutar una metodología de riesgos con el fin de que se minimicen los riesgos en la operación de la LOTENAL.

DECLARACIÓN DE LA POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Lotería Nacional para la Asistencia Pública protege toda la información que genera, procesa y resguarda por los diferentes medios de tecnologías de la información y comunicaciones (TIC) y/o físicos, a través de la confidencialidad, integridad y disponibilidad, asumiendo el compromiso y mejora continua en la seguridad de la información, a través del Grupo Estratégico de Seguridad de la Información (GESI), apoyándose en una Administración de Riesgos efectiva, de acuerdo con el Sistema de Gestión de Seguridad de la Información, basado en la Norma ISO/IEC27001:2013, logrando la confianza de nuestros clientes y otras partes interesadas.

EXCLUSIONES:

El Sistema de Gestión de Seguridad de la información, de la LOTENAL, no considera ninguna exclusión a los requisitos de la Norma ISO/IEC 27001:2013.

ACTIVOS:

En la LOTENAL se tiene el SAR, el cual permite administrar la lista o inventario de activos, así como el análisis y tratamiento de riesgos.

La lista de activos se maneja mediante el proceso que está definido dentro del alcance del SGSI, por lo que puede existir un activo que se encuentre en dos procesos distintos, también existen activos de apoyo para los procesos y consisten en aquellos que ayudan a varios procesos como lo son: servidores, correo electrónico, edificios, electricidad, agua potable, etc., y son atendidos por otras áreas que no se encuentran dentro del alcance.

El personal de la LOTENAL tiene acceso al sistema para consultar los registros, y soló el personal autorizado, puede administrar dicho sistema.

Se deben revisar los activos, así como, el análisis y tratamiento de riesgos como mínimo una vez al año, por las Gerencias al Alcance de la Certificación del SGSI y de la WLA; al momento que un activo sea dado de alta se debe aplicar la administración de riesgos.

VALOR DE NEGOCIO DE ACTIVOS

Consiste en un parámetro para tomar decisiones sobre el activo, en caso de que un activo de información sea vulnerado o dañado, este valor se asigna en base a cuatro factores: Confidencialidad, integridad, disponibilidad y un valor de 10 que se le da al activo, el resultado se expresa como un número.

Según el grado de confidencialidad, disponibilidad e integridad, se le asignan valores numéricos que se multiplican entre sí por el valor de 10, dando como resultado el valor de negocio del activo.

A continuación, se muestran las ponderaciones de la disponibilidad, confidencialidad e integridad para obtener el valor del negocio:

- **Disponibilidad.** Se refiere a la accesibilidad que tiene el activo, para determinar los valores se utiliza la siguiente tabla:

Factor numérico	Grado	Descripción
3	Inaplazable.	En caso de que el activo sufra daños, los procesos o procedimientos son interrumpidos de manera catastrófica.
2	Urgente.	En caso de que el activo sufra daños, los procesos o procedimientos pueden ser interrumpidos en un corto periodo.
1	Prorrogable.	En caso de que el activo sufra daños, los procesos o procedimientos no se afectan con el daño del activo, pero deben ser corregidos.

- **Confidencialidad**. Se refiere al nivel y privilegios de acceso al activo que tienen los usuarios, para determinar los valores se utiliza la siguiente tabla:

Factor numérico	Grado	Descripción
3	Restringido.	Activos altamente sensibles que sólo podrán ser accedidos por personal autorizado.

2	Privado.	Activos propiedad de la organización y que sólo son utilizados por personal de la organización y/o personal con acceso a la RED interna.
1	Público.	Activos propietarios pero que son utilizados por cualquier tipo de público.

- **Integridad**. La propiedad de salvaguardar la exactitud e integridad de los activos, para determinar los valores se utiliza la siguiente tabla:

Factor numérico	Grado	Descripción
3	Alto.	En caso de sufrir una corrupción o daño en el activo, se debe corregir de manera inmediata.
2	Medio.	En caso de sufrir una corrupción o daño en el activo, se deben corregir en un corto periodo de tiempo.
1	Bajo.	En caso de sufrir una corrupción o daño, no afecta al activo, pero debe ser corregido.

- **Valor de negocio**. Es el resultado aritmético de la multiplicación de los valores dados a los grados de confidencialidad, integridad y disponibilidad por el valor que se la da al activo (10), a este resultado se aplican los valores de alto, medio y bajo; en la siguiente tabla se muestra el valor numérico y el grado que se le asigna en la LOTENAL:

Factor numérico	Grado
10 – 60	Bajo (Verde)
80 – 90	Medio (Amarillo)
120 – 270	Alto (Rojo)

- **Localización.** Donde se encuentra físicamente el activo.

- **Descripción.** Que función realiza el activo dentro del o los procedimientos también considerar alguna característica especial del activo como puede ser, si interactúa con otras Áreas o algún mantenimiento.

Una vez que se obtiene el valor del negocio, se analiza por cada activo las vulnerabilidades amenazas y que controles son los que le aplican para que no se materialice la amenaza y no explote la vulnerabilidad deñando al activo.

VALOR DEL RIESGO DE ACTIVOS

Es absolutamente necesario analizar las posibles vulnerabilidades y amenazas que puedan sufrir los activos con que cuenta la organización, así como su impacto dentro de la misma y la probabilidad de que éstos ocurran más de una vez, esto genera lo que se conoce como el valor de riesgo y junto con el valor del negocio se determina la gravedad "Tratamiento de Riesgos" en caso de ser explotada dicha vulnerabilidad.

En el apartado de Anexos está el catálogo de vulnerabilidades y amenazas; los conceptos de los catálogos no son limitativos y pueden incrementar de acuerdo al análisis de cada activo.

- **Impacto.** Es el daño provocado por la interrupción del proceso que puede sufrir el negocio con la explotación de la vulnerabilidad, se mide de la siguiente manera:

Factor numérico	Grado	Descripción
3	Alto.	Interrupción de la operación de 12 a 24 horas, catastrófica.
2	Medio.	Interrupción de la operación de 8 a 12 horas, moderada.
1	Bajo.	Interrupción de la operación de 1 a 7 horas, menor.

- **Probabilidad.** Es la posibilidad de que ocurra o ha ocurrido la vulnerabilidad:

Factor numérico	Grado	Descripción
3	Alto.	Ocurrió una o más veces al mes.
2	Medio.	Ocurrió una o más veces de uno a seis meses.
1	Bajo.	Rara vez o hace más de seis meses.

- **Valor de riesgo.** Es el resultado aritmético de la multiplicación de los valores dados a los grados de impacto y probabilidad, el cual permite tener un parámetro para tomar decisiones sobre el activo en caso que un activo de información tenga un impacto alto y una probabilidad alta, existen tres valores:

Factor numérico	Grado
1 – 2	Bajo (Verde)
3 – 4	Medio (Amarillo)
6 – 9	Alto (Rojo)

En la siguiente tabla se muestran las diferentes combinaciones para el valor de riesgo:

Impacto	Probabilidad	Valor de Riesgo
Alto.	Alto.	Alto.
Alto.	Medio.	Alto.
Medio.	Alto.	Alto.
Medio.	Medio.	Medio.
Alto.	Bajo.	Medio.
Bajo.	Alto.	Medio.
Medio.	Bajo.	Bajo.
Bajo.	Medio.	Bajo.
Bajo.	Bajo.	Bajo.

- **Oportunidad de éxito.** Consiste en la mejora que se obtendría si cada dueño o administrador del activo implementa los controles del Anexo A de ISO/IEC 27001:2013 o realiza la mejora continua para evitar la explotación de la vulnerabilidad.

TRATAMIENTO DE RIESGOS

- **Tratamiento de riesgos.** De los resultados obtenidos del análisis de riesgos (Valor del Negocio y Valor del Riesgo), se identifica si el activo puede poner en riesgo la operación de la Gerencia o la operación de una Gerencia Externa, por lo que es importante priorizar el activo integrándolo a un Tratamiento de Riesgos. En la siguiente tabla se muestran las diferentes combinaciones para el Tratamiento de Riesgos.

Valor del negocio	Valor de riesgo	Tratamiento de Riesgo
Alto.	Alto.	Alto.
Alto.	Medio.	Alto.
Medio.	Alto.	Alto.
Medio.	Medio.	Medio.
Alto.	Bajo.	Medio.
Bajo.	Alto.	Medio.
Medio.	Bajo.	Bajo.
Bajo.	Medio.	Bajo.
Bajo.	Bajo.	Bajo.

Para los activos que estén en Tratamiento de Riesgo es fundamental que se tomen acciones para mitigar el riesgo tomando en cuenta lo siguiente:

1. El Gerente del área debe considerar si la mitigación del riesgo se puede hacer al interior de la gerencia, se documenta de acuerdo al plan de tratamiento de riesgos, generando la evidencia necesaria y se informa al Grupo Estratégico de Seguridad de la Información (GESI).

2. Si para la mitigación del riesgo es otra Gerencia o un Proveedor el que tiene que realizar las acciones, se informa al GESI y se realiza un plan de tratamiento de riesgos, generando la evidencia necesaria.

Para cualquiera de las opciones cada Gerente, debe evaluar si es necesario realizar una sesión extraordinaria o esperar a la sesión ordinaria del GESI.

La tolerancia de riesgo que se acepta son todos los activos que en su análisis de riesgos se encuentren en el nivel medio "amarillo" o bajo "verde", por lo que se consideran riesgos aceptables quedando el riesgo residual bajo; sin embargo, se deben de monitorear periódicamente con el fin de ver que no tengan incidentes de seguridad.

Se debe de contar con la información documentada del seguimiento del tratamiento de riesgos hasta su minimización de acuerdo a los siguientes puntos:

1. **Acción.**

   Determina el estatus del riesgo en que se encuentra el activo de acuerdo a los siguientes conceptos:

   - Mitigado.

     Se realizan acciones inmediatas bajando el riesgo de alto a medio o bajo.
   - Retenido.

     Se acepta el riesgo ya que para minimizarlo se llevará un largo plazo.
   - Transferido.

     El riesgo se transfiere a otra Gerencia, Proveedor y/o Aseguradora.

2. **Plan para mitigar el riesgo.**

   Se describen los acuerdos que se van a realizar para mitigar el riesgo.

3. **Seguimiento para mitigar el riesgo.**

   Se describe el seguimiento puntual de los acuerdos que se tuvieron para mitigar el riesgo.

4. **Riesgo residual aceptado.**

   Se describe el riesgo que se acepta en caso de que se vulnere el activo.

5. **Acción a realizar si se concreta el riesgo.**

   De acuerdo al riesgo residual que se aceptó, que acciones se realizaran si se vulnera el activo.

6. **Controles a Implementar.**

   Es el número de controles que se van a implementar para mitigar el riesgo.

7. **Fecha Cumplimiento.**

   Es la fecha de compromiso en la que se estipula para mitigar el riesgo.

8. **Grado de aseguramiento.**

   Es el grado de seguridad que el activo queda, de acuerdo al plan para mitigar el riesgo y los controles.

Grado	Descripción
Alto.	El riesgo es mitigado en un 90%
Medio.	El riesgo es mitigado en un 70%
Bajo.	El riesgo es mitigado en un 50%

9. **Riesgo residual.**

   Es el riesgo que no se puede mitigar en la aplicación del control, mismo que ***es aceptado por la Gerencia o inclusive por los miembros del GESI***. Es inversamente proporcional al grado de aseguramiento.

Grado de aseguramiento	Riesgo residual
Alto.	Bajo
Medio.	Medio
Bajo.	Alto

DECLARACIÓN DE APLICABILIDAD

Se comenzará en el 5 el cual corresponde al número de dominio de control, dentro de la norma ISO/IEC 27001:2013 anexo "A".

No.	Objetivo de control	Control	Aplica	Motivo
A.5.1	Directrices de Gestión de Seguridad de la Información.	A.5.1.1 Políticas para la seguridad de la información.	Sí	Llevar políticas mandatarias en la LOTENAL en cuestión del SGSI, para empleados y partes externas, mismas que se pueden localizar en esta metodología apartado políticas del SGSI.
		A.5.1.2 Revisión de las políticas de seguridad de la información.	Sí	Tener vigentes las políticas del SGSI, realizando revisiones y actualizaciones para una mejora continua de las políticas.
A.6.1	Organización Interna.	A.6.1.1 Los roles y las responsabilidades de seguridad de información.	Sí	Contar con un Grupo de Servidores Públicos con poder de toma de decisión, en el que traten y resuelvan temas relacionados con la Seguridad de la Información al Interior de la LOTENAL.
		A.6.1.2 La segregación de funciones.	Sí	Identificar a los responsables de las diferentes actividades que se realizan en la LOTENAL.
		A.6.1.3 El contacto con las autoridades.	Sí	Controlar contingencias o incidentes que rebasen la capacidad de control de la Entidad, teniendo áreas específicas que mantienen el contacto adecuado.

No.	Objetivo de control	Control	Aplica	Motivo
		A.6.1.4 El contacto con los grupos de interés especial.	Sí	Realizar el intercambio de información para tener una retroalimentación efectiva.
		A.6.1.5 Seguridad de la información en la gestión de proyectos.	Sí	Que en los proyectos que se realicen en la Entidad se lleve un adecuado análisis de riesgos y seguimiento involucrando las Áreas que requieran al desarrollo del proyecto y todas aquellas que intervengan en el mismo.
A.6.2	Los dispositivos móviles y el teletrabajo.	A.6.2.1 Política de dispositivo móvil.	Sí	Proteger la información de la LOTENAL, que se almacena en un dispositivo móvil.
		A.6.2.2 Teletrabajo.	No	La Entidad, no cuenta con la opción de trabajo a distancia o Teletrabajo.
A.7.1	Antes de empleo.	A.7.1.1 Proyección.	Sí	Tener la certeza de que los datos proporcionados por el aspirante son verdaderos y que no cuenten con antecedentes, evitando así una oportunidad de vulnerabilidad a la seguridad de la información.
		A.7.1.2 Términos y condiciones de empleo.	Sí	Verificar que la terminación del contrato anterior haya concluido en buenos términos, verificando que es un candidato serio.
A.7.2	Durante el empleo.	A.7.2.1 Responsabilidades de gestión.	Sí	Que todos los empleados, contratistas y terceras personas, que laboren o colaboren en la LOTENAL, se apeguen y cumplan las políticas de seguridad establecidas en el

No.	Objetivo de control	Control	Aplica	Motivo
				SGSI, así como, con los procedimientos normativos de la Entidad.
		A.7.2.2 Concienciación, educación y capacitación en seguridad de la información.	Sí	Que los empleados, contratistas y terceras personas que laboren o colaboren en la LOTENAL, tengan conocimiento de las políticas de seguridad establecidas en el SGSI, así como, la capacitación adecuada para al desempeño de sus funciones.
		A.7.2.3 Proceso disciplinario.	Sí	Contar con el o los procedimientos necesarios y correctos, para los empleados sospechosos de cometer algún incumplimiento en la seguridad.
A.7.3	Terminación y cambio de empleo.	A.7.3.1 La terminación o el cambio de las responsabilidades de empleo.	Sí	Tener la seguridad de que empleados, contratistas y terceras personas que ya no laboran en la Entidad no puedan ingresar a los sistemas de la Entidad y no exista el robo de información o manejo malintencionado de la información.
A.8.1	La responsabilidad de los activos.	A.8.1.1 Inventario de activos.	Sí	Tener identificados, los activos como. - (hardware, software, documentos, personal e Información) que son necesarios para llevar a cabo los procesos sustantivos de la LOTENAL.
		A.8.1.2 La propiedad de los activos.	Sí	Identificar quien hace uso de los activos y es responsable de

No.	Objetivo de control	Control	Aplica	Motivo
				verificar su correcto uso y funcionamiento.
		A.8.1.3 El uso aceptable de los activos.	Sí	Para que se le dé a cada activo el uso adecuado da acuerdo al propósito para el que está destinado.
		A.8.1.4 Retorno de los activos.	Sí	Para que los empleados, proveedores o terceros sustraigan o hagan mal uso da estos activos, una vez finalizado el acuerdo, contrato de prestación de servicios o actividades.
A.8.2	Clasificación de la información.	A.8.2.1 Clasificación de la información.	Sí	Para indicar la necesidad. prioridades y nivel de protección previsto para su tratamiento en relación a su valor, requisitos legales, sensibilidad y criticidad para la LOTENAL.
		A.8.2.2 Etiquetado de la información.	Sí	Es clasificar la información sensible, para darle el nivel adecuado de protección.
		A.8.2.3 Manipulado de la información.	Sí	Es asegurarse que la información sea resguardada, trasladada o desclasificada en la LOTENAL.
A.8.3	Manejo de los medios de comunicación.	A.8.3.1 Gestión de soportes extraíbles.	Sí	Minimizar los riesgos de los medios de comunicación por medio de procedimientos en la Entidad.
		A.8.3.2 La eliminación de soportes.	Sí	Evitar la fuga o robo de información de la LOTENAL.

No.	Objetivo de control	Control	Aplica	Motivo
		A.8.3.3 Soportes físicos en tránsito.	Sí	Proteger la información de la Entidad a través de tecnologías efectivas.
A.9.1	Los requerimientos del negocio de control de acceso.	A.9.1.1 Política de control de acceso.	Sí	Mantener, controlar y revisar el acceso a las áreas de la Entidad con reglamentos y procedimientos.
		A.9.1.2 Acceso a las redes y servicios de red.	SÍ	Que empleados, contratistas y terceras personas no tengan privilegios que puedan poner en riesgo la operación de la Entidad.
A.9.2	Gestión de acceso de usuario.	A.9.2.1 Registro y baja de usuario.	Sí	Mantener una trazabilidad adecuada de la entrada y salida de empleados, contratistas y terceras personas, a los sistemas y servicios de información en la Entidad.
		A.9.2.2 Provisión de acceso de usuario.	Sí	No poner en riesgo la información y/o los servicios de la Entidad identificando a empleados, contratistas y terceras personas, que tengan acceso a los sistemas y servicios en los tiempos acordados.
		A.9.2.3 Gestión de privilegios de acceso.	Sí	Asignar a los empleados acceso a los sistemas de acuerdo al perfil requerido.
		A.9.2.4 Gestión de la información secreta de autenticación de los usuarios.	Sí	Tener un control efectivo en la administración de contraseñas, otorgando diferentes niveles de acceso en base al tipo de usuario.

No.	Objetivo de control	Control	Aplica	Motivo
		A.9.2.5 Revisión de los derechos de acceso de usuario.	Sí	Identificar que los accesos a los sistemas de la Entidad estén vigentes y actualizados.
		A.9.2.6 Retirada o reasignación de los derechos de acceso.	Sí	Prevenir riesgos en los sistemas y/o mal uso de la información por los empleados, contratistas y/o terceras personas que ya terminaron su contrato o servicio en la Entidad.
A.9.3	Responsabilidades del usuario.	A.9.3.1 El uso de información secreta de autenticación.	Sí	Evitar el mal uso de la información y/o accesos no autorizados por empleados, contratistas y/o terceras personas.
A.9.4	Control del sistema y acceso a las aplicaciones.	A.9.4.1 Restricción de acceso Información.	Sí	Evitar que los empleados, contratistas y/o terceras personas tengan acceso a información no autorizada.
		A.9.4.2 Procedimientos seguros de inicio de sesión.	Sí	Mantener los registros de los sistemas en una alta integridad evitando que empleados, contratistas y/o terceras personas tengan acceso a sistemas no autorizados.
		A.9.4.3 Sistema de gestión de contraseña.	Sí	Proteger la información del usuario de ataques de intrusos ya sea internos o externos, con el fin de no alterar, destruir o hacer mal uso de la información del usuario.
		A.9.4.4	Sí	Evitar una contingencia en la operación de los sistemas públicos de la Entidad, por lo

No.	Objetivo de control	Control	Aplica	Motivo
		Uso de utilidades con privilegios del sistema.		que se controlan los roles y perfiles de los administradores de los servicios.
		A.9.4.5 Control de acceso al código fuente de los programas.	Sí	Mantener la integridad del código fuente, para que la operación y registros de los sistemas informáticos sean disponibles y confiables.
A.10.1	Controles criptográficos.	A.10.1.1 Política sobre el uso de controles criptográficos.	Sí	Que la información que viaja a través de la red o en los sistemas informáticos se mantenga segura e integra.
		A.10.1.2 Gestión de claves.	Sí	Evitar el mal uso de la información que viaja encriptada, a través de la red o en los sistemas informáticos actualizando las claves de encriptación.
A.11.1	Áreas seguras.	A.11.1.1 Perímetro de seguridad física.	Sí	Mantener, controlar y revisar el acceso a las áreas restringidas y/o críticas de la Entidad.
		A.11.1.2 Controles físicos de entrada.	Sí	Evitar el mal uso de las instalaciones y/o de los activos a través de controles de acceso a las áreas que lo requieran.
		A.11.1.3 Seguridad de oficinas, despachos y recursos.	Sí	Contar con herramientas adecuadas para minimizar el riesgo en caso de una contingencia en áreas internas.
		A.11.1.4	Sí	Mitigar la vulnerabilidad de exposición a daños por desastre natural, fuego, explosión o

No.	Objetivo de control	Control	Aplica	Motivo
		Protección contra las amenazas externas y ambientales.		desastre causado por el hombre.
		A.11.1.5 El trabajo en áreas seguras.	Sí	Resguardar la integridad de los empleados, contratistas y/o terceras personas en la Entidad.
		A.11.1.6 Áreas de carga y descarga.	Sí	Evitar el acceso a áreas no autorizadas a empleados, contratistas y/o terceras personas en áreas de acceso al público, o en las áreas de entrega en áreas de cargamento.
A.11.2	Equipo.	A.11.2.1 Emplazamiento y protección de equipos.	Sí	Mitigar riesgos de fallas ya sea por accesos no autorizados, peligros ambientales, riesgos y vulnerabilidades.
		A.11.2.2 Instalaciones de suministros .	Sí	Prevenir el daño o corrupción de los activos mediante métodos preventivos contra fallas de suministro eléctrico internos y externos.
		A.11.2.3 Seguridad en el cableado.	Sí	Proteger y mitigar la infraestructura eléctrica y de telecomunicaciones contra la interrupción de la operación por daños en el suministro eléctrico o en el cableado.
		A.11.2.4 Mantenimiento de los equipos.	Sí	Mitigar el riesgo de falla en la infraestructura y equipamiento para asegurar la correcta disponibilidad e integridad en las operaciones diarias de la Entidad al realizar de manera

No.	Objetivo de control	Control	Aplica	Motivo
				periódica mantenimiento a las mismas.
		A.11.2.5 Retirada de materiales propiedad de la empresa .	Sí	Mantener un control de los activos de seguridad mediante el registro y notificación de la salida de los mismos fuera de las instalaciones de la Entidad.
		A.11.2.6 Seguridad de los equipos fuera de las instalaciones.	Sí	Evitar la pérdida de la información contenida en los equipo que por necesidad de la operación salgan fuera de las instalaciones y pueda dañar la imagen de la Entidad.
		A.11.2.7 Reutilización o eliminación segura de equipos .	Sí	Garantizar que la información sensible o software bajo licencia de la Entidad sea eliminada de manera segura de los activos de seguridad cuando se de baja el mismo.
		A.11.2.8 Equipo de usuario desatendido.	Sí	Evitar que el equipo que no es utilizado continuamente tengan protección de acceso no autorizado mediante controles de autenticación.
		A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia.	Sí	Evitar la pérdida y/o robo de la información de manera física (documentos) o electrónica (archivos en el escritorio de la pc) en el lugar de trabajo del usuario a la vista y acceso de cualquier personal.
A.12.1	Procedimientos y responsabilida	A.12.1.1 Documentación de procedimientos de las operaciones.	Sí	Analizar y mantener un nivel adecuado de seguridad acerca de la información que está

No.	Objetivo de control	Control	Aplica	Motivo
	des operacionales.			contenida en los sistemas de información.
		A.12.1.2 Gestión del cambio.	Sí	Llevar una administración de todos los cambios en el desarrollo de los sistemas que se consideran sustantivos.
		A.12.1.3 Gestión de capacidades.	Sí	Asegurar el buen desempeño de los sistemas mediante monitoreo, adecuación y proyección del uso de los recursos.
		A.12.1.4 Separación de los recursos de desarrollo, prueba y operación.	Sí	Mantener íntegros, disponibles y confiables los registros de los sistemas que estén en producción.
A.12.2	Protección contra el malware.	A.12.2.1 Controles contra el código malicioso.	Sí	Mitigar el riesgo de la vulnerabilidad "*falta de protección contra virus*", así como de recuperación de información y concientización del personal.
A.12.3	Copia de seguridad.	A.12.3.1 Copias de seguridad de la información.	Sí	Evitar el uso o robo de software que pueda poner en riesgo la imagen de la Entidad.
A.12.4	Registro y seguimiento.	A.12.4.1 Registro de eventos.	Sí	Realizar el tratamiento adecuado de manera oportuna e inmediata de los activos, que pongan en riesgo la operación de la Entidad.
		A.12.4.2 Protección de la información de registro.	Sí	Controlar los accesos a la información de los incidentes y/o eventos contando con una trazabilidad.

No.	Objetivo de control	Control	Aplica	Motivo
		A.12.4.3 Registros de administración y operación.	Sí	Mantener la integridad en la operación de los sistemas informáticos de manera que se conserve segura su estructura interna.
		A.12.4.4 Sincronización del reloj.	Sí	Controlar la fecha y hora en que se realizan las operaciones de la Entidad, así como los accesos a las áreas.
A.12.5	El control de software operativo.	A.12.5.1 Instalación del software en explotación.	Sí	Mantener en óptimas condiciones los sistemas operativos de la Entidad, a través de una administración sana de la instalación del software.
A.12.6	Técnico de gestión de vulnerabilidades.	12.6.1 Gestión de vulnerabilidades técnicas.	Sí	No poner en riesgo el o los mantenimientos de los sistemas a través de los manuales técnicos de la Entidad.
		A.12.6.2 Restricción en la instalación de software.	Sí	No tener software malicioso instalado en los equipos de la Entidad que puedan llevarse información sustantiva o detener los programas sustantivos.
A.12.7	Sistemas de información consideraciones de auditoría.	A.12.7.1 Controles de auditoria de sistemas de información.	Sí	Contar con una trazabilidad desde que se inicia cualquier operación hasta el final de la misma, para identificar las operaciones de los usuarios en los sistemas sustantivos de la Entidad.
A.13.1		A.13.1.1 Controles de red.	Sí	Es cerciorarse que la seguridad de la información en las redes está protegida adecuadamente,

No.	Objetivo de control	Control	Aplica	Motivo
				así como, proteger los servicios conectados de accesos no autorizados.
	Gestión de la seguridad de red.	A.13.1.2 Seguridad de los servicios de red.	Sí	Evitar pérdida o mal uso de la Información que viaja a través de la red de la Entidad.
		A.13.1.3 Segregación en redes.	Sí	Mejorar el rendimiento del servicio al separar en la red a todos los empleados, contratistas y/o terceras personas, así como mantener los accesos administrados.
A.13.2	Información de transferencia.	A.13.2.1 Políticas y procedimientos de intercambio de información.	Sí	Asegurar que la información que viaja a través de la red por medio de una transferencia se realice con la más alta confidencialidad, integridad y disponibilidad.
		A.13.2.2 Acuerdos de intercambio de información.	Sí	Mantener los niveles de transferencia en alta disponibilidad e integridad por medio de los acuerdos y políticas establecidos.
		A.13.2.3 Mensajería electrónica.	Sí	Que la información sensible que maneja la Entidad tenga un nivel de protección adecuado y seguro.
		A.13.2.4 Acuerdos de confidencialidad o no revelación.	Sí	Impedir la fuga de información que pueda dañar la imagen de la Entidad.
A.14.1	Los requisitos de seguridad de los	A.14.1.1 Análisis de requisitos y especificaciones de	Sí	No tener un software con vulnerabilidades que ponga en

No.	Objetivo de control	Control	Aplica	Motivo
	sistemas de información.	seguridad de la información.		riesgo la operación de la Entidad.
		A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas .	Sí	Mantener una buena imagen con los clientes teniendo el servicio de redes en alta disponibilidad.
		A.14.1.3 Protección de las transacciones de servicios de aplicaciones .	Sí	Evitar pérdida de información que ponga en riesgo la imagen de la Entidad.
A.14.2	Seguridad en los procesos de desarrollo y de apoyo.	A.14.2.1 Política de desarrollo seguro.	Sí	Contar con las herramientas y mecanismo para el desarrollo del sistema de forma segura e integra.
		A.14.2.2 Procedimientos de control de cambio de sistema.	Sí	Contar con un historial del desarrollo del sistema, con el fin de regresar al procedimiento de ser necesario.
		A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Sí	Tener un software estable, disponible e íntegro en la Entidad para las operaciones sustantivas.
		A.14.2.4 Restricciones a los cambios en los paquetes de software.	Sí	No tener cambios en el software por personal no autorizado.
		A.14.2.5	Sí	Contar con sistemas más seguros, robustos y con un alto nivel de integridad.

No.	Objetivo de control	Control	Aplica	Motivo
		Principios de ingeniería de sistemas seguros.		
		A. 14.2.6 Entorno de desarrollo seguro.	Sí	Mantener el ciclo de vida del software en la etapa del desarrollo adecuadamente.
		A.14.2.7 Externalización del desarrollo de software.	Sí	Contar con la confidencialidad e integridad del software, así como con las especificaciones solicitadas por el personal externo.
		A.14.2.8 Pruebas funcionales de seguridad de sistemas.	Sí	Contar con un software con un alto nivel de seguridad para las operaciones de la Entidad.
		A.14.2.9 Pruebas de aceptación del sistemas.	Sí	Que cuando el sistema esté en producción no tenga ninguna falla para el usuario evitando retardos en la operación de la Entidad.
A.14.3	Los datos de prueba.	A.14.3.1 Protección de los datos de prueba.	Sí	Que la información sustantiva del sistema no se divulgue ni se confunda con la de producción.
A.15.1	Seguridad de la información en las relaciones con proveedores.	A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores.	Sí	Que los contratistas y terceras personas, sólo tengan la información necesaria para evitar el mal uso de la misma.
		A.15.1.2	Sí	Que los contratistas y terceras personas así como la Entidad estén de común acuerdo de la

No.	Objetivo de control	Control	Aplica	Motivo
		Requisitos de seguridad en contratos con terceros.		seguridad que se va a manejar en el proyecto.
		A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones.	Sí	Que los contratistas y terceras personas así como la Entidad estén de común acuerdo de los riesgos que tiene cada parte con el fin de hacerles frente.
A.15.2	Gestión de la prestación de servicios de proveedores.	A.15.2.1 Monitoreo y revisión de los servicios de los proveedores.	Sí	Mantener los servicios de la Entidad en alta disponibilidad.
		A.15.2.2 Gestión de cambios a los servicios de los proveedores.	Sí	Mantener administrados todos los cambios de los contratistas y/o terceras personas para contar con un nivel de servicio alto.
A.16	Información de gestión de incidentes de seguridad.	A.16.1.1 Responsabilidades y procedimientos.	Sí	Contar con una respuesta inmediata a los incidentes de seguridad de la información.
		A.16.1.2 Notificación de los eventos de seguridad de la información.	Sí	Dar un seguimiento oportuno al activo que tenga un incidente de seguridad.
		A.16.1.3 Notificación de puntos débiles de la seguridad.	Sí	Identificar las debilidades de los activos, por medio de empleados, contratistas y terceras personas.
		A.16.1.4 E Evaluación y decisión sobre los eventos de	Sí	Clasificar de manera oportuna aquellos activos que tengan un conflicto como incidentes de seguridad.

No.	Objetivo de control	Control	Aplica	Motivo
		seguridad de información.		
		A.16.1.5 Respuesta a incidentes de seguridad de la información.	Sí	No se detenga la operación de la Entidad, atendiendo el incidente de manera oportuna y rápida.
		A.16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Sí	Para identificar aquellos incidentes de seguridad que son repetitivos o de un alto riesgo.
		A.16.1.7 Recopilación de evidencias.	Sí	Contar con el material de evidencia adecuado en el caso de algún incidente de seguridad para así actuar de manera segura.
A .17	Los aspectos de seguridad de información de la gestión de la continuidad del negocio.	A.17.1.1 Planificación de la continuidad de la seguridad de la información.	Sí	Evitar que se detenga la operación sustantiva de la Entidad.
		A.17.1.2 Implementar la continuidad de la seguridad de la información.	Sí	Actuar de manera oportuna en una contingencia que ponga en riesgo la continuidad de la operación en la Entidad.
		A. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Sí	Identificar errores en los planes de continuidad de la operación, con el fin de mejorar el plan de contingencia.

Lotería Nacional para la Asistencia Pública

No.	Objetivo de control	Control	Aplica	Motivo
A.17.2	Redundancia.	A.17.2.1 Disponibilidad de los recursos de tratamiento de la información.	Sí	Que la información y registros de los sistemas se mantengan en alta disponibilidad para los usuarios de la Entidad.
A.18	Conformidad.	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales.	Sí	Tener conocimiento de las leyes y en su debido caso dar cumplimiento a lo aplicable de acuerdo a los lineamientos y normatividad interna, para no incumplir en ninguna.
		A.18.1.2 Derechos de propiedad intelectual (DPI).	Sí	Proteger la información, los productos, el software y los documentos que son propiedad de la Entidad de robo.
		A.18.1.3 Protección de los riesgos de la organización.	Sí	Resguardar en tiempo y ubicación, documentos como manuales de procedimientos, de organización, de contabilidad, registros en base de datos, convenidos y todos los documentos y registros que considere la Entidad como sustantivos en un lugar seguro.
		A.18.1.4 Protección y privacidad de la información de carácter personal.	Sí	Contar con controles que den la seguridad a los clientes, así como al personal de la Entidad, de que sus datos serán protegidos.
		A.18.1.5 Regulación de los controles criptográficos.	No	La LOTENAL, no realiza transacciones internacionales.
A.18.2		A.18.2.1	Sí	Realizar una revisión a los objetivos, controles, políticas, procesos y procedimientos de la

No.	Objetivo de control	Control	Aplica	Motivo
	Revisiones de seguridad de información.	Revisión independiente de la seguridad de la información.		Entidad para proporcionar un nivel adecuado sobre los requerimientos de la operatividad y leyes aplicables a la LOTENAL.
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad.	Sí	Que se tenga un adecuado monitoreo del complimiento de las políticas y controles de seguridad.
		A.18.2.3 Comprobación del cumplimiento técnico.	Sí	Que los sistemas de información cumplan con las políticas y controles adecuados para no poner en riesgo la operación de la Entidad.
A. LNLFT - ART26	Llevar a cabo en tiempo y forma la clasificación de la Información.	A LNLFT-ART26. 01 Los titulares de las unidades administrativas de las dependencias y entidades llevarán a cabo la clasificación de la información.	Sí	Tener en tiempo y forma la clasificación de la información de acuerdo al IFAI.
A. LNLFT - ART33	Resguardar los documentos clasificados como reservados.	A LNLFT-ART33. 02 Los expedientes y documentos clasificados como reservados, serán debidamente custodiados y conservados.	Sí	La información contenida en los documentos clasificados, se mantenga resguardada con los niveles de seguridad adecuados.
A. LNLFT - ART44	Todos los documentos en resguardo de la Entidad	A LNLFT-ART33. 03 Todo documento en posesión de la LOTENAL formará parte	Sí	Tener los documentos ordenados.

Lotería Nacional para la Asistencia Pública

* MANUAL ORIGINAL EN RESGUARDO *
POR LA
GERENCIA DE ORGANIZACION Y DESARROLLO DE PERSONAL

No.	Objetivo de control	Control	Aplica	Motivo
	son propiedad de la misma.	de un sistema de archivos.		
G1	Organización de la seguridad.	G.1.1.1 Foro/Comité de Seguridad. Debe estar formalmente Establecido un Foro de Seguridad, o cualquier otra estructura organizativa formada por Gestores Sénior, que supervise y revise el SGSI, manteniendo actas de las sesiones y reuniéndose a menos cada seis meses.	Sí	Es contar con un grupo de representantes que cuenten con el nivel jerárquico necesario para la toma de decisiones con respecto a los temas del SGSI.
		G1.1.2 Función de Seguridad. Debe existir la función de seguridad, responsable de proponer e implementar las estrategias de seguridad y los planes de actuación. Debe evaluar y estar implicada en todos los procesos de la organización que tengan relación con aspectos de la seguridad, incluyendo, pero no limitado a la protección	Sí	Que a través de la función de seguridad se identifiquen mejoras al SGSI y WLA y se minimicen los riesgos.

No.	Objetivo de control	Control	Aplica	Motivo
		de la información, las comunicaciones, la infraestructura física y los procesos de juego.		
		G.1.1.3 Dependencia de la Función de Seguridad. La función de seguridad debe depender de un nivel que no sea inferior a la Dirección Ejecutiva y no estará ubicada dentro de la función IT o dependiendo de ella.	Sí	Es contar con el apoyo necesario para el seguimiento y mejora continua del SGSI y WLA.
		G.1.1.4 Rango de la Función de Seguridad. La función de seguridad debe estar suficientemente facultada y tener acceso a todos los recursos corporativos necesarios para permitir una adecuada evaluación, gestión y reducción del riesgo.	Sí	Es que el análisis de riesgos se gestione en todas las Gerencias que se requiera, para minimizar el riesgo en la operación de la LOTENAL.
		G.1.1.5 Responsabilidad de la Función de Seguridad.	Sí	Es que se tenga una mejora continua sobre las políticas, cambios y gestión del SGSI y WLA.

No.	Objetivo de control	Control	Aplica	Motivo
		El encargado de la seguridad debe ser miembro permanente del foro de seguridad y debe ser responsable de recomendar políticas de seguridad y cambios.		
G2	Seguridad proveniente de las Personas.	G.2.1.1 Código de Conducta. Se debe entregar a toda persona que se incorpore una copia del Código de Conducta. Toda persona debe declarar aceptación formalmente, mediante acuse de recibo del mencionado Código.	Sí	Contar con una difusión efectiva con el objetivo de implantar los principios manifestados en el documento y qué este sea aplicado en todos los niveles de la Entidad, la Subgerencia de Capacitación y desarrollo se encarga de entregar el Código de Conducta.
		G.2.1.2 Cumplimiento y acción disciplinaria. El Código de Conducta debe incluir declaraciones respecto al cumplimiento de todas las políticas y procedimientos y sobre las acciones disciplinarias a las que podría conllevar cualquier incumplimiento o desacato al Código.	Sí	Lograr la asimilación de las políticas, así como el seguimiento a los procedimientos considerando en todo momento que el infringir lo estipulado contraerá acciones disciplinarias.

No.	Objetivo de control	Control	Aplica	Motivo
		G.2.1.3 Conflictos de Interés. El Código de Conducta debe requerir la notificación de conflictos de interés en el momento en que se produzcan. En el Código se deben citar ejemplos precisos de conflictos de interés.	Sí	Incluir definiciones para establecer de manera clara el manejo que debe prevalecer en el caso de un posible conflicto de intereses.
		G.2.1.4 Política sobre agasajos y obsequios. El Código de Conducta debe incluir una política respecto a dádivas y obsequios dados o recibidos de personas o entidades con las cuales la organización mantiene transacciones comerciales (negocios).	Sí	Que ningún empleado se vea involucrado en un acto deshonesto mediante algún obsequio de los proveedores.
G3	Seguridad Física y del Entorno.	G.3.1.1 Controles de acceso físico. El acceso físico a los centros de proceso de datos de los sistemas de juegos en producción,	Sí	Controlar y proteger de manera efectiva los activos de seguridad en áreas restringidas.

No.	Objetivo de control	Control	Aplica	Motivo
		salas de equipos informáticos, centros de operación/control de red y cualquier otra área identificada como crítica, debe estar controlada mediante mecanismos de autenticación de dos factores. Son aceptables mecanismos electrónicos de control de acceso basados en un solo factor, si el área está permanentemente ocupada por personal.		
G4	Gestión de las Actividades.	G.4.1.1 Acceso de usuarios remotos a los sistemas de juego. Debe estar establecido un procedimiento que permita un acceso remoto estrictamente controlado.	No	No se tiene contemplado el acceso remoto a los sistemas de juego de manera externa.
		G.4.1.2 Funcionalidades para usuarios de acceso remoto. El conjunto de funcionalidades disponibles para estos usuarios debe definirse de forma conjunta por	No	No se tiene contemplado el acceso remoto a los sistemas de juego de manera externa.

No.	Objetivo de control	Control	Aplica	Motivo
		los propietarios del proceso, la función IT y la función de seguridad.		
		G.4.1.3 Registro de acceso de usuarios remotos. Todas las acciones ejecutadas a través de acceso remoto deben registrarse y esos registros (logs) deben revisarse de forma.	No	No se tiene contemplado el acceso remoto a los sistemas de juego de manera externa.
G5	Control de Acceso regular.	G.5.1.1 Controles criptográficos para datos en equipos portátiles. Se deben cifrar los datos de la organización clasificados como no públicos. depositados en dispositivos portátiles (procesadores portátiles, dispositivos USB, etc.).	Sí	Los equipos que se consideran como un riesgo son los que salen de la instalación y son encriptados.
		G.5.1.2 Controles criptográficos para redes.	Sí	Que la información sensible que maneja la Entidad tenga un nivel de protección adecuado y seguro.

No.	Objetivo de control	Control	Aplica	Motivo
		Se debe cifrar la información sensible, incluyendo la validación o cualquier otra información crítica de juego, correo electrónico, etc., transmitida mediante redes para las que el análisis de riesgo indica que proveen un inadecuado nivel de protección.		
		G.5.1.3 Controles criptográficos para almacenamiento. Se deben aplicar medidas de integridad para almacenar la información contenida en los resguardos ganadores, así como de la información de validación.	Sí	Tener la información de los ganadores resguardada.
		G.5.1.4 Controles criptográficos para números de validación. Se deben cifrar los datos de validación de productos de lotería instantánea.	No	La Entidad no cuenta con sorteos de lotería instantánea.

No.	Objetivo de control	Control	Aplica	Motivo
		G.5.1.5 Controles criptográficos para transferencias. Se deben cifrar las transacciones financieras entre la organización y las Entidades bancarias.	No	Los bancos no tienen acceso a ningún servidor de la Entidad.
		G.5.2.1 Política de metodología de pruebas y datos. La política de metodología de pruebas debe incluir disposiciones dirigidas a impedir el uso de datos (reales) creados en un sistema de producción correspondiente a sorteos aún activos. Debe también incluir disposiciones dirigidas a impedir el uso de datos personales de los participantes.	Sí	Proteger y minimizar la posibilidad del mal uso de la información ya que al desarrollar un sistema con registros que no son reales o sorteos caducados, permite tener un adecuado nivel de protección.
G6	Gestión de la continuidad de negocio.	G.6.1.1 Gestión de las relaciones con los medios de comunicación y con el personal.	Sí	Prevenir la fuga de información o que esta quede comprometida por causa del acceso sin restricción a los equipos y/o dispositivos móviles y portátiles que puedan ser vulnerados; Se tiene encriptado el equipo que se va al sorteo foráneo.

No.	Objetivo de control	Control	Aplica	Motivo
		El plan de continuidad de negocio debe incluir planes para gestionar las relaciones con los medios de comunicación y el personal durante situaciones de crisis.		
		G.6.1.2 Aprobación de los Socios o del Consejo de Administración. La organización debe asegurar que el Consejo de Administración o los Socios de la organización están conformes con los requisitos de disponibilidad establecidos.	No	No hay socios comerciales en la LOTENAL.
		G.6.2.1 Plan de Continuidad del Negocio. Los ejercicios de continuidad del negocio se planificarán, realizarán y evaluarán en intervalos para que la organización esté preparada en situaciones de crisis.	Sí	Actuar de manera oportuna en una contingencia que ponga en riesgo la continuidad de la operación en la Entidad.

No.	Objetivo de control	Control	Aplica	Motivo
		G.6.2.2 Situaciones Violentas. Se deben planificar medidas de seguridad físicas, para proteger al personal y a los procesos de ataques terroristas u otras amenazas.	Sí	Resguardar la seguridad física del personal así como las operaciones de la LOTENAL, de amenazas externas.
L1	Billetes de lotería instantánea.	L.1.1.1 Procedimientos documentados de billetes de Lotería instantánea. Deben desarrollarse y estar documentados procedimientos formales que incluyan el diseño, desarrollo, producción y emisión del juego instantáneo.	Sí	Es tener documentadas todas las operaciones del sorteo desde el diseño hasta su emisión.
		L.1.1.2 Aprobación del diseño del juego. El diseño final del juego debe ser formalmente aprobado mediante un proceso que involucre al encargado de Seguridad.	Sí	Que el sorteo tenga los estándares de seguridad necesarios que minimicen el riesgo de ser vulnerado.

No.	Objetivo de control	Control	Aplica	Motivo
		L.1.1.3 Selección del proveedor. Los impresores / suministradores de billetes de lotería instantánea deben estar sujetos a un proceso de selección y aprobación. La aprobación debe involucrar a la función de seguridad.	Sí	Se asegure que los billetes de lotería tradicional, cuenten con la calidad y seguridad de impresión necesaria.
		L.1.1.4 Requisitos de seguridad. Los requisitos de seguridad concretos relativos al juego y al billete físico deben estar documentados y ser parte del contrato con el impresor / suministrador.	Sí	Que los billetes tradicionales cuenten con las medidas seguridad de impresión en el billete.
		L.1.1.5 Control de calidad. Los requisitos de control de calidad para la impresión de billetes de lotería instantánea deben estar documentados y ser parte del contrato con el impresor/proveedor.	Sí	Que los billetes tradicionales, tengan la calidad de impresión aceptable para la LOTENAL, así como para los clientes.

No.	Objetivo de control	Control	Aplica	Motivo
		L.1.1.6 Políticas de auditoría y pruebas en laboratorio. Debe estar establecer una política que describa las auditorías necesarias y las pruebas en laboratorio del diseño del juego e impresión de billetes.	Sí	Comprobar de manera fehaciente, las medidas de seguridad requeridas en los elementos que conforman los billetes de lotería, así como la impresión, calidad y el diseño del sorteo.
L1.2	Impresión de billetes de lotería instantánea.	L.1.2.1 Requisitos de impresión de billetes de lotería instantánea. La organización debe entregarle al impresor/proveedor una especificación del juego y requisitos detallados en materia de seguridad.	Sí	Contar con las especificaciones técnicas de los controles que se requieren de calidad y de la impresión de billetes tradicionales.
		L.1.2.2 Aseguramiento de la calidad de impresión. Los requisitos de seguridad deben incluir que el impresor/ proveedor tenga una función interna de aseguramiento de calidad.	Sí	Contar con las especificaciones técnicas de los controles de calidad que se requieren en la impresión de billetes tradicionales.

No.	Objetivo de control	Control	Aplica	Motivo
		L.1.2.3 Cifrado de números de validación. Los requisitos de seguridad deben incluir el cifrado de los números de validación.	No	La LOTENAL, no aplica este proceso en el billete tradicional.
		L.1.2.4 Cifrado de archivos de validación y ganadores. Los requisitos de seguridad deben incluir el cifrado de archivos de validación y de información de ganadores.	No	La LOTENAL, no aplica este proceso en el billete tradicional.
		L.1.2.5 Verificación de billete. Se deben realizar comprobaciones de muestras aleatorias de paquetes de billetes por juego para asegurar que estos cumplen con los márgenes de tolerancia dispuestos en la especificación de la organización.	Sí	Que los billetes tradicionales de la LOTENAL que salgan a la venta, cumplan con los niveles de seguridad del billete apropiados, así como la calidad necesaria para la satisfacción del cliente.

No.	Objetivo de control	Control	Aplica	Motivo
		L.1.2.6 Datos para pruebas de aceptación. Los requisitos de seguridad deben incluir la provisión de datos de inventario y validación a la función de seguridad o control de calidad designada por la organización para realizar pruebas de aceptación en cada primera ronda de impresión y antes del lanzamiento.	Sí	Contar con un control de entradas y salidas del billete antes de salir a la venta.
L 1.3	Envío de billetes de lotería instantánea.	L.1.3.1 Manifiesto de transporte. Los requisitos de transporte deben especificar que se debe enviar un manifiesto de transporte completo a la organización antes del despacho de cada envío.	Sí	Asegurarse que se entregue y reciba la cantidad de billetes tradicionales que se acordó.
		L.1.3.2 Modo de transporte. La organización debe asegurarse que el	Sí	Que los billetes tradicionales que se envían de la LOTENAL lleguen a su destino de manera segura, estructurada y controlada y que la logística que se acordó se respete.

No.	Objetivo de control	Control	Aplica	Motivo
		proceso de envíos se produce conforme al método de transporte acordado y que no se cambia sin la debida autorización de la organización.		
		L.1.3.3 Contenedores de transporte precintados. Los contenedores de transporte deben estar precintados y los números de los precintos deben constar en el manifiesto de transporte.	No	La LOTENAL, no aplica este proceso en el billete tradicional.
L 1.4	Almacenamiento y distribución de billetes de lotería instantánea.	L.1.4.1 Auditorías de almacenes. Debe estar establecido un procedimiento de inspección, por personal autorizado, de los almacenes de billetes de lotería instantánea, al menos una vez al año.	Sí	Mantener en óptimas condiciones, tanto en el almacén como en la ejecución de las acciones, para la distribución de los billetes tradicionales de manera segura.
		L.1.4.2 Verificación del transporte de billetes.	Sí	Comprobar que llegue la cantidad de billetes tradicionales que se acordó y